

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 985 332**

51 Int. Cl.:

**H04L 67/02** (2012.01)

**H04L 67/561** (2012.01)

**H04L 67/563** (2012.01)

**H04L 67/63** (2012.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **12.03.2021** **E 21162333 (5)**

97 Fecha y número de publicación de la concesión europea: **24.07.2024** **EP 3886401**

54 Título: **Método, aparato, y producto de programa informático para el manejo de errores en comunicaciones indirectas**

30 Prioridad:

**27.03.2020 IN 202041013452**

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

**05.11.2024**

73 Titular/es:

**NOKIA TECHNOLOGIES OY (100.0%)**

**Karakaari 7**

**02610 Espoo, FI**

72 Inventor/es:

**LANDAIS, BRUNO;**

**KHARE, SAURABH;**

**MOUKALLED, ALEX y**

**MOUROULIS, IOANNIS**

74 Agente/Representante:

**DEL VALLE VALIENTE, Sonia**

ES 2 985 332 T3

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

## DESCRIPCIÓN

Método, aparato, y producto de programa informático para el manejo de errores en comunicaciones indirectas

### 5 Campo técnico

Una realización a modo de ejemplo se refiere en general al manejo de errores para comunicaciones indirectas en una red de comunicaciones, y más particularmente a identificar la fuente del error para adaptar las comunicaciones posteriores según el origen del error.

10

### Antecedentes

Un sistema de comunicación puede considerarse como una instalación que permite sesiones de comunicación entre dos o más entidades, como terminales de usuario, estaciones base/puntos de acceso, funciones de red (NF) y/u otros nodos, proporcionando comunicación entre las distintas entidades que intervienen en la ruta de comunicación. Un sistema de comunicación se puede proporcionar, por ejemplo, por medio de una red de comunicación y uno o más dispositivos de comunicación compatibles. Se espera que las redes de telecomunicaciones, como la quinta generación de redes móviles (redes 5G), sean la próxima fase importante de los estándares de telecomunicaciones móviles y aporten muchas mejoras en la experiencia del usuario de las redes móviles. Por ejemplo, las redes 5G deberían proporcionar nuevas soluciones técnicas que permitan un mayor rendimiento, menor latencia, mayor confiabilidad, mayor conectividad y mayor rango de movilidad. Además de estas mejoras en cuanto a rendimiento, también se espera que las redes 5G amplíen la flexibilidad en el uso de la red y proporcionen a los usuarios una gama más amplia de casos de uso y modelos de negocio.

15

20

25

30

35

40

45

50

El Proyecto de Asociación de Tercera Generación (3GPP) es una organización de estándares que desarrolla protocolos para telefonía móvil y es conocida por el desarrollo y mantenimiento de diversos estándares, incluidos los estándares de segunda generación (2G), tercera generación (3G), cuarta generación (4G), Evolución a Largo Plazo (LTE) y quinta generación (5G). La red 5G de núcleo (5GC) ha sido diseñada como una arquitectura basada en servicios (SBA), por ejemplo, una arquitectura de sistema en la que la funcionalidad del sistema se logra mediante un conjunto de NF que brindan servicios a otras NF autorizadas para acceder a sus servicios. Como tal, los clientes NF (por ejemplo, un consumidor de servicios NF, o un cliente HTTP, que emite una solicitud de servicio o un Productor de servicios NF, o un cliente HTTP, que envía una solicitud de notificación) envían solicitudes de servicio a servidores NF (por ejemplo, un productor de servicios NF o consumidor de servicios NF respectivamente, o servidor HTTP). Esto se describe, por ejemplo, en la especificación técnica (TS) 29.500 de 3GPP. Generalmente, "Sintaxis y enrutamiento de mensajes" para HTTP y "Semántica y contenido" para HTTP se describen en los RFC 7230 y 7231 del IETF, respectivamente. Desde la versión 16 del 3GPP en adelante, la arquitectura basada en servicios (eSBA) mejorada del 3GPP introduce, entre otras características, el soporte de comunicación indirecta entre un cliente NF y un servidor NF, o entre un consumidor de servicios de función de red (NF) y un productor de servicios NF a través de una o más entidades de proxy de comunicación de servicios (SCP). La realización técnica del soporte de comunicación indirecta introduce problemas asociados con la identificación del autor de un error entre el servidor NF y una o más entidades intermediarias, lo que hace que cualquier procesamiento posterior de una solicitud sea ineficaz, ya que la solicitud puede volver a enviarse a través de la misma entidad que fue la fuente del error original. Específicamente, para las comunicaciones indirectas entre una NF de la red central 5G (5GC) a través de SCP y, más generalmente, para las comunicaciones entre una NF 5GC a través de cualquier entidad intermedia, si el cliente NF o una entidad intermedia que envía una solicitud de servicio no puede asignar una respuesta de error a la entidad intermediaria o al servidor NF que originó el error, esto evita que el cliente NF o la entidad intermediaria adapten el comportamiento de comunicación basándose en el originador del error y por lo tanto el error real y el cliente NF o la entidad intermediaria no puedan adaptar las comunicaciones posteriores en consecuencia, por lo tanto, la lógica del sistema no puede funcionar correctamente para establecer comunicaciones.

### Breve resumen

Un método según la reivindicación 1, un aparato según la reivindicación 6 y un producto de programa informático según la reivindicación 11 se describen para la identificación del origen del error de comunicación de red mediante la inserción de una indicación de la entidad de red que origina el error en la respuesta al error, o mediante una indicación de que una entidad intermedia ha transmitido una respuesta de error, tal como una información de error incluida dentro de la respuesta de error que se devuelve al cliente NF a través de una entidad intermedia. El cliente NF puede entonces aplicar un manejo de errores apropiado según el originador del error, por ejemplo, retransmitir la solicitud de servicio hacia un servidor NF alternativo o utilizando una entidad de red alternativa (por ejemplo, SCP), por ejemplo, a través de una ruta de red alternativa no asociada con la entidad de origen del error de comunicación de red identificada.

60

El método, aparato y producto de programa informático se describen según una realización ejemplar para redes 3GPP, que comprende arquitectura basada en servicios, comunicación basada en HTTP entre consumidores de servicios de función de red (NF), entidades proxy de red y productores de servicios NF. En algunas realizaciones, los respectivos mensajes de error basados en comunicación incluyen información sobre qué entidad produjo el error (por ejemplo, identificación del originador del error de comunicación).

65

Otros aspectos diversos también se describen en la siguiente descripción detallada y en las reivindicaciones adjuntas.

**Breve descripción de los dibujos**

5 Habiendo descrito de este modo ciertas realizaciones de la descripción en términos generales, ahora se hará referencia a los dibujos adjuntos, que no están necesariamente dibujados a escala, y en donde:

10 la Figura 1 ilustra un ejemplo de arquitectura para una red de comunicaciones, según algunas realizaciones;

la Figura 2 ilustra un ejemplo de arquitectura para una red de comunicaciones, según algunas realizaciones;

la Figura 3 ilustra un ejemplo de arquitectura para una red de comunicaciones, según algunas realizaciones;

15 la Figura 4 ilustra un dispositivo informático de ejemplo para comunicarse a través de redes de comunicación con otras entidades de red, según algunas realizaciones;

20 la Figura 5 es un diagrama de flujo de señales que ilustra una solicitud de comunicación fallida entre un consumidor de servicios NF y PCF, a través de un SCP intermedio, con un origen de error desconocido;

la Figura 6 es un diagrama de flujo de señales que ilustra una solicitud de comunicación fallida entre un consumidor de servicios NF y una PCF, a través de un SCP intermedio, con un originador de error conocido (en el SCP intermedio) y una solicitud de comunicación retransmitida con éxito a través de un SCP diferente;

25 la Figura 7 es un diagrama de flujo de señales que ilustra una solicitud de comunicación fallida entre un consumidor de servicios NF y una PCF, a través de un SCP intermedio, con un originador de error conocido (en la PCF) y una solicitud de comunicación retransmitida exitosamente a través del mismo SCP hacia una PCF diferente;

30 la Figura 8 es un diagrama de flujo que ilustra las operaciones realizadas, tales como por un consumidor de servicios NF u otro dispositivo cliente, según una realización de ejemplo;

la Figura 9 es un diagrama de flujo que ilustra las operaciones realizadas, tales como por un SCP u otra entidad intermediaria, según otra realización de ejemplo;

35 la Figura 10 es un diagrama de flujo que ilustra las operaciones realizadas, tales como por un consumidor de servicios NF u otro dispositivo cliente o por un SCP u otra entidad intermediaria, según una realización de ejemplo; y

40 la Figura 11 es un diagrama de flujo que ilustra las operaciones realizadas, tales como por un servidor NF, según una realización de ejemplo.

**Descripción detallada**

45 Ahora se describirán más completamente algunas realizaciones de la presente invención a continuación en la presente memoria con referencia a los dibujos adjuntos, en los que se muestran algunas, pero no todas, las realizaciones de la invención. De hecho, diversas realizaciones de la invención pueden implementarse de muchas formas diferentes y no deben interpretarse como limitadas a las realizaciones expuestas en la presente memoria; en vez de eso, estas realizaciones se proporcionan de modo que esta descripción satisfaga los requisitos legales aplicables. El término “o” se usa en la presente memoria tanto en sentido alternativo como conjuntivo, a menos que se indique lo contrario. Los términos “ilustrativo” y “a modo de ejemplo” se usan como ejemplos sin indicación del nivel de calidad. Los números de referencia similares se refieren a elementos similares en su totalidad. Como se usan en la presente memoria, los términos “datos”, “contenido”, “información” y términos similares pueden usarse de manera intercambiable para referirse a datos que pueden transmitirse, recibirse y/o almacenarse según realizaciones de la presente invención. Por lo tanto, no debe tomarse el uso de dichos términos como una limitación del alcance de las realizaciones de la presente invención.

55 Adicionalmente, como se usa en la presente memoria, el término “sistema de circuitos” se refiere a (a) implementaciones de circuito sólo en hardware (p. ej., implementaciones en sistemas de circuitos analógicos y/o sistemas de circuitos digitales); (b) combinaciones de circuitos y producto(s) de programa informático que comprenden instrucciones de software y/o firmware almacenadas en una o más memorias legibles por ordenador que funcionan juntas para hacer que un aparato realice una o más funciones descritas en la presente memoria; y (c) circuitos, tales como, por ejemplo, un(os) microprocesador(es) o una porción de un(os) microprocesador(es), que requieren software o firmware para su funcionamiento aunque el software o firmware no esté físicamente presente. Esta definición de “sistema de circuitos” se aplica a todos los usos de este término en la presente memoria, incluyendo en cualquier reivindicación. Como un ejemplo adicional, como se usa en la presente memoria, el término “sistema de circuitos” también incluye una implementación que comprende uno o más procesadores y/o parte o partes de los mismos y software y/o firmware adjuntos. Como otro ejemplo, el término “conjunto de circuitos” como se usa en la presente

memoria también incluye, por ejemplo, un circuito integrado de banda base o un circuito integrado de procesador de aplicaciones para un teléfono móvil o un circuito integrado similar en un servidor, un dispositivo de red celular, otro dispositivo de red y/u otro dispositivo informático.

5 Además, como se usan en la presente memoria, los términos “nodo”, “entidad”, “intermediario”, “entidad intermedia”, “mediador”, “intermediario” y términos similares se pueden usar indistintamente para referirse a ordenadores conectados a través de, o programas que se ejecutan en una red o pluralidad de redes capaces de crear, modificar, eliminar, transmitir, recibir y/o almacenar datos según realizaciones de la presente invención. Por lo tanto, no debe tomarse el uso de dichos términos como una limitación del alcance de las realizaciones de la presente invención.

10 Algunas realizaciones en la presente memoria hacen referencia específica al protocolo de transferencia de hipertexto (HTTP), sin embargo, la presente descripción contempla que se pueden usar protocolos alternativos. Por ejemplo, algunos protocolos alternativos son el protocolo seguro de transferencia de hipertexto (HTTPS), HTTP/2, HTTP/3, conexión a Internet con protocolo de datagramas de usuario rápido (QUIC), intercambio de datos de paquetes de software (SPDY), protocolo Gopher, protocolo de transferencia de archivos (FTP), protocolo de copia segura (SCP), protocolo de aplicación de Internet (IAP) y tecnologías similares conocidas que entiende un experto en la técnica a la luz de la presente descripción. La presente descripción contempla además que los métodos, aparatos y productos de programas informáticos descritos en la presente memoria también pueden ser aplicables para su uso con una variedad de estándares de red y comunicación.

20 Según se define en la presente memoria, un “medio de almacenamiento legible por ordenador”, que se refiere a un medio de almacenamiento físico no transitorio (por ejemplo, dispositivo de memoria volátil o no volátil), puede distinguirse de un “medio de transmisión legible por ordenador”, que se refiere a una señal electromagnética. Tal medio puede adoptar muchas formas, incluyendo, entre otras, un medio de almacenamiento no transitorio legible por ordenador (por ejemplo, medios no volátiles, medios volátiles) y medios de transmisión. Los medios de transmisión incluyen, por ejemplo, cables coaxiales, alambres de cobre, cables de fibra óptica y ondas portadoras que viajan a través del espacio sin alambres ni cables, como ondas acústicas y ondas electromagnéticas, incluidas ondas de radio, ópticas e infrarrojas. Las señales incluyen variaciones transitorias artificiales de amplitud, frecuencia, fase, polarización u otras propiedades físicas transmitidas a través de los medios de transmisión. Los ejemplos de medios no transitorios legibles por ordenador incluyen un medio magnético legible por ordenador (por ejemplo, un disquete, disco duro, cinta magnética, cualquier otro medio magnético), un medio óptico legible por ordenador (por ejemplo, una memoria de sólo lectura de disco compacto (CD-ROM), un disco versátil digital (DVD), un disco Blu-Ray, o similares), una memoria de acceso aleatorio (RAM), una memoria de sólo lectura programable (PROM), una memoria de sólo lectura programable borrable (EPROM), una FLASH-EPROM, o cualquier otro medio no transitorio desde el que pueda leer un ordenador. El término medio de almacenamiento legible por ordenador se usa en la presente memoria para referirse a cualquier medio legible por ordenador excepto los medios de transmisión. Sin embargo, se apreciará que cuando se describen realizaciones para utilizar un medio de almacenamiento legible por ordenador, se pueden sustituir o utilizar otros tipos de medios legibles por ordenador además del medio de almacenamiento legible por ordenador en realizaciones alternativas.

40 A continuación, se explican determinadas realizaciones con referencia a dispositivos de comunicación capaces de comunicarse a través de una red cableada y/o inalámbrica y sistemas de comunicación que dan servicio a dichos dispositivos de comunicación. Antes de explicar en detalle las realizaciones ejemplificadoras, se explican brevemente determinados principios generales de un sistema de comunicación alámbrico y/o inalámbrico, sistemas de acceso al mismo y dispositivos de comunicación con referencia a las Figuras 1-3 para ayudar a comprender la tecnología subyacente a los ejemplos descritos.

50 Según algunas realizaciones, se puede proporcionar un dispositivo o terminal de comunicación para el acceso inalámbrico a través de células, estaciones base, puntos de acceso o similares (por ejemplo, nodos transmisores y/o receptores inalámbricos que proporcionan puntos de acceso para un sistema de comunicación de acceso por radio y/u otras formas de redes cableadas y/o inalámbricas). Dichas redes cableadas y/o inalámbricas incluyen, entre otras, redes configuradas para cumplir con 2G, 3G, 4G, LTE, 5G y cualquier otro estándar de redes de comunicación similar o futuro. La presente descripción contempla que cualquier método, aparato, código de programa informático y cualquier porción o combinación de los mismos también puede implementarse con redes de comunicación aún no desarrolladas y estándares asociados en el futuro y ser entendido por un experto en la técnica a la luz de la presente descripción.

60 Los puntos de acceso y, por tanto, las comunicaciones a su través, son controladas típicamente por al menos un aparato de control apropiado para posibilitar su funcionamiento y la gestión de dispositivos de comunicación móvil en comunicación con los mismos. En algunas realizaciones, un aparato de control para un nodo puede integrarse, acoplarse y/o proporcionarse de otro modo para controlar los puntos de acceso. En algunas realizaciones, el aparato de control puede disponerse para permitir comunicaciones entre un equipo de usuario y una red central o una entidad de red de la red central. Para ello, el aparato de control puede comprender al menos una memoria, al menos una unidad de procesamiento de datos, como un procesador o similar, y una interfaz de entrada/salida. A través de la interfaz, el aparato de control se puede acoplar a otros componentes relevantes del punto de acceso. El aparato de control se puede configurar para ejecutar un código de software apropiado para proporcionar las funciones de control.

Se apreciará que se pueden proporcionar componentes similares en un aparato de control proporcionado en alguna otra parte en el sistema de red, por ejemplo, en una entidad de red medular. El aparato de control se puede interconectar con otras entidades de control. El aparato de control y las funciones se pueden distribuir entre varias unidades de control. En algunas realizaciones, cada estación base puede comprender un aparato de control. En realizaciones alternativas, dos o más estaciones base pueden compartir un aparato de control.

Los puntos de acceso y los controladores asociados se pueden comunicar entre sí a través de una conexión de línea fija y/o mediante una interfaz de radio. La conexión lógica entre los nodos de estación base puede ser proporcionada, por ejemplo, por una interfaz X2, interfaz S1 y/o similar. Esta interfaz se puede usar, por ejemplo, para la coordinación del funcionamiento de las estaciones y realizar operaciones de reelección o traspaso. La conexión de comunicación lógica entre el nodo de comunicación inicial (por ejemplo, el dispositivo consumidor o consumidor de servicios NF) y el nodo de comunicación final en la red (por ejemplo, el productor de servicios NF) puede comprender una pluralidad de nodos intermediarios (por ejemplo, SCP o SEPP). Además, cualquiera de los nodos (por ejemplo, inicial, final, intermediario) puede agregarse y eliminarse de la conexión de comunicación lógica según sea necesario para establecer y mantener una comunicación de función de red.

El dispositivo de comunicación o equipo de usuario puede comprender cualquier dispositivo adecuado capaz de recibir al menos una señal de comunicación que comprenda datos. La señal de comunicación se puede transmitir a través de una conexión por cable, una conexión inalámbrica o alguna combinación de las mismas. Por ejemplo, el dispositivo puede ser un dispositivo de procesamiento de datos de mano equipado con un aparato de recepción de radio, de procesamiento de datos y de interfaz de usuario. Los ejemplos no limitativos incluyen una mobile station (estación móvil - MS) tal como un teléfono móvil o lo que se conoce como un "teléfono inteligente", un ordenador portátil tal como un portátil o un ordenador de tipo tableta dotado de una tarjeta de interfaz inalámbrica u otra facilidad de interfaz, un personal data assistant (asistente de datos personal - PDA) dotado de capacidades de comunicación inalámbrica, o cualesquiera combinaciones de estos o similares. Los ejemplos adicionales incluyen dispositivos inalámbricos portátiles como los integrados en relojes o relojes inteligentes, gafas, cascos, sombreros, vestimenta, auriculares con conectividad inalámbrica, joyas, etc., universal serial bus (memorias de bus serie universal - USB) con capacidades inalámbricas, tarjetas de datos de módem, dispositivos de tipo máquina o cualquier combinación de estos o similares.

En algunas realizaciones, un dispositivo de comunicación, por ejemplo, configurado para la comunicación con la red inalámbrica o una entidad de red central, puede ejemplificarse mediante un dispositivo de comunicación portátil o de otro modo móvil (o equipo de usuario UE). Un dispositivo de comunicación móvil puede dotarse de capacidades de comunicación inalámbrica y de un aparato de control electrónico apropiado para posibilitar el funcionamiento del mismo. Por tanto, el dispositivo de comunicación puede estar provisto de al menos una entidad de procesamiento de datos, por ejemplo una unidad central de procesamiento y/o un procesador central, al menos una memoria y otros posibles componentes como procesadores y memorias adicionales para su uso en la ejecución asistida por software y hardware de las tareas para las que está diseñado. Los aparatos de procesamiento y de almacenamiento de datos y otros aparatos de control relevantes pueden proporcionarse en una placa de circuito apropiada y/o en unos circuitos integrados auxiliares. Las funciones de procesamiento de datos y de memoria proporcionadas por el aparato de control del dispositivo de comunicación están configuradas para provocar operaciones de control y de señalización según ciertas realizaciones como se describe más adelante en esta descripción. Un usuario puede controlar el funcionamiento del dispositivo de comunicación por medio de una interfaz de usuario adecuada tal como un panel o pantalla sensible al tacto y/o un teclado numérico, uno de más botones de accionamiento, órdenes de voz, combinaciones de estos o similares. Típicamente, también se proporcionan un altavoz y un micrófono. Adicionalmente, un dispositivo de comunicación móvil puede comprender conectores apropiados (o bien cableados o bien inalámbricos) a otros dispositivos y/o para conectar accesorios externos, por ejemplo, equipo de manos libres, al mismo.

En algunas realizaciones, un dispositivo de comunicación se puede comunicar de forma inalámbrica a través de un aparato apropiado para recibir y transmitir señales. En algunas realizaciones, se puede conectar una unidad de radio al aparato de control del dispositivo. La unidad de radio puede comprender una parte de radio y una disposición de antena asociada. La disposición de antena se puede disponer interna o externamente al dispositivo de comunicación.

En algunas realizaciones, se hace referencia a las siguientes abreviaturas: red central 5G (5GC), función de red (NF), función de repositorio de red (NRF), función de control de políticas (PCF), red móvil terrestre pública (PLMN), arquitectura basada en servicios (SBA), interfaz basada en servicios (SBI), servicio proxy de comunicación (SCP), proxy de protección de borde de seguridad (SEPP) y función de gestión de sesión (SMF).

Las Figuras 1 a 3 ilustran varios ejemplos de arquitecturas para una red de comunicaciones 100 en la que se pueden llevar a cabo y/o usar diversos métodos, aparatos y productos de programas informáticos. En algunas realizaciones, la red de comunicaciones 100 puede comprender cualquier configuración, número, orientación, posicionamiento y/o dimensiones adecuadas de componentes y equipos especializados configurados para proporcionar una interfaz aérea (por ejemplo, New Radio (NR)) para comunicación o conexión entre un equipo de usuario 102 (UE 102) y una red de datos 116 (DN 116) a través de una red central 101 (CN 101) de la red de comunicaciones 100. El UE 102 puede estar asociado con uno o más dispositivos asociados con uno o más consumidores de servicios NF. Como se ilustra en la Figura 1, se puede proporcionar una red de comunicaciones 100 en la que el UE 102 está en comunicación operativa con la RAN 104, tal como a través de una torre de transmisión, una estación base, un punto de acceso, un nodo de

red y/o similares. En algunas realizaciones, la RAN 104 puede comunicarse con el CN 101 o un componente o entidad del mismo. En algunas realizaciones, el CN 101 puede facilitar la comunicación entre el UE 102 y el DN 116, tal como para enviar datos, mensajes, solicitudes y/o similares. En algunas realizaciones, el DN 116 o el CN 101 pueden estar en comunicación con un servidor de aplicaciones o función de aplicación 112 (AS/AF 112). La RAN 104, CN 101, DN 116 y/o AS/AF 112 pueden asociarse con una NRF, un productor de servicios NF, un SCP, un SEPP, un PCF, similares o cualquier combinación de los mismos.

En el contexto de una red de quinta generación (5G), como se ilustra en las Figuras 2 y 3, la red de comunicaciones 100 puede comprender una serie de dispositivos de red conectados y hardware especializado que se distribuye a lo largo de una región de servicio, estado, provincia, ciudad o país, y una o más entidades de red, que pueden almacenarse en y/o alojado en uno o más de los dispositivos de red conectados o hardware especializado. En algunas realizaciones, el UE 102 puede conectarse a la RAN 104, que luego puede retransmitir las comunicaciones entre el UE 102 y el CN 101, estando conectado el CN 101 al DN 116, que puede estar en comunicación con uno o más AS/AF 112. En algunas realizaciones, el UE 102 puede estar en comunicación con una red de acceso por radio 104 (RAN 104), que puede actuar como un relé entre el UE 102 y otros componentes o servicios del CN 101. Por ejemplo, en algunas realizaciones, el UE 102 puede comunicarse con la RAN 104, que a su vez puede comunicarse con una Función de Gestión de Acceso y Movilidad 108 (AMF 108). En otros casos o realizaciones, el UE 102 puede comunicarse directamente con el AMF 108. En algunas realizaciones, el AMF 108 puede estar en comunicación con una o más funciones de red (NF), tales como una Función de Servidor de Autenticación 120 (AUSF 120), una Función de Selección de Segmento de Red 122 (NSSF 122), una Función de Repositorio de Red 124 (NRF 124), una función de cobro de políticas 114 (PCF 114), una función de análisis de datos de red 126 (NWDAF 126), una función de gestión de datos unificada 118 (UDM 118), el AS/AF 112, una función de gestión de sesiones 110 (SMF 110), y/o similares.

En algunas realizaciones, el SMF 110 puede estar en comunicación con una o más Funciones 106 del Plano de Usuario (UPF 106, UPF 106a, UPF 106b, colectivamente "UPF 106"). Sólo a modo de ejemplo, en algunas realizaciones, el UPF 106 puede estar en comunicación con la RAN 104 y el DN 116. En otras realizaciones, el DN 116 puede estar en comunicación con un primer UPF 106a y la RAN 104 puede estar en comunicación con un segundo UPF 106b, mientras que el SMF 110 está en comunicación tanto con el primer como con el segundo UPF 106a, b y el primer y las segundas UPF 106a, b están en comunicación entre sí.

En algunas realizaciones, el UE 102 puede comprender un dispositivo de modo único o de modo dual de modo que el UE 102 pueda conectarse a una o más RAN 104. En algunas realizaciones, la RAN 104 se puede configurar para implementar una o más tecnologías de acceso de radio (RAT), tales como Bluetooth, Wi-Fi y GSM, UMTS, LTE o 5G NR, entre otras, que se pueden usar para conectar la UE 102 a la CN 101. En algunas realizaciones, la RAN 104 puede comprender o implementarse usando un chip, tal como un chip de silicio, en el UE 102 que puede emparejarse con o reconocerse de otro modo por un chip similar en el CN 101, de modo que la RAN 104 pueda establecer una conexión o línea de comunicación entre el UE 102 y el CN 101 identificando y emparejando el chip dentro del UE 102 con el chip dentro del CN 101. En algunas realizaciones, la RAN 104 puede implementar una o más estaciones base, torres o similares para comunicarse entre el UE 102 y el AMF 108 del CN 101.

En algunas realizaciones, la red de comunicaciones 100 o componentes de la misma (por ejemplo, estaciones base, torres, etc.) pueden configurarse para comunicarse con un dispositivo de comunicación (por ejemplo, el UE 102) tal como un teléfono celular o similar a través de múltiples frecuencias diferentes. bandas, por ejemplo, FR1 (por debajo de 6 GHz), FR2 (onda mm), otras bandas de frecuencia adecuadas, subbandas de las mismas y/o similares. En algunas realizaciones, la red de comunicaciones 100 puede comprender o emplear antenas masivas de múltiples entradas y múltiples salidas (MIMO masiva). En algunas realizaciones, la red de comunicaciones 100 puede comprender antenas MIMO multiusuario (MU-MIMO). En algunas realizaciones, la red de comunicaciones 100 puede emplear computación de borde mediante la cual los servidores informáticos están comunicativamente, física, computacional y/o temporalmente más cerca del dispositivo de comunicaciones (por ejemplo, UE 102) para reducir la latencia y la congestión del tráfico de datos. En algunas realizaciones, la red de comunicaciones 100 puede emplear otras tecnologías, dispositivos o técnicas, tales como celdas pequeñas, RAN de baja potencia, formación de haces de ondas de radio, convergencia celular WIFI, acceso múltiple no ortogonal (NOMA), codificación de canales y similares.

Como se ilustra en la Figura 3, el UE 102 puede configurarse para comunicarse con la RAN 104 en una interfaz N1, por ejemplo, según un protocolo de estrato sin acceso (NAS). En algunas realizaciones, la RAN 104 puede configurarse para comunicarse con la CN 101 o un componente de la misma (por ejemplo, la AMF 108) en una interfaz N2, por ejemplo, en un plano de control entre una estación base de la RAN 104 y la AMF 108. En algunas realizaciones, la RAN 104 se puede configurar para comunicarse con la UPF 106 en una interfaz N3, por ejemplo, en un plano de usuario. En algunas realizaciones, el AMF 108 y/o el SMF 110 pueden configurarse para comunicarse con otros servicios o entidades de red dentro del CN 101 en diversas interfaces diferentes y/o según varios protocolos diferentes. Por ejemplo, en algunas realizaciones, el AMF 108 y/o el SMF 110 pueden configurarse para comunicarse con el AUSF 120 en una interfaz Nausf o una interfaz N12. En algunas realizaciones, el AMF 108 y/o el SMF 110 se pueden configurar para comunicarse con el NSSF 122 en una interfaz Nnssf. En algunas realizaciones, el AMF 108 y/o el SMF 110 se pueden configurar para comunicarse con el NRF 124 en una interfaz Nnrf. En algunas realizaciones, el AMF 108 y/o el SMF 110 se pueden configurar para comunicarse con el PCF 114 en una interfaz Npcf o una interfaz N7. En algunas realizaciones, el AMF 108 y/o el SMF 110 se pueden configurar para comunicarse con el NWDAF 126 en

una interfaz Nnwdaf. En algunas realizaciones, el AMF 108 y/o el SMF 110 se pueden configurar para comunicarse con el UDM 118 en una interfaz Nudm, una interfaz N8 o una interfaz N10. En algunas realizaciones, el AMF 108 y/o el SMF 110 se pueden configurar para comunicarse con el AS/AF 112 en una interfaz Naf. En algunas realizaciones, el SMF 110 se puede configurar para comunicarse con el UPF 106 en una interfaz N4, que puede actuar como un puente entre el plano de control y el plano de usuario, tal como actuar como un conducto para una Unidad de datos de protocolo (PDU). sesión durante la cual se transmite información entre, por ejemplo, el UE 102 y el CN 101 o componentes/servicios del mismo.

Se apreciará que determinadas realizaciones de ejemplo descritas en la presente memoria surgen en el contexto de una red de telecomunicaciones, que incluye, entre otras, una red de telecomunicaciones que se ajusta a una arquitectura de quinta generación (5G) y/o de otro modo incorpora aspectos de ella. Mientras que las Figuras 1-3 ilustran diversas configuraciones y/o componentes de una arquitectura de ejemplo de la red de comunicaciones 100, muchos otros sistemas, configuraciones de sistemas, redes, entidades de red y vías/protocolos para comunicación en los mismos se contemplan y consideran dentro del alcance de esta presente descripción.

Si bien los métodos, dispositivos y productos de programas informáticos descritos en la presente memoria se describen dentro del contexto de un sistema y una red central de quinta generación (5GC), tal como se ilustra en las Figuras 1 a 3 y descritos anteriormente en la presente memoria, los métodos, dispositivos y productos de programas informáticos descritos pueden, no obstante, aplicarse en un contexto más amplio dentro de cualquier sistema, red, estándar y/o protocolo de telecomunicaciones adecuado.

Volviendo ahora a la Figura 4, ejemplos de un aparato, tal como un aparato de red central (CNA) (que incluye, por ejemplo, uno o más de los servicios de red central: UPF 106, AMF 108, SMF 110, PCF 114 y/u otra NF y/o NRF), pueden estar representados por un consumidor de servicios de NF u otro cliente de NF, un SCP u otra entidad intermediaria o un productor de servicios de NF u otra NF. servidor configurado según una realización de ejemplo de la presente descripción. Como se describe a continuación en conjunción con los diagramas de flujo de las Figuras 8, 9, 12 y 13, el aparato 200 de una realización de ejemplo puede configurarse para realizar las funciones descritas en la presente memoria. En cualquier caso, el aparato 200 puede ser encarnado más generalmente por un dispositivo informático, como un servidor, un ordenador personal, una estación de trabajo informática u otro tipo de dispositivo informático, incluidos los que funcionan como un equipo de usuario y/o un componente de una red de área local inalámbrica. Independientemente de la forma en la que el aparato 200 esté encarnado, el aparato de una realización de ejemplo puede estar configurado como se muestra en la Figura 4 para incluir, estar asociado con o estar en comunicación con un procesador 202 y un dispositivo de memoria 204 y, en algunas realizaciones, y/o una interfaz de comunicación 206. En algunas realizaciones, el UE 102, un SCP, un punto de acceso o estación base que incluye un Consumidor de Servicios NF, por ejemplo, SMG, y/o un Productor de Servicios NF u otros elementos del sistema 100 pueden incorporarse mediante un aparato 200 como se muestra en la Figura 4.

El procesador 202 (y/o coprocesadores o cualquier otro circuito que asista o esté asociado con el procesador) puede estar en comunicación con el dispositivo de memoria 204 a través de un bus para pasar información entre los componentes del aparato 200. El dispositivo de memoria puede incluir, por ejemplo, una o más memorias volátiles y/o no volátiles, como un dispositivo de memoria no transitorio. Dicho de otro modo, por ejemplo, el dispositivo de memoria puede ser un dispositivo de almacenamiento electrónico (por ejemplo, un medio de almacenamiento legible por ordenador) que comprende puertas configuradas para almacenar datos (por ejemplo, bits) que pueden recuperarse por una máquina (por ejemplo, un dispositivo informático como el procesador). El dispositivo de memoria puede estar configurado para almacenar información, datos, contenido, aplicaciones, instrucciones o similares para permitir que el aparato lleve a cabo diversas funciones según una realización ilustrativa. Por ejemplo, el dispositivo de memoria puede estar configurado para almacenar en memoria intermedia datos de entrada para su procesamiento por el procesador. Adicional o alternativamente, el dispositivo de memoria puede estar configurado para almacenar instrucciones para su ejecución por el procesador.

El aparato 200 puede, en algunas realizaciones, realizarse en diversos dispositivos informáticos, tal como se describió anteriormente. Sin embargo, en algunas realizaciones, el aparato puede implementarse como un chip o conjunto de chips. Dicho de otro modo, el aparato puede comprender uno o más paquetes físicos (por ejemplo, chips) que incluyen materiales, componentes y/o cables en un conjunto estructural (por ejemplo, una placa base). El conjunto estructural puede proporcionar resistencia física, conservación de tamaño y/o limitación de interacción eléctrica para un conjunto de circuitos de componentes incluido en el mismo. Por tanto, en algunos casos, el aparato puede estar configurado para implementar una realización de la presente invención en un único chip o como un único "sistema en un chip". Como tal, en algunos casos, un chip o conjunto de chips puede constituir medios para realizar una o más operaciones para proporcionar las funcionalidades descritas en la presente memoria.

El procesador 202 puede realizarse de varias maneras diferentes. Por ejemplo, el procesador puede implementarse como uno o más de diversos medios de procesamiento de hardware tales como un coprocesador, un microprocesador, un controlador, un procesador de señales digitales (DSP), un elemento de procesamiento con o sin un DSP adjunto, o varios otros conjuntos de circuitos incluyendo circuitos integrados tales como, por ejemplo, un ASIC (circuito integrado de aplicación específica), un FPGA (matriz de puertas programables en campo), una unidad de microcontrolador (MCU), un acelerador de hardware, un chip de ordenador de propósito especial o similar. Como tal,

5 en algunas realizaciones, el procesador puede incluir uno o más núcleos de procesamiento configurados para funcionar de manera independiente. Un procesador de múltiples núcleos puede permitir un procesamiento múltiple dentro de un único paquete físico. Adicional o alternativamente, el procesador puede incluir uno o más procesadores configurados en tándem a través del bus para permitir la ejecución independiente de instrucciones, canalización y/o multitratamiento.

10 En una realización ilustrativa, el procesador 202 puede estar configurado para ejecutar instrucciones almacenadas en el dispositivo 204 de memoria o accesibles de cualquier otra manera para el procesador. Alternativa o adicionalmente, el procesador puede estar configurado para ejecutar una funcionalidad codificada fija. Como tal, tanto si está configurado por métodos de hardware o de software, o por una combinación de los mismos, el procesador puede representar una entidad (por ejemplo, implementarse físicamente en conjunto de circuitos) que puede realizar operaciones según una realización de la presente invención mientras se configura en consecuencia. Así, por ejemplo, cuando el procesador se implementa como un ASIC, FPGA o similar, el procesador puede ser hardware específicamente configurado para realizar las operaciones descritas en la presente memoria. Alternativamente, como otro ejemplo, cuando el procesador se implementa como un elemento de ejecución de instrucciones de software, las instrucciones pueden configurar específicamente el procesador para realizar los algoritmos y/u operaciones descritos en la presente memoria cuando se ejecutan las instrucciones. Sin embargo, en algunos casos, el procesador puede ser un procesador de un dispositivo específico (por ejemplo, un codificador y/o un decodificador) configurado para emplear una realización de la presente invención mediante una configuración adicional del procesador mediante instrucciones para realizar los algoritmos y/o u operaciones descritas en la presente memoria. El procesador puede incluir, entre otras cosas, un reloj, una unidad de lógica aritmética (ALU) y puertas lógicas configuradas para soportar el funcionamiento del procesador.

25 En las realizaciones que incluyen una interfaz de comunicación 206, la interfaz de comunicación puede ser cualquier medio como un dispositivo o circuito incorporado en hardware o en una combinación de hardware y software que está configurado para recibir y/o transmitir datos desde/a una red y/o cualquier otro dispositivo o módulo en comunicación con el aparato 200, como NF, NRF, una estación base, un punto de acceso, SCP, UE 102, red de acceso radioeléctrico, servicios de red central, un servidor/función de aplicación, una base de datos u otro dispositivo de almacenamiento, etc. A este respecto, la interfaz de comunicación puede incluir, por ejemplo, una antena (o múltiples antenas) y hardware y/o software de soporte para permitir las comunicaciones con una red de comunicación inalámbrica. Adicional o alternativamente, la interfaz de comunicación puede incluir el conjunto de circuitos para interactuar con la(s) antena(s) para provocar la transmisión de señales a través de la(s) antena(s) o para gestionar la recepción de señales recibidas a través de la(s) antena(s). En algunos entornos, la interfaz de comunicación puede soportar, alternativa o adicionalmente, comunicación por cable. Como tal, por ejemplo, la interfaz de comunicación puede incluir un módem de comunicación y/u otro hardware/software para soportar la comunicación a través de cable, línea de abonado digital (DSL), bus serie universal (USB) u otros mecanismos. En algunas realizaciones, una función de gestión de sesión puede comprender una función de gestión de sesión 5GC para cualquier arquitectura adecuada de control y separación de planos de usuario (CUPS), tal como para el nodo de soporte GPRS de puerta de enlace (GGSN-C), TWAG-C, BNG-CUPS, N4, Sxa, Sxb, Sxc, núcleo de paquete evolucionado (EPC) SWG-C, EPC PGW-C, EPC TDF-C y/o similares.

45 Como se ilustra, el aparato 200 puede incluir un procesador 202 en comunicación con una memoria 204 y configurado para proporcionar señales y recibir señales desde una interfaz de comunicación 206. En algunas realizaciones, la interfaz de comunicación 206 puede incluir un transmisor y un receptor. En algunas realizaciones, el procesador 202 puede configurarse para controlar el funcionamiento del aparato 200, al menos en parte. En algunas realizaciones, el procesador 202 puede configurarse para controlar el funcionamiento del transmisor y del receptor efectuando una señalización de control a través de unos cables eléctricos que van hasta el transmisor y el receptor. Asimismo, el procesador 202 puede configurarse para controlar otros elementos del aparato 200 efectuando una señalización de control a través de unos cables eléctricos que conectan el procesador 202 a los demás elementos, tal como una pantalla o la memoria 204.

55 El aparato 200 puede ser capaz de funcionar con uno o más estándares de interfaz aérea, protocolos de comunicación, tipos de modulación, tipos de acceso y/o similares. Las señales enviadas y recibidas por el procesador 202 pueden incluir una información de señalización según un estándar de interfaz aérea de un sistema celular aplicable, y/o cualquier número de distintas técnicas de conexión en red cableadas o inalámbricas, que comprenden, sin limitación, técnicas wifi de wireless local access network (red de acceso local inalámbrica - WLAN), tales como las 802.11, 802.16 y 802.3 del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), ADSL, la DOCSIS y/o similares. Además, estas señales pueden incluir datos de voz, datos generados por el usuario, datos pedidos por el usuario y/o similares.

60 Por ejemplo, el aparato 200 y/o un módem celular en el mismo puede(n) ser capaz(es) de funcionar según diversos protocolos de comunicación de primera generación (1G), protocolos de comunicación de segunda generación (2G o 2.5G), protocolos de comunicación de tercera generación (3G), protocolos de comunicación de cuarta generación (4G), protocolos de comunicación de quinta generación (5G), protocolos de comunicación Internet Protocol Multimedia Subsystem (Subsistmea multimedia IP - IMS) (p. ej., el session initiation protocol [protocolo de inicio de sesión - SIP]) y/o similares. Por ejemplo, el aparato 200 puede ser capaz de funcionar según los protocolos de comunicación inalámbrica de 2G IS-136, Time Division Multiple Access (TDMA), Global System for Mobile Communications (GSM),

IS-95, Code Division Multiple Access (CDMA) y/o similares. Además, por ejemplo, el aparato 200 puede ser capaz de funcionar según los protocolos de comunicación inalámbrica de 2.5G General Packet Radio Service (GPRS), Enhanced Data GSM Environment (EDGE) y/o similares. Además, por ejemplo, el aparato 200 puede ser capaz de funcionar según protocolos de comunicación inalámbrica de 3G tales como Universal Mobile Telecommunications System (UMTS), Code Division Multiple Access 2000 (CDMA2000), Wideband Code Division Multiple Access (WCDMA), Time Division-Synchronous Code Division Multiple Access (TD-SCDMA) y/o similares. El NA 200 puede ser capaz de funcionar según protocolos de comunicación inalámbrica de 3.9G tales como Long Term Evolution (LTE), Evolved Universal Terrestrial Radio Access Network (E-UTRAN) y/o similares. Adicionalmente, por ejemplo, el aparato 200 puede ser capaz de funcionar según protocolos de comunicación inalámbrica de 4G tales como LTE Advanced, 5G y/o protocolos similares, así como a protocolos de comunicación inalámbrica similares que puedan desarrollarse en el futuro. En algunas realizaciones, el aparato 200 puede ser capaz de operar según o dentro del marco de cualquier arquitectura CUPS adecuada, como por ejemplo para el nodo de soporte GPRS de pasarela (GGSN-C), pasarela de acceso inalámbrico de confianza (TWAG-C), pasarelas de red de banda ancha (BNGs), N4, Sxa, Sxb, Sxc, núcleo de paquetes evolucionado (EPC) SWG-C, EPC PGW-C, EPC TDF-C, y/o similares.

Algunas de las realizaciones descritas en la presente memoria pueden implementarse en software, hardware, lógica de aplicación o una combinación de software, hardware y lógica de aplicación. El software, la lógica de aplicación y/o el hardware pueden residir en la memoria 204, el procesador 202 o en unos componentes electrónicos, por ejemplo. En algunas realizaciones de ejemplo, se mantiene la lógica de aplicación, el software o un conjunto de instrucciones en uno cualquiera de diversos medios legibles por ordenador convencionales. En el contexto de este documento, un "medio legible por ordenador" puede ser cualquier medio no transitorio que pueda contener, almacenar, comunicar, propagar o transportar las instrucciones para su uso por o en conexión con un sistema, aparato o dispositivo de ejecución de instrucciones, tal como un ordenador o un sistema de circuitos de procesador de datos, con ejemplos representados en la Figura 4, el medio legible por ordenador puede comprender un medio de almacenamiento legible por ordenador no transitorio que puede ser cualquier medio que pueda contener o almacenar las instrucciones para su uso por o en conexión con un sistema, aparato o dispositivo de ejecución de instrucciones, tal como un ordenador.

La Figura 5 ilustra un flujo de señal entre una pluralidad de entidades de red y demuestra el problema abordado por la presente descripción. En la Figura 5, un cliente NF en forma de un consumidor 102 de servicios de función de red (NF) genera una solicitud de servicio en forma de una solicitud 606 de descubrimiento de función de repositorio de red (NRF) para un servidor NF en forma de una función de control de políticas (PCF) 604. En respuesta, la NRF 124 transmite una respuesta de descubrimiento de NRF 608 al consumidor de servicios NF 102. La respuesta de descubrimiento de NRF 608 comprende información para uno o más perfiles de PCF 604 que corresponden a la solicitud de descubrimiento de función de repositorio de red (NRF) 606 del consumidor de servicios NF 102. Los perfiles PCF 604 pueden incluir al menos uno de una dirección IP, FQDN, información de capacidad, información de prioridad o similar, o cualquier combinación de los mismos. Al recibir la solicitud de descubrimiento de NRF 606, el consumidor de servicios NF 102 de este ejemplo selecciona PCF1 y genera una solicitud HTTP POST y transmite la solicitud HTTP 610 con el perfil PCF seleccionado a un proxy de comunicación de servicio (SCP). Como se ilustra en la Figura 5, el primer SCP1 recibe la solicitud HTTP 610 y transmite un mensaje 612 al PCF1 seleccionado. PCF1 transmite una comunicación de mensaje de error 614 a SCP1 y SCP1 transmite la comunicación de mensaje de error 616 al consumidor de servicio NF 102. Las comunicaciones de mensajes de error 614, 616 pueden comprender cualquier código de error HTTP (por ejemplo, 503, 429, etc.) o detalles de identificación de error de protocolo similares. Las razones del error HTTP u otro protocolo pueden ser cualquier falla, incluido el rechazo debido a una sobrecarga. El consumidor de servicios NF 102, en el escenario de comunicación ilustrado representado en la FIG. 5, no se proporciona el origen del error de comunicación. Sin conocer el origen del error, el consumidor 102 del servicio NF no está informado sobre cómo enrutar o redirigir la solicitud (y posiblemente otras solicitudes posteriores) para establecer comunicaciones exitosamente con la PCF1. En el escenario de comunicación indirecta, ilustrado en la FIG. 5, entre, por ejemplo, un consumidor de servicios 5GC NF 102 a través de un SCP 602, u otra entidad intermedia (por ejemplo, proxy de protección de borde de seguridad (SEPP) para comunicaciones entre PLMN), la fuente del error no se puede determinar como un resultado de la pluralidad de entidades que sirven para retransmitir el mensaje entre el consumidor del servicio NF y la PCF1. En este sentido, el error puede ocurrir en cualquier nodo que reciba y/o transmita el mensaje (por ejemplo, SCP 602, PCF 604, consumidor de servicios NF 102, etc.). Sin la identificación del originador del error, el consumidor de servicios NF 102 u otro dispositivo cliente, por ejemplo, el cliente HTTP, no puede adaptar la solicitud de comunicación basándose en el error real para retransmitir una solicitud o enviar solicitudes posteriores. Además, la política de selección de pares del consumidor de servicios NF 102 no funciona correctamente sin la identificación del autor del error. Además, la falta de información sobre el autor del error también crea ineficiencias para la resolución de problemas y la depuración de la solicitud HTTP 610 y el origen del error.

La presente descripción contempla que el error de comunicación puede ocurrir en cualquier nodo en el flujo de comunicación lógico. A este respecto, una solicitud de un cliente NF, por ejemplo, un consumidor de servicios NF, u otro dispositivo cliente, por ejemplo, un cliente HTTP, puede atravesar una o más funciones de proxy de red, por ejemplo, SCP, SEPP u otras entidades intermedias y, opcionalmente, SCP para señalización entre PLMN y puede fallar en un servidor SCP, SEPP, NRF o HTTP. Según una realización de ejemplo, la entidad que es la fuente del error, tal como un SCP, SEPP u otra entidad de red intermedia, así como el servidor NF, tal como un Productor de Servicios NF, por ejemplo, PCF1, puede ser el fuente de un error (por ejemplo, 400 Bad Request, etc.). Además, un SCP, SEPP u otra entidad de red intermedia también está configurado para reenviar mensajes de error recibidos de otras

entidades, por ejemplo, aguas arriba (por ejemplo, SCP, SEPP, servidor HTTP, NRF, etc.). En un caso en el que el cliente NF, por ejemplo, un consumidor de servicios NF, u otro dispositivo cliente, por ejemplo, el cliente HTTP, es informado del origen del error, el cliente NF u otro dispositivo cliente, por ejemplo, el cliente HTTP, es configurado para ajustar su comportamiento a través de la red para retransmitir con éxito solicitudes de comunicación o enviar solicitudes de servicio posteriores (por ejemplo, solicitar una redirección para un SCP alternativo en un caso en el que el SCP actual genera un error 429 o solicitar una redirección para un PCF alternativo en un (por ejemplo, el PCF actual genera un error 429) para aumentar la probabilidad de que el servidor NF reciba correctamente la solicitud. En una realización de ejemplo, el origen del error no se puede determinar basándose en la presencia o ausencia de una estructura ProblemDetails en una respuesta HTTP, porque un servidor NF, por ejemplo, un productor de servicios NF, y/o una entidad intermedia, como un SCP, puede devolver mensajes de error con o sin una estructura ProblemDetails.

A modo de ejemplo, la Figura 6 ilustra un flujo de llamadas entre una pluralidad de entidades de red donde el error de comunicación se origina en SCP1. Como se ilustra, en la Figura 6, el consumidor de servicios de función de red (NF) 102 genera una solicitud de descubrimiento de función de repositorio de red (NRF) 606 para una función de control de políticas (PCF) 604. En respuesta, la NRF 124 transmite una respuesta de descubrimiento de NRF 608 al consumidor de servicios NF 102. La respuesta de descubrimiento de NRF 608 comprende información para uno o más perfiles de PCF 604 que corresponden a la solicitud de descubrimiento de función de repositorio de red (NRF) 606 del consumidor de servicios NF 102. Los perfiles PCF 604 pueden incluir al menos uno de una dirección IP, FQDN, información de capacidad, información de prioridad o similar, o cualquier combinación de los mismos. Al recibir la solicitud de descubrimiento de NRF 606, el consumidor de servicios NF 102 selecciona PCF1 y genera una solicitud HTTP POST y transmite la solicitud HTTP 610 con la información del perfil PCF1 seleccionado al SCP1. El SCP1 recibe la solicitud HTTP 610 y encuentra un error. En respuesta al error, SCP1 genera un mensaje de error 616 con un encabezado estándar HTTP (por ejemplo, servidor) e inserta una identificación del autor del error en el mensaje que se devuelve, tal como en el encabezado. En algunas realizaciones, los datos de origen de error de ejemplo insertados en el encabezado del mensaje incluyen, al menos, Servidor: scp-scp1.com, Servidor: scp, Servidor: sepp-sepp1.operator.com, Servidor: nrf-xyz o Servidor: udm. El mensaje de error generado 616 con la información de error identificada en el encabezado HTTP se transmite al consumidor de servicios NF 102. Basándose en el originador identificado del error de comunicación en el mensaje de error recibido 616, el consumidor del servicio NF está configurado para generar una nueva solicitud HTTP 710 con instrucciones de comunicación que identifican otro SCP distinto de SCP1 (por ejemplo, SCP2). El consumidor del servicio NF transmite la nueva solicitud HTTP 710 al SCP2. SCP2 recibe la nueva solicitud HTTP 710 y transmite un mensaje correspondiente 712 al PCF1 seleccionado. PCF1 recibe la comunicación 712. PCF1 transmite un mensaje de respuesta 714 a SCP2 y SCP2 transmite un mensaje 716 al consumidor de servicios NF 102, transmitiendo así exitosamente el mensaje y recibiendo la respuesta de PCF1.

Como otro ejemplo, la Figura 7 ilustra un flujo de señal entre una pluralidad de entidades de red donde el error de comunicación se origina en PCF1. Como se ilustra en la Figura 7, el consumidor de servicios de función de red (NF) 102 genera una solicitud de descubrimiento de función de repositorio de red (NRF) 606 para una función de control de políticas (PCF) 604. En respuesta, la NRF 124 transmite una respuesta de descubrimiento de NRF 608 al consumidor de servicios NF 102. La respuesta de descubrimiento de NRF 608 comprende información para uno o más perfiles de PCF 604 que corresponden a la solicitud de descubrimiento de función de repositorio de red (NRF) 606 del consumidor de servicios NF 102. Los perfiles PCF 604 pueden incluir al menos uno de una dirección IP, FQDN, información de capacidad, información de prioridad o similar, o cualquier combinación de los mismos. Al recibir la solicitud de descubrimiento de NRF 606, el consumidor de servicios NF 102 selecciona PCF1 y genera una solicitud HTTP POST y transmite la solicitud HTTP 610 con la información del perfil PCF1 seleccionado al SCP1. El SCP1 recibe la solicitud HTTP 610 y transmite una comunicación 612 a la PCF1. PCF1 recibe la comunicación 612 de SCP1 y encuentra un error. En respuesta al error, PCF1 genera un mensaje de error 614 con un encabezado HTTP (por ejemplo, un encabezado de servidor) e inserta la identificación del autor del error en el encabezado (por ejemplo, PCF1). En algunas realizaciones, los datos de origen de error de ejemplo insertados en el encabezado del mensaje incluyen, al menos, Servidor: pcf-pcf1.com, Servidor: pcf, Servidor: pcf-pcf1.operator.com, Servidor: nrf-pcf o Servidor: udm. El mensaje de error generado 614 con la información de error identificada en el encabezado HTTP se transmite a SCP1 y SCP1 inserta información de transmisión adicional en el encabezado HTTP (por ejemplo, un encabezado Via) del mensaje de error y transmite el mensaje de error correspondiente 616 con el originador identificado del error al consumidor de servicios NF 102. Basándose en el originador PCF1 identificado del error de comunicación en el mensaje de error recibido 616, el consumidor de servicios NF genera una nueva solicitud HTTP 810 con instrucciones de redireccionamiento de comunicación que identifican otro PCF 604 distinto de PCF1 (por ejemplo, PCF2). El consumidor del servicio NF transmite la nueva solicitud HTTP 810 al SCP1. SCP1 recibe la nueva solicitud HTTP 710 y transmite un mensaje correspondiente 812 al PCF2 seleccionado. PCF2 recibe el mensaje 812. PCF2 transmite una respuesta 814 a SCP1 y SCP1 transmite un mensaje correspondiente 816 al consumidor de servicios NF 102, transmitiendo así exitosamente el mensaje y recibiendo la respuesta de PCF2.

Haciendo referencia ahora a la Figura 8, un diagrama de flujo de las operaciones de un método 910 realizado por un aparato 200 incorporado por el originador de la solicitud de servicio, tal como un cliente NF, por ejemplo, un consumidor de servicios NF, un dispositivo cliente, un productor de servicios NF, por ejemplo, un HTTP cliente, o similar, según una realización de ejemplo. Como se muestra en el bloque 911, el aparato 200 incluye medios, tales como el procesador 202, la interfaz de comunicación 206 o similares, para provocar que una solicitud de servicio para un servidor de función de red se transmita a través de una función de proxy de red, tal como un SCP o SEPP, hacia o

hacia el destino, como el servidor NF, por ejemplo, productor de servicios NF o Consumidor de servicios NF. Como se muestra en el bloque 912, el aparato 200 incluye medios, tales como el procesador 202, la interfaz de comunicación 206 o similares, para recibir una respuesta de servicio que comprende al menos un mensaje de error. Como se muestra en el bloque 913, el aparato 200 incluye medios, tales como el procesador 202 o similares, para determinar a partir de la respuesta del servicio, un originador del mensaje de error. Como se muestra en el bloque 914, el aparato 200 incluye medios, tales como el procesador 202, la interfaz de comunicación 206 o similares, para responder de manera diferente al mensaje de error dependiendo del autor del mensaje de error.

Por ejemplo, es posible que el servidor NF necesite dirigir la solicitud de servicio a otro servidor NF, por ejemplo debido a una sobrecarga o porque se va a cerrar. En este caso, la solicitud de servicio puede dirigirse a un servidor NF diferente. Alternativamente, es posible que un SCP no pueda procesar la solicitud de servicio o desee dirigir la solicitud de servicio a otro SCP, por ejemplo, debido a una sobrecarga o porque no es el SCP correcto a utilizar para el segmento de red correspondiente, o porque está para desconectar. En este caso, la solicitud de servicio puede dirigirse al mismo servidor NF a través de un SCP diferente. Como tal, la solicitud de servicio original, como se indica ahora, no encontrará la misma entidad que originó el error junto con la solicitud de servicio original. En algunas realizaciones, el cliente NF, tal como un consumidor de servicios NF, un productor de servicios NF u otro dispositivo cliente, puede determinar la función de proxy de red diferente, por ejemplo, SCP, o un servidor NF diferente, por ejemplo, un productor de servicios NF o un consumidor de servicios NF. al que debe dirigirse la solicitud de servicio y luego retransmitir la solicitud de servicio o transmitir una solicitud de servicio posterior de tal manera que evite al originador del mensaje de error. Alternativamente, la determinación de la función de proxy de red diferente, por ejemplo, SCP, o servidor NF diferente, por ejemplo, productor de servicios NF o consumidor de servicios NF, puede basarse en información proporcionada por la función de proxy de red o el servidor NF que identifica la red diferente. función de proxy, por ejemplo, SCP, o el servidor NF diferente, por ejemplo, productor de servicios NF, tal como en un encabezado de ubicación como se describe a continuación o dentro de la carga útil del mensaje de respuesta (por ejemplo, dentro de la información detallada del problema), de modo que el cliente NF pueda redirigir la solicitud de servicio a la función de proxy de red diferente o al servidor NF diferente. Si bien se puede redirigir una única solicitud de servicio, tal como a través de una redirección HTTP, en algunas realizaciones, el aparato 200, tal como el procesador 202, de otras realizaciones hace que se redirija una pluralidad de solicitudes de servicio, tal como a diferentes SCP y/o a diferentes proveedores de servicios NF, para aumentar la probabilidad de recibir la respuesta de servicio esperada.

Como se describió anteriormente, con referencia a las Figuras 6 y 7, se incluye información en la respuesta del servicio HTTP, o protocolo similar, para identificar al autor del error. Luego, esta información se transmite entre nodos de la red según sea necesario para informar a las entidades de comunicación de red apropiadas sobre el origen del error. Específicamente, la información relativa al originador del error puede incluirse como un mensaje de error en un encabezado que puede ser utilizado por el cliente NF para determinar el originador del error de modo que pueda determinarse el comportamiento adaptativo apropiado para posteriormente eludir la entidad que es el autor del error. En algunas realizaciones, el mensaje de error puede añadirse a una cabecera HTTP, por ejemplo mediante una cabecera Server, una cabecera Via o similar, o puede crearse una cabecera 3GPP Custom. En este sentido, el mensaje de error puede consistir en un encabezado HTTP Via configurado además para indicar el tipo (por ejemplo, "SCP") o la identidad (por ejemplo, un nombre de dominio completo) de la función de proxy de red que reenvía la respuesta de error, un servidor HTTP. encabezado configurado además para indicar el tipo (p. ej., "PCF", "SCP", "SEPP") o la identidad (p. ej., un nombre de dominio completo o una identidad de instancia NF) del autor del error, o un nuevo encabezado HTTP personalizado que contiene el tipo de NF y/o el identificador del originador del error (por ejemplo, SCP FQDN o ID de instancia de NF), y/o el tipo (por ejemplo, "SCP") o identificador de la entidad que reenvía el mensaje de error (por ejemplo, FQDN, un identificador de instancia NF o un identificador de entidad de red).

A modo de ejemplo, en un caso en el que el mensaje de error se proporciona con una cabecera Via que identifica una función proxy de red que reenvió la respuesta de servicio, el aparato 200, tal como el procesador 202, está configurado para determinar que el originador del mensaje de error no es la función proxy de red que proporcionó la respuesta de servicio con la cabecera Via, por ejemplo, el SCP de siguiente salto. En cambio, el autor del mensaje de error puede identificarse, por ejemplo mediante el encabezado del Servidor que puede identificar el servidor de función de red o una función de proxy de red ascendente como el autor del mensaje de error.

En relación con un encabezado de Servidor, el encabezado de Servidor puede incluir el tipo y/o la identificación del servidor NF o la función de proxy de red que es el origen del error. En una realización, el encabezado del Servidor puede comenzar con el valor del tipo (por ejemplo, "nrf", "scp", "sepp", "udm") seguido de un "-" y cualquier otra información específica, como la identificación, por ejemplo, FQDN, del servidor NF o función de red que es el origen del error. Los ejemplos incluyen Servidor: scp-scp1.com, Servidor: scp, Servidor: sepp-sepp1.operator.com, Servidor: nrf-xyz y Servidor: udm. En algunas realizaciones, la presencia del encabezado del Servidor en la respuesta del servicio indica al cliente NF que la entidad o entidades de red identificadas, identificadas por la información de identificación, son los originadores del error. En algunas realizaciones, la información contenida en las cabeceras, como las cabeceras Via y Server o la cabecera Custom puede ser utilizada para la resolución de problemas, depuración y/o por el cliente NF para determinar la lógica de respuesta apropiada (por ejemplo, cancelar, redirigir, reintentar, etc.). En algunas realizaciones, el cliente NF puede iniciar un tiempo de espera o enfriamiento antes de volver a intentar establecer comunicaciones con el servidor NF y/u otra entidad de red identificada.

Mientras que la Figura 8 representó las operaciones realizadas en una realización de ejemplo desde la perspectiva del originador de la solicitud de servicio, tal como un cliente NF, por ejemplo, un consumidor de servicios NF, u otro dispositivo cliente, por ejemplo, un cliente HTTP, o similar, la FIG. 9 ilustra un diagrama de flujo de las operaciones de un método 1010 realizado, en algunas realizaciones, por el aparato 200 materializado por una función de proxy de red, por ejemplo, SCP, SEPP u otra entidad intermedia, para facilitar la identificación del originador del error y Redirección de un mensaje una vez identificado el autor del error. Como se muestra en el bloque 1011, el aparato 200 incluye medios, tales como el procesador 202, la interfaz de comunicación 206 o similares, para recibir una solicitud de servicio, tal como la originada por un cliente NF, por ejemplo, consumidor de servicios NF, productor de servicios NF, u otro dispositivo cliente, por ejemplo, un cliente HTTP, y para provocar que la solicitud de servicio se transmita hacia un servidor NF, por ejemplo, un productor de servicios NF o un consumidor de servicios NF. Como muestra el bloque 1012, el aparato 200 incluye medios, tales como el procesador 202, la interfaz de comunicación 206 o similares, para recibir una respuesta de servicio que comprende al menos un mensaje de error con opcionalmente una indicación del originador del error. La respuesta del servicio se recibe del servidor NF, ya sea directamente o a través de una o más funciones de proxy de red.

El bloque 1013 muestra que el aparato 200 incluye medios, tales como el procesador 202 o similares, para modificar la respuesta de servicio para incluir una indicación adicional de que la respuesta de servicio ha sido transmitida a través de la función de proxy de red, incluido el tipo o identidad de la función de proxy de red. La respuesta del servicio puede modificarse de diversas maneras. En una realización, la respuesta del servicio se modifica para incluir un encabezado adicional, por ejemplo, un encabezado Via, que identifica el SCP o SEPP que está transmitiendo la respuesta del servicio al cliente NF. Por ejemplo, un encabezado HTTP Via puede configurarse además para indicar el tipo (por ejemplo, "SCP") o la identidad (por ejemplo, un nombre de dominio completo) de la función de proxy de red que reenvía la respuesta de error. El encabezado Via puede proporcionarse en combinación con un encabezado de Servidor que puede incluir el mensaje de error, incluida la identificación del autor del error. A este respecto, un encabezado de servidor HTTP puede configurarse además para indicar el tipo (por ejemplo, "PCF", "SCP", "SEPP") o la identidad (por ejemplo, un nombre de dominio completo o una identidad de instancia NF) del originador del error. La entidad, como el servidor NF o una función proxy de red ascendente, que es la originadora del error puede haber añadido el mensaje de error incluyendo su identidad como originadora del error a la cabecera, como la cabecera Servidor, de la respuesta de servicio. Alternativamente, la entidad, tal como el servidor NF o una función de proxy de red ascendente, que es el originador del error puede haber incluido el mensaje de error incluyendo su identidad como el originador del error en la respuesta del servicio, pero no en el encabezado. En este caso, el aparato 200 representado por el SCP no sólo puede agregar un encabezado Via que incluye su identidad, sino que también puede incluir el mensaje de error y la identificación del originador del error a un encabezado de servidor. En otra realización, la respuesta del servicio no incluye un encabezado Via o un encabezado de servidor, pero se modifica para incluir un encabezado diferente, tal como un encabezado personalizado, que incluye la identidad del SCP que está transmitiendo la respuesta del servicio al cliente NF. Este encabezado adicional, como un encabezado personalizado, también puede incluir el mensaje de error, incluida la identificación del autor del error. A este respecto, el aparato 200 materializado por el SCP puede agregar el mensaje de error que incluye la identificación del autor del error al encabezado personalizado, o la entidad, por ejemplo, el servidor NF, que es el autor del error puede crear el Encabezado personalizado e incluye el mensaje de error, incluida la identificación del autor del error dentro del mismo y la función de proxy de red, por ejemplo, SCP, puede agregar su identidad al encabezado personalizado como una entidad que reenvió el mensaje de error. Por ejemplo, un encabezado personalizado puede contener el tipo de NF y/o el identificador del autor del error (por ejemplo, FQDN de SCP o ID de instancia de NF) y/o el tipo o identificador de la entidad que reenvía el mensaje de error (por ejemplo, "SCP").

Con referencia ahora al bloque 1014, el aparato 200 de esta realización de ejemplo, tal como se materializa por el SCP u otra entidad intermedia, también puede incluir medios, tales como el procesador 202, la interfaz de comunicaciones 206 o similares, para provocar la respuesta de servicio, según se modifique, para ser enviado al cliente NF, por ejemplo, consumidor de servicios NF, productor de servicios NF u otro dispositivo cliente, por ejemplo, un cliente HTTP. Como se describió anteriormente, la respuesta del servicio se ha modificado para incluir no solo el mensaje de error que incluye una identificación de la fuente del error, sino también la identidad del SCP u otra entidad intermedia que envió la respuesta del servicio. Como tal, la solicitud de servicio puede retransmitirse inteligentemente o puede enviarse una solicitud de servicio posterior de tal manera que se evite intencionalmente confiar en la entidad que originó el error.

Con respecto a los encabezados que pueden incluir la identidad del SCP que está transmitiendo la respuesta del servicio al cliente NF, el encabezado aVia 1110 de una realización de ejemplo puede configurarse además para definir al menos el tipo o identidad de la función de proxy de red, por ejemplo, el SCP o SEPP, transmitiendo el mensaje de error como se describe anteriormente con referencia a la Figura 9. En algunas realizaciones, el encabezado Via se construye mediante el aparato 200 incorporado por el SCP como se representa en la Figura 9, y se inserta en la respuesta para indicar al cliente NF, por ejemplo, consumidor de servicios NF u otro dispositivo cliente, por ejemplo, un cliente HTTP, que el error informado asociado es reenviado por el SCP intermedio y no es un error de SCP. Las funciones de proxy de red que transmiten la respuesta del servicio y se identifican mediante el encabezado Via incluyen no sólo un SCP, sino también otras entidades intermedias (por ejemplo, SEPP, etc.). Determinadas realizaciones de ejemplo de la manera en que el encabezado Via identifica el SCP intermedio pueden incluir al menos "Via: 2.0 SCP", "Via: 2.0 scp1.com", o similares, o cualquier combinación de los mismos. La respuesta del servicio puede incluir uno

o más encabezados adicionales además del encabezado Via. En algunas realizaciones, por ejemplo, la respuesta de servicio proporcionada por las NF de 5GC y otras entidades de red (por ejemplo, SEPP, SCP, PCF, etc.) también puede incluir uno o más encabezados de servidor que pueden incluir el mensaje de error e identificar el autor del error. En algunas realizaciones, la respuesta de servicio proporcionada por las 5GC NF y otras entidades de red (por ejemplo, SEPP, SCP, PCF, etc.) también puede incluir uno o más encabezados Via además del encabezado Via construido por el SCP.

Como alternativa al encabezado Via, la identidad del SCP que transmite el mensaje de error, incluido el autor del error, al cliente NF puede, en cambio, incluirse en un encabezado personalizado. El encabezado personalizado de una realización tiene un formato configurado para ser aplicable a todas las interfaces basadas en servicios 5GC. En algunas realizaciones, el encabezado personalizado identifica si el error lo origina una entidad intermedia (por ejemplo, un SCP, SEPP, etc.) o un servidor NF (por ejemplo, un productor de servicios NF, etc.). En algunas realizaciones, un encabezado personalizado (por ejemplo, "3GPP-Sbi-SCP-Error: <scp fqdn>"), se usa para diferenciar los errores que surgen de un SCP de los errores generados por otras entidades de la red. En algunas realizaciones, el encabezado personalizado contiene un identificador (por ejemplo, dirección IP, etc.) de una entidad de red que origina un error. En este sentido, un encabezado personalizado contiene el tipo de NF y/o el identificador del autor del error (por ejemplo, SCP FQDN o NF Instance ID), y/o el tipo o identificador de la entidad que reenvía el mensaje de error (por ejemplo, "SCP "). En algunas realizaciones, un encabezado personalizado se define como un encabezado "3GPP-Sbi-Error", que contiene el tipo de NF y/o el identificador del originador del error (por ejemplo, un FQDN de SCP o un ID de instancia de NF de destino), y/ o el identificador de la entidad que transmite el error. Por ejemplo, el encabezado personalizado asociado a un error generado por un SCP puede comprender al menos: "Servicio HTTP 503 no disponible" y "3GPP-Sbi-Error: orig=scp; fqdn=scp1.com". Como otro ejemplo, el encabezado personalizado de un error reenviado por un SCP puede comprender al menos: "Servicio HTTP 503 no disponible" y "Error 3GPP-Sbi: forw=scp; fqdn=scp1.com". Alternativamente, el encabezado personalizado para un error generado por un PCF puede comprender al menos: "HTTP 429 demasiadas solicitudes" y "3GPP-Sbi-Error: orig=pcf; nfnstanceld=54804518-4191-46b3-955c-ac631f953ed8", mientras que el encabezado personalizado para un error PCF reenviado por un SCP puede comprender al menos: "HTTP 429 demasiadas solicitudes" y "3GPP-Sbi-Error: orig=pcf; nfnstanceld=54804518-4191-46b3-955c-ac631f953ed8, forw=scp; fqdn=scp1.com". En algunas realizaciones que se describen a continuación, el componente ProblemDetails de una respuesta de error también se puede ampliar con un nuevo atributo que indique el origen del error (por ejemplo, tipo de NF, ID de instancia de NF, dirección IP, FQDN, etc.).

Como se describió anteriormente junto con el bloque 914 de la Figura 8, el aparato 200 incorporado por el cliente NF, por ejemplo, el consumidor de servicios NF u otro dispositivo cliente, por ejemplo, un cliente HTTP, está configurado para responder de manera diferente al mensaje de error contenido en la respuesta del servicio dependiendo del originador del error. Por ejemplo, la solicitud de servicio puede retransmitirse o se puede transmitir una solicitud de servicio posterior de una manera que no dependa ni se comunique con la entidad que creó previamente el error. Alternativamente, la solicitud de acceso puede ser redirigida. En un caso en el que el originador del error es una función de proxy de red, a diferencia del servidor NF, la respuesta del servicio puede incluir información de redireccionamiento que indica una función de proxy de red alternativa que se utilizará junto con la solicitud de servicio redirigido. Aunque la redirección de la solicitud de servicio puede realizarse de varias maneras, un ejemplo de la manera en que la solicitud de servicio puede ser reenviada se representa en la Figura 10. A este respecto, el método 1310 incluye el bloque 1215 muestra que el aparato 200 encarnado por el cliente NF incluye medios, tales como el procesador 202, la interfaz de comunicación 206 o similares, para hacer que una solicitud de servicio para un servidor de función de red, por ejemplo, servidor NF, se transmita a través de al menos una función de proxy de red, por ejemplo, SCP, SEPP, etc. de la manera descrita anteriormente. Como se muestra en el bloque 1216, el aparato 200 incluye medios, tales como el procesador 202, la interfaz de comunicación 206 o similares, para recibir una respuesta de servicio que comprende al menos un mensaje de error. El aparato 200 también incluye medios, tales como el procesador 202 o similares, para determinar a partir de la respuesta del servicio que la solicitud debe redirigirse hacia otra función de proxy de red, en lugar de hacia otro servidor de función de red. Véase el bloque 1217. El aparato 200 de esta realización de ejemplo incluye adicionalmente medios, tales como el procesador 202 o similares, para identificar la otra función de proxy de red a la que se redirigirá la solicitud de servicio basándose en una identificación de la otra función de proxy de red con el mensaje de error. Por tanto, como se describe con más detalle a continuación, el mensaje de error de esta realización de ejemplo puede no solo identificar la función de proxy de red como el originador del error, sino que también puede identificar otra función de proxy de red a la que se debe redirigir la solicitud de servicio. Véase el bloque 1218. Con respecto a identificar la función de proxy de red como el originador del error, la respuesta del servicio puede, por ejemplo, incluir un encabezado de servidor o un encabezado personalizado que identifica el tipo de entidad, por ejemplo, SCP o SEPP, y la identidad del entidad, por ejemplo, FQDN, que fue el origen del error. La respuesta de servicio también puede identificar la otra función de proxy de red a la que se debe redirigir la solicitud de servicio. Además, el aparato 200 de esta realización de ejemplo incluye medios, tales como el procesador 202, la interfaz de comunicación 206 o similares, para redirigir la solicitud de servicio para el mismo servidor de función de red a través de la otra función de proxy de red que fue identificada por el mensaje de error. evitando así la función de proxy de red que fue la causante del error. Véase el bloque 1219.

En una realización, el aparato 200, tal como el procesador 202, está configurado para determinar a partir de la respuesta del servicio que la solicitud debe redirigirse hacia otra función de proxy de red, en lugar de hacia otro servidor

de función de red, identificando un error del protocolo SCP\_REDIRECTION. en el mensaje de error. Por ejemplo, la función de proxy de red que origina el error puede incluir un mensaje de error, como un error 503, 400 o 429, que incluye una estructura ProblemDetails que indica un error de protocolo de "SCP\_REDIRECTION", es decir, SCP envía, por ejemplo, 503, 400, 429... respuesta con ProblemDetails que indica "SCP\_REDIRECTION" en la respuesta de servicio que se proporciona al cliente NF. El aparato 200, tal como el procesador 202, de esta realización de ejemplo también puede configurarse para identificar otra función de proxy de red a la que debe redirigirse la solicitud de servicio basándose en una identidad de la otra función de proxy de red incluida en los detalles del problema del mensaje de error. A este respecto, los detalles del problema también pueden incluir un nuevo atributo que lleva la identificación, tal como el FQDN, de la otra función de proxy de red, por ejemplo, otro SCP, hacia el cual se debe redirigir la solicitud de servicio.

En otra realización, el aparato 200, tal como el procesador 202, está configurado para determinar a partir de la respuesta de servicio que la solicitud debe redirigirse hacia otra función de proxy de red, en lugar de hacia otro servidor de función de red, determinando que la respuesta de servicio incluye un encabezado de servidor o un encabezado personalizado que identifica la función de proxy de red como originadora. El aparato 200, tal como el procesador 202, de esta realización de ejemplo también está configurado para identificar otra función de proxy de red a la que se redirigirá la solicitud de servicio basándose en una identidad de la otra función de proxy de red incluida dentro de un encabezado de ubicación del servicio. respuesta o dentro de la carga útil de respuesta (por ejemplo, dentro de la información de detalles del problema). Por ejemplo, la función de proxy de red que origina el error puede incluir un mensaje de error, tal como una redirección 307/308, que incluye un encabezado de ubicación que identifica la identidad, por ejemplo, FQDN, de la otra función de proxy de red a la que la solicitud de servicio debe ser redirigida. Junto con la identificación de la función de proxy de red original en el encabezado del servidor o el encabezado personalizado, el cliente NF de esta realización de ejemplo interpreta el mensaje de error como una solicitud para redirigir la solicitud de servicio a una función de proxy de red diferente, por ejemplo, un SCP diferente. sin cambios en el servidor NF al que se dirige la solicitud de servicio, por ejemplo, encabezado 3gpp-Sbi-Target-apiRoot.

Aunque se describe en la presente memoria junto con la Figura 10 en relación con la redirección de la solicitud de servicio por parte del consumidor de servicios NF u otro dispositivo cliente, la redirección de la solicitud de servicio que incluye las operaciones representadas en la Figura 10 puede, en cambio, ser realizado por el SCP u otra entidad intermediaria en otra realización de ejemplo.

De manera similar a la realización descrita anteriormente relacionada con el error de protocolo SCP\_REDIRECTION, un error de protocolo "NF\_REDIRECTION" puede ser definido e incluido, por ejemplo, por el servidor NF en la respuesta de error (por ejemplo, error HTTP 503, 400, 429, etc.) con detalles del problema que indica "NF\_REDIRECTION" e incluye, adicionalmente, un nuevo atributo que identifica un productor de servicios NF diferente al que se debe redirigir la solicitud de servicio, por ejemplo proporcionando el FQDN, u otra información de identificación de entidad de red, del productor de servicios NF hacia al cual se debe redirigir la solicitud de servicio.

Si bien las Figuras 8 y 11 ilustran las operaciones realizadas desde la perspectiva del cliente NF, por ejemplo, un consumidor de servicios NF, un productor de servicios NF u otro dispositivo cliente y un SCP u otra entidad intermedia, respectivamente, la Figura 11 representa un diagrama de flujo de un método 1310 realizado, en algunas realizaciones, por un aparato 200 incorporado por un servidor NF, tal como el productor de servicios NF, el consumidor de servicios NF u otro servidor de destino, por ejemplo, el servidor HTTP. Como se muestra en el bloque 1311, el aparato 200 incorporado por el servidor de red incluye medios, tales como el procesador 202, la interfaz de comunicación 206 o similares, para recibir una solicitud de servicio desde un cliente NF. Con referencia al bloque 1312, el aparato 200 incorporado por el servidor de red incluye medios, tales como el procesador 202 o similares, para determinar que existe una condición de error con respecto al procesamiento de la solicitud de servicio.

El bloque 1313 muestra que el aparato 200 incorporado por el servidor NF incluye medios, tales como el procesador 202 o similares, para identificar un mensaje de error en relación con la condición de error. Y, el bloque 1314 muestra que el aparato 200 incorporado por el servidor NF incluye medios, tales como el procesador 202, la interfaz de comunicación 206 o similares, para provocar que una respuesta de servicio se transmita al cliente NF, tal como a través de un SCP u otra entidad intermedia. La respuesta de servicio comprende al menos el mensaje de error e incluye una indicación del originador del error que identifica el tipo o identidad del origen, por ejemplo, el tipo 5GC NF, un ID de instancia NF, una dirección IP u otra dirección, de la entidad, como el servidor NF, que es el originador del error para permitir que la solicitud de servicio se retransmita o redirija correctamente como se describe anteriormente.

A modo de ejemplos no limitantes, ahora se describirán algunos escenarios de errores de comunicación de red y las soluciones proporcionadas para los mismos según ciertas realizaciones de ejemplo. Tal como se usa con referencia a los escenarios descritos a continuación, el símbolo "/" se usa para representar una nueva línea.

En un escenario de ejemplo, una primera NF, es decir, NF1, transmite una solicitud de servicio a una segunda NF, concretamente, NF2, a través de una entidad intermedia, SCP, y se produce un error XX en NF2. NF2 devuelve una respuesta de servicio con un mensaje de error que identifica a NF2 como la fuente del error, con o sin detalles del problema, al SCP y, a su vez, a NF1.

En una realización, NF2 agrega “Servidor= NF2” identificando al originador del error como NF2 y luego el SCP agrega “Via= SCP” identificando que el SCP está reenviando el mensaje de error. El consumidor del servicio NF, NF1, recibe “Error XX/Servidor = NF2/Vía= SCP” en el mensaje de error que identifica el error XX, el originador del error como NF2 identificado por el encabezado del servidor y la entidad de reenvío como el SCP como lo identifica el encabezado Vía. Basándose en el encabezado del servidor, el consumidor del servicio NF, NF1, recibe información que identifica que el error ocurrió en NF2. Por lo tanto, NF1 puede seleccionar un productor de servicios NF diferente en la solicitud de servicio retransmitida o en una solicitud de servicio posterior.

En otra realización que usa un encabezado personalizado, el NF2 agrega “3GPP-Sbi-Error: orig=NF2type; NFInstanceId=NF2” identifica al autor del error como NF2 y luego el SCP agrega “3GPP-Sbi-Error: forw=scp; fqdn=SCP FQDN” identifica que el SCP está reenviando el mensaje de error. El consumidor del servicio NF, NF1, recibe el “Error XX/3GPP-Sbi-Error: orig=NF2type; / NFInstanceId=NF2, / forw=scp; fqdn=SCP/FQDN” en el mensaje de error que identifica el error XX, el autor del error se identifica como NF2 mediante el encabezado personalizado y la entidad de reenvío se identifica como SCP mediante el encabezado personalizado. Basándose en el encabezado personalizado 3GPP-Sbi-Error, el consumidor del servicio NF, NF1, recibe información que identifica que el error ocurrió en NF2. Como antes, NF1 puede seleccionar un productor de servicios NF diferente en la solicitud de servicio retransmitida o en la solicitud de servicio posterior.

En otro escenario de ejemplo, una primera NF, NF1, transmite una solicitud de servicio a una segunda NF, NF2, a través de una entidad intermedia, SCP, y se produce un error XX en el SCP. El SCP devuelve el error al consumidor del servicio NF, NF 1.

En una realización de ejemplo, el SCP agrega “Servidor = SCP” identificando que el SCP es el originador del error. El consumidor del servicio NF, NF1, recibe “Error XX/Servidor = SCP” en el mensaje de error que identifica el error XX y el autor del error se identifica como SCP mediante el encabezado del Servidor. Basándose en el encabezado del servidor, el consumidor del servicio NF recibe información que identifica que el error ocurrió en el SCP. Por tanto, el consumidor del servicio NF, NF1, puede seleccionar el mismo NF2 objetivo a través de un SCP diferente en la solicitud de servicio retransmitida o en la solicitud de servicio posterior.

En otra realización que usa un encabezado personalizado, el SCP agrega “3GPP-Sbi-Error=orig=scp; fqdn=SCP FQDN” que identifica al autor del error como el SCP. El consumidor del servicio NF, NF1, recibe “Error XX/3GPP-Sbi-Error= orig=scp; fqdn=SCP/FQDN” en el mensaje de error que identifica el error XX y el autor del error se identifica como SCP mediante el encabezado personalizado. Basándose en el encabezado personalizado 3GPP-Sbi-Error, el consumidor del servicio NF, NF1, recibe información que identifica que se produjo el error en el SCP. Por tanto, el consumidor del servicio NF, NF1, puede seleccionar el mismo NF2 objetivo a través de un SCP diferente en una solicitud de servicio retransmitida o solicitud de servicio posterior.

En otro escenario de ejemplo, una primera NF, NF1, transmite una solicitud de servicio a una segunda NF, NF2, a través de dos entidades intermedias, SCP1 y SCP2, y se produce un error XX en SCP2. SCP2 devuelve el error a la NF1.

En una realización, SCP2 agrega “Servidor = SCP2” identificando al originador del error como SCP2 y luego el SCP1 agrega “Via = SCP1” identificando que SCP1 está reenviando el mensaje de error. El consumidor del servicio NF, NF1, recibe “Error XX / Servidor = SCP2 / Via = SCP1” en el mensaje de error que identifica el error XX, el autor del error se identifica como SCP2 mediante el encabezado del servidor y la entidad de reenvío se identifica como SCP1 por el encabezado Via. Basándose en el encabezado del servidor y el encabezado Via, el consumidor del servicio NF, NF1, recibe información que identifica que el error ocurrió en SCP2. Por tanto, el consumidor del servicio NF, NF1, puede seleccionar el mismo NF2 objetivo a través del mismo SCP1 y un SCP2 diferente para una solicitud de servicio retransmitida. En algunas realizaciones, basándose en la política del operador, SCP1 determina una ruta diferente (por ejemplo, utilizando un SCP2 diferente).

En otra realización que usa un encabezado personalizado, SCP2 agrega “3GPP-Sbi-Error=orig=scp; fqdn=SCP2 FQDN” identifica al originador del error como SCP2 y luego el SCP1, opcionalmente, agrega “3GPP-Sbi- Error= orig=scp; fqdn=SCP2 FQDN” identificando que el SCP1 está reenviando el mensaje de error. El consumidor del servicio NF, NF1, recibe “Error XX/3GPP-Sbi-Error= orig=scp; fqdn=SCP2/FQDN” en el mensaje de error que identifica el error XX, el autor del error se identifica como SCP2 mediante el encabezado personalizado y la entidad de reenvío se identifica como SCP mediante el encabezado personalizado. Basándose en el encabezado personalizado 3GPP-Sbi-Error, el consumidor del servicio NF, NF1, recibe información que identifica que el error ocurrió en SCP2. Por tanto, el consumidor del servicio NF, NF1, puede seleccionar el mismo NF2 objetivo a través del mismo SCP1 y un SCP2 diferente en una solicitud de retransmisión. En algunas realizaciones, basándose en la política del operador, SCP1 determina una ruta diferente (por ejemplo, utilizando un SCP2 diferente).

En otro escenario de ejemplo, una primera NF, NF1, transmite una solicitud de servicio a una segunda NF, NF2, a través de una entidad intermedia, SCP1, y se produce un error XX en SCP1. Luego, SCP1 dirige a NF1 a otro SCP, es decir, SCP2.

En una realización de ejemplo, SCP1, opcionalmente, agrega “Servidor = SCP1” que identifica al originador del error como SCP1 y luego el SCP1 agrega Detalles del problema que incluyen “SCP\_REDIRECTION” y un nuevo atributo que indica “SCP\_FQDN” que identifica que el SCP1 está redirigiendo la comunicación. a SCP2. El consumidor del servicio NF, NF1, recibe “Error 307/308 / Server = SCP1 / ProblemDetails:” que incluye “SCP\_REDIRECTION” y el nuevo atributo que indica “SCP\_FQDN” en el mensaje de error que sirve para identificar el error XX. Además, el autor del error se identifica como SCP1 mediante el encabezado del servidor opcional y la redirección a SCP2 se identifica mediante Detalles del problema. Basándose en el código de error identificado, el encabezado del servidor y los detalles del problema, el consumidor del servicio NF, NF1, recibe información que identifica que el error ocurrió en SCP1 y SCP1 solicita una redirección a SCP2.

En otra realización de ejemplo que usa un encabezado personalizado, SCP1 agrega “3GPP-Sbi-Error= orig=scp1” y “Encabezado de ubicación =SCP2” identificando al originador del error como SCP1 y al SCP2 como la ubicación de redirección. El consumidor del servicio NF, NF1, recibe “Error XX / 3GPP-Sbi-SCP-Error= SCP1 / Encabezado de ubicación =SCP2” en el mensaje de error que identifica el error XX, el origen del error se identifica como SCP1 mediante el encabezado Personalizado. y la entidad de redirección se identifica como SCP2 mediante el encabezado personalizado. Basándose en el encabezado personalizado, el consumidor del servicio NF, NF1, recibe información que identifica que el error ocurrió en SCP1 y SCP1 solicita una redirección a SCP2.

En otro escenario de ejemplo, una primera NF, NF1, transmite una solicitud de servicio a una segunda NF, NF2, a través de una entidad intermedia, SCP1, y NF2 luego dirige a otra NF, NF3.

En una realización de ejemplo, NF2 agrega “Encabezado de ubicación = NF3” e incluye “NF\_REDIRECTION” en el mensaje de error junto con un nuevo atributo que indica el “NF\_FQDN” que identifica NF3 al cual NF2 está redirigiendo la solicitud de servicio. El consumidor del servicio NF, NF1, recibe “Error 307/308/Encabezado de ubicación = NF3” en el mensaje de error que identifica la redirección. Basándose en el encabezado Ubicación, el consumidor del servicio NF, NF1, recibe información que identifica que NF2 solicita una redirección a NF3.

En otra realización de ejemplo que usa un encabezado personalizado, NF2 agrega “3GPP-Sbi-Error= orig=NF2type” y “Location header = NF3” identificando al originador como NF2 y NF3 como la ubicación de redirección. SCP1 agrega además “Via = SCP1” al transmitir la respuesta del servicio a NF1. El consumidor del servicio NF, NF1, recibe “Error 307/308/Encabezado de ubicación = NF3/Vía = SCP1” en el mensaje de error que identifica la redirección. Basándose en el encabezado de Ubicación, el consumidor del servicio NF, NF1, recibe información a través de SCP1 identificando que NF2 solicita una redirección a NF3.

En otro escenario de ejemplo, se produce un tiempo de espera en el cliente NF, NF1, porque no se recibe respuesta del SCP solicitado durante un período de tiempo predefinido y rastreado desde el inicio de la solicitud de servicio realizada por el cliente NF. Basándose en la política del operador predefinida, el cliente NF define indicadores clave de rendimiento (KPI), como el tiempo de respuesta antes del tiempo de espera. El cliente NF está configurado para decidir seleccionar un SCP diferente y volver a enviar la solicitud de servicio si se alcanza el umbral del intervalo de tiempo de espera. En algunas realizaciones, el cliente NF define una pluralidad de umbrales de KPI, tales como intervalos de tiempo de espera predefinidos, ventana(s), número mínimo de intentos de llamada, ubicaciones de red bloqueadas, ubicaciones de red permitidas o similares, o cualquier combinación de los mismos. Por ejemplo, si otras solicitudes de servicio tienen éxito y el KPI es alto, el cliente NF puede configurarse para determinar que el problema probablemente esté relacionado con el servidor NF y definirá un servidor NF diferente para la solicitud de servicio. Además, el cliente NF puede configurarse para determinar que si de repente muchas solicitudes de servicio caducan, como por ejemplo más de un número predefinido de solicitudes de servicio, y se alcanza el umbral de degradación de KPI, es probable que el problema esté en el SCP y pueda identificar un SCP diferente para las solicitudes de servicio.

Como se describió anteriormente, los diagramas de flujo referenciados de métodos que pueden llevarse a cabo mediante un aparato según productos de programas informáticos relacionados que comprenden código de programa informático. Se entenderá que cada bloque de los diagramas de flujo, y combinaciones de bloques en los diagramas de flujo, pueden implementarse mediante diversos medios, tales como hardware, firmware, procesador, conjunto de circuitos y/u otros dispositivos asociados con la ejecución de software que incluye una o más instrucciones de programa informático. Por ejemplo, uno o más de los procedimientos descritos anteriormente pueden implementarse mediante instrucciones de programa informático. Con respecto a esto, las instrucciones de programa informático que implementan los procedimientos descritos anteriormente pueden almacenarse por un dispositivo de memoria, por ejemplo, 204, de un aparato, por ejemplo, 200, que emplea una realización de la presente invención y ejecutarse por un procesador, por ejemplo, 202, del aparato. Como se apreciará, cualquiera de tales instrucciones de programa informático puede cargarse en un ordenador u otro aparato programable (por ejemplo, hardware) para producir una máquina, de modo que el ordenador u otro aparato programable resultante implementa las funciones especificadas en los bloques de diagrama de flujo. Estas instrucciones de programa informático también pueden almacenarse en una memoria legible por ordenador que puede dirigir un ordenador u otro aparato programable para funcionar de una manera particular, de modo que las instrucciones almacenadas en la memoria legible por ordenador producen un artículo de fabricación cuya ejecución realiza la función especificada en los bloques de diagrama de flujo. Las instrucciones de programa informático también pueden cargarse en un ordenador u otro aparato programable para hacer que se realice una serie de operaciones en el ordenador u otro aparato programable para producir un

procedimiento implementado por ordenador de tal modo que las instrucciones que ejecutan en el ordenador u otro aparato programable proporcionan operaciones para implementar las funciones especificadas en los bloques de diagrama de flujo.

5 Por tanto, se define un producto de programa informático en aquellas instancias en las que las instrucciones de programa informático, tales como las porciones de código de programa legibles por ordenador, se almacenan por al menos un medio de almacenamiento legible por ordenador no transitorio con las instrucciones de programa informático, tales como las porciones de código de programa legibles por ordenador, configuradas, tras la ejecución, para realizar las funciones descritas anteriormente. En otras realizaciones, las instrucciones de programa informático, tales como las porciones de código de programa legibles por ordenador, no necesitan almacenarse o incorporarse de otra manera por un medio de almacenamiento legible por ordenador no transitorio, pero pueden, en cambio, incorporarse por un medio transitorio con las instrucciones de programa informático, tales como las porciones de código de programa legibles por ordenador, que aún están configuradas, tras la ejecución, para realizar las funciones descritas anteriormente.

15 Por consiguiente, los bloques del diagrama de flujo soportan combinaciones de medios para realizar las funciones especificadas y combinaciones de operaciones para realizar las funciones especificadas para realizar las funciones especificadas. También se entenderá que uno o más bloques de los diagramas de flujo, y combinaciones de bloques en los diagramas de flujo, pueden implementarse mediante sistemas informáticos basados en hardware de propósito especial que realizan las funciones especificadas, o combinaciones de hardware de propósito especial e instrucciones informáticas.

20 En algunas realizaciones, algunas de las operaciones anteriores pueden modificarse o amplificarse adicionalmente. Además, en algunas realizaciones, pueden incluirse operaciones opcionales adicionales. Las modificaciones, sumas, restas, inversiones, correlaciones, relaciones proporcionales, relaciones desproporcionadas, atenuaciones y/o amplificaciones de las operaciones anteriores se pueden realizar en cualquier orden y en cualquier combinación.

25 Muchas modificaciones y otras realizaciones de las invenciones expuestas en la presente memoria se le ocurrirán a un experto en la técnica a la que pertenecen estas invenciones que tenga el beneficio de las enseñanzas presentadas en las descripciones anteriores y los dibujos asociados. Por lo tanto, debe entenderse que las invenciones no deben limitarse a las realizaciones específicas descritas. Además, aunque las descripciones anteriores y los dibujos asociados describen realizaciones ilustrativas en el contexto de determinadas combinaciones ilustrativas y/o funciones, debe apreciarse que pueden proporcionarse diferentes combinaciones de elementos y/o funciones mediante realizaciones alternativas sin abandonar el ámbito de las reivindicaciones adjuntas. Con respecto a esto, por ejemplo, también se contemplan combinaciones de elementos y/o funciones diferentes de las descritas anteriormente de manera explícita como se puede establecer en algunas de las reivindicaciones adjuntas. Aunque en la presente memoria se emplean términos específicos, se usan sólo en un sentido genérico y descriptivo y no con fines de limitación.

**REIVINDICACIONES**

1. Un método que comprende:

5 provocar que una solicitud de servicio para un servidor (604) de función de red se transmita a través de al menos uno de un proxy de comunicación de servicio, SCP (602),

y un proxy de protección del borde de seguridad, SEPP;

10 recibir una respuesta de servicio que comprende al menos un mensaje de error, en donde la respuesta de servicio comprende un protocolo de transferencia de hipertexto, HTTP, encabezado de servidor que incluye un tipo de originador del mensaje de error o un encabezado HTTP vía que incluye un tipo de SCP (602) o, respectivamente, el SEPP que transmite la respuesta del servicio; y

15 determinar, a partir de la respuesta del servicio, un originador del mensaje de error, siendo el originador del mensaje de error el servidor (604) de función de red o el SCP (602) o el SEPP; y:

20 cuando se determina que el originador del mensaje de error es el SCP (602) o el SEPP, provocando que la solicitud de servicio se transmita al servidor (604) de función de red a través de un SCP diferente o, respectivamente, un SEPP diferente; y

cuando se determina que el originador del mensaje de error es el servidor (604) de función de red, provocando que la solicitud de servicio se transmita a un servidor de función de red diferente usando el mismo o diferente SCP y/o el mismo o diferente SEPP.

25 2. El método según la reivindicación 1, en donde el encabezado del servidor HTTP incluye una identidad del originador del mensaje de error, o en donde el encabezado vía HTTP incluye una identidad del SCP o, respectivamente, del SEPP que retransmite la respuesta del servicio.

30 3. El método según la reivindicación 1 o 2, en donde determinar a partir de la respuesta de servicio el originador del mensaje de error comprende, en un caso en el que el encabezado HTTP vía indica que el SCP o, respectivamente, el SEPP retransmitió el mensaje de error o en un instancia en la que el encabezado del servidor HTTP identifica el servidor de función de red como el originador del mensaje de error, determinando que el originador del mensaje de error no es ni el SCP ni, respectivamente, el SEPP.

35 4. El método según la reivindicación 2 o el método según la reivindicación 3 cuando depende de la reivindicación 2, en donde la identidad del autor del mensaje de error comprende un nombre de dominio completo, FQDN, o un identificador de instancia de función de red.

40 5. El método según la reivindicación 2 o el método según las reivindicaciones 3 o 4 cuando depende de la reivindicación 2, en donde la identidad del SCP o SEPP que transmite la respuesta del servicio es un nombre de dominio completamente calificado, FQDN, un identificador de instancia de función de red o un identificador de entidad de red.

45 6. Un aparato (102) que comprende:

medios para provocar que una solicitud de servicio para un servidor (604) de función de red se transmita a través de al menos uno de un proxy de comunicación de servicio, SCP (602), y un proxy de protección de borde de seguridad, SEPP;

50 medios para recibir una respuesta de servicio que comprende al menos un mensaje de error, en donde la respuesta de servicio comprende un protocolo de transferencia de hipertexto, HTTP, encabezado de servidor que incluye un tipo de originador del mensaje de error o un encabezado HTTP vía que incluye un tipo de SCP (602) o, respectivamente, el SEPP que transmite la respuesta del servicio; y

55 medios para determinar, a partir de la respuesta del servicio, un originador del mensaje de error, siendo el originador del mensaje de error el servidor (604) de función de red o el SCP (602) o el SEPP; y:

60 medios para provocar, cuando se determina que el originador del mensaje de error es el SCP (602) o el SEPP, que la solicitud de servicio se transmita al servidor (604) de función de red a través de un SCP diferente o, respectivamente, un SEPP diferente; y

65 medios para provocar, cuando se determina que el originador del mensaje de error es el servidor (604) de función de red, que la solicitud de servicio se transmita a un servidor de función de red diferente usando el mismo o un SCP diferente y/o el mismo o un diferentes SEPP.

7. El aparato según la reivindicación 6, en donde el encabezado del servidor HTTP incluye una identidad del originador del mensaje de error, o en donde el encabezado vía HTTP incluye una identidad del SCP o, respectivamente, del SEPP que retransmite la respuesta del servicio.
- 5 8. El aparato según la reivindicación 6 o 7, en donde los medios para determinar a partir de la respuesta de servicio el originador del mensaje de error están configurados además para determinar, en un caso en el que el encabezado HTTP vía indica que el SCP o, respectivamente, el SEPP retransmitió el mensaje de error o en un caso en el que el encabezado del servidor HTTP identifica el servidor de función de red como el originador del mensaje de error, que el originador del mensaje de error no es ni el SCP ni, respectivamente, el SEPP.
- 10 9. El aparato según la reivindicación 7 o el aparato según la reivindicación 8 cuando depende de la reivindicación 7, en donde la identidad del originador del mensaje de error comprende un nombre de dominio completo, FQDN, o un identificador de instancia de función de red.
- 15 10. El aparato según la reivindicación 7 o el aparato según las reivindicaciones 8 o 9 cuando depende de la reivindicación 7, en donde la identidad del SCP o del SEPP que transmite la respuesta del servicio es un nombre de dominio totalmente calificado, FQDN, un identificador de instancia de función de red o un identificador de entidad de red.
- 20 11. Un programa informático que comprende instrucciones que, cuando el programa es ejecutado por un ordenador, hacen que el ordenador lleve a cabo un método según una cualquiera de las reivindicaciones 1 a 5.

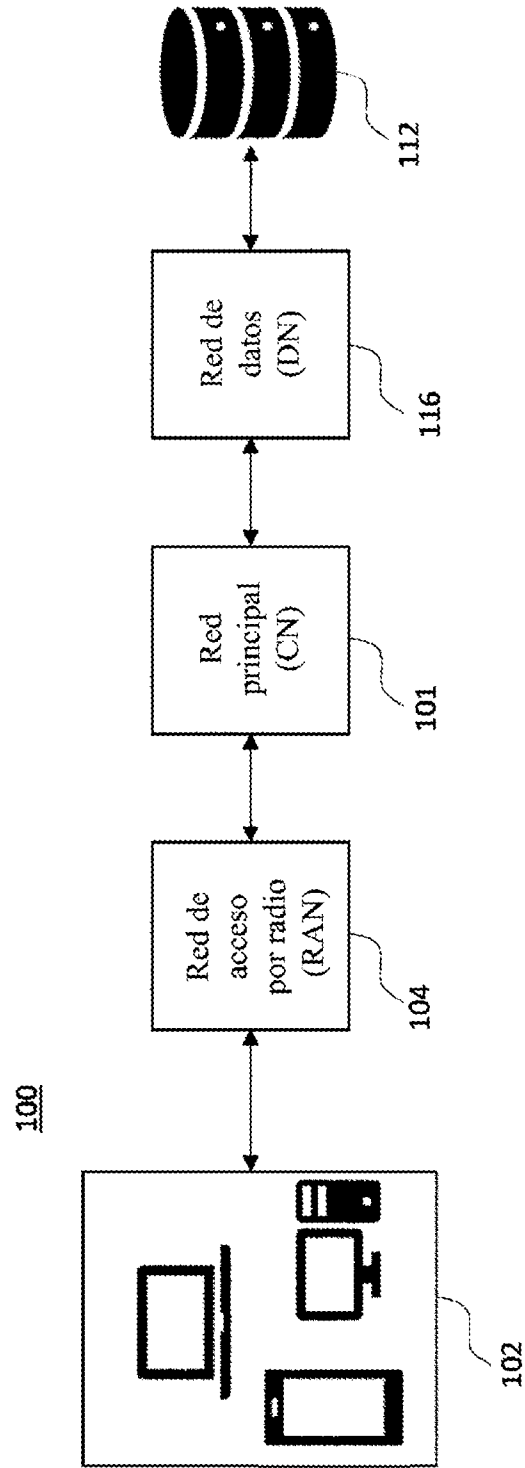


Figura 1

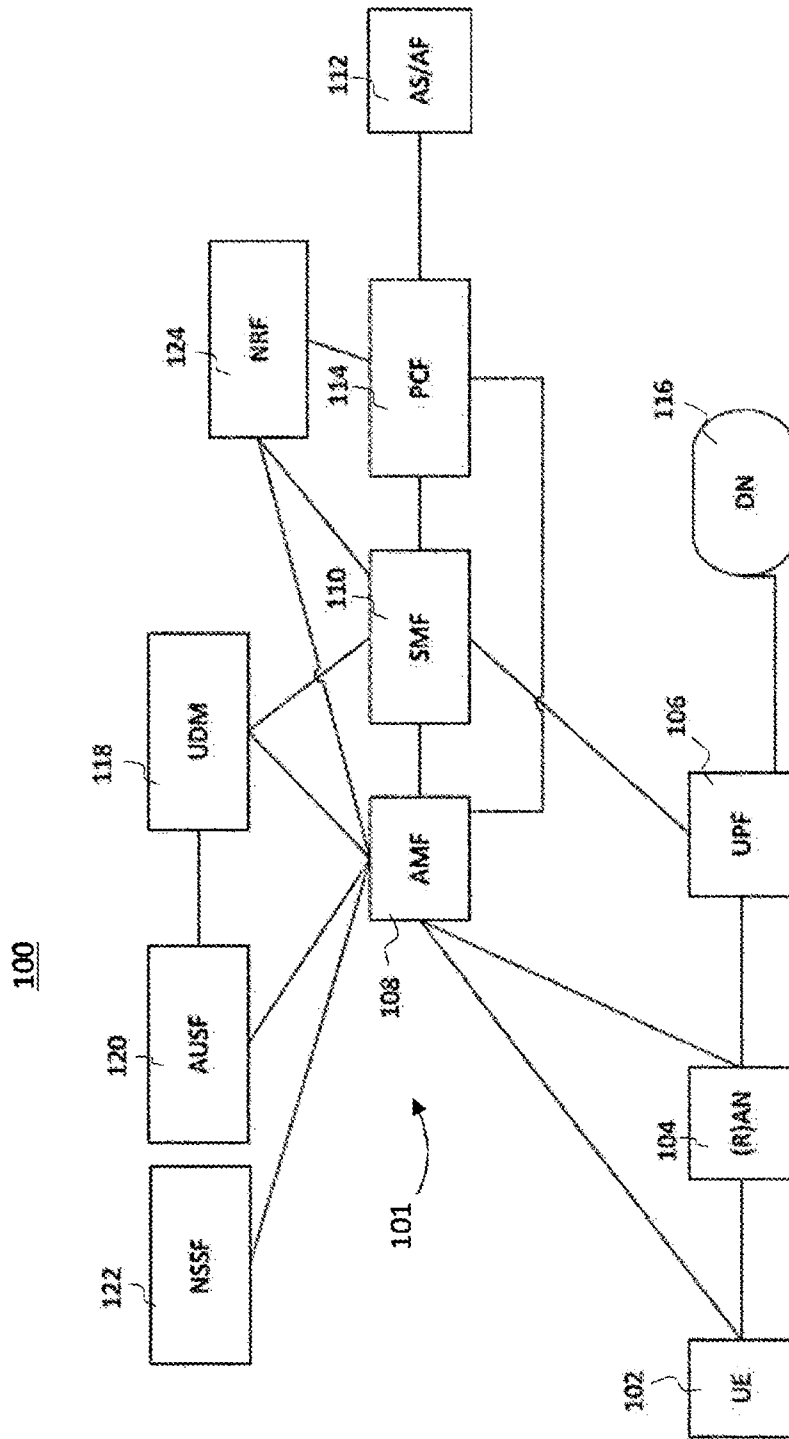


Figure 2

100

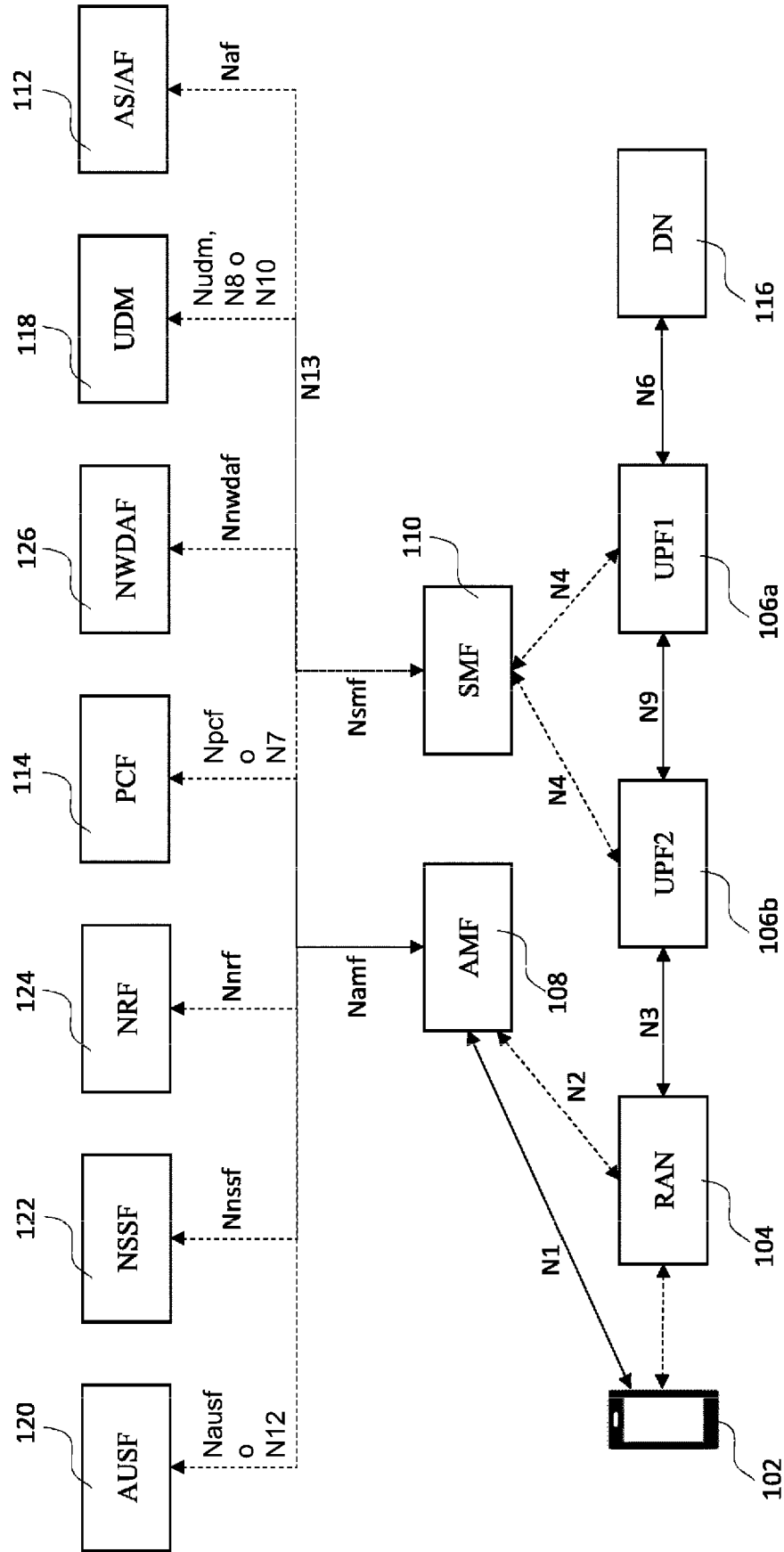


Figura 3

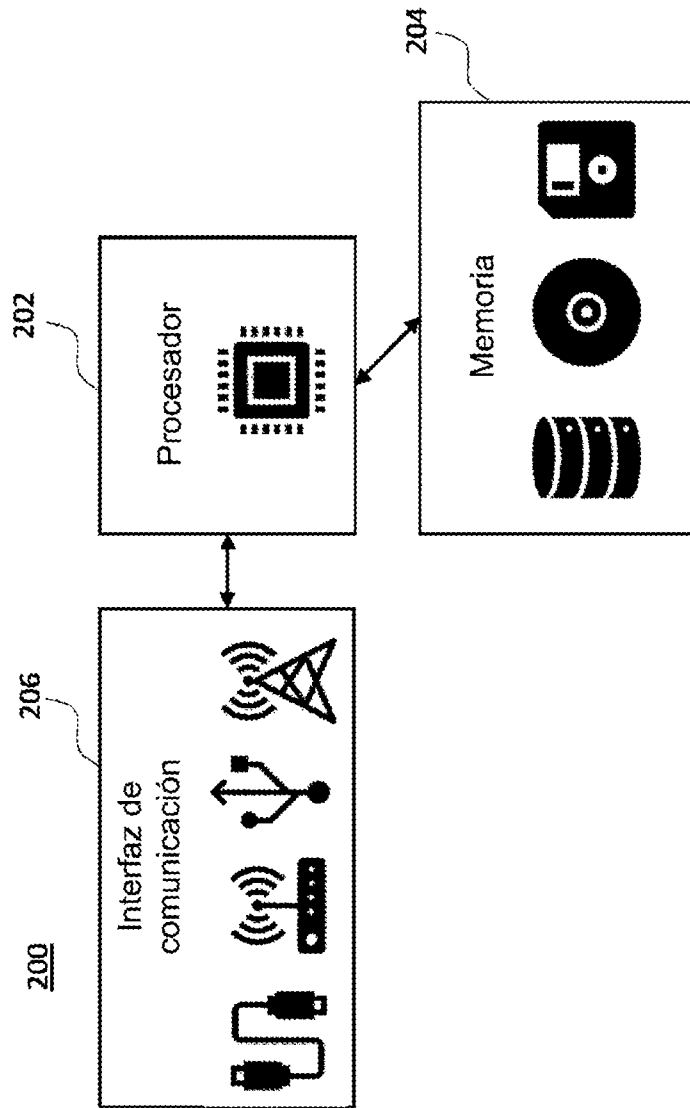


Figura 4

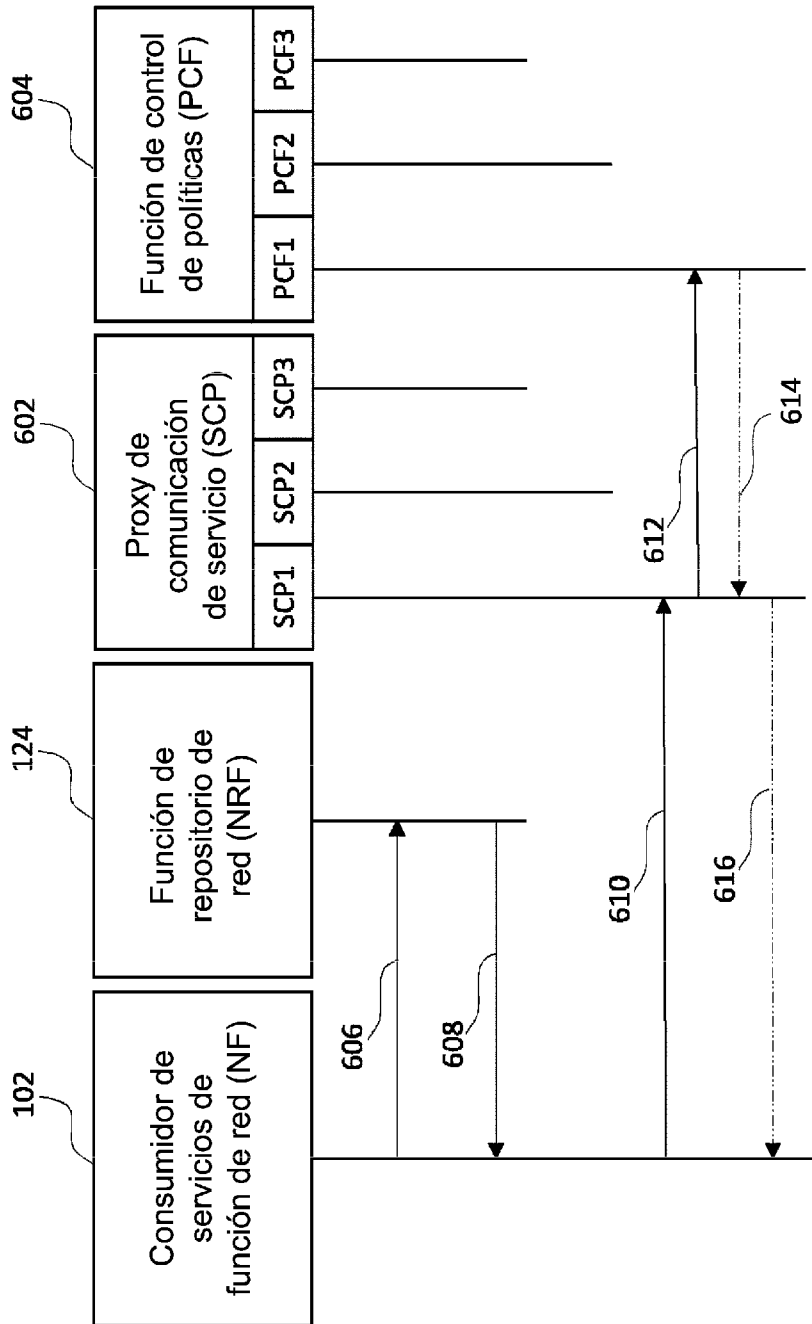


Figura 5

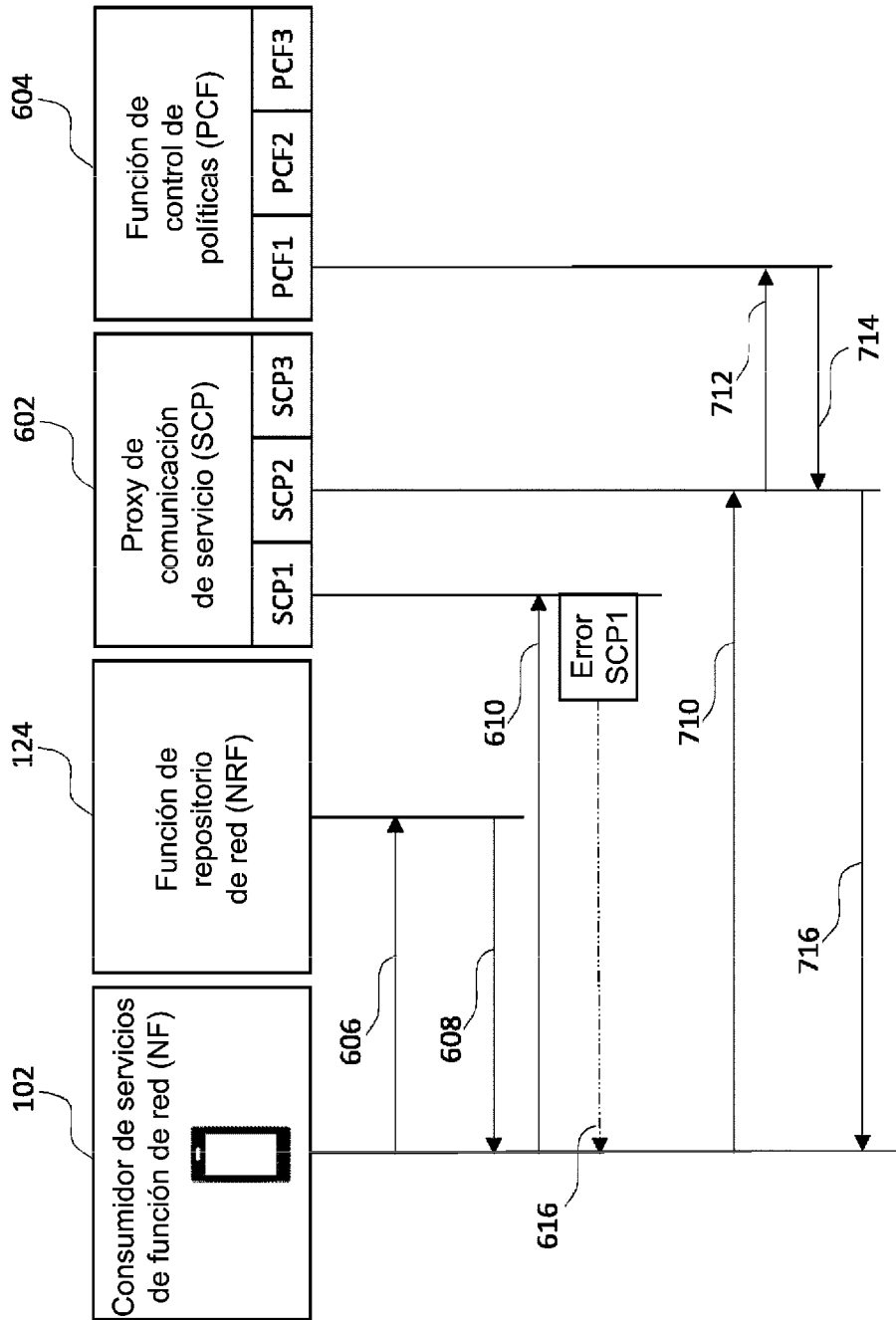


Figura 6

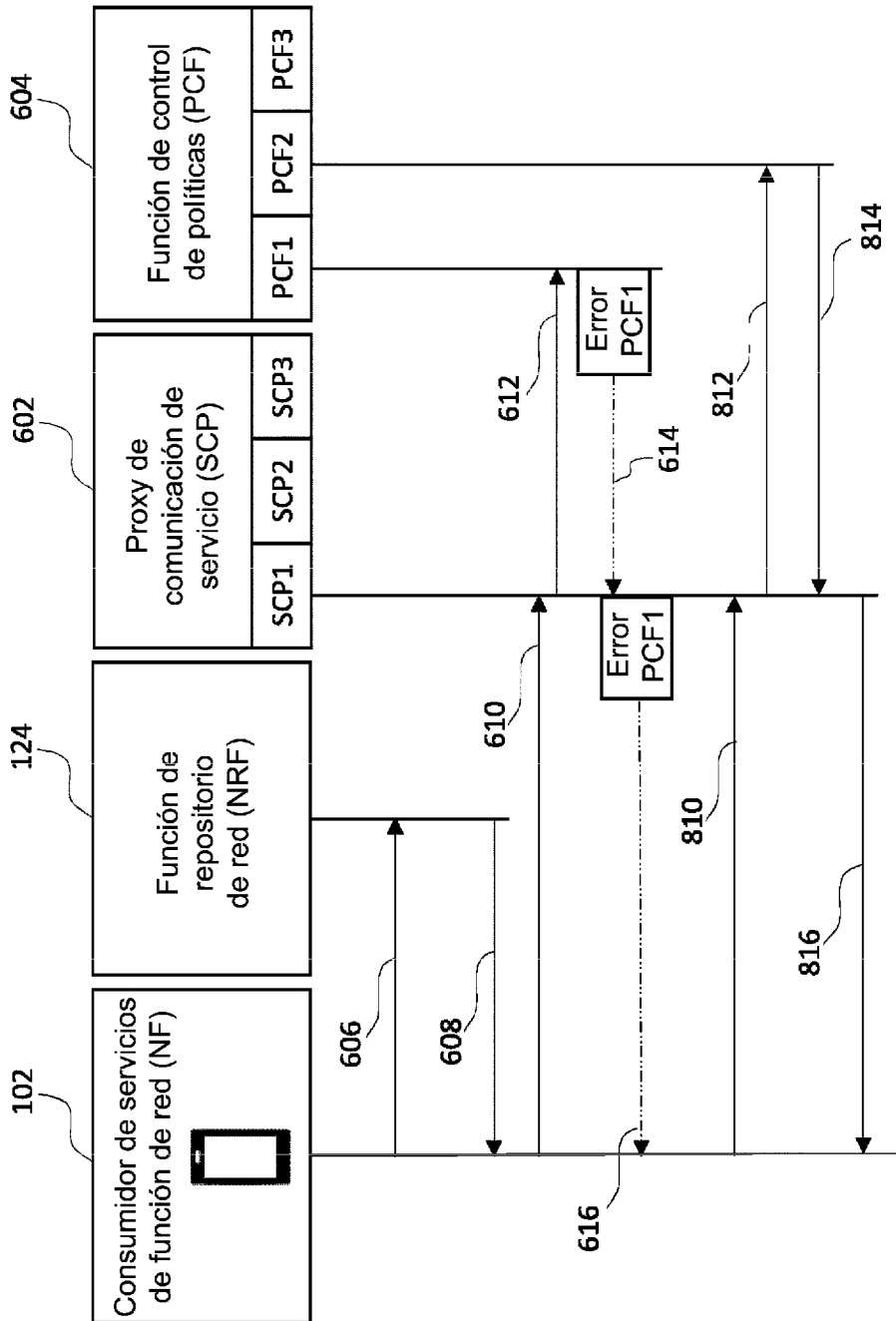


Figura 7

910

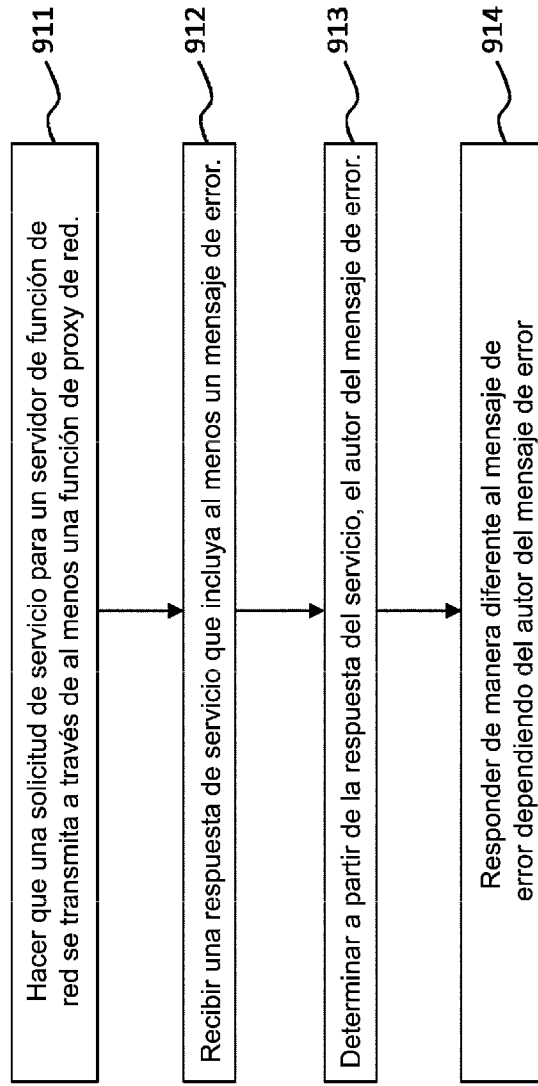


Figura 8

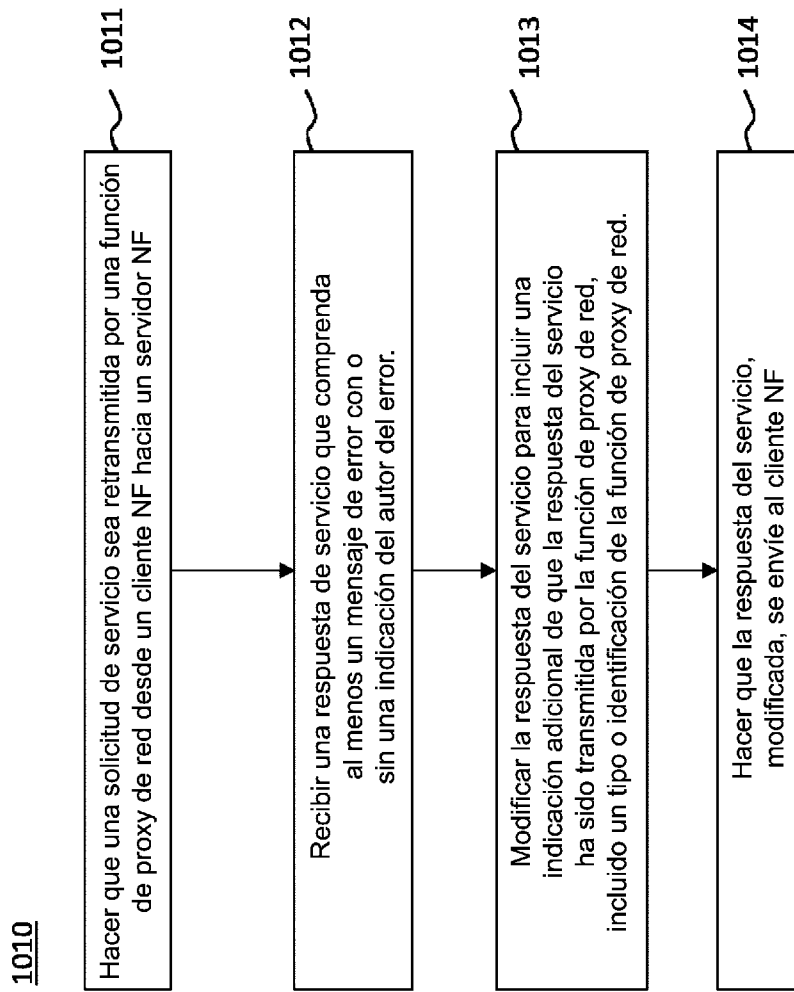


Figura 9

1210

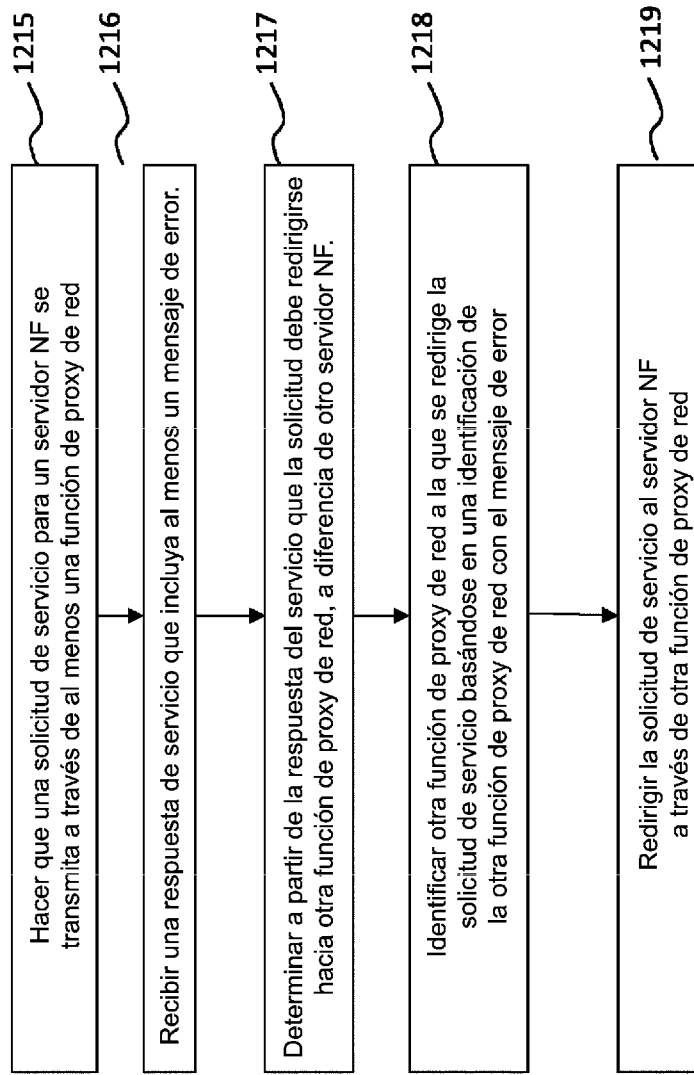


Figura 10

1310

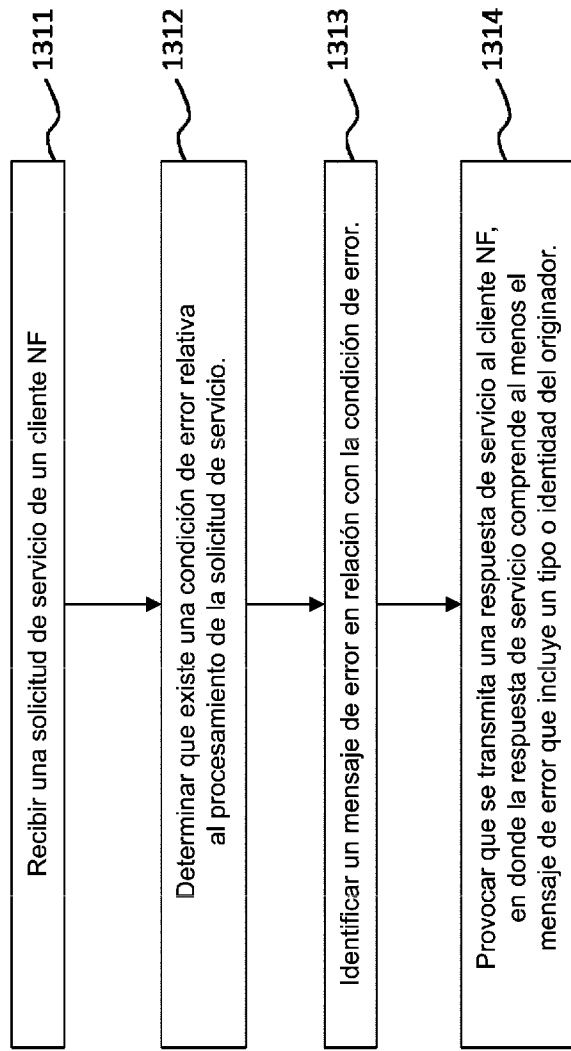


Figura 11