(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 876 311**

(51) Int. CI.:

H04L 12/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.09.2015 PCT/EP2015/072201**

(87) Fecha y número de publicación internacional: **07.04.2016 WO16050663**

(96) Fecha de presentación y número de la solicitud europea: **28.09.2015 E 15770527 (8)**

(97) Fecha y número de publicación de la concesión europea: **17.03.2021 EP 3202086**

(54) Título: **Replicación de estado de instancias de función de red virtual**

(30) Prioridad:

29.09.2014 EP 14186821

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.11.2021

(73) Titular/es:

KONINKLIJKE KPN N.V. (33.3%)
Wilhelminakade 123
3072 AP Rotterdam, NL;
IMEC VZW (33.3%) y
UNIVERSITEIT GENT (33.3%)

(72) Inventor/es:

COLLE, DIDIER y
TAVENIER, WOUTER

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Replicación de estado de instancias de función de red virtual

CAMPO DE LA INVENCIÓN

La divulgación se refiere, en general, al campo de funciones de red virtual (VNF). En particular, aunque no necesariamente, la divulgación se refiere a métodos, sistemas y productos de programa informático para replicar un estado de una instancia de VNF de una agrupación de VNF en al menos otra instancia de VNF de la agrupación.

ANTECEDENTES

En las redes de telecomunicación convencionales, se despliegan funciones tales como, por ejemplo, cortafuegos, equilibradores de carga y optimizadores de red de acceso inalámbrico (WAN) en servidores de hardware especializados dedicados en las redes de los operadores de red y centros de datos. Estas funciones son importantes ya que sirven como los bloques de construcción de todos los servicios de red. Una tendencia reciente ha sido virtualizar estas funciones, es decir, desacoplar las funciones de su hardware dedicado implementándolas como instancias de función de red virtual (instancias de VNF), por ejemplo, ejecutarlas como software en servidores de propósito general.

Un desafío con el despliegue de funciones de red como instancias de VNF es la fiabilidad puesto que los mecanismos de fiabilidad de las instancias de software de tales funciones actualmente no se encuentran en el mismo nivel en comparación con las implementaciones de hardware más convencionales diseñadas para disponibilidad de X nueves. Xia et al. proporcionan un análisis de los requisitos de fiabilidad claves para aplicaciones y funciones que pueden alojarse en un entorno virtualizado en un borrador de Internet del IETF llamado "Requirements and Use Cases for Virtual Network Functions". Estos requisitos de ingeniería de NFV están basados en una diversidad de casos de uso y objetivos, que incluyen fiabilidad, escalabilidad, rendimiento, operación y automatización.

Un enfoque actual que intenta garantizar la fiabilidad de las implementaciones de VNF sigue la arquitectura de agrupación de servidores fiable (RSerPool) que emplea una agrupación de VNF de múltiples instancias de VNF que proporcionan la misma función. Este enfoque ha sido descrito por Dreibholz et al. en un borrador de Internet del IETF llamado "The Applicability of Reliable Server Pooling (RSerPool) for Virtual Network Function Resource Pooling (VNFPOOL)". La Figura 1 proporciona una ilustración esquemática de una arquitectura RSerPool 100 mientras que la Figura 2 proporciona una ilustración esquemática de una arquitectura de agrupación de VNF 200 que sigue la arquitectura RSerPool mostrada en la Figura 1.

Como se muestra en la Figura 1, la arquitectura RSerPool 100 utiliza tres tipos de componentes: un elemento de agrupación (PE) 102, un registrador de agrupación 104 y un usuario de agrupación 106. El PE 102 indica un servidor en una agrupación 108, comprendiendo la agrupación 108 mostrada en el ejemplo de la Figura 1 tres instancias del PE 102, estando todas las instancias del PE 102 en la agrupación 108 configuradas para proporcionar el mismo servicio de red mediante la implementación de una cierta función de red. El PU 106 indica un cliente que usa el servicio de la agrupación 108. El PR 104 indica el componente de gestión, que gestiona la agrupación 108, y posiblemente otras agrupaciones no mostradas en la Figura 1. La funcionalidad del PR 104 y el PU 106 se describe con mayor detalle a continuación. La agrupación 108, el PR 104, y el PU 106 se comunican usando el protocolo de acceso de servidor agregado (ASAP), como se muestra con las flechas dobles entre estos elementos.

La arquitectura de agrupación de VNF 200 de la Figura 2 sigue la arquitectura de la Figura 1 que emplea una agrupación de VNF 208 que comprende diferentes instancias de VNF como los elementos de agrupación 202 (mostrados en el ejemplo de la Figura 2 como los elementos VNF i1, i2, e i3), gestionados mediante un registrador de VNF 204, y configurados para dar servicio a un usuario 206 de la agrupación de VNF 208. Un ejemplo del usuario 206 sería un sistema de control de cadena de función de servicio (SFC), que es una entidad de control a cargo de la organización de la SFC como se define en la estructura de control de SFC que se define mediante el grupo de trabajo de la SFC del IETF. Las instancias de VNF 202 son análogas al PE 102, el registrador de VNF 204 es análogo al PR 104, el sistema de control de SFC 206 es análogo al PU 106, y la agrupación de VNF 208 es análoga a la agrupación 108, anteriormente descritos. De manera similar a los elementos de la arquitectura RSerPool 100, las instancias de VNF 202, el registrador de VNF 204 y el usuario 206 pueden comunicarse usando ASAP.

El proceso de arranque de una agrupación de VNF también se hereda de la arquitectura RSerPool y se representa en la Figura 3. En primer lugar, el PR 104, que en el contexto de las VNF sería el registrador de VNF 204, se anuncia a sí mismo a diversos elementos de agrupación usando un mensaje ASAP 302. Un PE de elemento de agrupación particular 102, que en el contexto de las VNF sería la VNF i 202, por ejemplo, la VNF i1, puede a continuación elegir el PR 104 para registrar en la agrupación 108, que en el contexto de las VNF sería la agrupación de VNF 208, usando un mensaje ASAP 304. Una vez que se confirma el registro, el PR 204 se denomina como el PR-H (registrador de agrupación doméstico), mostrado en la Figura 3 como PR-H 306. A partir de este momento, el estado del PE 102 registrado con el PR 104 se monitoriza de manera activa mediante el PR 104 mediante mensajes de confirmación 308 y 310, con una tasa de intercambio normalmente del orden de segundos. El PU 106, que en el contexto de las VNF

podría ser, por ejemplo, el sistema de control de SFC 206, puede a continuación solicitar un servicio de una instancia de PE (es decir, una instancia de VNF) desde el PR 104 usando, por ejemplo, un mensaje 312, denominándose el proceso "resolución de manejador". En respuesta a la solicitud 312, el PR 104 puede a continuación seleccionar un manejador 312 que corresponde a un PE particular 102 para volver al PU 106, por ejemplo, basándose en una política estática o una adaptativa.

Si el PR 104 detecta que el PE activo está inactivo, por ejemplo, detectando un tiempo de espera en el procedimiento de confirmación, puede actualizar el manejador hacia el PU 106. Por otra parte, si el PU 106 es el primero en detectar un fallo del PE activo, puede informar al PR 104 y solicitar un manejador alternativo.

RSerPool se diseñó para ser independiente de la aplicación. Por lo tanto, la replicación de estado entre los PE en la misma agrupación se considera que es una tarea de los usuarios de agrupación. Sin embargo, RSerPool proporciona algunos mecanismos de soporte soportados mediante su protocolo de mensajería ASAP. Un mecanismo de este tipo implica cookies, que son mensajes de estado particulares ("volcados") que pueden enviarse desde el PE activo al PU usando el servicio del PE activo para proporcionar al PU el último estado del PE activo. Después del fallo del PE activo, esta información puede enviarse mediante el PU al PE recién elegido. Como se usa en el presente documento, la expresión "PE activo" o "PE primario", y de manera similar las expresiones "instancia de VNF activa" e "instancia de VNF primaria", hacen referencia al PE o a la instancia de VNF para la que el manejador ha sido usado por última vez, o está siendo usado actualmente, por el PU o por el usuario de la agrupación de VNF.

La Figura 4A proporciona una ilustración esquemática de un proceso de migración tras error por defecto con replicación de estado entre diferentes instancias de VNF de la misma agrupación que se basa en un intercambio regular de los mensajes de cookie 402 entre la instancia de VNF activa, mostrada en la Figura 4A como "PE1", y el PU 106. En un caso de este tipo, el PU 106 es responsable por sí mismo de restaurar el estado en el PE recién seleccionado, mostrado en la Figura 4A como "PE2". El proceso de la Figura 4A ilustra que el estado de los PE 102 de la agrupación 108 que se registran con el PR 104 (en el ejemplo de la Figura 4A-PE1 y PE2) se monitoriza de manera activa mediante el PR-H 104 mediante mensajes de confirmación 404 y 408 para el PE2 y PE1, respectivamente, siendo los mensajes 404 y 408 análogos al mensaje 308 mostrado en la Figura 3. Un mensaje 406, análogo al mensaje 310 mostrado en la Figura 3, ilustra que el PE2 realiza acuse de recibo del mensaje KEEP_ALIVE 404 del PR-H, mientras que el evento de tiempo de espera 410 ilustra que el PE primario, PE1, no realiza acuse de recibo del mensaje KEEP_ALIVE 408. Cuando eso ocurre, el PR 104 notifica al PU 106 acerca del PE alternativo, PE2, como se muestra con un mensaje 414, es decir, el PR 104 proporciona al PU 106 un manejador 412 para el PE2, haciendo de esta manera al PE2 el PE activo o el primario. Después de la recepción de esta notificación, el PU 106 puede transferir toda la información de estado para el PE1 recibida mediante un mensaje de cookie 402, hacia el PE2 de respaldo alternativo, como se muestra en la Figura 4A, con un mensaje 414. El PE2 puede a continuación actualizar su estado al del PE1 en la etapa 416. En otras palabras, el estado de PE1 se replica a continuación en el PE2.

Una flecha doble etiquetada "TIEMPO DE MIGRACIÓN TRAS ERROR 418" en la Figura 4A ilustra un denominado tiempo de migración tras error, que hace referencia al periodo de tiempo desde la detección de un fallo del PE activo, PE1, a la restauración del estado de PE1 en el PE alternativo, PE2. Cuando se aprovisionan servicios de red usando VNF encadenadas en forma de una SFC, el manejo rápido de fallos de VNF en el plano de datos, es decir, tiempo de migración tras error corto, es de importancia crucial. En particular, los servicios de red de telecomunicaciones a menudo demandan fiabilidad de 5 nueves y tiempos de migración tras error del orden de 50 milisegundos (ms). La conmutación de plano de datos sin impacto es, por lo tanto, una característica altamente necesaria, por ejemplo, para funciones de red de cortafuegos o funcionalidad de conmutación.

Existen varios problemas al intentar implementar mecanismos de migración tras error para instancias de VNF en una agrupación de VNF basándose en el intercambio activo de mensajes de volcado de cookie/estado como se describe en la Figura 4A. Un problema es que el usuario de la agrupación de VNF, que podría ser la misma entidad que el PU, tiene que ser responsable de la replicación de estado desde el PE primario al alternativo, lo que no siempre es deseable. Otro problema es que muchas funciones de red mantienen un estado que puede requerir fácilmente más de cientos de MB de memoria, lo que da como resultado retardos del orden de segundos a minutos para copiar el estado implicado usando el mensaje de cookie 414 tras la conmutación a un PE alternativo. Otro problema más es que proporcionar los mensajes de cookie 402 desde el PE primario al PU en el primer lugar requiere un ancho de banda significativo entre el PE primario y el PU.

Por ejemplo, una gran clase de instancias de VNF se controla mediante una entidad de control/gestión que a su vez podría ser una VNF. Una entidad de este tipo se denomina en el presente documento como una "entidad de control" o "VNF de control". Los ejemplos de tales instancias de VNF y entidades de control correspondientes incluyen conmutadores OpenFlow y su interacción con controladores OpenFlow que usan el protocolo OpenFlow entre la entidad de control y la instancia de VNF para comunicar las reglas que van a instalarse en la instancia de VNF, cortafuegos configurados mediante gestión o inspección de paquetes profunda (DPI) automática o módulos de detección de intrusión, o una clase más general de funciones de red configuradas mediante el protocolo de configuración de red (NETCONF) o el protocolo sencillo de gestión de red (SNMP). En el contexto de OpenFlow, el estado de tales instancias de VNF se determina a continuación mediante una tabla de reglas comunicadas desde la entidad de control a la instancia de VNF, denominándose la tabla una "tabla de flujo". El proceso de migración tras

error por defecto en este contexto se ilustra en la Figura 4B. La Figura 4B es similar a la Figura 4A en que ilustra todos los elementos 402-418 descritos para la Figura 4A (por lo tanto, su descripción no se repite para la Figura 4B) pero también ilustra un intercambio de mensajes de control 422 y sus acuses de recibo 424 entre una VNF de control 420 y el PE primario, PE1. Como se muestra en la Figura 4B, los mensajes de control 422 incluyen reglas, mostradas como REGLA 1 a REGLA n, que se proporcionan periódicamente desde el PE primario, PE1, al PU 106 en el mensaje de cookie 402 anteriormente descrito. El mensaje de cookie 402 en un caso de este tipo incluye una tabla de flujo 426 que comprende una estructura de datos que almacena las reglas de OpenFlow o las entradas de flujo. El número, n, de reglas en un conmutador de OpenFlow puede ser fácilmente del orden de 10 000 entradas de flujo, que representan un estado de más de cientos de MB de memoria, lo que da como resultado un tiempo de migración tras error significativo.

Aunque el análisis anterior se concentró principalmente en el proceso de migración tras error, surgen problemas similares en situaciones que requieren la replicación de estado de una instancia de VNF de una agrupación de VNF en al menos otra instancia de VNF de la agrupación en ausencia de un fallo de la VNF primaria. Tales situaciones incluyen, por ejemplo, conmutar un servicio proporcionado por una instancia de VNF a otra instancia de VNF de la agrupación de VNF, por ejemplo, cuando la última instancia de VNF tiene más capacidad en caso de una situación cerca de sobrecarga, o compartición de carga de un servicio entre dos instancias de VNF. El tiempo de migración tras error 418 también es de preocupación en tales situaciones, donde la expresión "tiempo de migración tras error" en ese contexto es mejor renombrarla como un "tiempo de conmutación" ya que representa el tiempo que toma conmutar entre dos instancias de VNF diferentes de una agrupación de VNF, aunque no ocurriera fallo real.

Lo que es necesario en la técnica es una técnica para replicar un estado de una instancia de VNF de una agrupación de VNF en al menos otra instancia de VNF de la agrupación de VNF que pueda mejorar o eliminar al menos algunas de las desventajas anteriormente analizadas.

SUMARIO

El alcance de la invención se define mediante las reivindicaciones adjuntas. Por consiguiente, los aspectos de la presente invención pueden tomar la forma de una realización completamente de hardware, una realización completamente de software (que incluye firmware, software residente, microcódigo, etc.) o una realización que combina aspectos de software y hardware a los que se puede hacer referencia en general en el presente documento como un "circuito", "módulo" o "sistema". Las funciones descritas en esta divulgación pueden implementarse como un algoritmo ejecutado mediante un microprocesador de un ordenador. Adicionalmente, los aspectos de la presente invención pueden tomar la forma de un producto de programa informático incorporado en uno o más medios legibles por ordenador que tiene código de programa legible por ordenador incorporado, por ejemplo, almacenado, en el mismo.

Puede utilizarse cualquier combinación de uno o más medios legibles por ordenador. El medio legible por ordenador puede ser un medio de señal legible por ordenador o un medio de almacenamiento legible por ordenador. Un medio de almacenamiento legible por ordenador puede ser, por ejemplo, pero sin limitación, un sistema, aparato o dispositivo electrónico, magnético, óptico, electromagnético, de infrarrojos o de semiconductores o cualquier combinación adecuada de los anteriores. Ejemplos más específicos (una lista no exhaustiva) del medio de almacenamiento legible por ordenador incluirían los siguientes: una conexión eléctrica que tiene uno o más cables, un disquete de ordenador portátil, un disco duro, una memoria de acceso aleatorio (RAM), una memoria de sólo lectura (ROM), una memoria de sólo lectura borrable programable (EPROM o memoria flash), una fibra óptica, una memoria de sólo lectura de disco compacto portátil (CD-ROM), un dispositivo de almacenamiento óptico, un dispositivo de almacenamiento magnético, o cualquier combinación adecuada de los anteriores. En el contexto de este documento, un medio de almacenamiento legible por ordenador puede ser cualquier medio tangible que pueda contener, o almacenar un programa para su uso mediante o en conexión con un sistema, aparato o dispositivo de ejecución de instrucciones.

Un medio de señal legible por ordenador puede incluir una señal de datos propagada con código de programa legible por ordenador incorporado en el mismo, por ejemplo, en banda base o como parte de una onda portadora. Una señal propagada de este tipo puede tomar cualquiera de una diversidad de formas, que incluyen, pero sin limitación, electromagnética, óptica o cualquier combinación adecuada de las mismas. Un medio de señal legible por ordenador puede ser cualquier medio legible por ordenador que no sea un medio de almacenamiento legible por ordenador y que pueda comunicar, propagar o transportar un programa para su uso mediante o en conexión con un sistema, aparato o dispositivo de ejecución de instrucciones.

El código de programa incorporado en un medio legible por ordenador puede transmitirse usando cualquier medio apropiado, incluyendo, pero sin limitación, inalámbrico, alámbrico, fibra óptica, cable, RF, etc., o cualquier combinación adecuada de los anteriores. El código de programa informático para llevar a cabo las operaciones para aspectos de la presente invención puede escribirse en cualquier combinación de uno o más lenguajes de programación, incluyendo un lenguaje de programación orientado a objetos tal como Java(TM), Smalltalk, C++ o similares y lenguajes de programación procedurales convencionales, tales como el lenguaje de programación "C" o lenguajes de programación similares. El código de programa puede ejecutarse en su totalidad en el ordenador del usuario, parcialmente en el ordenador del usuario, como un paquete de software independiente, parcialmente en el ordenador del usuario y

parcialmente en un ordenador remoto, o en su totalidad en el ordenador o servidor remoto. En el último escenario, el ordenador remoto puede conectarse al ordenador del usuario a través de cualquier tipo de red, incluyendo una red de área local (LAN) o una red de área extensa (WAN), o la conexión puede realizarse a un ordenador externo (por ejemplo, a través de Internet usando un proveedor de servicio de Internet).

Se describen a continuación aspectos de la presente invención con referencia a ilustraciones de diagrama de flujo y/o diagramas de bloques de los métodos, aparato (sistemas), y productos de programa informático de acuerdo con las realizaciones de la invención. Se entenderá que cada bloque de las ilustraciones de diagrama de flujo y/o diagramas de bloques, y combinaciones de bloques en las ilustraciones de diagrama de flujo y/o diagramas de bloques, puede implementarse mediante instrucciones de programa informático. Estas instrucciones de programa informático pueden proporcionarse a un procesador, en particular, un microprocesador o unidad de procesamiento central (CPU), de un ordenador de propósito general, ordenador de propósito especial, u otro aparato de procesamiento de datos programable para producir una máquina, de manera que las instrucciones, que se ejecutan mediante el procesador del ordenador, otro aparato de procesamiento de datos programable, u otros dispositivos, crean medios para implementar las funciones/actos especificados en el bloque o bloques del diagrama de flujo y/o diagrama de bloques.

Estas instrucciones de programa informático pueden almacenarse también en un medio legible por ordenador que puede dirigir un ordenador, otro aparato de procesamiento de datos programable, u otros dispositivos para funcionar de una manera particular, de manera que las instrucciones almacenadas en el medio legible por ordenador producen un artículo de fabricación que incluye instrucciones que implementan la función/acto especificado en el bloque o bloques del diagrama de flujo y/o diagrama de bloques.

Las instrucciones de programa informático pueden cargarse también en un ordenador, otro aparato de procesamiento de datos programable, u otros dispositivos para hacer que se realice una serie de etapas operacionales en el ordenador, otro aparato programable u otros dispositivos para producir un proceso implementado por ordenador de manera que las instrucciones que se ejecutan en el ordenador u otro aparato programable proporcionen procesos para implementar las funciones/actos especificados en el bloque o bloques del diagrama de flujo y/o diagrama de bloques.

El diagrama de flujo y diagramas de bloques en las figuras ilustran la arquitectura, funcionalidad y operación de posibles implementaciones de sistemas, métodos y productos de programa informático de acuerdo con diversas realizaciones de la presente invención. En este sentido, cada bloque en el diagrama de flujo o diagramas de bloques puede representar un módulo, segmento, o porción de código, que comprende una o más instrucciones ejecutables para implementar la función o funciones lógicas especificadas. Debería observarse también que, en algunas implementaciones alternativas, las funciones observadas en los bloques pueden tener lugar fuera del orden indicado en las figuras. Por ejemplo, dos bloques mostrados en sucesión, de hecho, pueden ejecutarse sustancialmente de manera concurrente, o los bloques pueden ejecutarse, en ocasiones, en el orden inverso, dependiendo de la funcionalidad implicada. También ha de observarse que cada bloque de las ilustraciones de diagramas de bloques y/o de diagrama de flujo, y combinaciones de bloques en las ilustraciones de diagramas de bloques y/o de diagrama de flujo, pueden implementarse mediante sistemas basados en hardware de propósito especial que realizan las funciones o actos especificados, o combinaciones de hardware de propósito especial e instrucciones informáticas.

Para reducir o eliminar al menos algunos de los problemas anteriormente analizados, de acuerdo con un aspecto de una realización de la presente invención, se desvela un método implementado por ordenador para llevarse a cabo mediante un elemento de interfaz entre una agrupación de VNF y una entidad de control. La agrupación de VNF comprende una pluralidad de instancias de VNF que incluyen al menos una primera instancia de VNF (VNF i1) y una segunda instancia de VNF (VNF i2). La entidad de control está configurada para controlar las instancias de VNF de la agrupación de VNF. El método posibilita que el elemento de interfaz ayude en la replicación de un estado de la primera instancia de VNF al menos en la segunda instancia de VNF. El método incluye las etapas de obtener, de alguna manera, es decir, recibir, interceptar, determinar, etc., un mensaje de control proporcionado desde la entidad de control a la primera instancia de VNF, proporcionar el mensaje de control obtenido al menos a la primera instancia de VNF y a la segunda instancia de VNF, y proporcionar un acuse de recibo del mensaje de control a la entidad de control cuando el elemento de interfaz tiene un acuse de recibo, explícito o implícito, tanto del mensaje de control proporcionado a la primera instancia de VNF como del mensaje de control proporcionado a la segunda instancia de VNF.

Como se usa en el presente documento, la expresión "instancia de VNF" hace referencia a software que se ejecuta en un servidor informático, por ejemplo, un servidor de propósito general, proporcionando de esta manera la virtualización de la aplicación, el servidor informático, sistema, componente de hardware o funciones de red, a un segmento de una función de red física que puede compartir su funcionalidad entre múltiples usuarios, o una combinación tanto del software como del segmento de una función de red física.

Como se usa en el presente documento, la expresión "mensaje de control" hace referencia a cualquier mensaje de control o de gestión enviado mediante la entidad de control y destinado a alcanzar una instancia de VNF.

Las realizaciones de la presente invención están basadas en el reconocimiento de que proporcionar un elemento de

interfaz entre instancias de VNF de una agrupación de VNF y una entidad de control que controla las instancias de VNF permite duplicar mensajes de control enviados mediante la entidad de control a una de las instancias de VNF a otras instancias de VNF. Puesto que los mensajes de control recibidos mediante las instancias de VNF definen su estado, tal duplicación permite la replicación de un estado de una instancia de VNF en una o más instancias diferentes de VNF en la agrupación. Por lo tanto, como se usa en el presente documento, la expresión "replicar un estado de una instancia de VNF en otra instancia de VNF" y expresiones similares hacen referencia a un elemento de interfaz que ayuda a que el estado de la primera instancia de VNF se replique en la segunda instancia de VNF mediante el elemento de interfaz que proporciona mensajes de control destinados a la primera instancia de VNF para no únicamente la primera, sino también para la segunda instancia de VNF.

La replicación de estado, a su vez, proporciona diversas ventajas en diferentes escenarios que pueden requerir que se proporcione un manejador para una nueva instancia de VNF a un usuario de la agrupación de VNF, ya sea, en lugar de, o, además, del manejador para la instancia de VNF primaria proporcionado al usuario de la agrupación, donde, como se usa en el presente documento, el término "manejador" hace referencia a un identificador direccionable, tal como, por ejemplo, una dirección de IP o MAC, de un componente de red, en este contexto una instancia de VNF.

Un escenario de este tipo está relacionado con una migración tras error, donde, como se usa en el presente documento, la expresión "migración tras error" hace referencia a la conmutación a una aplicación, servidor informático, sistema, componente de hardware, máquina virtual o red redundante o en reposo (es decir, auxiliar) después del fallo o terminación anómala de la aplicación, servidor informático, sistema, componente de hardware, máquina virtual o red previamente activa (es decir, primaria). La replicación de estado entre diferentes instancias de VNF de una agrupación de VNF asistida mediante el elemento de interfaz, como se describe en el presente documento, permite la recuperación rápida en caso de que la instancia de VNF primaria falle puesto que el usuario de la agrupación únicamente necesita recibir un manejador para una de las otras instancias de VNF en la agrupación de VNF. Ya no es necesario que el usuario de la agrupación restaure el estado en la instancia de VNF recién seleccionada puesto que el estado de la instancia de VNF fallida, que era la instancia de VNF primaria antes del fallo, ya se ha replicado en la instancia de VNF recién seleccionada.

Aunque las realizaciones de la presente invención se han descrito principalmente en el presente documento con referencia a una migración tras error, un experto en la materia reconocerá que replicar un estado de una instancia de VNF en al menos otra instancia de VNF de la agrupación de VNF proporciona ventajas también en ausencia de fallo alguno en las instancias de VNF. Por ejemplo, tener un estado de una instancia de VNF replicado al menos a otra instancia de VNF permite la conmutación rápida de un servicio proporcionado por la primera instancia de VNF a la última instancia de VNF, por ejemplo, cuando la última instancia de VNF tiene más capacidad en caso de una situación cerca de sobrecarga, o cuando se comparte un servicio entre dos instancias de VNF.

La implementación del elemento de interfaz, como se describe en el presente documento, proporciona un mecanismo más rápido, más transparente y eficaz en recursos para replicar un estado de una instancia de VNF de una agrupación de VNF a una o más instancias diferentes de VNF de la agrupación de VNF en todos los escenarios donde tal estado de replicación pueda desearse, especialmente, para las instancias de VNF de configuración intensiva.

En una realización, las instancias de VNF pueden incluir dos o más instancias de VNF, preferentemente tres o más instancias de VNF. La etapa de que el elemento de interfaz proporcione el mensaje de control al menos a la primera instancia de VNF y a la segunda instancia de VNF puede comprender entonces proporcionar el mensaje de control al menos a dos de, pero preferentemente a todas, las instancias de VNF de la agrupación de VNF. En una realización de este tipo, el método puede incluir adicionalmente las etapas de que el elemento de interfaz identifique instancias de VNF de las dos o más instancias de VNF de la agrupación de VNF desde las que el elemento de interfaz no recibió un acuse de recibo del mensaje de control, y que proporcione una indicación de las instancias de VNF identificadas a un registrador de agrupación de VNF (PR-H) con el que están registradas las instancias de VNF de la agrupación de VNF. Proporcionar la agrupación de VNF que tiene tres o más instancias de VNF permite la posibilidad de replicar el estado de la primera instancia de VNF en números mayores de diferentes instancias de VNF, aumentando por lo tanto la fiabilidad en caso de conmutación desde la primera instancia de VNF a alguna otra instancia de VNF si fuera necesario. El elemento de interfaz que no recibe un acuse de recibo del mensaje de control proporcionado a una de las instancias de VNF indica que el estado de la primera instancia de VNF puede no haberse replicado en tales instancias de VNF. Identificar tales instancias de VNF y compartir esta información con el registrador de agrupación de VNF permite que el elemento de interfaz actualice la agrupación de VNF considerada mediante el registrador de la agrupación de VNF (es decir, actualizar qué instancias de VNF ha de considerarse que están "en la agrupación") de modo que, en caso de una conmutación, el registrador de la agrupación de VNF no proporcionaría un manejador a una de las instancias de VNF en las que puede no haberse replicado el estado de la primera instancia de VNF.

En una realización, el método puede incluir adicionalmente una etapa de que el elemento de interfaz establezca un canal de comunicación base, preferentemente un canal TCP, entre el elemento de interfaz y cada una de la entidad de control, la primera instancia de VNF, y la segunda instancia de VNF. Como se usa en el presente documento, se usa la expresión "canal de comunicación base" para describir un medio físico bidireccional (por ejemplo, un cable) o un medio lógico bidireccional (que puede multiplexarse en un medio físico) entre dos puntos terminales a través de los cuales pueden intercambiarse mensajes en cualquier dirección, por ejemplo, usando datagramas binarios

codificados. La comunicación a través de un canal de comunicación base puede ser susceptible a la escucha clandestina (un denominado ataque de "hombre en el medio"), donde un atacante haría conexiones independientes con ambos puntos terminales y retransmitiría mensajes entre ellos sin informar a los puntos terminales.

El establecimiento de tales canales de comunicación base permite que el elemento de interfaz obtenga los mensajes de control enviados mediante la VNF de control a una de las instancias de VNF y proporcione los mensajes de control obtenidos a otras instancias de VNF.

En una realización, los canales de comunicación base pueden establecerse usando una toma de contacto de tres vías como es conocido en la técnica, por ejemplo, una toma de contacto de 3 vías similar a TCP. Una realización de este tipo proporciona la ventaja de proporcionar una entrega fiable, ordenada y con comprobación de errores de un flujo de octetos entre dos procesos interconectados mediante el medio de comunicación.

En una realización adicional a la que implica el establecimiento de un canal de base, las instancias de VNF de la agrupación de VNF pueden incluir dos o más instancias de VNF, preferentemente tres o más instancias de VNF, y la etapa de que el elemento de interfaz establezca el canal de comunicación base puede incluir el establecimiento del canal de comunicación base entre el elemento de interfaz y cada una de las al menos dos de, pero preferentemente todas, las instancias de VNF de la agrupación de VNF. En una realización de este tipo, el método puede comprender adicionalmente las etapas de que el elemento de interfaz identifique instancias de VNF de la agrupación de VNF con las que el canal de comunicación base no pudiera establecerse y/o estuviera roto, y que el elemento de interfaz proporcione una indicación de las instancias de VNF identificadas a un registrador de la agrupación de VNF (PR-H) con el que están registradas las instancias de VNF de la agrupación de VNF. Una realización de este tipo proporciona la ventaja de que cualquier fallo en el establecimiento y/u operación de un canal de comunicación base puede servir como una indicación para que el registrador de la agrupación de VNF excluya algunas instancias de VNF de la agrupación de VNF puesto que un estado de la primera instancia de VNF no puede replicarse satisfactoriamente en una instancia de VNF con la que un canal de comunicación base no se ha establecido y/o estaba roto. De esta manera, en el caso de que sea necesaria la conmutación desde una instancia de VNF a otra instancia de VNF o la compartición de carga entre dos instancias de VNF, el registrador de la agrupación de VNF no proporcionaría un manejador a una de las instancias de VNF en las que el estado de la primera instancia de VNF puede no haberse replicado debido a errores en el canal o canales de comunicación base.

En una realización, el método puede incluir adicionalmente una etapa de que el elemento de interfaz establezca un canal de comunicación seguro a través del canal de comunicación base establecido entre el elemento de interfaz y cada una de la entidad de control, la primera instancia de VNF y la segunda instancia de VNF (y preferentemente todas las instancias de VNF en la agrupación).

Como se usa en el presente documento, la expresión "canal de comunicación seguro" se usa para describir un canal de comunicación tal como el canal de comunicación base anteriormente descrito, que también es confidencial y auténtico. Un canal confidencial proporciona una manera de transferencia de datos que es resistente a la escucha clandestina (es decir, la lectura del contenido), pero no necesariamente resistente a la manipulación. Un canal auténtico proporciona una manera de transferencia de datos que es resistente a la manipulación, pero no necesariamente resistente a la escucha clandestina. Por lo tanto, un canal de comunicación seguro es resistente tanto a la escucha clandestina como a la manipulación.

Establecer un canal de comunicación seguro permite ventajosamente asegurar los datos intercambiados entre el elemento de interfaz y la VNF de control, así como los datos intercambiados entre el elemento de interfaz y las instancias de VNF. De esta manera, es posible conectividad de múltiples puntos entre la entidad de control y las instancias de VNF individuales resistentes a la escucha y la manipulación. El elemento de interfaz puede considerarse como tal como un hombre en el medio confiable para facilitar la conectividad segura entre las instancias de VNF y la entidad de control.

Como se usa en el presente documento, la expresión "elemento de interfaz que establece un canal de comunicación", aplicable tanto al canal base como al canal seguro hace referencia únicamente al hecho de que el elemento de interfaz participa en el establecimiento del canal y no indica qué entidad inicia un establecimiento de este tipo. En algunas realizaciones, podría ser que la entidad de interfaz inicie el establecimiento de un canal de comunicación particular, mientras que en otras alguna otra entidad podría hacer eso, por ejemplo, la entidad de control descrita en el presente documento.

En una realización adicional, el canal o canales de comunicación seguros podrían comprender un canal o canales basados en SSL/TLS. Esta realización permite ventajosamente usar un proceso de toma de contacto normalizado, tal como, por ejemplo, una toma de contacto de 4 fases basada en SSL, para establecer los canales seguros entre el elemento de interfaz y cada una de la VNF de control y las diferentes instancias de VNF.

En otra realización adicional, el canal de comunicación seguro entre el elemento de interfaz y cada una de la entidad de control, la primera instancia de VNF y la segunda instancia de VNF podría establecerse sustancialmente en paralelo. Esta realización proporciona la ventaja de acelerar el establecimiento de la conectividad de múltiples puntos

entre la entidad de control y las instancias de agrupación de VNF individuales resistentes a la escucha y manipulación. En una realización, las instancias de VNF podrían comprender dos o más instancias de VNF, preferentemente tres o más instancias de VNF, y la etapa de que el elemento de interfaz establezca el canal de comunicación seguro podría comprender establecer el canal de comunicación seguro entre el elemento de interfaz y cada una de al menos dos de, pero preferentemente todas, las instancias de VNF de la agrupación de VNF. En una realización de este tipo, el método puede incluir adicionalmente las etapas de que el elemento de interfaz identifique instancias de VNF de la agrupación de VNF con las que el canal de comunicación seguro no pudiera establecerse y/o estuviera roto, y que proporcione una indicación de las instancias de VNF identificadas al registrador de la agrupación de VNF con el que están registradas las instancias de VNF de la agrupación de VNF. Esta realización puede proporcionar la ventaja de que cualquier fallo en el establecimiento y/u operación de un canal de comunicación seguro puede servir como una indicación al registrador de la agrupación de VNF para excluir de la agrupación de VNF algunas instancias de VNF (en concreto, aquellas instancias de VNF con las que el canal de comunicación seguro no pudiera establecerse satisfactoriamente y/o estuviera roto). Proporcionar una indicación de este tipo permite que el elemento de interfaz actualice la agrupación de VNF considerada mediante el registrador de la agrupación de VNF de modo que, en caso de que sea necesaria la conmutación desde una instancia de VNF a otra instancia de VNF o la compartición de carga entre dos instancias de VNF, el registrador de la agrupación de VNF no proporcionaría un manejador a una de las instancias de VNF que pueden no haberse detectado debido a la ausencia del canal de comunicación seguro.

De acuerdo con otro aspecto de la presente invención, se proporciona un sistema de procesamiento de datos y un nodo (es decir, un dispositivo o una entidad de red tal como, por ejemplo, 3GPP P-GW, S-GW de la red de telecomunicaciones celular del proveedor de servicio) para llevar a cabo las etapas del método como se describen en el presente documento. Cada uno del sistema de procesamiento de datos y el nodo comprenden al menos un procesador configurado para llevar a cabo las etapas del método descritas en el presente documento. Un sistema de procesamiento de datos de este tipo podría estar incluido en el nodo.

De acuerdo con otro aspecto más de la presente invención, se desvela un sistema. El sistema puede incluir una agrupación de VNF que comprende una pluralidad de instancias de VNF que incluyen al menos una primera instancia de VNF (VNF i1) y una segunda instancia de VNF (VNF i2), una entidad de control configurada para controlar las instancias de VNF de la agrupación de VNF, y una entidad de interfaz conectada de manera comunicativa a las instancias de VNF y a la entidad de control, comprendiendo la entidad de interfaz al menos un procesador configurado para llevar a cabo las etapas del método descritas en el presente documento. En una realización, un sistema de este tipo podría incluir adicionalmente el registrador de la agrupación de VNF con el que están registradas las instancias de VNF de la agrupación de VNF, el registrador de la agrupación de VNF conectado de manera comunicativa al elemento de interfaz y configurado al menos para recibir desde el elemento de interfaz las instancias de VNF identificadas por el elemento de interfaz de acuerdo con las diferentes realizaciones anteriormente descritas. En una realización adicional, el registrador de la agrupación de VNF podría estar configurado adicionalmente para proporcionar a un usuario de la agrupación un manejador para la segunda instancia de VNF en caso de un fallo u operación inapropiada de la primera instancia de VNF y/o en caso de compartición de carga entre dos o más instancias de VNF que van a usarse en el plano de datos. El usuario de la agrupación podría reconfigurar posteriormente la red para usar la instancia de VNF alternativa.

La divulgación puede referirse también a un programa informático, implementado en medio de almacenamiento legible por ordenador, y a un medio de almacenamiento legible por ordenador, preferentemente no transitorio, que almacena un programa informático de este tipo. El programa informático puede comprender porciones de código de software configuradas para, cuando se ejecutan en un ordenador, ejecutar las etapas del método de acuerdo con cualquiera de los métodos descritos en la presente divulgación.

La divulgación se ilustrará adicionalmente con referencia a los dibujos adjuntos, que muestran esquemáticamente realizaciones de acuerdo con la divulgación. Se entenderá que la divulgación no está restringida de manera alguna a estas realizaciones específicas. Además, combinaciones de cualquiera de las realizaciones y limitaciones están contempladas por la divulgación.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Se explicarán aspectos de la invención con mayor detalle por referencia a realizaciones a modo de ejemplo mostradas en los dibujos, en los que:

La Figura 1 proporciona una ilustración esquemática de una arquitectura RSerPool, de acuerdo con el estado de la técnica;

La Figura 2 proporciona una ilustración esquemática de una arquitectura de agrupación de VNF que sigue la arquitectura RSerPool mostrada en la Figura 1;

La Figura 3 proporciona una ilustración esquemática de un proceso de arranque de una agrupación de VNF según se hereda desde la arquitectura RSerPool de la Figura 1 y aplicable a la arquitectura de agrupación de VNF de la Figura 2;

La Figura 4A proporciona una ilustración esquemática de un proceso de migración tras error por defecto con replicación de estado entre diferentes instancias de VNF de la misma agrupación que se basa en un intercambio regular de mensajes de cookie entre la instancia de VNF activa y el PU;

La Figura 4B proporciona una ilustración esquemática de un proceso de migración tras error por defecto de la Figura 4A cuando el estado de las diferentes instancias de VNF se define mediante mensajes de control proporcionados a las respectivas instancias de VNF mediante una entidad de control;

La Figura 5 proporciona una ilustración esquemática de una arquitectura de agrupación de VNF, de acuerdo con una realización de la presente invención;

La Figura 6 proporciona una ilustración esquemática de la replicación de un estado de una primera instancia de VNF en una segunda instancia de VNF, de acuerdo con una realización de la presente invención;

La Figura 7 proporciona una ilustración esquemática de un proceso de arranque para establecer canales de comunicación base individuales, de acuerdo con una realización de la presente invención;

La Figura 8 ilustra el proceso de toma de contacto de 4 fases basado en SSL normalizado existente entre un cliente y un proceso de servidor;

La Figura 9 proporciona una ilustración esquemática del establecimiento de canales de comunicación seguros individuales, de acuerdo con una realización de la presente invención;

La Figura 10 proporciona una ilustración esquemática de un proceso de migración tras error cuando se define el estado de diferentes instancias de VNF mediante mensajes de control proporcionados a las respectivas instancias de VNF mediante una entidad de control, de acuerdo con una realización de la presente invención;

La Figura 11 proporciona una ilustración esquemática de una arquitectura de plano de datos que podría usarse con la funcionalidad del elemento de interfaz como se describe en el presente documento, de acuerdo con una realización de la presente invención;

La Figura 12 proporciona un diagrama de bloques que ilustra un sistema de procesamiento de datos a modo de ejemplo que puede usarse para llevar a cabo etapas del método descritas en el presente documento, de acuerdo con una realización de la presente invención; y

La Figura 13 proporciona una ilustración esquemática de sistemas de telecomunicaciones que podrían usarse para implementar la funcionalidad del elemento de interfaz descrito en el presente documento.

DESCRIPCIÓN DETALLADA

La Figura 5 proporciona una ilustración esquemática de una arquitectura de agrupación de VNF 500, de acuerdo con una realización de la presente invención. De manera similar a la arquitectura 200 anteriormente descrita, la arquitectura de agrupación de VNF 500 utiliza tres tipos de componentes: 1) una pluralidad de elementos de agrupación 502, mostrados como tres instancias de VNF 502: VNF i1, VNF i2, y VNF i3, 2) un registrador de la agrupación, mostrado como el registrador de VNF 504, y 3) un usuario de la agrupación, mostrado como el PU 506. Cada una de las instancias de VNF 502 podría ser un servidor. Todas las instancias de VNF 502 realizan la misma función de red y juntas pueden formar una agrupación de VNF 508. Aunque se muestra que la agrupación 508 en el ejemplo de la Figura 5 comprende tres instancias de los elementos de la agrupación, las realizaciones de la presente invención son aplicables a cualquier número de elementos de la agrupación que sea igual o mayor que dos. El PU 506 es un cliente, tal como, por ejemplo, un sistema de control de SFC, que usa el servicio de la agrupación 508. El registrador de VNF 504 está configurado para realizar las funciones de registro y gestión de las instancias de VNF 502 de la agrupación 508 y proporciona manejadores a instancias de VNF individuales 502 para el PU 506 como se hace actualmente en la técnica y como se ha resumido anteriormente para el componente de PR en asociación con la Figura 1 y para el componente de registrador de VNF en asociación con la Figura 2. Las instancias de VNF 502 de la agrupación de VNF 508, el registrador de VNF 504 y el PU 506 pueden comunicarse entre sí usando ASAP, como se muestra con las flechas dobles entre estos elementos.

La arquitectura 500 también ilustra una entidad de control 520, que es una entidad de control/gestión que, por sí misma, podría ser, pero no tiene que ser, una VNF, encargada del control de las instancias de VNF 502. Como se ha descrito anteriormente, el estado de las instancias de VNF 502 se determina mediante los mensajes de control comunicados desde la entidad de control 520 a cada una de las instancias de VNF 502. Son aplicables en este punto ejemplos de las funciones de red implementadas como instancias de VNF controladas mediante una entidad de control proporcionada anteriormente y, por lo tanto, no se repiten.

La arquitectura 500 está caracterizada adicionalmente por comprender un elemento de interfaz 510. El elemento de

interfaz 510 proporciona una interfaz entre las instancias de VNF 502 de la agrupación de VNF 508 y la entidad de control 520 en el sentido de que puede obtener mensajes desde la entidad de control 520 destinados para una de las instancias de VNF 502 y a continuación proporcionar los mensajes de control obtenidos a la respectiva instancia de VNF así como a otras instancias de VNF en la agrupación de VNF 508. De esta manera, el elemento de interfaz 510 sirve como una interfaz de VNF lógica entre la entidad de control 520 y las instancias de VNF individuales 502. Esto se ilustra en el diagrama de mensajería de la Figura 6 que se describe a continuación.

Aunque la Figura 5 ilustra una única entidad de control 520 desde la configuración o interacción con la que se establece el estado de una instancia de VNF particular, este puede no ser siempre el caso. En otras palabras, no necesariamente puede reducirse un estado de una instancia de VNF a interacciones con una única entidad de control. En un caso de este tipo, pueden aplicarse los mismos principios como se describe en el presente documento para la entidad de control 520 para todas las otras interfaces de las instancias de VNF, donde el elemento de interfaz 510 serviría de nuevo como una interfaz de VNF lógica.

Como se muestra en la Figura 6, en primer lugar, el elemento de interfaz 510 obtiene un mensaje de control 602. Considérese que en ese momento la instancia de VNF activa, es decir, la instancia de VNF para la que el registrador de VNF 504 proporcionó un manejador al PU 506, es VNF i1 y el mensaje 602 se envió mediante la entidad de control 520 a la VNF i1. El elemento de interfaz 510 puede obtener un mensaje de control de este tipo de varias maneras diferentes, todas ellas incluidas dentro del alcance de la presente invención. Por ejemplo, el elemento de interfaz 510 puede interceptar el mensaje 602 a través de un datagrama recibido desde un medio de punto a punto o de múltiples puntos físico (LAN). En otro ejemplo, el elemento de interfaz 510 puede recibir el mensaje 602 desde la entidad de control 520 (es decir, la entidad de control 520 transmite de manera intencionada el mensaje 602 para la VNF i1 al elemento de interfaz 510) puesto que hay un canal de comunicación base establecido, tal como un canal de TCP, entre el elemento de interfaz 510 y la entidad de control 520. El elemento de interfaz 510 puede a continuación proporcionar el mensaje de control 602 no únicamente para la VNF i1 a la que estaba destinado el mensaje en primer lugar, sino también al menos a otra instancia de VNF de la agrupación de VNF 508. Esto se muestra en la Figura 6 proporcionando el elemento de interfaz 510 una copia del mensaje 602, un mensaje que comprende el mensaje 602, o un mensaje indicativo de la recepción y/o indicativo del contenido del mensaje 602 a la primera y segunda instancias de VNF como los mensajes 604 y 608, respectivamente. Al proporcionar el mensaje 602 destinado para una instancia de VNF a esa y al menos a otra instancia de VNF, el elemento de interfaz 510 posibilita la replicación del estado de la primera instancia de VNF en la segunda instancia de VNF.

En una realización, el elemento de interfaz 510 puede estar configurado para proporcionar los mensajes 604 y 608 sustancialmente en paralelo.

En algún punto después de la provisión del mensaje 604, el elemento de interfaz obtiene un acuse de recibo desde la primera instancia de VNF que la primera instancia de VNF recibió el mensaje 604. De manera similar, en algún punto después de la provisión del mensaje 608, el elemento de interfaz obtiene un acuse de recibo desde la segunda instancia de VNF que la segunda instancia de VNF recibió el mensaje 608. Los acuses de recibo desde la primera y segunda instancias de VNF se ilustran en la Figura 6 como mensajes 606 y 610, respectivamente.

Una vez que el elemento de interfaz 510 tiene los acuses de recibo desde tanto la primera como la segunda instancias de VNF que han recibido los mensajes 604 y 608, respectivamente, proporciona un mensaje de acuse de recibo 612 a la entidad de control 520, indicando de esta manera que se replica un estado de la primera instancia de VNF en la segunda instancia de VNF puesto que han recibido satisfactoriamente el mismo mensaje de control. Puesto que el elemento de interfaz 510 obtiene mensajes de control desde la entidad de control 520 y devuelve acuses de recibo a la entidad de control, actúa como una interfaz de VNF lógica para la entidad de control 520.

Un experto en la materia se daría cuenta que además de recibir los mensajes de acuse de recibo explícitos 606 y 610, hay otras maneras para que el elemento de interfaz 510 tenga tales acuses de recibo, todas ellas incluidas dentro del alcance de la presente invención. Por ejemplo, en línea con el TCP (es decir, cuando hay un canal de TCP base entre la entidad de interfaz 510 y cada una de la primera y segunda instancias de VNF), cuando los CTRL_MSG<n> 604 y 608 obtienen un número de secuencia (n), en lugar de realizar acuse de recibo explícitamente de estos mensajes con los mensajes 606 y 610, respectivamente, la respectiva instancia de VNF puede realizar acuse de recibo de la recepción implícitamente, por ejemplo, enviando un mensaje "Estoy lista para recibir CTRL_MSG<n+1>". En otro ejemplo, si el mensaje de control 602 fuera del formato "establecer regla X = < ... >" entonces los mensajes 606 y 610 devueltos al elemento de interfaz 510 desde cada una de las instancias de VNF podrían ser del formato "informar: regla X = < ... >". En otro ejemplo más, cuando no hay mensajes de acuse de recibo explícitos o implícitos enviados al elemento de interfaz 510, el elemento de interfaz puede estar configurado para obtener tales acuses de recibo requiriendo que la entidad de control 520 interrogue explícitamente el estado cambiado para verificar que cambió. El elemento de interfaz 510 estaría implicado entonces en la funcionalidad de virtualización consolidando la respuesta a esta interrogación en un único mensaje y, en el proceso, obteniendo los acuses de recibo deseados. Son también posibles realizaciones cuando el elemento de interfaz 510 obtiene un acuse de recibo desde una instancia de VNF de una manera mientras que obtiene un acuse de recibo desde otra instancia de VNF de otra manera.

De manera similar al análisis anterior, mientras que se ilustra el acuse de recibo 612 en la Figura 6 como un mensaje

de acuse de recibo explícito, en diversas realizaciones, el elemento de interfaz 510 puede estar configurado para proporcionar un acuse de recibo de este tipo en otras formas, ya sean explícitas o implícitas, por ejemplo, en cualquiera de las maneras anteriormente descritas.

Aunque la Figura 6 ilustra la replicación de un estado únicamente para la primera y segunda instancias de VNF de la agrupación de VNF 508, en otras realizaciones donde hay más instancias de VNF que realizan la misma función de red, tal replicación puede realizarse para más de, y preferentemente para todas, estas instancias de VNF. A continuación, el elemento de interfaz 510 puede estar configurado para proporcionar una indicación al registrador de VNF 504 en cuanto a en qué instancias de VNF se ha replicado el estado de la primera instancia de VNF, actualizando por lo tanto qué instancias de VNF considera el registrador de VNF 504 que están dentro de la agrupación de VNF 508. Preferentemente, las instancias de VNF a las que es posible que el estado de la primera instancia de VNF no pudiera replicarse (por ejemplo, puesto que el elemento de interfaz 510 no obtuvo un acuse de recibo como se describe en la Figura 6), se llevan fuera de la agrupación de VNF 508 ya que el registrador de VNF no proporcionaría un manejador a tal instancia de VNF para el PU 506.

Replicando un estado de una instancia de VNF en al menos otra instancia de VNF duplicando automáticamente comandos de control como se ha descrito anteriormente se asegura que los estados de estas instancias de VNF están en sincronización desde el momento que su configuración cambia, sin necesitar de manera activa enviar mensajes entre cualquiera de las instancias de VNF y el PU 506 o entre las instancias de VNF mismas. En un caso de este tipo, desde el momento que necesita proporcionarse un manejador para una nueva instancia de VNF al PU 506 (ya sea en lugar de o además del manejador antiguo proporcionado), el registrador de VNF 504 puede seleccionar inmediatamente cualquiera de los manejadores a las instancias de VNF que el registrador considera para formar la agrupación 508 puesto que el estado de la instancia de VNF previamente activa ya ha sido replicado para estas instancias de VNF. Esto permite una migración tras error, conmutación o compartición de carga más rápida así como mejora el uso de recursos de red global.

La comunicación fiable entre el elemento de interfaz 510 y la entidad de control 520 y entre el elemento de interfaz 510 y cada una de las instancias de VNF en la agrupación que participan en la replicación del estado puede conseguirse estableciendo canales de comunicación base entre estos componentes, por ejemplo, en forma de canales de TCP. Estableciendo adicionalmente un canal de comunicación seguro, tal como, por ejemplo, el canal SSL/TLS, a través del canal de comunicación base, puede garantizarse la seguridad al intercambiar datos entre las entidades implicadas. Por lo tanto, en una realización, el elemento de interfaz 510 puede estar configurado para establecer un canal de comunicación base con la entidad de control 520 para garantizar la fiabilidad y, preferentemente, para establecer también un canal de comunicación seguro con la entidad de control 520 para garantizar la seguridad. De manera similar, el elemento de interfaz 510 puede estar configurado para establecer un canal de comunicación base y, preferentemente, un canal de comunicación seguro, con cada una de las instancias de VNF individuales que van a estar participando en la replicación estableciendo sesiones de comunicación individuales con estas instancias.

La Figura 7 proporciona una ilustración esquemática de un proceso de arranque para establecer canales de comunicación base individuales, de acuerdo con una realización de la presente invención.

La configuración de un canal implica normalmente un mecanismo similar a la toma de contacto. La Figura 7 ilustra un ejemplo particular de un proceso para una toma de contacto de tres vías similar a TCP. En el ejemplo mostrado en la Figura 7 se supone que el establecimiento de la conexión base se inicia mediante la entidad de control 520 enviando un mensaje SYN 702 hacia la instancia de VNF primaria de la que tiene control. Continuando con el ejemplo de la Figura 6, se considera que la primera instancia de VNF, VNF i1, es la instancia de VNF primaria. Como la función de red realizada mediante la primera instancia de VNF se implementa de manera redundante a través de la agrupación de VNF 508, el mensaje SYN se procesa mediante el elemento de interfaz 510 que, de nuevo, actúa como la interfaz de VNF lógica. A continuación, el elemento de interfaz 510 inicia un mensaje de SYN reflejado al menos hacia la primera y la segunda, pero preferentemente todas las, instancias de VNF 502 de la agrupación de VNF 508. Preferentemente, este proceso ocurre en paralelo. Los mensajes SYN duplicados hacia la primera y segunda instancias de VNF se muestran en la Figura 7 como mensajes 704 y 708, respectivamente.

En respuesta de este mensaje SYN, las respectivas instancias de VNF responden con un mensaje SYN+ACK hacia la entidad de interfaz 510, mostrada en la Figura 7 para la primera y segunda instancias de VNF como los mensajes 706 y 710, respectivamente. Cuando se recibe un mensaje SYN+ACK mediante el elemento de interfaz 510 al menos desde la primera y segunda instancias de VNF, pero preferentemente mediante todas las instancias de VNF de la agrupación de VNF 508, el elemento de interfaz 510 devuelve un mensaje SYN+ACK 712 hacia la entidad de control 520 para entrar en la segunda fase de la toma de contacto. La última activa la entidad de control 520 para responder con un mensaje de ACK final 714 hacia el elemento de interfaz 510. En el nivel del elemento de interfaz 510 que inicia el establecimiento de canales de comunicación base con las instancias de VNF individuales, se envía ahora un ACK desde el elemento de interfaz 510 hacia las instancias de VNF individuales como una última fase de la toma de contacto, mostrada en la Figura 7 para la primera y segunda instancias de VNF como los mensajes 716 y 718, respectivamente.

Cuando no se recibe un mensaje SYN+ACK mediante el elemento de interfaz 510 desde al menos la primera y

segunda instancias de VNF o cuando no se recibe desde ninguna de las instancias de VNF a las que se proporcionó el mensaje SYN, el elemento de interfaz 510 puede determinar que el proceso de toma de contacto falló y que no arrancó el mecanismo de protección de VNF y, preferentemente, proporciona una indicación de esto a la entidad de control 520. Entonces podría repetirse el proceso de establecimiento de los canales de comunicación base.

En una realización, el elemento de interfaz 510 puede estar configurado para proporcionar una indicación de un fallo en cualquier punto en el establecimiento del canal de comunicación base al registrador de VNF 504. A su vez, el registrador de VNF puede considerar actualizar qué instancias de VNF 502 considera que están comprendidas en la agrupación de VNF 508. Por ejemplo, si un acuse de recibo del mensaje SYN no se recibió desde una de las instancias de VNF en las que el elemento de interfaz 510 duplicó el mensaje SYN, el elemento de interfaz podría identificar una instancia de VNF de este tipo y proporcionar esta información al registrador de VNF 504 que podría a continuación excluir esa instancia de VNF de la agrupación de VNF 508.

Una vez que se ha establecido el canal de comunicación base, tal como la conexión de TCP ilustrada en la Figura 7, puede establecerse un canal de comunicación seguro, tal como, por ejemplo, un canal basado en SSL/TLS en la parte superior del canal base en un mecanismo de toma de contacto de capa superior. De nuevo, la solución propuesta tiene como objetivo establecer un canal seguro entre al menos dos, pero preferentemente todas las, instancias de VNF de la agrupación de VNF 508 y el elemento de interfaz 510, así como entre el elemento de interfaz 510 y la entidad de control 520. Esto requiere que cada nodo implicado, es decir, las instancias de VNF 502, la entidad de control 520 y el elemento de interfaz 510, tenga un par de claves privada/pública y un certificado que firme esa clave pública. En diversas realizaciones, estas claves pueden auto-generarse y auto-firmarse mediante las instancias de VNF individuales, o pueden recibirse en iteración con una autoridad de certificado confiable. En esta configuración, el par de claves del elemento de interfaz 510 puede representar el par de claves de la VNF lógica con la que interconecta la entidad de control 520.

La Figura 8 ilustra el proceso de toma de contacto de 4 fases basado en SSL normalizado existente entre un cliente y un servidor. Como se muestra en la Figura 8, los mensajes hello (fase 1) implican la negociación del ID de sesión, el algoritmo de intercambio de clave, algoritmo de MAC, algoritmo de encriptación e intercambio de número aleatorio inicial. A continuación, el servidor puede enviar su certificado y mensaje de intercambio de clave, y puede solicitar que el cliente envíe un certificado. El servidor a continuación señaliza el final de la fase hello (fase 2). Posteriormente, el cliente envía el certificado si se solicita y puede enviar un mensaje de verificación de certificado explícito y el cliente siempre envía su mensaje de intercambio de clave (fase 3). Finalmente, se cambia la especificación de cifrado y se finaliza la toma de contacto (fase 4). Como reconocería un experto en la materia, la especificación de cifrado puede especificar un algoritmo de encriptación de datos en bruto, tal como, por ejemplo, DES, y un algoritmo de función de troceo, tal como, por ejemplo, MD5 o SHA-1, y puede definir atributos criptográficos, tales como un tamaño de función de troceo. En la Figura 8, las líneas discontinuas indican que el mensaje es opcional, mientras que las líneas continuas indican que el mensaje es obligatorio para que la toma de contacto sea satisfactoria.

La Figura 9 proporciona una ilustración esquemática del establecimiento de canales de comunicación seguros individuales, de acuerdo con una realización de la presente invención. En particular, la Figura 9 ilustra una configuración paralela de tres canales de SSL seguros, siguiendo cada uno el mecanismo de toma de contacto de 4 fases como se representa en la Figura. 8. Un canal se encuentra entre la entidad de control 520 y el elemento de interfaz 510, donde el mecanismo de toma de contacto de 4 fases de la Figura 8 se indica como una toma de contacto de SSL de 4 vías 902. Otro canal se encuentra entre la primera instancia de VNF, VNF i1, y el elemento de interfaz 510, donde el mecanismo de toma de contacto de 4 fases de la Figura 8 se indica como una toma de contacto de SSL de 4 vías 906. El tercer canal se encuentra entre la segunda instancia de VNF, VNF i2, y el elemento de interfaz 510, donde el mecanismo de toma de contacto de 4 fases de la Figura 8 se indica como una toma de contacto de SSL de 4 vías 904.

Como se ha descrito anteriormente para el canal de comunicación base, en una realización, el elemento de interfaz 510 puede estar configurado para proporcionar una indicación de un fallo en cualquier punto en el establecimiento del canal de comunicación seguro al registrador de VNF 504. A su vez, el registrador de VNF puede considerar actualizar qué instancias de VNF 502 considera que están comprendidas en la agrupación de VNF 508.

En una realización preferida, el mecanismo de replicación descrito en asociación con la Figura 6 se realiza únicamente una vez que el proceso de arranque de establecimiento del canal de comunicación base como se describe para la Figura 7 y, preferentemente, también el canal de comunicación seguro como se describe para la Figura 9, se ha ejecutado satisfactoriamente (es decir, cuando los canales de control se consideran como activos).

A diferencia del estado de la técnica, las soluciones propuestas no requieren ancho de banda adicional entre las instancias de VNF 502 y el PU 506 para la replicación del estado, ya que no se requieren mensajes de cookie. Además, el proceso resultante de la conmutación a, o activación de, una nueva instancia de VNF en las soluciones propuestas puede ahora ser significativamente más rápido. Estas ventajas pueden observarse volviendo a la Figura 4A y observando que el proceso de migración tras error con la replicación del estado entre diferentes instancias de VNF de la misma agrupación que se basa en el uso de la arquitectura 500 como se ha descrito anteriormente no requeriría las etapas 402, 414, y 416. El resto de la descripción del proceso de migración tras error proporcionada para la Figura 4A

sería aplicable para la arquitectura 500, sustituyendo el PE 1 por VNF i1, sustituyendo PE 2 por VNF i2, sustituyendo PR-H 104 por el registrador de VNF 504 y sustituyendo PU 106 por PU 506, cuya ilustración y descripción por lo tanto no se repiten en este punto. A partir del momento cuando falla la conectividad hacia PE1, es decir, desde el tiempo de espera de la confirmación, el registrador de VNF 504 puede notificar al PU 506 con un manejador hacia la segunda instancia de VNF, VNF i2. A partir del momento que se recibe este mensaje mediante el PU 506, la migración tras error puede considerarse como finalizada, puesto que el estado de la VNF i1 ya se ha replicado continuamente en la VNF i2 como resultado de los procesos anteriormente descritos.

La Figura 10 proporciona una ilustración esquemática de un proceso de migración tras error por defecto cuando se define el estado de las diferentes instancias de VNF 502 mediante mensajes de control proporcionados a las respectivas instancias de VNF mediante la entidad de control 520, de acuerdo con una realización de la presente invención. La Figura 10 es comparable a la Figura 4B que ilustra un escenario análogo de acuerdo con el estado de la técnica. Por lo tanto, la Figura 10 también ilustra un proceso en el caso de que las instancias de VNF 502 bajo consideración sean funciones de red controladas por OpenFlow, tales como, por ejemplo, un cortafuegos OpenFlow. Como se muestra en la Figura 10 con el mensaje 1002, la entidad de control 520, en este caso, un controlador OpenFlow, comunica nuevas entradas de flujo (por ejemplo, REGLA x) a la instancia de VNF activa, es decir, la instancia de VNF para la que el registrador de VNF 504 proporcionó un manejador al PU 506, en este ejemplo VNF i1, y el elemento de interfaz 510 obtiene el mensaje.El elemento de interfaz 510 duplica esta información de control hacia los elementos de agrupación individuales, en este caso, conmutadores OpenFlow, VNF i1 y VNF i2, mostrados con los mensajes 1008 y 1004, respectivamente, de una manera como se describe en asociación con la Figura 6, con los canales de comunicación establecidos entre las entidades implicadas según se describe en asociación con las Figuras 7 y 9. También, como se ha descrito anteriormente para la Figura 6, el elemento de interfaz 510 envía un acuse de recibo hacia la entidad de control 520, mostrada en la Figura 10 con el mensaje 1012, únicamente cuando el elemento de interfaz 510 tiene los acuses de recibo desde las instancias de VNF, VNF i1 y VNF i2, mostradas en la Figura 10 con mensajes explícitos 1010 y 1006, respectivamente. Como se ha descrito anteriormente, este proceso asegura que el estado de los elementos de agrupación individuales VNF i1 y VNF i2 esté siempre en sincronización. Mientras tanto, el proceso de confirmación entre el registrador de VNF 504 (PR-H) y las instancias de VNF i1 e i2 monitoriza si estos elementos de agrupación están aún operando apropiadamente, mostrados en la Figura 10 con los mensajes 1018 y 1014, respectivamente. Tras un fallo del elemento de agrupación primario VNF i1, se agota la correspondiente sesión de confirmación (mostrado en la Figura 10 con la etapa 1020), y el registrador de VNF 504 actualiza el PU 506 (por ejemplo, el sistema de control de SFC) con el nuevo manejador en forma de un manejador a la VNF i2, mostrada en la Figura 10 con la etapa 1022 (con la condición de que no haya fallo con el elemento de agrupación VNF i2, como se muestra en la Figura 10 con la etapa 1016). Esto posibilita al PU 506 el reaprovisionamiento de la configuración de cadena de función de red/servicio con respecto al plano de datos. Puesto que el estado se ha mantenido en sincronización continuamente, se finaliza la migración tras error tan pronto como se finaliza la conmutación de plano de datos, que implica la recepción de la actualización del manejador mediante el PU 506 y la ejecución de la conmutación del plano de datos en la red. Como ya no es necesario que se replique ningún estado adicional, la recuperación puede ser inmediata.

Puesto que podrían usarse las realizaciones de la presente invención para posibilitar la conmutación sin impacto en el plano de datos, podrían usarse técnicas de protección de red, es decir, un aprovisionamiento proactivo de la ruta de respaldo. En el caso de protección, el sistema de control de red debe conocer el manejador de la instancia de VNF de respaldo antes de que ocurra realmente el fallo, para poder aprovisionar previamente la ruta de red hacia la VNF de respaldo. Los manejadores de instancias de VNF alternativas podrían intercambiarse, por ejemplo, a través de un mensaje de manejador ampliado 314 desde el registrador de VNF (PR-H) hacia el PU que incluye: i) el manejador activo, y ii) los manejadores de las VNF de respaldo. Como es conocido en la técnica, cuando se usa protección de red, se envía una señal de indicación de fallo y/o una alarma desde el sistema de control de red (que podría ser el mismo PU 506, o un sistema de control de red que se notifica directamente mediante el PU 506) hacia los puntos de ramal que necesitan conmutarse entre el segmento/ruta primario y de respaldo desde el momento que se detecta un fallo y se notifica desde el PR-H hacia la instancia de control (en este caso, el PU 506, por ejemplo, el sistema de control de SFC).

Las técnicas de protección de red son conocidas por ofrecer tiempos de recuperación de red en menos de 50 ms. La Figura 11 proporciona una ilustración esquemática de una arquitectura de plano de datos 1100 que podría usarse con la funcionalidad del elemento de interfaz 510 como se describe en el presente documento, de acuerdo con una realización de la presente invención.

La Figura 11 ilustra una agrupación de VNF 508 con dos elementos de agrupación, una instancia de VNF primaria (primera) VNF i1 y una instancia de VNF de respaldo (segunda) VNF i2. La interfaz de control entre la primera y segunda VNF 502 y la entidad de control 520 se maneja mediante el elemento de interfaz 510 como se ha descrito anteriormente. En el plano de datos, cada una de la VNF i1 y VNF i2 puede tener n interfaces, mostradas en la Figura 11 como interfaces if1 a ifn, que están interconectadas a n puntos de conexión de servicio (SAP), mostrados en la Figura 11 como dos SAP - SAP1 1102 a SAP2 1104 mediante una red de interconexión. Parte de la ruta de red entre los SAP y las interfaces de VNF de las instancias de VNF primaria y de respaldo puede ser solapando hasta los puntos de ramal mostrados en la Figura 11 como los puntos de ramal b1 a bn, donde b1 es el punto de ramal para la ruta de red a la primera interfaz, hasta bn, para el punto de ramal de la ruta de red a la enésima interfaz. Un papel del PU 506

es asegurar que se aprovisionará la ruta de red hacia la instancia de VNF respaldo, por ejemplo, usando el control de OpenFlow o protocolos de señalización de conmutación de etiqueta de múltiples protocolos/generalizada (G/MPLS). Desde el momento que se da instrucción al PU 506 para usar una instancia de VNF alternativa, puede tomar la acción para cambiar la ruta de red entre los SAP hacia la VNF de respaldo. En el caso de usar técnicas de protección, esto implica dar instrucciones a los puntos de ramal para conmutar hacia los segmentos de respaldo, es decir, conmutar usando las interconexiones de línea discontinua mostradas en la Figura 11.

Las etapas del método descritas en el presente documento que van a realizarse mediante la entidad de interfaz 510 pueden realizarse mediante cualquier clase de un sistema de procesamiento de datos que incluye al menos un procesador configurado para llevar a cabo estas etapas del método. Un ejemplo de un sistema de procesamiento de datos de este tipo se ilustra en la Figura 12 como un sistema de procesamiento de datos 1200, y se proporciona un análisis de dónde un sistema de procesamiento de datos de este tipo podría implementarse después la descripción de la Figura 12.

El sistema de procesamiento de datos 1200 puede incluir al menos un procesador 1202 acoplado a elementos de memoria 1204 a través de un bus de sistema 1210. Como tal, el sistema de procesamiento de datos puede almacenar un código de programa en elementos de memoria 1204. Además, el procesador 1202 puede ejecutar el código de programa accedido desde los elementos de memoria 1204 mediante el bus de sistema 1210. En un aspecto, el sistema de procesamiento de datos 1200 puede implementarse como un ordenador que es adecuado para almacenar y/o ejecutar un código de programa. Sin embargo, debería apreciarse que el sistema 1200 puede implementarse en forma de cualquier sistema que incluya un procesador y memoria que pueda realizar las funciones descritas en esta memoria descriptiva.

Los elementos de memoria 1204 pueden incluir uno o más dispositivos de memoria física, tales como, por ejemplo, memoria local 1206 y uno o más dispositivos de almacenamiento masivo 1208. Memoria local puede hacer referencia a memoria de acceso aleatorio u otro dispositivo o dispositivos de memoria no persistente generalmente usados durante la ejecución real del código de programa. Un dispositivo de almacenamiento masivo puede implementarse como un disco duro u otro dispositivo de almacenamiento de datos persistente. El sistema de procesamiento 1200 puede incluir también una o más memorias caché (no mostradas) que proporcionan almacenamiento temporal de al menos algún código de programa para reducir el número de veces que el código de programa debe recuperarse desde el dispositivo de almacenamiento masivo 1208 durante la ejecución.

Los dispositivos de entrada/salida (E/S) representados como el dispositivo de entrada 1212 y el dispositivo de salida 1214 pueden estar acoplados opcionalmente al sistema de procesamiento de datos. Ejemplos de dispositivo de entrada pueden incluir, pero sin limitación, por ejemplo, un teclado, un dispositivo apuntador, tal como un ratón, o similares. Ejemplos de dispositivo de salida pueden incluir, pero sin limitación, por ejemplo, un monitor o pantalla, altavoces, o similares. El dispositivo de entrada y/o dispositivo de salida pueden estar acoplados al sistema de procesamiento de datos directamente o a través de controladores de E/S intermedios. Un adaptador de red 1216 puede también estar acoplado al sistema de procesamiento de datos para posibilitarle que se acople a otros sistemas, sistemas informáticos, dispositivos de red remotos, y/o dispositivos de almacenamiento remoto a través de redes privadas o públicas intermedias. El adaptador de red puede comprender, en particular, un receptor de datos 1218 para recibir datos que se transmiten mediante dichos sistemas, dispositivos y/o redes para dichos datos y un transmisor de datos 1220 para transmitir datos a dichos sistemas, dispositivos y/o redes. Módems, módems de cable y tarjetas Ethernet son ejemplos de diferentes tipos de adaptador de red que pueden usarse con el sistema de procesamiento de datos 1200.

Los elementos de memoria 1204 pueden almacenar una aplicación (no mostrada). Debería apreciarse que el sistema de procesamiento de datos 1200 puede ejecutar adicionalmente un sistema operativo (no mostrado) que puede facilitar la ejecución de la aplicación. La aplicación, que se implementa en forma de código de programa ejecutable, puede ejecutarse mediante el sistema de procesamiento de datos 1200, por ejemplo, mediante el procesador 1202. En respuesta a la ejecución de la aplicación, el sistema de procesamiento de datos 1200 puede estar configurado para realizar una o más etapas del método descritas en el presente documento.

Los expertos en la materia reconocerán que aunque se muestran los elementos 1202-1220 en la Figura 12 como elementos separados, en otras realizaciones, su funcionalidad podría implementarse en menor número de elementos individuales o distribuirse a través de un número mayor de componentes.

La Figura 13 proporciona una ilustración esquemática de un sistema de telecomunicaciones 1300. El sistema de telecomunicaciones 1300 comprende una red de acceso por radio 1302 (también indicada como E-UTRAN o RAN en la Figura 13) y una red principal 1304 que contiene diversos elementos o nodos como se describe con mayor detalle a continuación.

En el sistema de telecomunicaciones de la Figura 13, se representan esquemáticamente tres generaciones de redes juntas para los fines de brevedad. Puede hallarse una descripción más detallada de la arquitectura y vista general en 3GPP TS 23.002 que se incluye en la presente solicitud por referencia en su totalidad.

El ramal inferior de la Figura 13 representa una red de telecomunicaciones de GPRS o UMTS.

Para una red de telecomunicaciones de GSM/GPRS (es decir, una red de telecomunicaciones 2G/2.5G), una red de acceso por radio 1302 comprende una pluralidad de estaciones base (combinación de un BSC y una BTS) y uno o más controladores de red de radio (RNC), no mostrados de manera individual en la Figura 13. La red principal 1304 comprende un nodo de soporte de GPRS de pasarela (GGSN), un nodo de soporte de GPRS de servicio (SGSN, para GPRS) o centro de conmutación móvil (MSC, para GSM, no mostrado en la Figura 13), y un registro de localización doméstico (HLR) combinado con un centro de autenticación (AuC). El HLR contiene información de suscripción para dispositivos móviles 1306 (en ocasiones denominados como "equipo de usuario" (UE) o dispositivos de usuario) y el AuC contiene una clave secreta compartida K que va a usarse para procedimientos de autenticación y acuerdo de clave (AKA).

Para una red de acceso por radio de UMTS (UTRAN) (es decir, una red de telecomunicaciones 3G), la red de acceso por radio 1302 también comprende un controlador de red de radio (RNC) conectado a una pluralidad de Nodos B, tampoco mostrados. En la red principal 1304, el GGSN y el SGSN/MSC están conectados de manera convencional al HLR/AuC que contiene información de suscripción y claves de secreto compartido K de los dispositivos móviles 1306.

Debería observarse que la funcionalidad de RNC en redes GSM y UMTS es formalmente parte de la RAN. La funcionalidad del RNC puede implementarse en una o más estaciones base. Una configuración de este tipo es conocida como una arquitectura contraída.

El ramal superior en la Figura 13 representa una red de telecomunicaciones de la siguiente generación, indicada comúnmente como sistema de la evolución a largo plazo (LTE) o sistema de paquetes evolucionado (EPS) (es decir, una red de telecomunicaciones 4G). En una red de este tipo, la red de acceso por radio 1302, indicada como E-UTRAN, comprende Nodos B evolucionados (eNodos B o eNB) que proporcionan acceso inalámbrico para los dispositivos móviles 1306. La red principal 1304 comprende una pasarela de PDN (P-GW) y una pasarela de servicio (S-GW). La E-UTRAN del EPS está conectada a la S-GW mediante una red por paquetes. La S-GW está conectada a un servidor de abonado doméstico HSS y a una entidad de gestión de movilidad MME para fines de señalización. El HSS incluye un repositorio de perfil de suscripción SPR y está combinado con un centro de autenticación (AuC) que almacena una clave secreta compartida K para procedimientos AKA. Puede encontrarse más información sobre la arquitectura general de una red de EPS en 3GPP TS 23.401.

Para redes de telecomunicaciones GPRS, UMTS y LTE, la red principal 1304 está conectada, en general, a una red adicional 1308, por ejemplo, Internet, usando, por ejemplo, una pasarela (por ejemplo, la P-GW).

En diversas realizaciones, el elemento de interfaz 510 descrito en el presente documento puede implementarse en hardware, software, o una combinación de hardware y software. Por ejemplo, en las redes ilustradas en la Figura 13, el sistema de procesamiento de datos 1200 configurado para actuar como el elemento de interfaz 510 descrito en el presente documento podría implementarse como una parte de la S-GW, P-GW o el SGSN o GGSN de la red principal, o el elemento de interfaz 510, como se describe en el presente documento, podría implementarse como una función de software en una o una combinación de estos elementos de la red principal. Por supuesto, pueden usarse también arquitecturas distintas de las definidas mediante 3GGP, por ejemplo, WiMAX, en el contexto de la presente divulgación.

Diversas realizaciones de la invención pueden implementarse como un producto de programa para su uso con un sistema informático o un procesador, donde el programa o programas del producto de programa definen funciones de las realizaciones (incluyendo los métodos descritos en el presente documento). En una realización, el programa o programas pueden estar contenidos en una diversidad de medios de almacenamiento no transitorios legibles por ordenador (denominados, en general, como "almacenamiento"), donde, como se usa en el presente documento, la expresión "medio de almacenamiento no transitorio legible por ordenador" comprende todos los medios legibles por ordenador, con la única excepción de que sea una señal de propagación transitoria. En otra realización, el programa o programas pueden estar contenidos en una diversidad de medios de almacenamiento transitorios legibles por ordenador. Los medios de almacenamiento legibles por ordenador ilustrativos incluyen, pero sin limitación: (i) medios de almacenamiento no escribibles (por ejemplo, dispositivos de memoria de solo lectura en un ordenador, tales como discos CD-ROM legibles por una unidad de CD-ROM, chips ROM o cualquier tipo de memoria de semiconductores no volátil de estado sólido) en los que se almacena permanentemente la información; y (ii) medios de almacenamiento escribibles (por ejemplo, memoria flash, discos flexibles en una unidad de disquete o unidad de disco duro o cualquier tipo de memoria de semiconductores de acceso aleatorio de estado sólido) en los que se almacena información alterable. El programa informático puede ejecutarse en el procesador 1202 descrito en el presente documento.

REIVINDICACIONES

1. Un método para la comunicación de un elemento de interfaz (510) entre una agrupación de funciones de red virtual (508) y una entidad de control (520), comprendiendo la agrupación de funciones de red virtual una pluralidad de instancias de función de red virtual (502) que incluyen al menos una primera instancia de función de red virtual y una segunda instancia de función de red virtual, donde la pluralidad de instancias de función de red virtual (502) están registradas con un registrador de agrupación de funciones de red virtual (504) comunicativamente conectado con el elemento de interfaz (510), proporcionando el registrador de agrupación de funciones de red virtual (504) un manejador a una de las instancias de función de red virtual (502) a un usuario de agrupación (506), controlando la entidad de control (520) las instancias de función de red virtual de la agrupación de funciones de red virtual mediante el envío de mensajes de control, donde el elemento de interfaz ayuda en la replicación de un estado de la primera instancia de función de red virtual al menos en la segunda instancia de función de red virtual, comprendiendo el método las etapas de:

- obtener, mediante el elemento de interfaz, el mensaje de control desde la entidad de control a la primera instancia de función de red virtual, en donde el mensaje de control define el estado de la primera instancia de función de red virtual;
- proporcionar, mediante el elemento de interfaz, el mensaje de control, o una derivación del mismo, al menos a la primera instancia de función de red virtual y a la segunda instancia de función de red virtual; y
- proporcionar, mediante el elemento de interfaz, un acuse de recibo del mensaje de control a la entidad de control cuando el elemento de interfaz tiene un acuse de recibo del mensaje de control, o de la derivación del mismo, proporcionado a la primera instancia de función de red virtual y un acuse de recibo del mensaje de control, o de la derivación del mismo, proporcionado a la segunda instancia de función de red virtual.

2. El método de acuerdo con la reivindicación 1, en donde las instancias de función de red virtual comprenden dos o más instancias de función de red virtual, preferentemente tres o más instancias de función de red virtual, en donde la etapa de que el elemento de interfaz proporcione el mensaje de control al menos a la primera instancia de función de red virtual y a la segunda instancia de función de red virtual comprende proporcionar el mensaje de control al menos a dos de, preferentemente a todas, las instancias de función de red virtual de la agrupación de funciones de red virtual, y en donde el método comprende adicionalmente las etapas de:

- identificar, mediante el elemento de interfaz, instancias de función de red virtual de la agrupación de funciones de red virtual desde las cuales el elemento de interfaz no recibió un acuse de recibo del mensaje de control; y

- proporcionar, mediante el elemento de interfaz, una indicación de las instancias de función de red virtual identificadas al registrador de agrupación de funciones de red virtual (504).

3. El método de acuerdo con las reivindicaciones 1 o 2, que comprende adicionalmente una etapa de establecer un canal de comunicación base entre el elemento de interfaz y cada una de la entidad de control, la primera instancia de función de red virtual y la segunda instancia de función de red virtual.

4. El método de acuerdo con la reivindicación 3, en donde el canal de comunicación base es un canal de TCP.

5. El método de acuerdo con las reivindicaciones 3 o 4, en donde las instancias de función de red virtual comprenden dos o más instancias de función de red virtual, preferentemente tres o más instancias de función de red virtual, en donde la etapa de que el elemento de interfaz establezca el canal de comunicación base comprende establecer el canal de comunicación base entre el elemento de interfaz y cada una de las al menos dos de, preferentemente todas, las instancias de función de red virtual de la agrupación de funciones de red virtual, y en donde el método comprende adicionalmente las etapas de:

- identificar, mediante el elemento de interfaz, instancias de función de red virtual de la agrupación de funciones de red virtual con las que el canal de comunicación base no pudiera establecerse y/o estuviera roto; y

- proporcionar, mediante el elemento de interfaz, una indicación de las instancias de función de red virtual identificadas al registrador de agrupación de funciones de red virtual (504).

6. El método de acuerdo con una cualquiera de las reivindicaciones 3-5, que comprende adicionalmente una etapa de que el elemento de interfaz establezca un canal de comunicación seguro a través del canal de comunicación base establecido entre el elemento de interfaz y cada una de la entidad de control, la primera instancia de función de red virtual y la segunda instancia de función de red virtual.

7. El método de acuerdo con la reivindicación 6, en donde el canal de comunicación seguro comprende un canal basado en SSL/TLS.

8. El método de acuerdo con las reivindicaciones 6 o 7, en donde el canal de comunicación seguro entre el elemento de interfaz y cada una de la entidad de control, la primera instancia de función de red virtual y la segunda instancia de

función de red virtual se establece en paralelo.

9. El método de acuerdo con una cualquiera de las reivindicaciones 6-8, en donde las instancias de función de red virtual comprenden dos o más instancias de función de red virtual, preferentemente tres o más instancias de función de red virtual, en donde la etapa de que el elemento de interfaz establezca el canal de comunicación seguro comprende establecer el canal de comunicación seguro entre el elemento de interfaz y cada una de las al menos dos de, preferentemente todas, las instancias de función de red virtual de la agrupación de funciones de red virtual, y en donde el método comprende adicionalmente las etapas de:

- identificar, mediante el elemento de interfaz, instancias de función de red virtual de la agrupación de funciones de red virtual con las que el canal de comunicación seguro no pudiera establecerse y/o estuviera roto; y
- proporcionar, mediante el elemento de interfaz, una indicación de las instancias de función de red virtual identificadas al registrador de agrupación de funciones de red virtual.

10. Un producto de programa informático, preferentemente almacenado en un medio de almacenamiento no transitorio legible por ordenador, que comprende porciones de código de software configuradas para, cuando se ejecutan en un procesador, llevar a cabo etapas de método de acuerdo con una cualquiera de las reivindicaciones 1-9.

11. Un sistema de procesamiento de datos (1200) que comprende al menos un procesador (1202) configurado para llevar a cabo etapas de método de acuerdo con una cualquiera de las reivindicaciones 1-9.

12. Un sistema (500) que comprende:

- una agrupación de funciones de red virtual (508) que comprende una pluralidad de instancias de función de red virtual (502) que incluyen al menos una primera instancia de función de red virtual y una segunda instancia de función de red virtual;
- una entidad de control (520) configurada para controlar las instancias de función de red virtual de la agrupación de funciones de red virtual mediante el envío de mensajes de control;
- un registrador de agrupación de funciones de red virtual (504) con el que están registradas las instancias de función de red virtual (502) de la agrupación de funciones de red virtual (508) y que está configurado para proporcionar un manejador a una de las instancias de función de red virtual (502) a un usuario de agrupación (506), y
- un elemento de interfaz (510) comunicativamente conectado a cada una de las instancias de función de red virtual, al registrador de agrupación de funciones de red virtual y a la entidad de control, donde el elemento de interfaz está comunicativamente conectado entre instancias de función de red virtual y la entidad de control, en donde el elemento de interfaz está configurado para
- obtener un mensaje de control desde la entidad de control a la primera instancia de función de red virtual, en donde el mensaje de control define el estado de la primera instancia de función de red virtual;
- proporcionar el mensaje de control, o una derivación del mismo, al menos a la primera instancia de función de red virtual y a la segunda instancia de función de red virtual; y
- proporcionar un acuse de recibo del mensaje de control a la entidad de control cuando el elemento de interfaz tiene un acuse de recibo del mensaje de control, o de la derivación del mismo, proporcionado a la primera instancia de función de red virtual y un acuse de recibo del mensaje de control, o de la derivación del mismo, proporcionado a la segunda instancia de función de red virtual.

13. El sistema de acuerdo con la reivindicación 12, en donde el registrador de agrupación de funciones de red virtual (504) está configurado para al menos recibir desde el elemento de interfaz las instancias de función de red virtual identificadas por el elemento de interfaz de acuerdo con una cualquiera de las reivindicaciones 2, 4 y 8.

14. El sistema de acuerdo con la reivindicación 13, en donde el registrador de agrupación de funciones de red virtual está configurado adicionalmente para proporcionar al usuario de agrupación (506) un manejador a una instancia de función de red virtual de respaldo en caso de una conmutación desde la primera instancia de función de red virtual.

15. El sistema de acuerdo con la reivindicación 13, en donde el registrador de agrupación de funciones de red virtual está configurado adicionalmente para proporcionar al usuario de agrupación un manejador a una segunda instancia de función de red virtual en caso de compartición de carga entre al menos la primera instancia de función de red virtual y la segunda instancia de función de red virtual en el plano de datos.

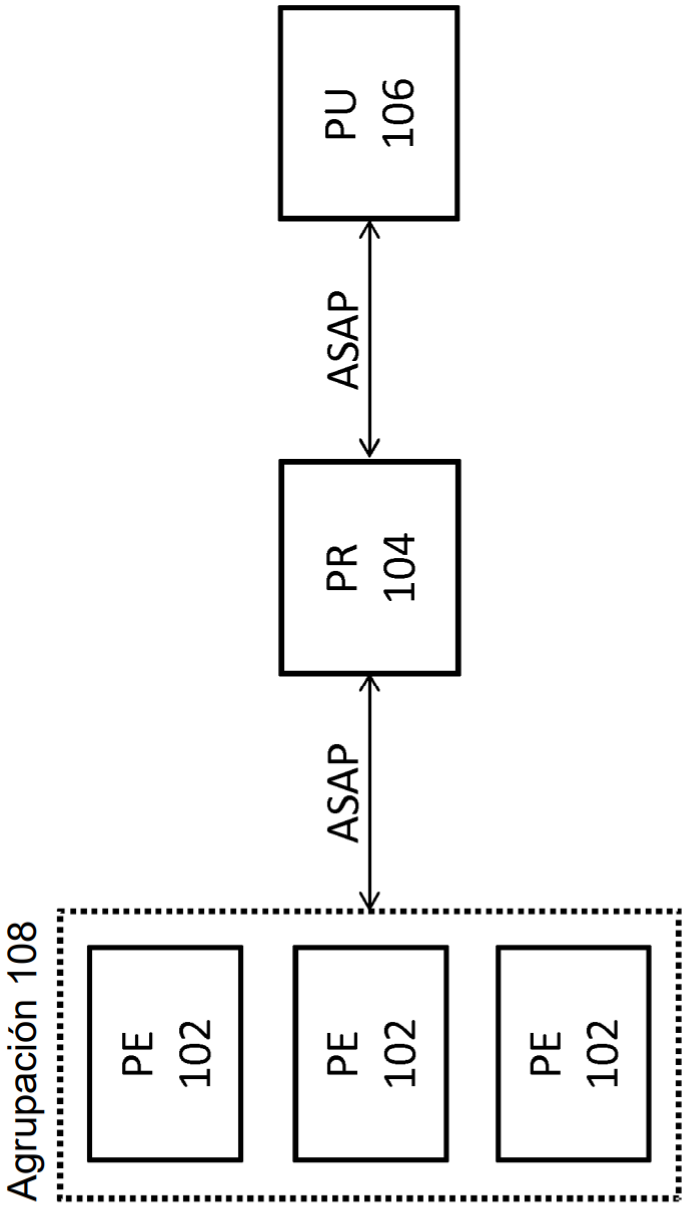

FIG. 1

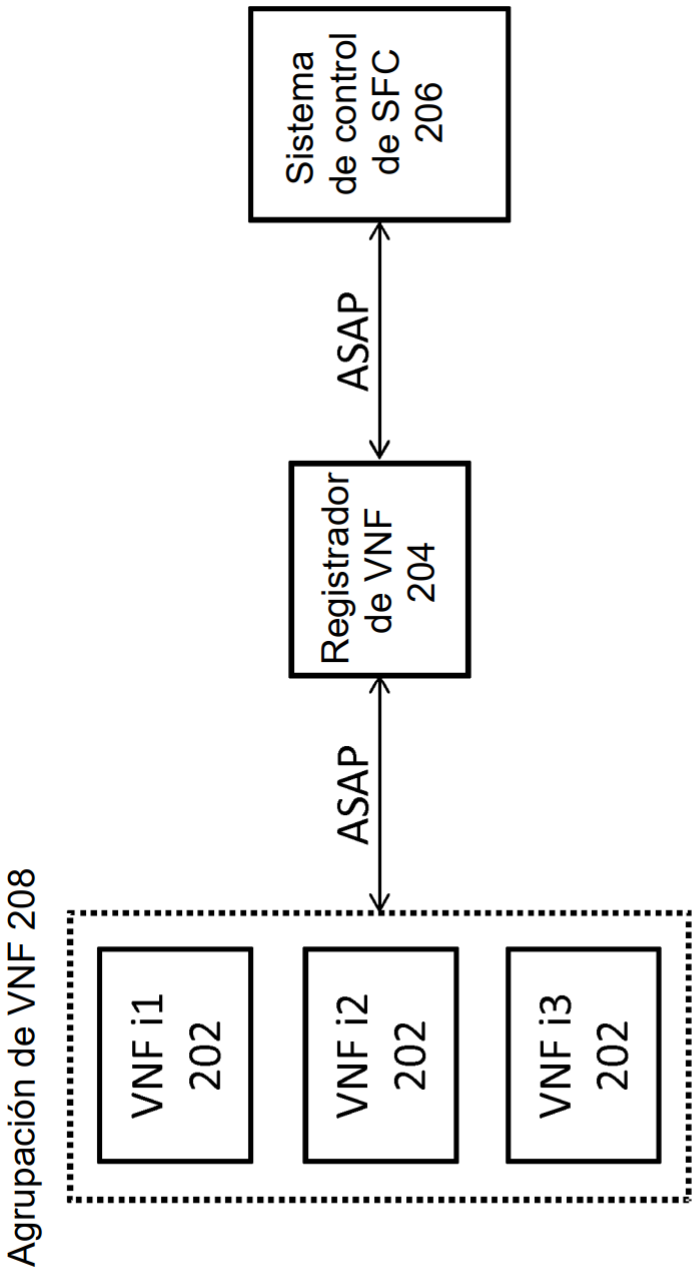
Sistema de control de SFC 206
ASAP
Registrador de VNF 204
ASAP
Agrupación de VNF 208
VNF i1 202
VNF i2 202
VNF i3 202
200

FIG. 2

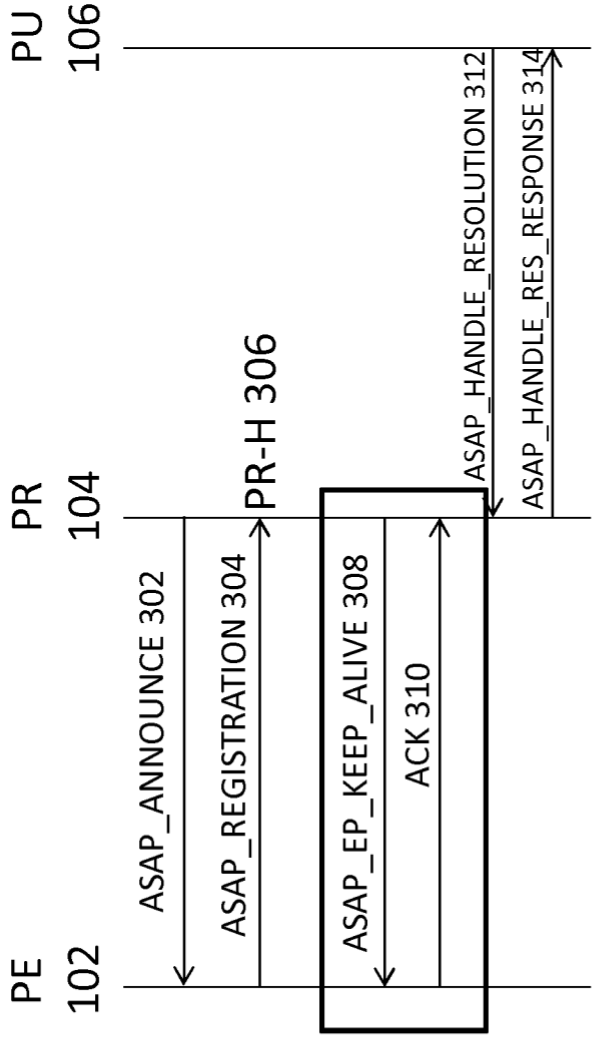
PU
106
PR
104
PE
102
PR-H 306
ASAP_ANNOUNCE 302
ASAP_REGISTRATION 304
ASAP_EP_KEEP_ALIVE 308
ACK 310
ASAP_HANDLE_RESOLUTION 312
ASAP_HANDLE_RES_RESPONSE 314

FIG. 3

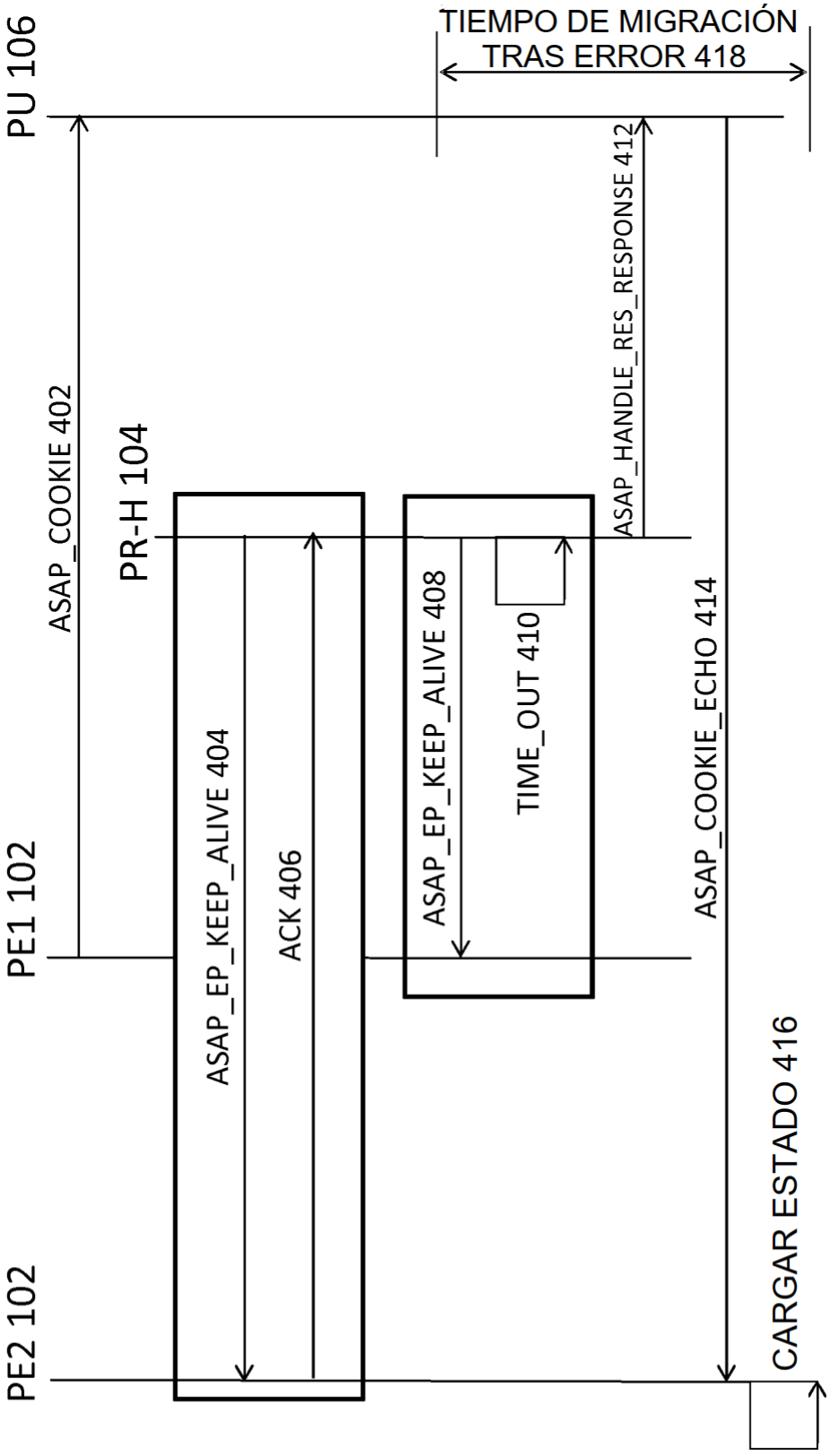
PU 106
TIEMPO DE MIGRACIÓN TRAS ERROR 418
ASAP_COOKIE 402
PR-H 104
ASAP_HANDLE_RES_RESPONSE 412
ASAP_EP_KEEP_ALIVE 404
ACK 406
ASAP_EP_KEEP_ALIVE 408
TIME_OUT 410
ASAP_COOKIE_ECHO 414
PE1 102
PE2 102
CARGAR ESTADO 416

FIG. 4A

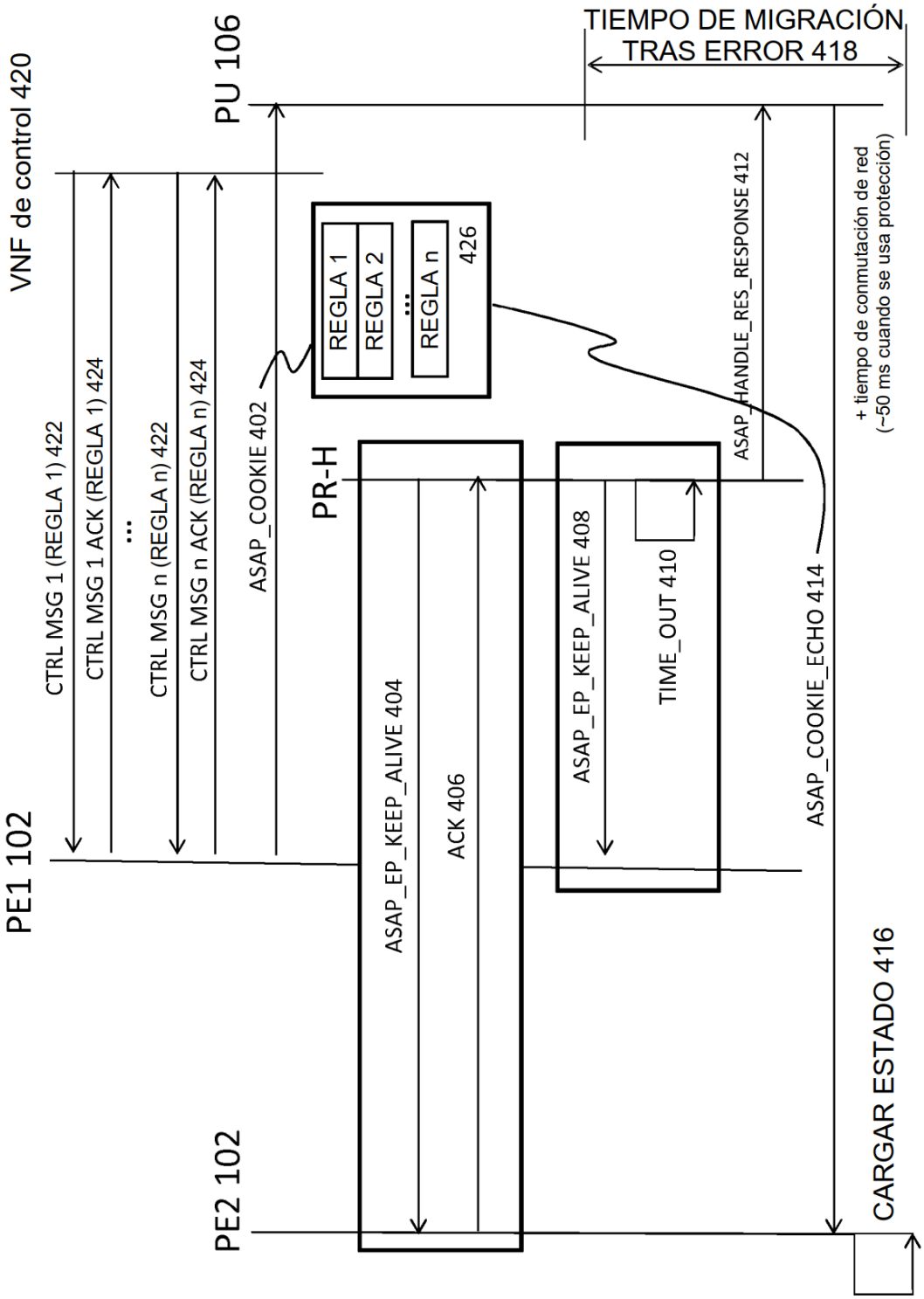
VNF de control 420
PU 106
TIEMPO DE MIGRACIÓN TRAS ERROR 418
CTRL MSG 1 (REGLA 1) 422
CTRL MSG 1 ACK (REGLA 1) 424
CTRL MSG n (REGLA n) 422
CTRL MSG n ACK (REGLA n) 424
ASAP_COOKIE 402
REGLA 1
REGLA 2
REGLA n
426
ASAP_HANDLE_RES_RESPONSE 412
+ tiempo de conmutación de red (~50 ms cuando se usa protección)
PR-H
PE1 102
ASAP_EP_KEEP_ALIVE 404
ACK 406
ASAP_EP_KEEP_ALIVE 408
TIME_OUT 410
ASAP_COOKIE_ECHO 414
PE2 102
CARGAR ESTADO 416

FIG. 4B

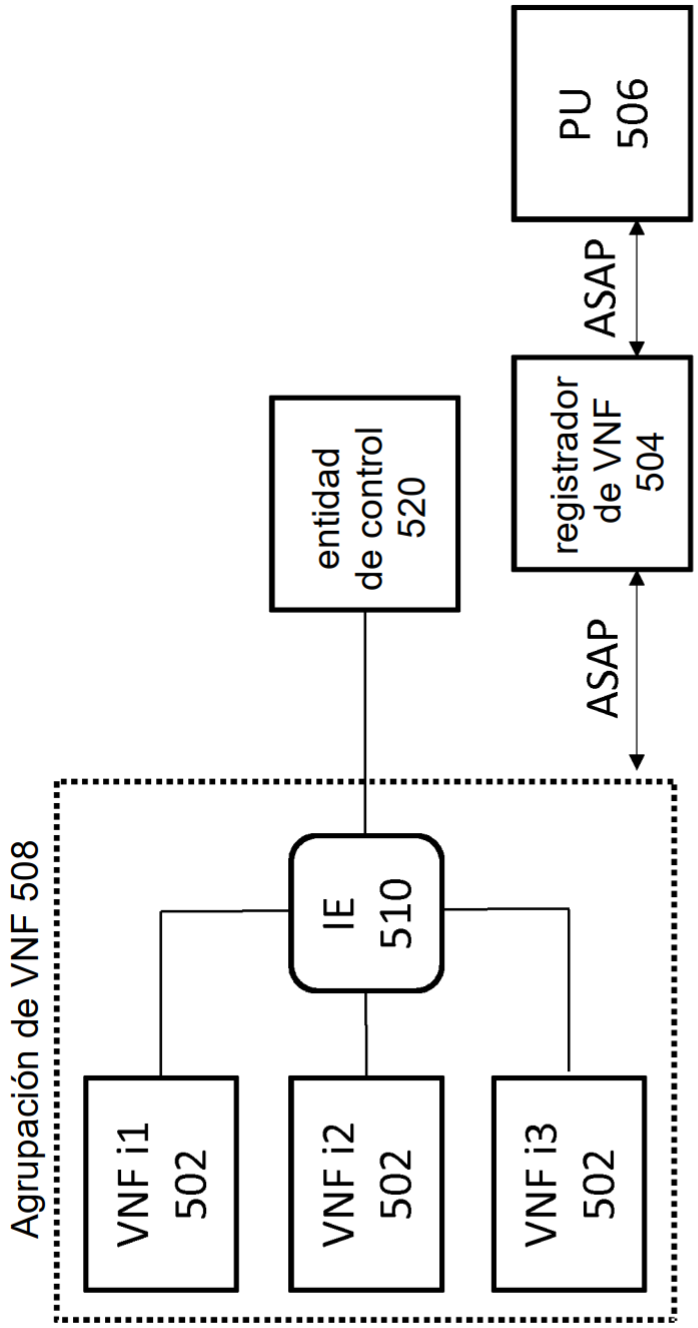
PU
506
ASAP
registrador
de VNF
504
entidad
de control
520
ASAP
IE
510
Agrupación de VNF 508
VNF i1
502
VNF i2
502
VNF i3
502
500

FIG. 5

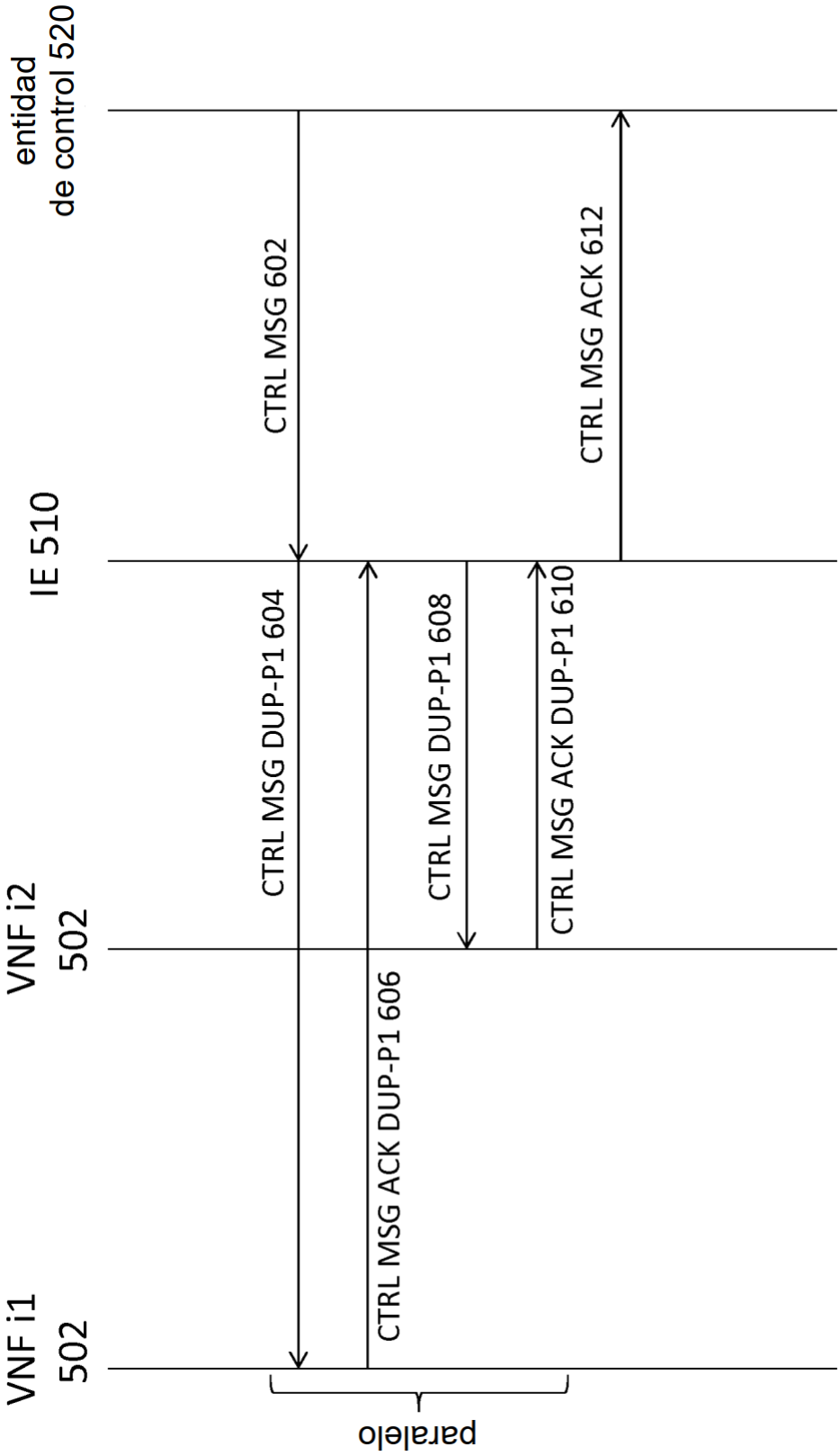
entidad de control 520
IE 510
VNF i2 502
VNF i1 502
CTRL MSG 602
CTRL MSG ACK 612
CTRL MSG DUP-P1 604
CTRL MSG DUP-P1 608
CTRL MSG ACK DUP-P1 610
CTRL MSG ACK DUP-P1 606
paralelo

FIG. 6

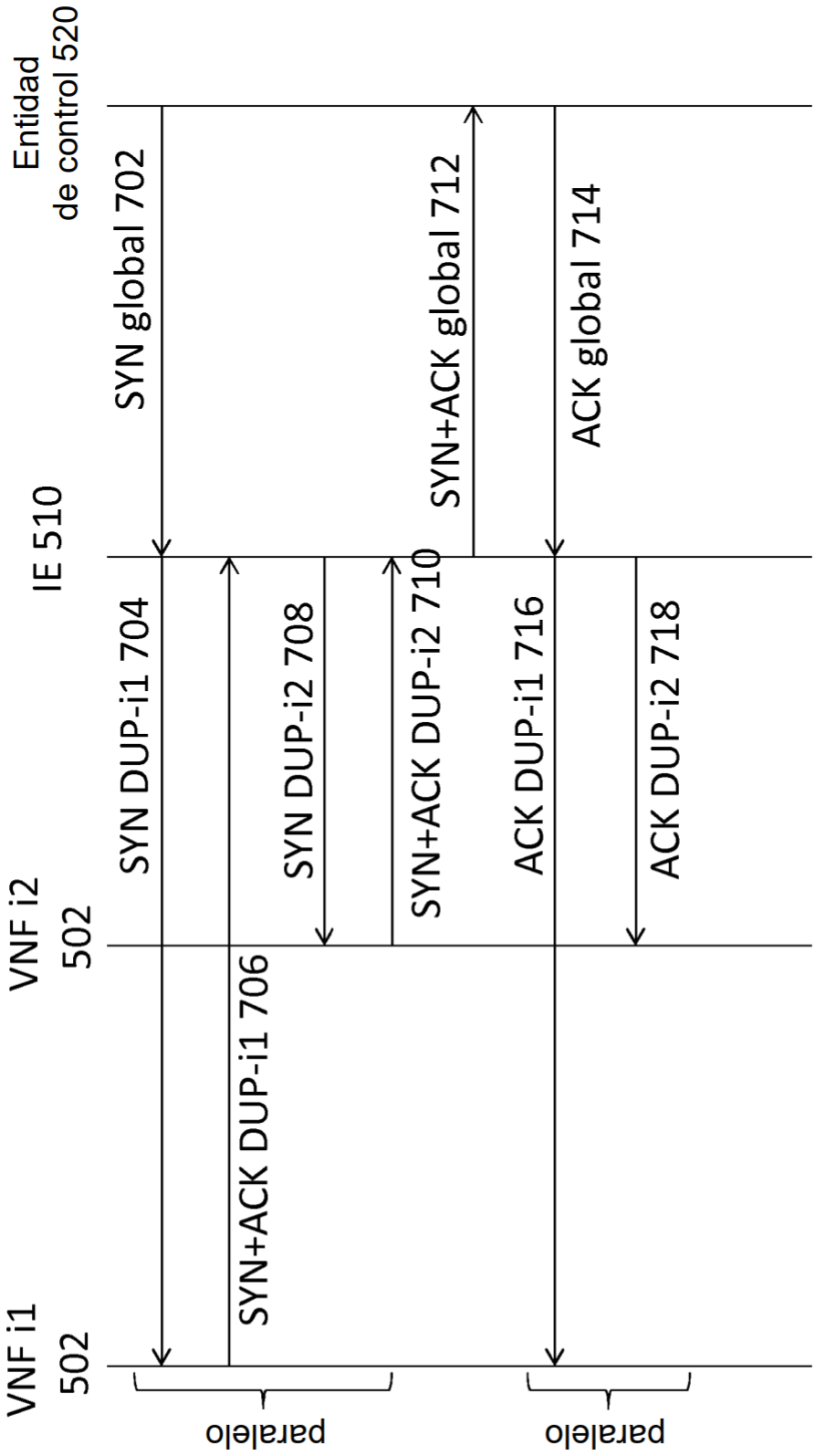
Entidad de control 520
IE 510
VNF i2 502
VNF i1 502
SYN global 702
SYN+ACK global 712
ACK global 714
SYN DUP-i1 704
SYN DUP-i2 708
SYN+ACK DUP-i2 710
ACK DUP-i1 716
ACK DUP-i2 718
SYN+ACK DUP-i1 706
paralelo
paralelo

FIG. 7

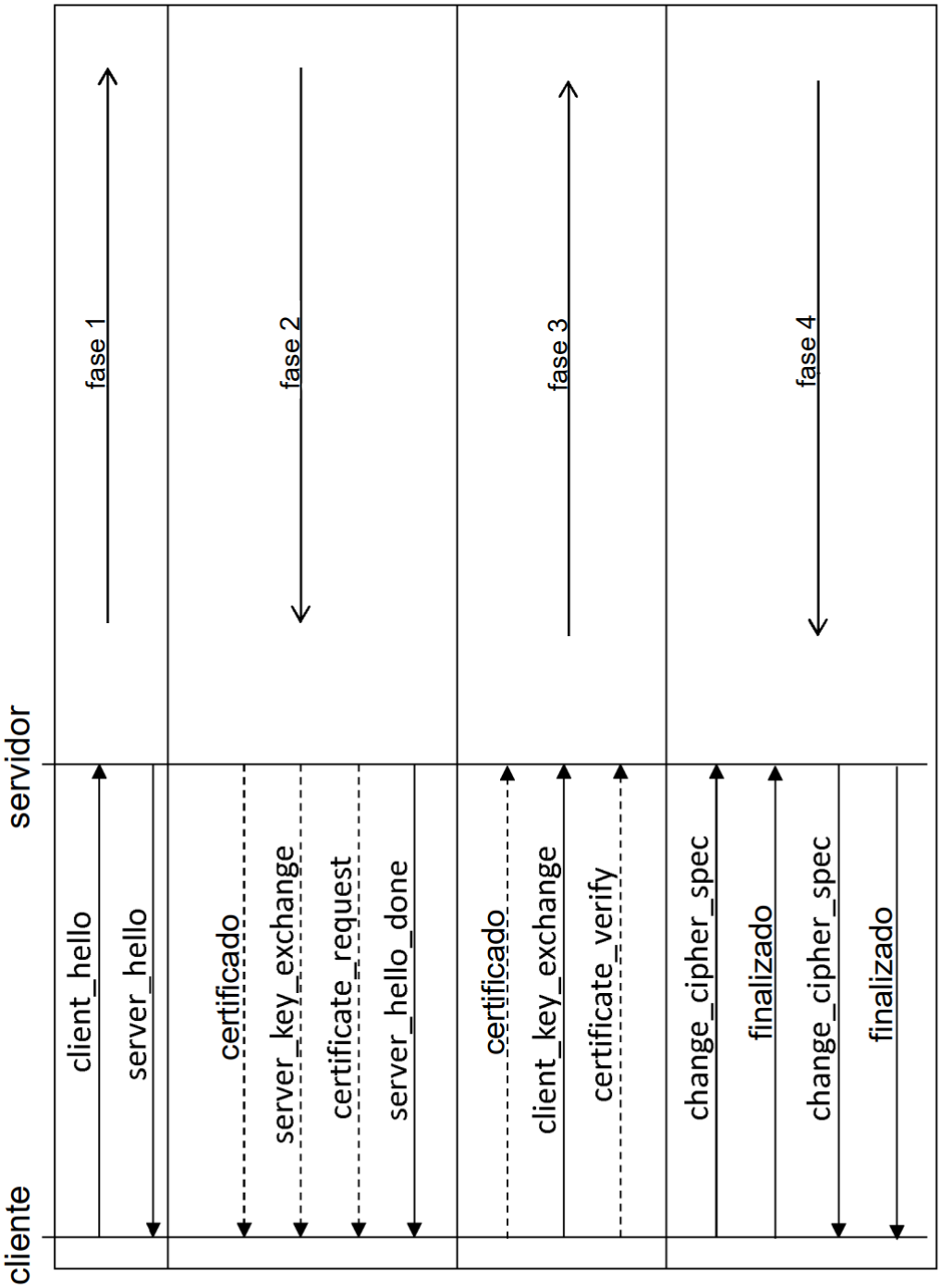
cliente
servidor
fase 1
fase 2
fase 3
fase 4
client_hello
server_hello
certificado
server_key_exchange
certificate_request
server_hello_done
certificado
client_key_exchange
certificate_verify
change_cipher_spec
finalizado
change_cipher_spec
finalizado

FIG. 8

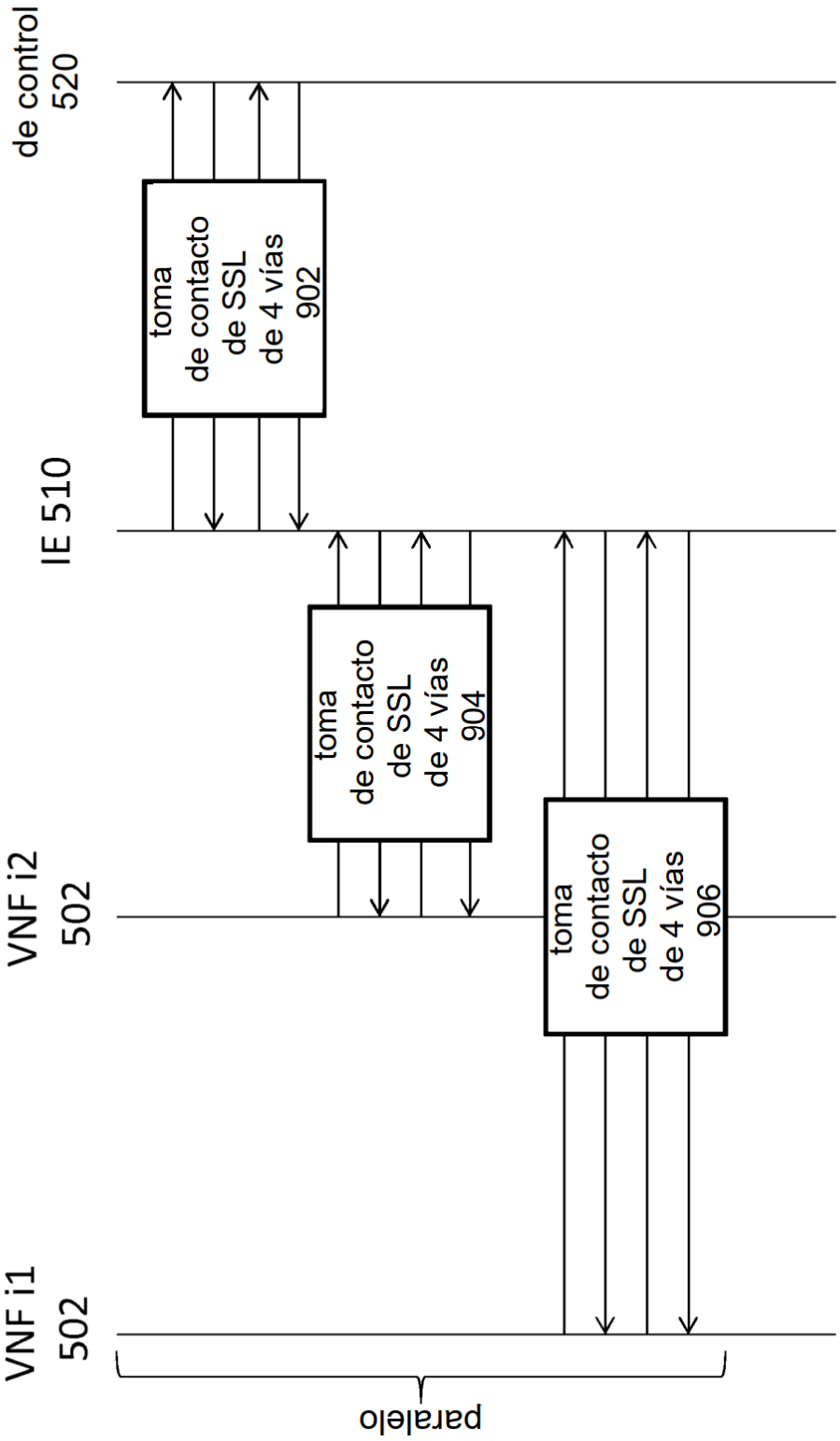
entidad de control 520
toma de contacto de SSL de 4 vías 902
IE 510
toma de contacto de SSL de 4 vías 904
VNF i2 502
toma de contacto de SSL de 4 vías 906
VNF i1 502
paralelo

FIG. 9

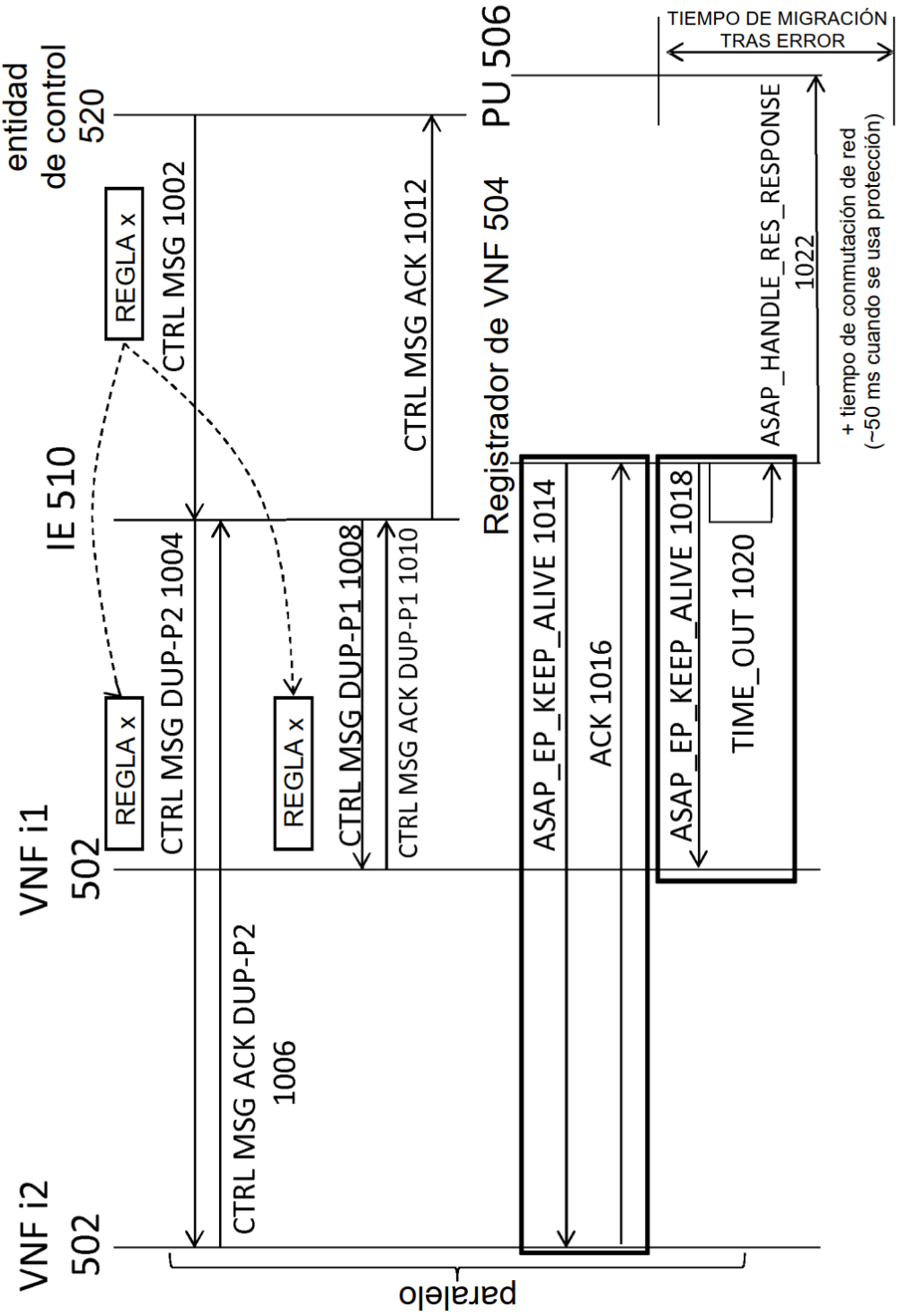
entidad de control 520
IE 510
VNF i1 502
VNF i2 502
PU 506
Registrador de VNF 504
TIEMPO DE MIGRACIÓN TRAS ERROR
REGLA x
CTRL MSG 1002
CTRL MSG ACK 1012
CTRL MSG DUP-P2 1004
CTRL MSG DUP-P1 1008
CTRL MSG ACK DUP-P1 1010
CTRL MSG ACK DUP-P2 1006
ASAP_EP_KEEP_ALIVE 1014
ACK 1016
ASAP_EP_KEEP_ALIVE 1018
TIME_OUT 1020
ASAP_HANDLE_RES_RESPONSE 1022
+ tiempo de conmutación de red (~50 ms cuando se usa protección)
paralelo

FIG. 10

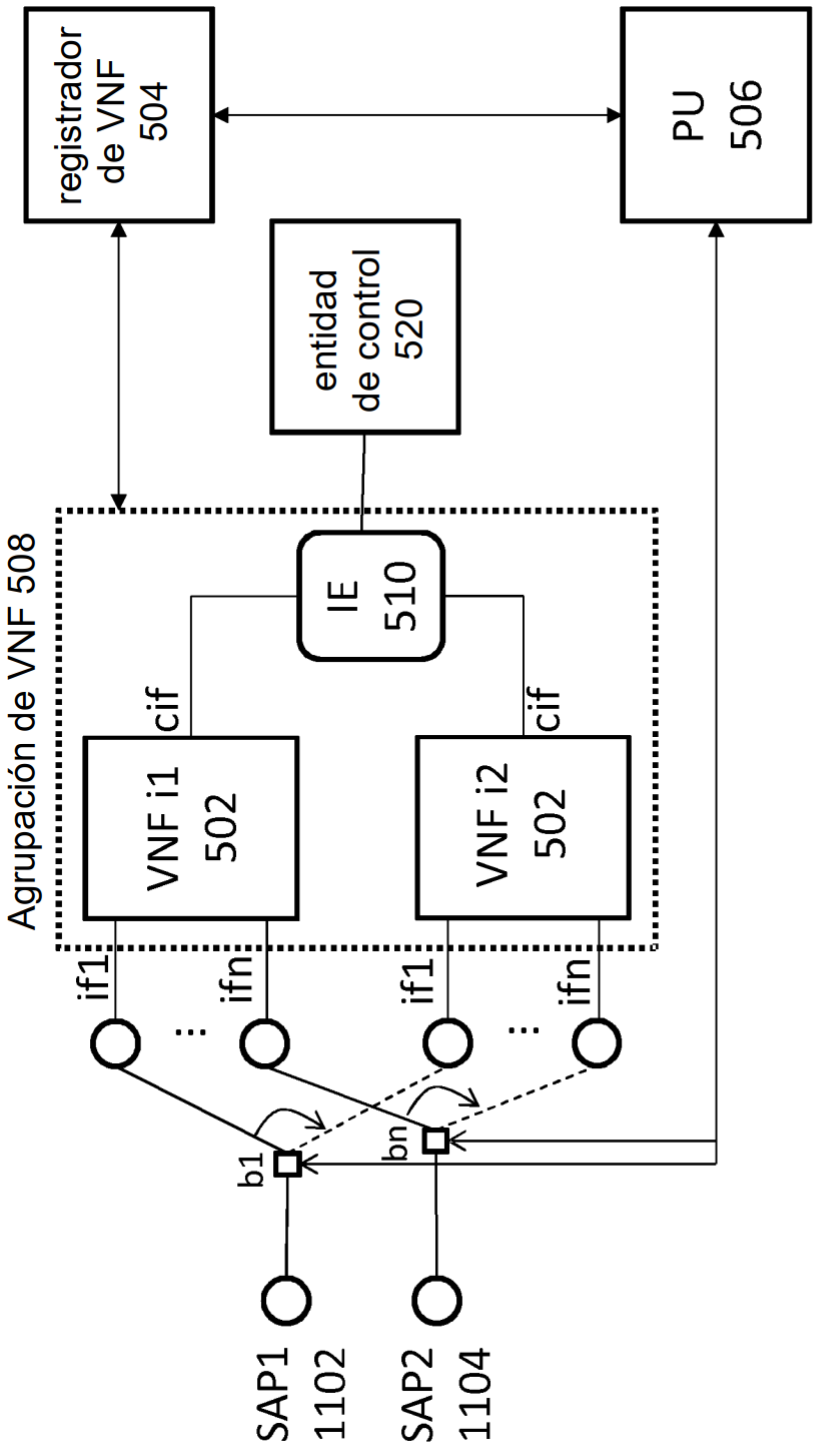
registrador de VNF 504
PU 506
entidad de control 520
IE 510
Agrupación de VNF 508
cif
cif
VNF i1 502
VNF i2 502
if1
ifn
if1
ifn
b1
bn
SAP1 1102
SAP2 1104
1100

FIG. 11

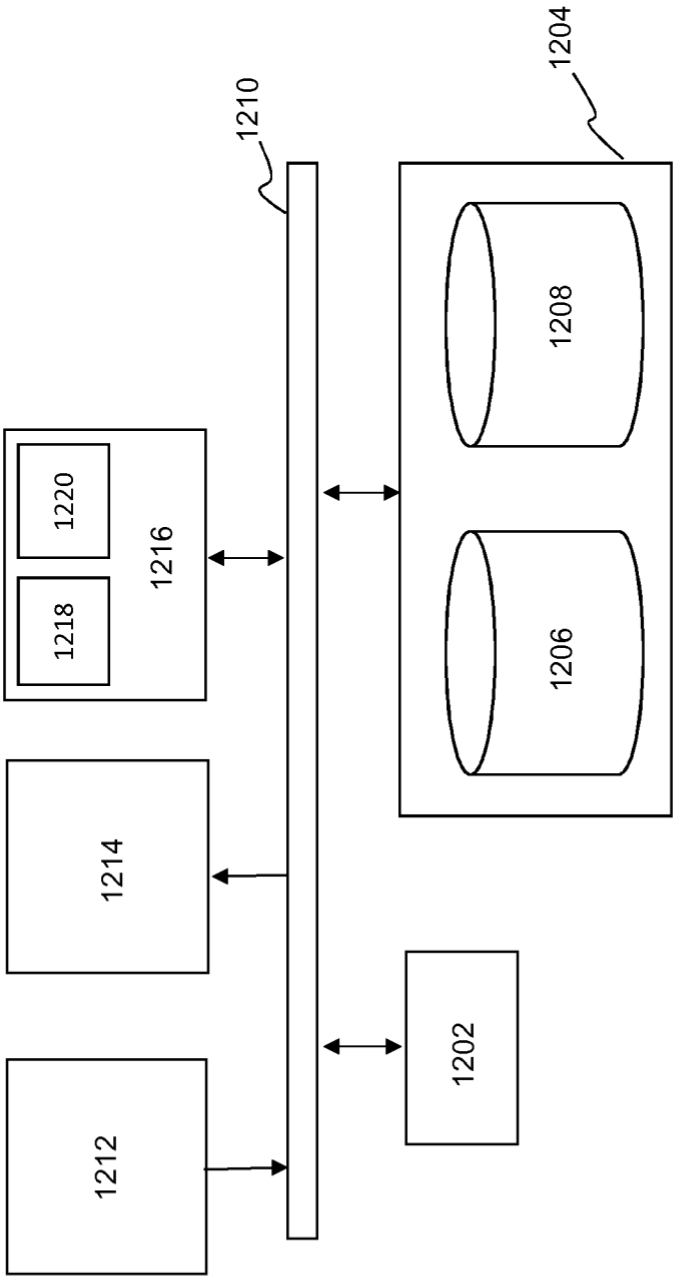

FIG. 12

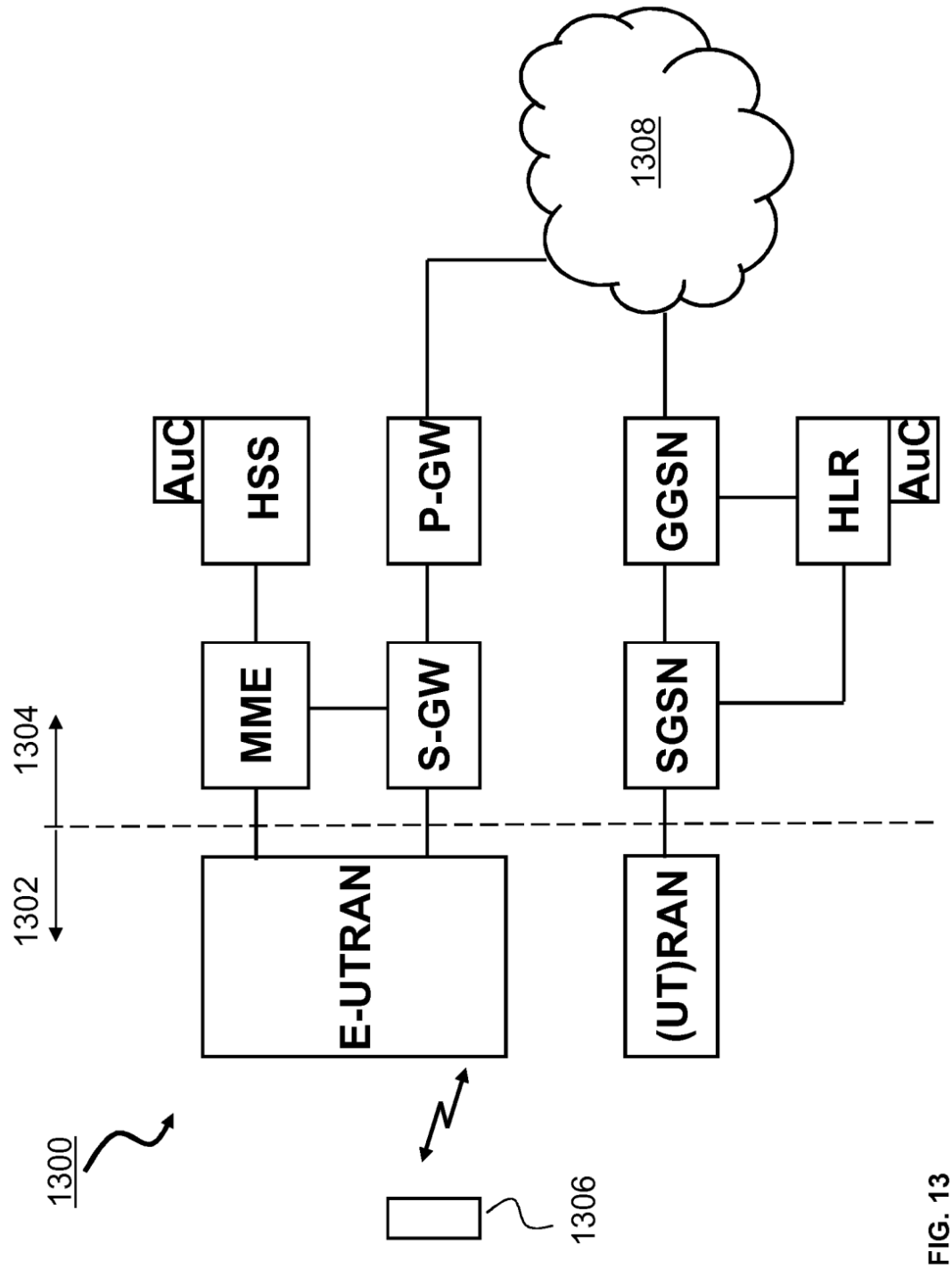
1308
AuC
HSS
P-GW
GGSN
HLR
AuC
MME
S-GW
SGSN
1304
1302
E-UTRAN
(UT)RAN
1300
1306

FIG. 13