(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 716 657**

(51) Int. CI.:

H04L 9/06 (2006.01)
H04L 9/32 (2006.01)
H04L 12/833 (2013.01)
H04L 12/801 (2013.01)
H04L 29/06 (2006.01)
H04L 12/70 (2013.01)
H04L 12/715 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.04.2016 E 16382153 (1)**

(97) Fecha y número de publicación de la concesión europea: **09.01.2019 EP 3229418**

(54) Título: **Un método para asegurar el recorrido de paquetes de datos correcto a través de una trayectoria particular de una red**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.06.2019

(73) Titular/es:

TELEFONICA, S.A. (100.0%)
Gran Via, 28
28013 Madrid, ES

(72) Inventor/es:

ARANDA GUTIÉRREZ, PEDRO A.;
LÓPEZ, DIEGO R. y
OREA BARRIOS, NORISY C.

(74) Agente/Representante:

ARIZTI ACHA, Monica

DESCRIPCIÓN

Un método para asegurar el recorrido de paquetes de datos correcto a través de una trayectoria particular de una red

Campo técnico

La presente invención se refiere, en general, al campo de Concatenación de Función de Servicio. En particular, la invención se refiere a un método para asegurar el recorrido de paquetes de datos correcto a través de una trayectoria particular de una red usando procedimientos criptográficos.

Antecedentes de la invención

Existe una necesidad de plataformas tecnológicas más flexibles y fáciles de desarrollar, con la capacidad de soportar migraciones desde entornos físicos a unos virtuales, y para el fin de desplegar modelos para funciones de servicio no estrechamente acopladas a la topología de red y recursos físicos. De esta manera sería posible hacerlo alejado de la naturaleza estática de los modelos de despliegue actuales que limitan la introducción de nuevos servicios o modificar los existentes y/o las funciones de servicio.

Para tratar los problemas anteriores, un mecanismo de arquitectura de red posible que facilita la definición y la creación de instancias de un conjunto ordenado de funciones de servicio y dirección posterior de tráfico a través de ellas es la arquitectura de Concatenación de Función de Servicio (SFC) [1]. Otras posibilidades incluyen puntos de unión como se usa en las plataformas en la nube del estado de la técnica [2].

La arquitectura de SFC se establece en independencia topológica de la topología de reenvío subyacente. En esta, como puede observarse en la Figura 1, los paquetes de datos se clasifican en el nodo de entrada para manejar mediante el conjunto requerido de Funciones de Servicio (SF) y a continuación se reenvían a través de ese conjunto ordenado de funciones para procesamiento mediante cada función a su vez. Como resultado de este procesamiento los paquetes tal vez se reclasifiquen.

La arquitectura de SFC incluye Reenviadores de Función de Servicio (SFF), como pueden observarse en la Figura 2, responsables de reenviar paquetes de datos recibidos desde la red a una o más SF asociadas con un SFF dado. El tráfico desde las SF eventualmente vuelve al mismo SFF, que es responsable de inyectar el tráfico de vuelta en la red.

El orden implicado puede no ser una progresión lineal ya que la arquitectura permite a las SFC copiar más de una rama, y permite también casos donde hay flexibilidad en el orden en el que se aplican las funciones de servicio.

La entrega de servicios de extremo a extremo a menudo requiere diversas SF que incluyen SF de red tradicional (por ejemplo, cortafuegos y balanceadores de carga de servidor, entre otros), así como características específicas de la aplicación tales como manipulación de encabezamiento de HTTP. Las SF pueden entregarse en el contexto de un usuario aislado (por ejemplo, un arrendatario) o compartirse entre muchos usuarios o grupos de usuarios.

Los modelos de despliegue actual para las SF están a menudo estrechamente acoplados a la topología de red y recursos físicos, dando como resultado por lo tanto despliegues relativamente rígidos y estáticos. La naturaleza estática de tales despliegues reduce enormemente y limita, en muchos casos, la capacidad de un operador para introducir nuevos servicios o modificar los existentes y/o las SF. Adicionalmente existe un efecto en cascada: cambiar uno o más elementos de una cadena de SF a menudo afecta a otros elementos en la cadena y/o los elementos de red usados para construir la cadena.

Este problema es particularmente grave en entornos de servicio elásticos que requieren creación, destrucción o movimiento relativamente rápidos de SF físicas o virtuales o elementos de red. Adicionalmente, el paso a plataformas virtuales requiere un modelo de inserción de servicio ágil que soporte entrega de servicio elástica y muy granular, modificación a posteriori y el movimiento de las SF y cargas de trabajo de aplicación en la red existente. El modelo de inserción de servicio debe retener también las políticas de red y servicio y la capacidad para unir fácilmente política de servicio a información granular tal como por estado de abonado.

Los despliegues de servicio de red no de SFC están acoplados a menudo a la topología de red, ya sea física, virtualizada o una híbrida de las dos. Tal dependencia impone restricciones en la entrega de servicio y limita la escala, capacidad y redundancia a través de los recursos de red, pero por otro lado permite a los operadores de redes y usuarios de servicio verificar la aplicación efectiva de los servicios requeridos para flujos de paquetes

verificando la topología.

A medida que se requieren más funciones de servicio -- a menudo con ordenación estricta -- son necesarios cambios de topología "delante" y "detrás" de cada SF, dando como resultado cambios de red y configuración de dispositivo complejos. En tales topologías, todo el tráfico, se necesite aplicar una SF o no, a menudo pasa a través del mismo orden estricto. Pero, de nuevo, esto proporciona un aseguramiento estricto de la aplicación de función.

La naturaleza dinámica de la arquitectura de SFC, que desacopla el servicio de las dependencias de la topología, soporta una configuración muy flexible y escalable de cómo se aplican los servicios a flujos de paquetes, pero limita la capacidad de una verificación efectiva de la aplicación real del procesamiento requerido tanto a flujos como a paquetes individuales. Existen casos de uso donde se requiere una fuerte evidencia de que cada paquete pasa a través de una trayectoria particular en una cadena, en particular en entornos sensibles a seguridad, y cada vez que se han de aplicar políticas de alta prioridad. Un caso arquetípico son servicios de red aplicados en entornos financieros.

Puesto que la práctica actual para proporcionar una fuerte evidencia de aplicación de SF en estos casos de uso requiere verificación física de concatenación de anfitrión y evidencia de topología directa, estos requisitos invalidan virtualmente (o al menos limitan seriamente) la aplicación de SFC en estos entornos.

Por lo tanto son necesarias más tecnologías para asegurar la aplicación efectiva de una cadena de las SF a los flujos de paquetes de datos que provienen desde una red para asegurar un orden dado de recorrido de las SF y para proporcionar fuerte evidencia de que los paquetes de datos han recorrido la trayectoria correcta en la cadena. El documento US20150333930, de 19 de noviembre de 2015 (2015-11-19), describe recursos computacionales distribuidos que pueden ser organizados en una plataforma de servicios para proporcionar determinados servicios con valor añadido – tal como inspección profunda de paquetes, transcodificación, intercepción legal -, o de otra manera utilizando un modelo de encadenamiento de la función de servicio

Referencias:

[1] [RFC7665] J. Halpern, Ed. y C. Pignataro, Ed., "Service Function Chaining (SFC) Architecture", RFC 7665, DOI 10.17487/RFC7665, octubre de 2015, <http://www.rfc-editor.org/info/rfc7665>.

[2] Centina Systems, "NFV and SDN Assurance; Monitor and optimize virtual networks comprehensively", http://www.centinasystems.com/solutions/nfv-and-sdn-assurance/

Descripción de la invención

Para este fin, las realizaciones de la presente invención proporcionan un método para asegurar el recorrido de paquetes de datos correcto a través de una trayectoria particular en una red, en el que dicha red está basada en una cadena de Funciones de Servicio (SF) individuales que están compuestas para implementar servicios de red. El método de una manera característica comprende: la asignación, en un nodo de entrada de una arquitectura de red, a al menos un paquete de datos recibido mediante dicho nodo de entrada desde la red, de una etiqueta criptográfica única; el procesamiento de la etiqueta criptográfica única asignada por medio de una función criptográfica específica para cada Función de Servicio (SF) particular; y la verificación final, en cualquier punto dado de la arquitectura de red, preferentemente en un nodo de salida de la misma, de la etiqueta criptográfica única procesada por medio de aplicar una función de verificación criptográfica.

De acuerdo con el método propuesto, dicha función de verificación criptográfica está compuesta mediante las funciones inversas de las funciones criptográficas asociadas a las SF recorridas mediante el paquete o paquetes de datos.

De acuerdo con la invención, las funciones criptográficas específicas para cada SF que pueden usarse pueden incluir: un Algoritmo de Firma Digital (DSA), un algoritmo SHA256, un Algoritmo de Firma Digital de Curva Elíptica (ECDSA), un algoritmo secp256k1, entre otros. Las diferentes SF pueden usar la misma o diferentes funciones criptográficas. Es decir, una SF dada puede usar un DSA mientras que la siguiente SF en la trayectoria puede usar un algoritmo secp256k1, o como alternativa, ambas SF en la trayectoria pueden usar la misma función criptográfica.

De acuerdo con una realización preferida, dicha arquitectura de red comprende una arquitectura de Cadena de Función de Servicio (SFC). En este caso particular, dicho procesamiento de la etiqueta criptográfica única asignada puede realizarse mediante cualquiera de los Reenviadores de Función de Servicio (SFF) o mediante las SF de la trayectoria particular cuando el paquete de datos se envía a cada SF, o como alternativa a cada intermediario de SF.

De acuerdo con una realización, la etiqueta criptográfica única asignada a un paquete de datos está incluida en un Encabezamiento de Función de Red (NSH) del paquete de datos. El NSH tiene una clave única que está asociada con cada SF. Preferentemente, la asignación de la etiqueta criptográfica única en el NSH se hace teniendo en cuenta un formato tipo-longitud-valor, TLV.

De acuerdo con una realización, se proporciona una plataforma de Concatenación de Bloques para asegurar la secuencia de procesamiento para el paquete o paquetes de datos recibidos desde la red. En este caso particular, cada transacción que entra en la arquitectura de red (por ejemplo la arquitectura de SFC) se usa para crear un bloque de la plataforma de Concatenación de Bloques que se agrega en la cadena y se replica en una arquitectura entre iguales descentralizada que comprende una pluralidad de nodos, en el que cada Trayectoria de Función de Servicio (SFP) de la arquitectura de red comprende un nodo.

De acuerdo con otra realización, la etiqueta criptográfica única no es parte de unos metadatos del paquete o paquetes de datos recibidos desde la red, en este caso, el método propuesto comprende proporcionar una plataforma de Concatenación de Bloques separada del plano de servicio de la arquitectura de red para asegurar la secuencia de procesamiento para el paquete o paquetes de datos, teniendo dichos metadatos una clave que está relacionada con un bloque correspondiente de la plataforma de Concatenación de Bloques.

Por lo tanto, la presente invención garantiza la secuencia correcta de procesamiento de paquete o paquetes de datos mediante una trayectoria de función de servicio, y de esta manera puede aprovechar la flexibilidad operativa y de gestión adicional de la arquitectura de red, reduciendo complejidad de las operaciones y el mantenimiento en plataformas de servicio de red avanzadas. Adicionalmente, la presente invención contribuye a mejorar la escalabilidad y reutilización de estas plataformas, con respecto a soluciones específicas basadas en modelos físicos.

Además, la presente invención garantiza la aplicación eficaz de las SF en una trayectoria de acuerdo con una arquitectura de red específica (preferentemente la arquitectura SFC), asegurando un orden dado de recorrido de las SF, con un nivel de aseguramiento equivalente (o incluso superior a) una verificación física de concatenación de anfitrión.

Además, la presente invención también posibilita maneras más potentes para gestionar plataformas de servicio de red virtualizadas con un flujo interno garantizado (u orden de ejecución de SF), y hace la SFC aplicable en casos donde esta ejecución garantizada se requiere estrictamente.

Breve descripción de los dibujos

Las anteriores y otras ventajas y características se entenderán más completamente a partir de la siguiente descripción detallada de las realizaciones, con referencia a las figuras adjuntas, que deben considerarse de una manera ilustrativa y no limitante, en las que:

La Figura 1 ilustra el flujo de tráfico básico para la arquitectura de SFC.

La Figura 2 ilustra la secuencia de procesamiento para paquetes de datos mediante los SFF.

La Figura 3 ilustra un flujo de un paquete de datos en la arquitectura de SFC para asegurar la secuencia de procesamiento de acuerdo con una realización preferida de la presente invención.

La Figura 4 ilustra un flujo de un paquete de datos en la arquitectura de SFC con aseguramiento de secuencia usando SFF de acuerdo con una realización de la presente invención.

La Figura 5 ilustra un flujo de un paquete de datos en la arquitectura de SFC con aseguramiento de secuencia usando las SF y/o Intermediarios de acuerdo con una realización de la presente invención.

Las Figuras 6a-6c ilustran el procesamiento de los paquetes de datos de la realización de la Figura 5 de acuerdo con el tipo de SF o el Intermediario respectivo. La Figura 6a ilustra el caso particular para una SF que es sensible a SFC y sensible a criptografía; La Figura 6b ilustra el caso particular para una SF que es sensible a SFC y no es sensible a criptografía; y la Figura 6c ilustra el caso particular para una SF que no es sensible a SFC y no es sensible a criptografía.

La Figura 7 ilustra una realización del método propuesto en el que se usa una plataforma de Concatenación de Bloques para asegurar la secuencia de procesamiento para paquetes de datos, en el que cada Trayectoria de

Función de Servicio (SFP) tiene un nodo que contiene la plataforma de Concatenación de Bloques.

La Figura 8 ilustra una realización del método propuesto en el que la etiqueta criptográfica única asignada no es parte de los metadatos del paquete de datos.

Descripción detallada de la invención y de realizaciones preferidas

De acuerdo con la invención, pueden usarse los siguientes elementos/entidades:

Cadena de Función de Servicio (SFC): define un conjunto ordenado de funciones de servicio abstractas y restricciones de ordenación que deben aplicarse a paquetes de datos y flujos seleccionados como resultado de la clasificación. Un ejemplo de una función de servicio abstracta es "un cortafuegos".

Función de Servicio (SF): una función de red que es responsable de tratamiento específico de paquetes de datos recibidos. Una SF puede actuar en diversas capas de una pila de protocolo (por ejemplo, en la capa de red u otras capas de OSI). Como un elemento lógico, una SF puede realizarse como un elemento virtual o embeberse en un elemento de red físico. Una o más Funciones de Servicio (SF) pueden embeberse en el mismo elemento de red. Una SF puede ser sensible a encapsulación de SFC (es decir, recibe y actúa sobre información en la encapsulación de SFC) o no sensible (caso en el que, los datos reenviados a la SF no contienen la encapsulación de SFC). Esto se hace referencia en las diferentes figuras de la invención como "sensible a SFC" y "no sensible a SFC", respectivamente. Una SF puede incluir: cortafuegos, DPI, NAT, función de Enriquecimiento de Encabezamiento de HTTP, optimizador de TCP, balanceador de carga, IDS, IPS, etc.

Encapsulación de SFC: la encapsulación de SFC proporciona, como mínimo, identificación de SFP, y se usa mediante las funciones sensibles a SFC, tal como las SF de SFF y sensibles a SFC. La encapsulación de SFC no se usa para reenvío de paquetes de red. Además de identificación de SFP, la encapsulación de SFC lleva metadatos que incluyen información de contexto del plano de datos.

Encabezamiento de Servicio de Red (NSH): una técnica para encapsulación de SFC definida mediante un encabezamiento común que codifica la identificación de SFP y metadatos usando preferentemente el formato TLV. Se define mediante el IETF I-D draft-ietf-sfc-nsh.

Intermediario SFC: elimina e inserta encapsulación de SFC en beneficio de una función de servicio no sensible a SFC. Los intermediarios de SFC son elementos lógicos.

Reenviador de Función de Servicio (SFF): un SFF es responsable de reenviar tráfico a una o más SF conectadas de acuerdo con información llevada en la Encapsulación de SFC, así como manejar tráfico que vuelve desde la SF. Adicionalmente, un SFF es responsable de entregar tráfico a un clasificador cuando sea necesario y se soporte, transportar tráfico a otro SFF (en el mismo o diferente tipo de solapamiento), y terminar la Trayectoria de Función de Servicio (SFP).

La Figura 3 muestra una realización preferida del método propuesto para el caso particular en el que la arquitectura de red es una arquitectura de Concatenación de Función de Servicio (SFC). De acuerdo con esta realización preferida, en primer lugar, los paquetes de datos desde una red se reciben mediante un nodo de entrada de la arquitectura de SFC para realizar la clasificación inicial, por lo que los paquetes se amplían con los metadatos apropiados, que incluyen la identificación de la Trayectoria de Función de Servicio (SFP) asignada que estos paquetes de datos deben seguir. Los Reenviadores de Función de Servicio (SFF) son responsables de reenviar los paquetes de datos recibidos a una o más Funciones de Servicio (SF) asociadas a los SFF particulares, aplicando los metadatos de SFC para los paquetes procesados. Finalmente, el método propuesto asegura el recorrido de paquetes de datos correcto a través de esa trayectoria particular en la cadena de servicio de red basada en SFC aplicando una función de verificación en el extremo de la trayectoria de SFC.

La presente invención proporciona dos opciones para asegurar la secuencia de procesamiento de paquetes de datos, una primera opción usando los SFF, y una segunda opción usando los diferentes tipos de SF y/o el Intermediario correspondiente (cuando esto se aplique).

La Figura 4 ilustra una realización del método propuesto para recorrido de cadena de servicio de red asegurado usando los SFF. En el flujo de paquetes de datos el método propuesto asegura la secuencia de procesamiento para paquetes de datos usando una etiqueta criptográfica única, que se asigna a cada paquete de datos que proviene desde la red en el nodo de entrada, y que se actualiza (es decir, procesa) mediante cada SFF en la trayectoria cuando se envía a cada SF (o como alternativa, a cada intermediario de SF). Preferentemente, la actualización se

realiza por medio de una función criptográfica que incluye, pero sin limitación, un DSA, un SHA256, un ECDSA, y/o un secp256k1. En este caso particular, el recorrido de trayectoria se consigue mediante un nodo de salida de la arquitectura de SFC que ejecuta una función de verificación en la etiqueta criptográfica única asignada inicialmente mediante el nodo de entrada. La función de verificación comprende la ejecución mediante dicho nodo de salida de una función de verificación criptográfica que es la función inversa de la función o funciones criptográficas previamente usadas.

La función de verificación se implementa preferentemente en la salida de la última SF en la trayectoria. Sin embargo, de acuerdo con la invención, el proceso de verificación puede implementarse en la salida de cualquier SFF en la trayectoria.

La Figura 5 ilustra otra realización del método propuesto para recorrido de cadena de servicio de red asegurado usando SF y/o Intermediario de SFC. La realización de la Figura 5 se diferencia de la realización de la Figura 4 en que la etiqueta criptográfica única asignada inicialmente en el nodo de entrada se actualiza mediante cada SF, o como alternativa mediante un Intermediario correspondiente (cuando esto se aplica, es decir la SF no es sensible a SFC). Se ha de observar que el mismo flujo puede estar presente en una trayectoria de SFC cuando se requiere más de un SFF.

De acuerdo con el tipo de SF (o el respectivo Intermediario) el procesamiento puede ser como se describe a continuación en las Figuras 6a-6c.

Con referencia a la Figura 6a, se ilustra en la misma el procesamiento para el caso de una SF que es sensible a SFC y sensible a criptografía. En este caso, el paquete de datos completo se reenvía desde el SFF a la SF, en la que procesa la etiqueta criptográfica única (CT en las figuras) antes de devolver el paquete de datos al SFF, que genera una nueva firma (CT' en las figuras) que prueba que el paquete de datos ha pasado a través de esta SF específica. Es decir, CT' es la etiqueta criptográfica única cuando el paquete de datos ha atravesado una respectiva SF.

Con referencia a la Figura 6b, se ilustra en la misma el procesamiento para el caso de una SF que es sensible a SFC y no es sensible a criptografía. En este caso, cuando el paquete de datos se reenvía a la SF, en primer lugar un Intermediario de Criptografía elimina la etiqueta criptográfica única asignada, este nuevo paquete de datos se reenvía a la SF y a continuación se devuelve al Intermediario de Criptografía para actualizar (es decir, procesar) la etiqueta criptográfica única asignada, que prueba que el paquete de datos ha pasado a través de esta SF específica.

Con referencia a la Figura 6c, se ilustra en la misma el procesamiento para el caso de una SF que no es sensible a SFC y no es sensible a criptografía. En este caso, la SF requiere dos intermediarios, uno de ellos que trata con metadatos de SFC y el otro con la etiqueta criptográfica única asignada, para el procesamiento del paquete de datos a través del SFC.

De acuerdo con una realización, la etiqueta criptográfica única se asigna en el Encabezamiento de Servicio de Red (NSH), (H como se denomina en las diferentes figuras), extendiendo por lo tanto la extensión normal del NSH. La etiqueta criptográfica de cada paquete de datos se obtiene a partir del contenido de paquete de datos y de los metadatos y una clave única que está asociada con cada SF en la trayectoria. La etiqueta criptográfica puede implementarse como un encabezamiento de contexto usando el formato TLV.

Por lo que, de acuerdo con dicha realización, el NSH comprenderá la siguiente información:

Encabezamiento Basado	Proporciona información acerca del encabezamiento de servicio y del protocolo de cabida útil.
Encabezamiento de Trayectoria de Servicio	Proporciona identificación de trayectoria y localización en una trayectoria.
Encabezamientos de Contexto	Lleva metadatos opacos e información codificada de longitud variable.

Etiqueta Criptográfica	Esta es la etiqueta criptográfica que se actualiza mediante los SFF en la trayectoria cuando se envía a cada SF. Puede implementarse como un encabezamiento de contexto usando el formato TLV, por ejemplo.

Tabla 1: NSH Extendido

Con referencia ahora a la Figura 7, esta figura ilustra otra realización del método propuesto en el que se usa una plataforma de Concatenación de Bloques para asegurar la secuencia de procesamiento para paquetes de datos. Cada transacción, activada mediante un paquete de datos que entra en la Arquitectura de SFC, se usa para crear un bloque de la plataforma de Concatenación de Bloques y este consiste en un encabezamiento (CT), es decir la etiqueta criptográfica única, que enlaza el bloque anterior y proporciona integridad para la plataforma de Concatenación de Bloques y un cuerpo (contenido de paquete de datos y metadatos) que contiene un registro de transacciones que se verificaron durante la creación de bloques.

Cada bloque se agrega en la cadena y se replica en una arquitectura entre pares descentralizada con nodos que están asociados con una SFP (tiene al menos un SFF y una SF), usando una plataforma de aplicaciones transaccionales que establece confianza, responsabilidad y transparencia mientras agiliza procesos empresariales y proporciona un contrato inteligente. Las transacciones necesitan autenticarse, y la criptografía es fundamental para estos procesos. Los pares de protocolo validan y cometen transacciones para alcanzar consenso.

Con referencia ahora a la Figura 8, esta figura ilustra otra realización del método propuesto en el que la etiqueta criptográfica única asignada no es parte de los metadatos del paquete de datos. Se proporciona una plataforma de Concatenación de Bloques separada de un plano de servicio de la arquitectura de SFC para asegurar la secuencia de procesamiento de paquetes de datos. Para este escenario los metadatos de paquetes de datos tienen una clave que está conectada con el bloque correspondiente.

Incluso aunque las realizaciones anteriores se han descrito para el caso de usar una arquitectura de SFC, el método propuesto, de acuerdo con las realizaciones alternativas, en este caso no ilustradas, puede implementar también otras arquitecturas de red tales como plataformas en la nube.

El alcance de la presente invención se define en el siguiente conjunto de reivindicaciones.

REIVINDICACIONES

1. Un método para asegurar el recorrido de paquetes de datos correcto a través de una trayectoria particular de una red, en el que dicha red está basada en una cadena de Funciones de Servicio, SF, individuales que están compuestas para implementar Servicios de Red, NS, estando el método **caracterizado porque** comprende:

- asignar, en cada nodo de entrada de una arquitectura de red, a al menos un paquete de datos recibido mediante dicho nodo de entrada desde la red, una etiqueta criptográfica única;

- procesar dicha etiqueta criptográfica única asignada usando una función criptográfica específica para cada Función de Servicio, SF; y

- verificar, en un punto dado de la arquitectura de red, dicha etiqueta criptográfica única procesada aplicando una función de verificación criptográfica, estando compuesta dicha función de verificación criptográfica mediante las funciones inversas de las funciones criptográficas asociadas con las SF recorridas mediante el al menos un paquete de datos.

2. El método de la reivindicación 1, en el que la etiqueta criptográfica única está asignada en un Encabezamiento de Función de Red, NSH, de dicho al menos un paquete de datos recibido, teniendo el NSH una clave única que está asociada con cada SF.

3. El método de la reivindicación 2, que comprende asignar la etiqueta criptográfica única teniendo en cuenta un formato tipo-longitud-valor, TLV.

4. El método de la reivindicación 1, en el que se proporciona una plataforma de Concatenación de Bloques para asegurar la secuencia de procesamiento para dicho al menos un paquete de datos recibido, en el que cada transacción activada mediante el al menos un paquete de datos que entra en la arquitectura de red se usa para crear un bloque de la plataforma de Concatenación de Bloques que se agrega en la cadena y se replica en una arquitectura entre iguales descentralizada con una pluralidad de nodos, en el que cada Trayectoria de Función de Servicio, SFP, de la arquitectura de red comprende un nodo.

5. El método de la reivindicación 1, en el que la etiqueta criptográfica única no es parte de un metadato del al menos un paquete de datos recibido, y el método comprende proporcionar una plataforma de Concatenación de Bloques separada de un plano de servicio de la arquitectura de red para asegurar la secuencia de procesamiento para el al menos un paquete de datos recibido, teniendo dichos metadatos una clave que está relacionada con un bloque correspondiente de la plataforma de Concatenación de Bloques.

6. El método de la reivindicación 1, en el que el punto dado es un nodo de salida de la arquitectura de red.

7. El método de cualquiera de las reivindicaciones anteriores, en el que la arquitectura de red comprende una arquitectura de Cadena de Función de Servicio, SFC.

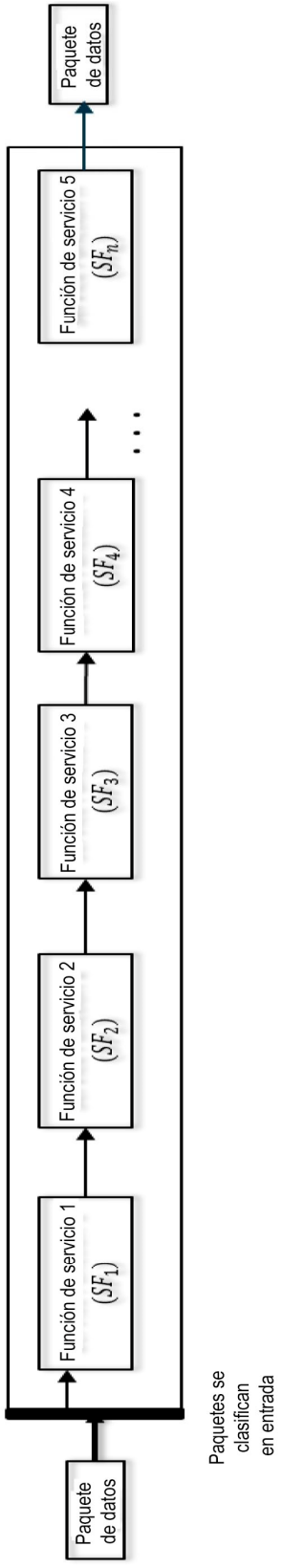

Paquete de datos
Función de servicio 5 (SF_n)
Función de servicio 4 (SF_4)
Función de servicio 3 (SF_3)
Función de servicio 2 (SF_2)
Función de servicio 1 (SF_1)
Paquetes se clasifican en entrada
Paquete de datos

Fig. 1

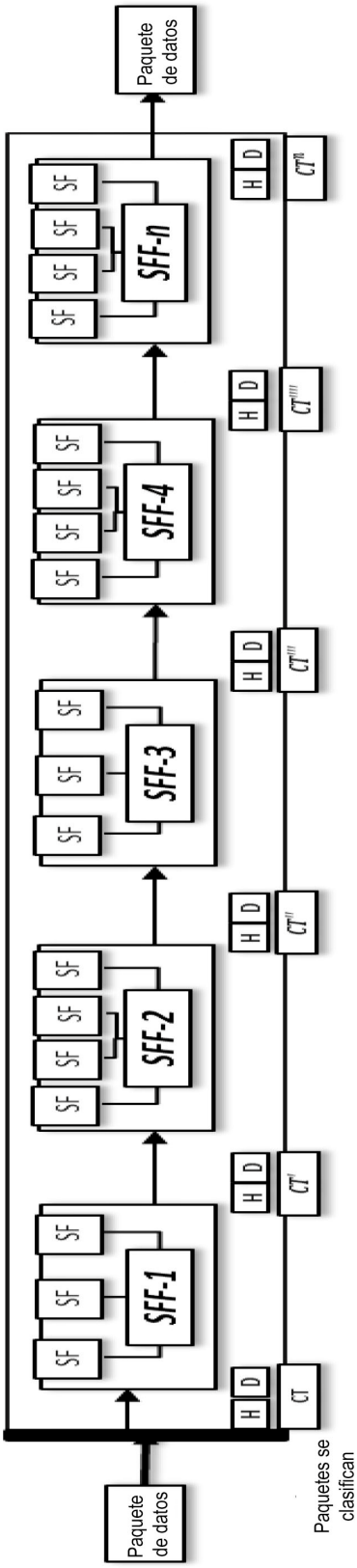

Paquete de datos
SFF-n
SFF-4
SFF-3
SFF-2
SFF-1
SF
H
D
CT
CT'
CT''
CT'''
CT''''
CT'n
Paquetes se clasifican en entrada
Paquete de datos

Fig. 2

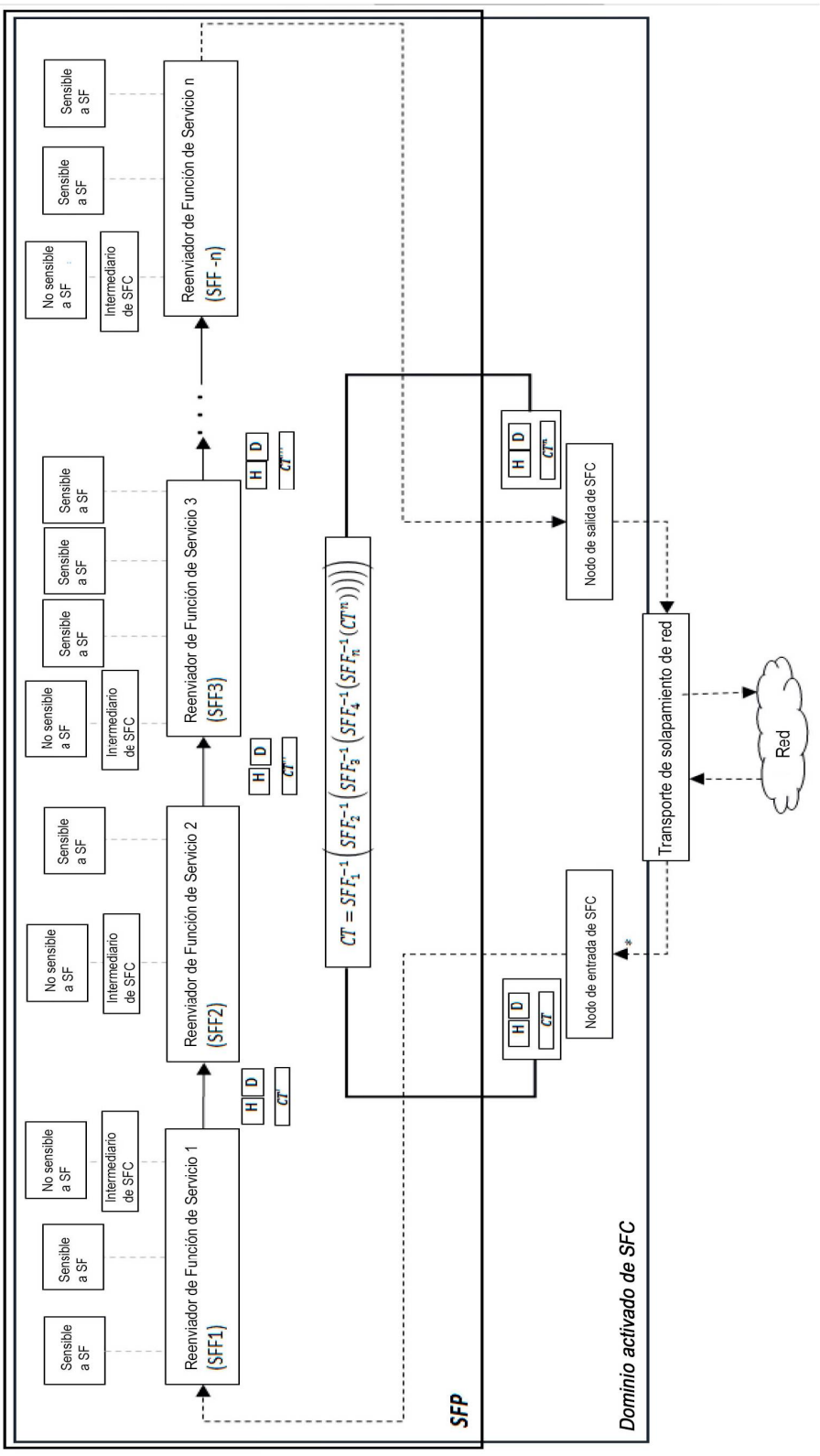

Reenviador de Función de Servicio 1
(SFF1)
Reenviador de Función de Servicio 2
(SFF2)
Reenviador de Función de Servicio 3
(SFF3)
Reenviador de Función de Servicio n
(SFF -n)
Sensible a SF
No sensible a SF
Intermediario de SFC
H
D
$CT = SFF_1^{-1}(SFF_2^{-1}(SFF_3^{-1}(SFF_4^{-1}(SFF_n^{-1}(CT^n)))))$
Nodo de entrada de SFC
Nodo de salida de SFC
Transporte de solapamiento de red
Red
SFP
Dominio activado de SFC

Fig. 3

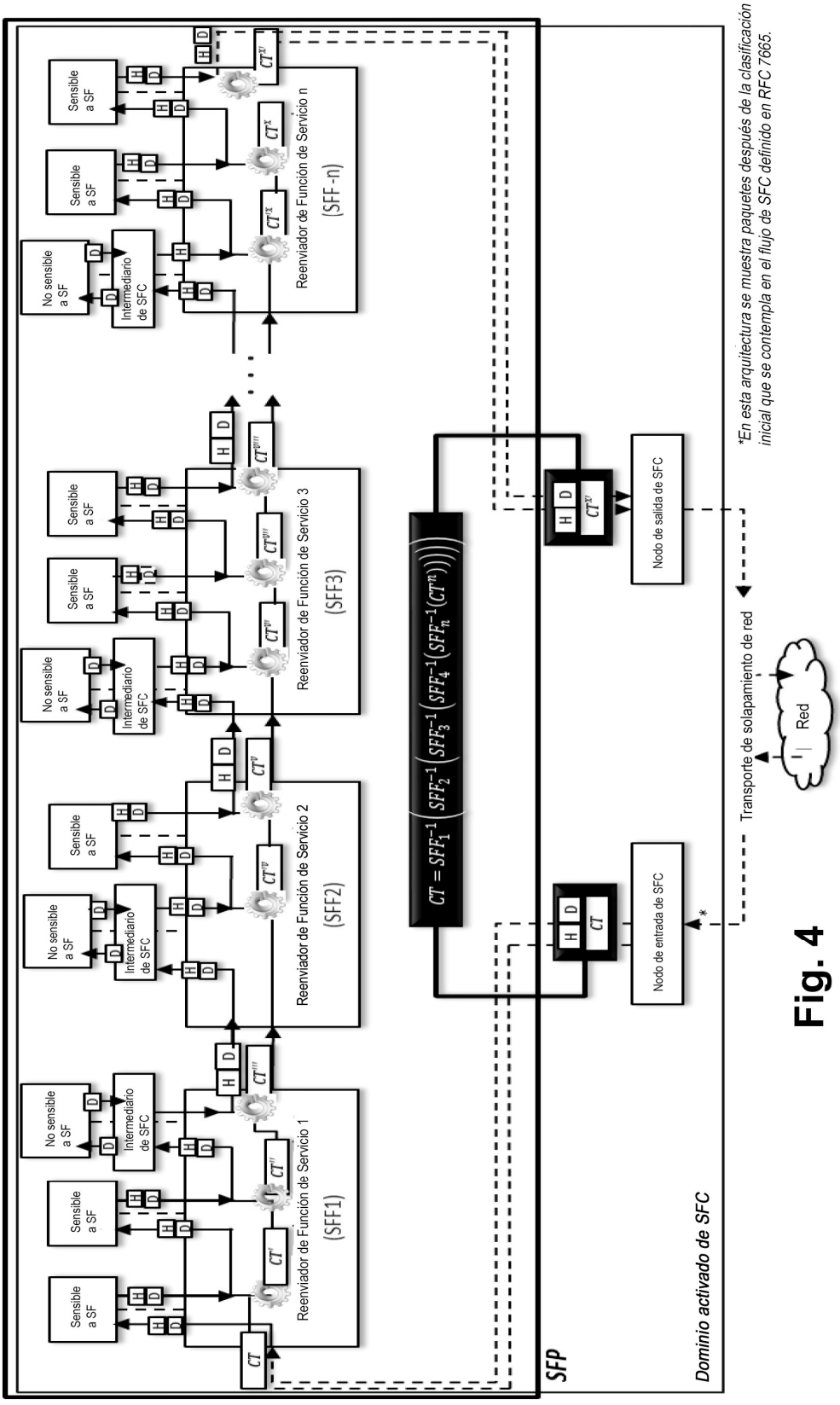

SFP
Dominio activado de SFC
Nodo de entrada de SFC
Nodo de salida de SFC
Transporte de solapamiento de red
Red
Reenviador de Función de Servicio 1
(SFF1)
Reenviador de Función de Servicio 2
(SFF2)
Reenviador de Función de Servicio 3
(SFF3)
Reenviador de Función de Servicio n
(SFF-n)
Sensible a SF
No sensible a SF
Intermediario de SFC
H
D
CT
$CT = SFF_1^{-1}\left(SFF_2^{-1}\left(SFF_3^{-1}\left(SFF_4^{-1}\left(SFF_n^{-1}(CT^n)\right)\right)\right)\right)$
*En esta arquitectura se muestra paquetes después de la clasificación inicial que se contempla en el flujo de SFC definido en RFC 7665.

Fig. 4

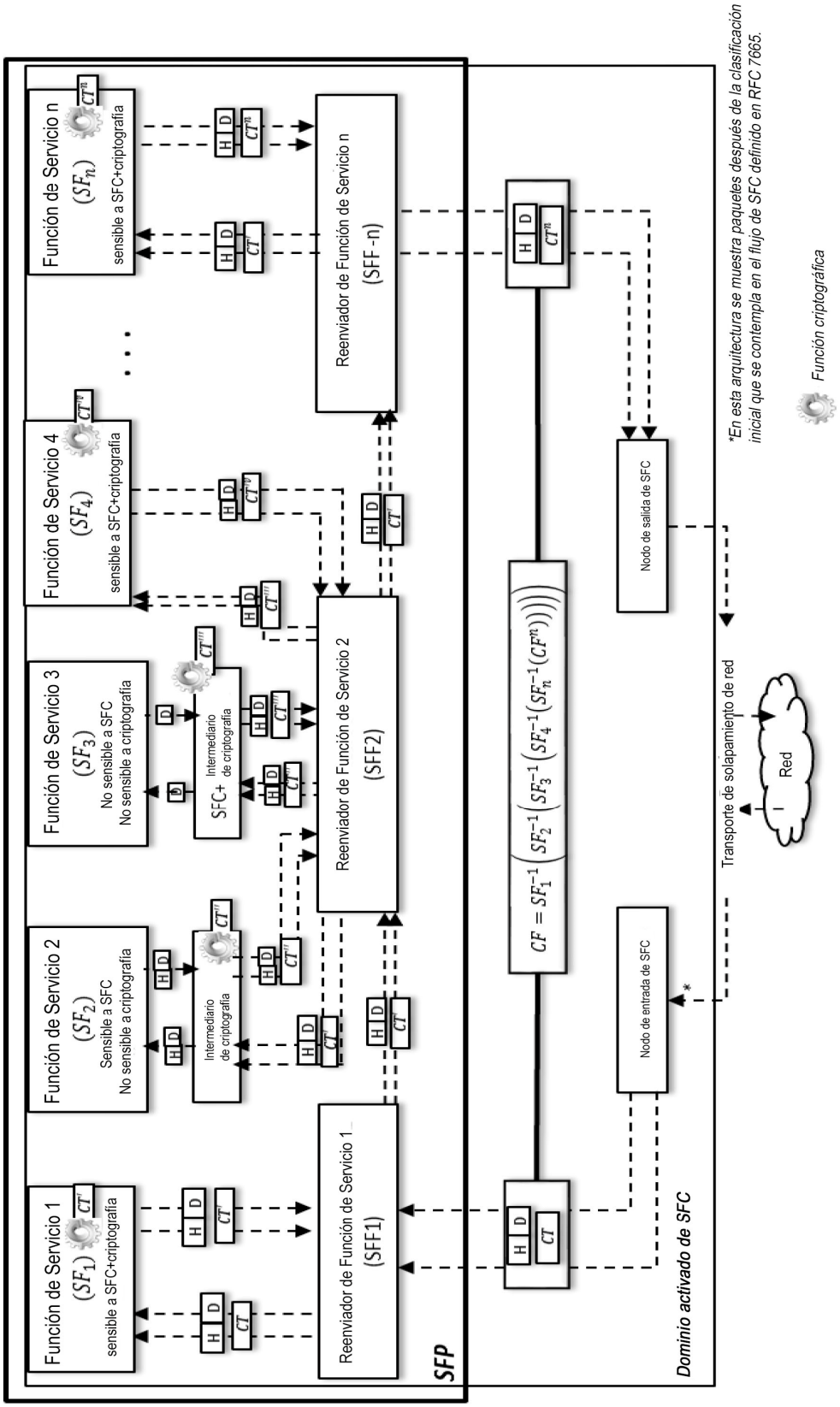

Función de Servicio 1
(SF_1)
sensible a SFC+criptografía
Función de Servicio 2
(SF_2)
Sensible a SFC
No sensible a criptografía
Función de Servicio 3
(SF_3)
No sensible a SFC
No sensible a criptografía
Función de Servicio 4
(SF_4)
sensible a SFC+criptografía
Función de Servicio n
(SF_n)
sensible a SFC+criptografía
Reenviador de Función de Servicio 1
(SFF1)
Reenviador de Función de Servicio 2
(SFF2)
Reenviador de Función de Servicio n
(SFF -n)
Intermediario de criptografía
SFC+ Intermediario de criptografía
Nodo de entrada de SFC
Nodo de salida de SFC
$CF = SF_1^{-1}\left(SF_2^{-1}\left(SF_3^{-1}\left(SF_4^{-1}\left(SF_n^{-1}(CF^n)\right)\right)\right)\right)$
Transporte de solapamiento de red
Red
SFP
Dominio activado de SFC
*En esta arquitectura se muestra paquetes después de la clasificación inicial que se contempla en el flujo de SFC definido en RFC 7665.
Función criptográfica

Fig. 5

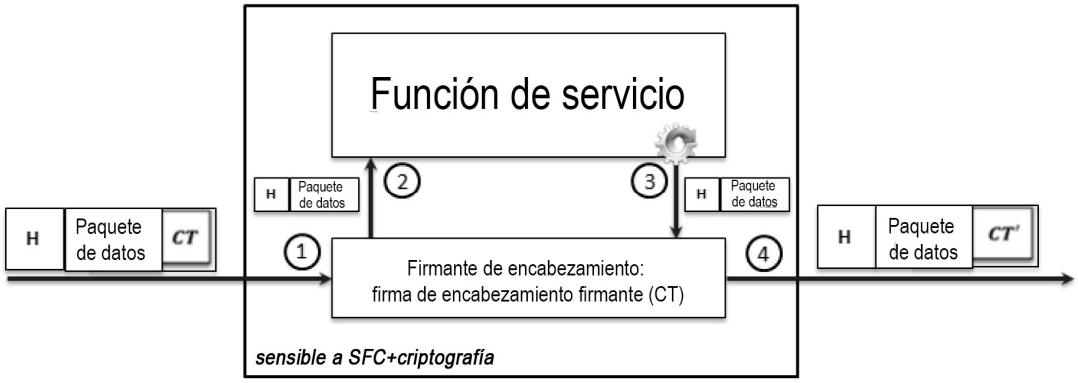

Función de servicio
H
Paquete de datos
CT
1
2
3
4
Firmante de encabezamiento: firma de encabezamiento firmante (CT)
CT'
sensible a SFC+criptografía

Fig. 6a

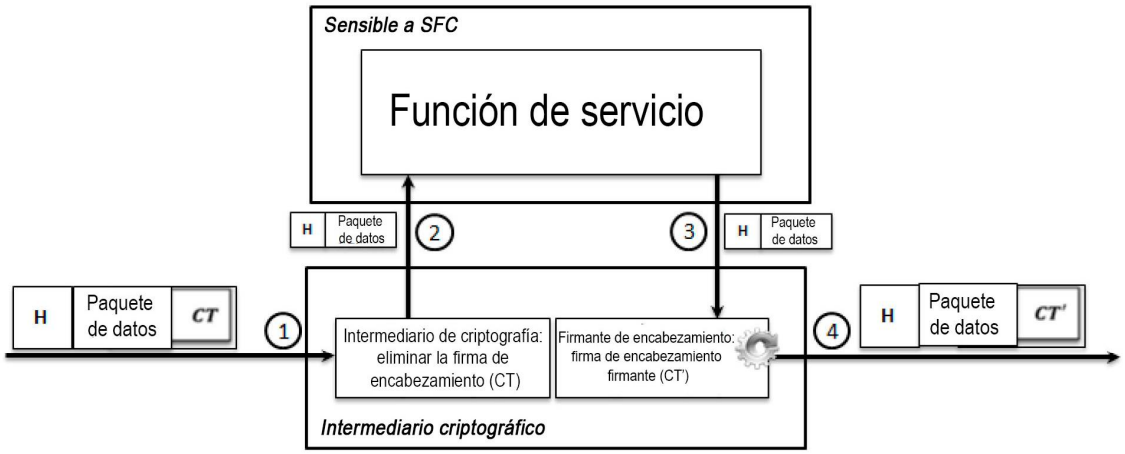

Sensible a SFC
Función de servicio
H
Paquete de datos
CT
1
2
3
4
Intermediario de criptografía: eliminar la firma de encabezamiento (CT)
Firmante de encabezamiento: firma de encabezamiento firmante (CT')
CT'
Intermediario criptográfico

Fig. 6b

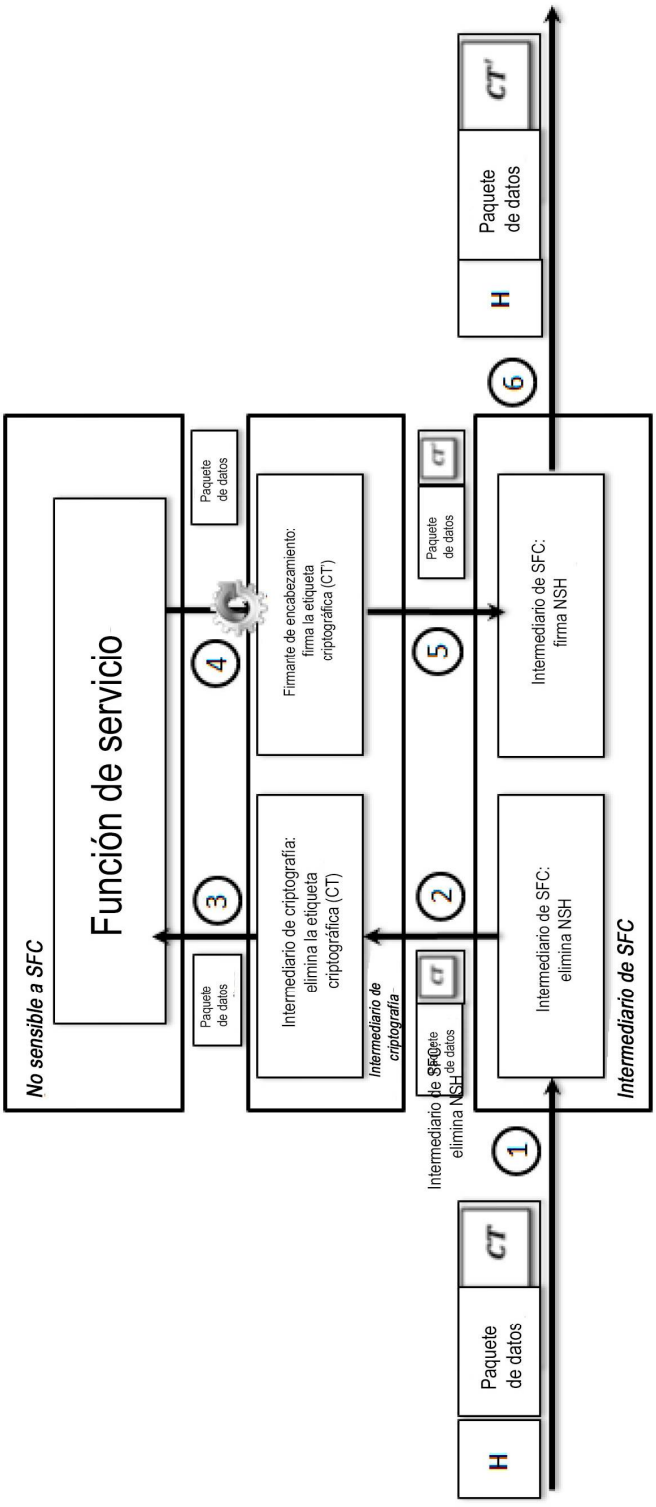
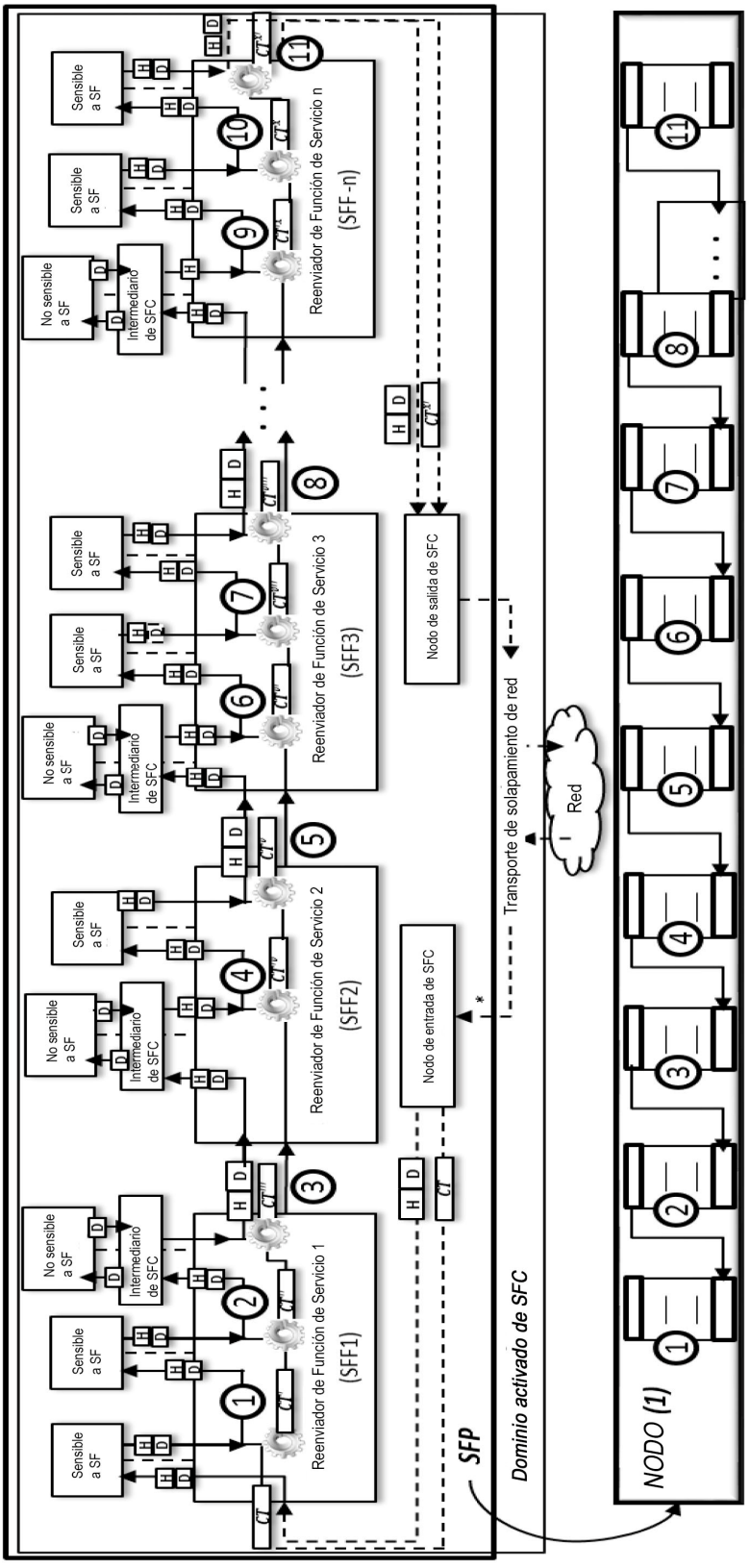

No sensible a SFC
Función de servicio
Paquete de datos
Intermediario de criptografía
Intermediario de criptografía: elimina la etiqueta criptográfica (CT)
Firmante de encabezamiento: firma la etiqueta criptográfica (CT)
Intermediario de SFC
Intermediario de SFC: elimina NSH
Intermediario de SFC: firma NSH
H
CT
CT'
1
2
3
4
5
6

Fig. 6c



*En esta arquitectura se muestra paquetes después de la clasificación inicial que se contempla en el flujo de SFC definido en RFC 7665.

Función criptográfica

Fig. 7

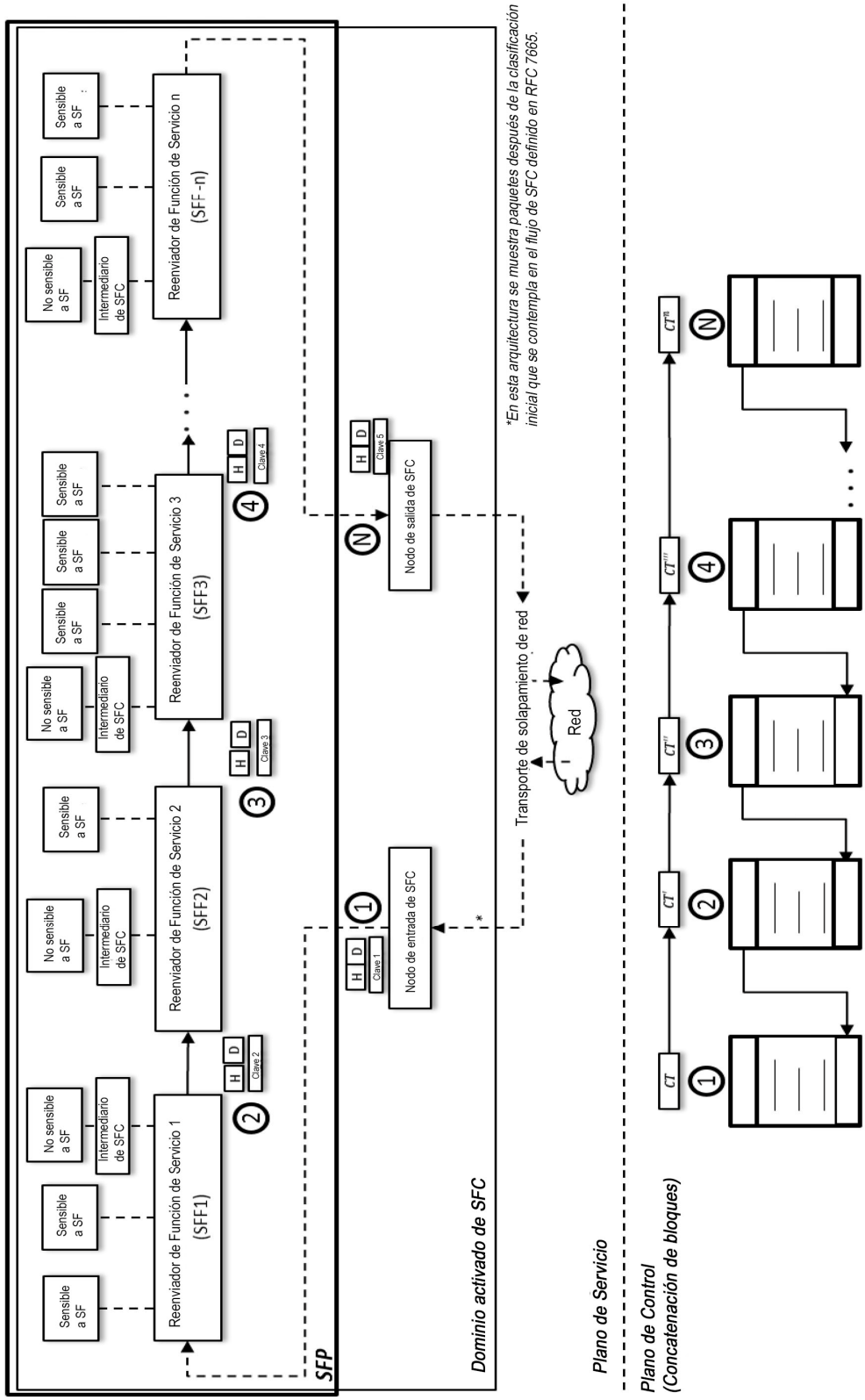

SFP
Reenviador de Función de Servicio 1 (SFF1)
Reenviador de Función de Servicio 2 (SFF2)
Reenviador de Función de Servicio 3 (SFF3)
Reenviador de Función de Servicio n (SFF-n)
Sensible a SF
No sensible a SF
Intermediario de SFC
H D
Clave 1
Clave 2
Clave 3
Clave 4
Clave 5
Nodo de entrada de SFC
Nodo de salida de SFC
Transporte de solapamiento de red
Red
*En esta arquitectura se muestra paquetes después de la clasificación inicial que se contempla en el flujo de SFC definido en RFC 7665.
Dominio activado de SFC
Plano de Servicio
Plano de Control (Concatenación de bloques)
CT
CT'
CT''
CT'''
CT'n

Fig. 8