(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 385 531**

(51) Int. CI.:

H04L 12/46 (2006.01)
H04L 29/08 (2006.01)
H04L 29/12 (2006.01)
H04L 29/06 (2006.01)
H04L 12/28 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08847163 .6**
(96) Fecha de presentación: **24.10.2008**
(97) Número de publicación de la solicitud: **2207321**
(97) Fecha de publicación de la solicitud: **14.07.2010**

(54) Título: **Un método de acceso, sistema y equipo de sesión de la capa 3**

(30) Prioridad:
29.10.2007 CN 200710165461

(45) Fecha de publicación de la mención BOPI:
26.07.2012

(45) Fecha de la publicación del folleto de la patente:
26.07.2012

(73) Titular/es:
Huawei Technologies Co., Ltd.
Huawei Administration Building Bantian
Longgang District, Shenzhen
Guangdong 518129 , CN

(72) Inventor/es:
YANG, Zhenting

(74) Agente/Representante:
Lehmann Novo, Isabel

DESCRIPCIÓN

Un método de acceso, sistema y equipo de sesión de la capa 3.

Campo de la invención

La presente invención está relacionada con el campo de las comunicaciones y, más específicamente, con un método, un sistema y un equipo para acceder a una sesión de capa 3.

Antecedentes

Una Red Privada Virtual a través de Teléfono (VPDN) utiliza una función de llamada de la red pública para establecer una Red Privada Virtual, de modo que proporciona un servicio de acceso a las empresas, pequeños Proveedores de Servicio de Red (NSP), y aquellos en oficinas móviles. La VPDN establece una red privada segura para una empresa en la red pública utilizando un protocolo de comunicación cifrado de red privada. Las oficinas regionales y el personal de la empresa en viaje de negocios puede conectarse con las oficinas centrales de la empresa sobre la red pública utilizando un túnel de cifrado virtual; mientras que otros usuarios de la red pública no pueden pasar por el túnel virtual para acceder a recursos internos dentro de una intranet.

En la actualidad, el funcionamiento más habitual es mediante un mecanismo del Protocolo de Túnel de la Capa Dos (L2TP). Por ejemplo, la solicitud de patente de los EE.UU. Núm. 2003/163577A1 está relacionada con un sistema de seguridad para acceder a un servicio de red privada basado en L2TP. LAU J y otros: “Layer Two Tunneling Protocol-Version 3 (versión 3 del Protocolo de Túnel de la Capa Dos) (L2TPv3); rfc3931.txt” del IETF, publicado el 1 de marzo de 2005, introduce una tercera versión del Protocolo de Túnel de la Capa Dos que define el protocolo de control básico y la encapsulación de múltiples conexiones de túnel de la Capa 2 entre dos nodos IP. En la Figura 1 se ilustra el procedimiento de acceso del Protocolo Punto a Punto (PPP) mediante el L2TP. El procedimiento de acceso incluye los siguientes pasos.

Paso s101: un usuario remoto inicia una llamada PPP sobre Ethernet (PPPoE) utilizando un Equipo en las Instalaciones del Cliente (CPE) en un cliente con PPPoE integrado. Para establecer una sesión PPPoE, el CPE negocia con una Pasarela de Red de Banda Ancha (BNG), un Servidor de Acceso de Red (NAS) en una red de acceso como, por ejemplo, un Servidor de Acceso Remoto de Banda Ancha (BRAS), por ejemplo, un equipo Concentrador de Acceso L2TP (LAC).

Paso s102: en la red de acceso, el CPE inicia una autenticación PPP frente a un dispositivo, NAS 1.

Paso s103: el NAS 1 de la red de acceso solicita autenticación y autorización de acceso a un servidor de Autenticación, Autorización y Registro (AAA) de la red de acceso, y obtiene información de una red de origen del usuario, por ejemplo, una dirección de NAS 2 de la red de origen del usuario, por ejemplo una red IP de un Servidor de Red L2TP (LNS).

Paso s104: el NAS (LAC) 1 establece un túnel L2TP con el NAS 2 (LNS) de la red de origen del usuario.

Paso s105: para autenticar al usuario, el NAS 1 envía al NAS 2 (LNS) información de autenticación PPP del usuario a través de un mensaje L2TP.

Paso s106: el NAS 2 solicita al servidor AAA 2 de la red de origen del usuario la autenticación y autorización de acceso del usuario.

Paso s107: la autenticación llevada a cabo por el servidor AAA 2 es satisfactoria y, por lo tanto, el usuario es autorizado para acceder a la red a través del túnel y, a continuación, el NAS 2 establece una sesión PPP y una sesión L2TP. De este modo, el usuario accede a la red a través de la sesión PPP y utiliza el servicio.

Debido a que el tratamiento del acceso de la propia sesión PPP tiene muchas limitaciones, en los desarrollos futuros se convierte en tendencia un nuevo mecanismo de acceso de Sesión de Capa 3 (por ejemplo, IP). La Sesión IP representa una sesión de conexión a la que se accede a través de una red junto con una dirección IP del usuario. La sesión IP equivale a la sesión PPP, y es una sesión basada en IP. Además, la Sesión IP normalmente termina en un equipo final IP o en un equipo NAS (BNG/BRAS), es decir, la Sesión IP es una conexión de sesión establecida entre el equipo de usuario y el equipo final IP. La dirección IP asignada a la sesión de acceso es fundamental para identificar la Sesión IP. Más aún, normalmente el servidor del Protocolo de Configuración Dinámica de Equipos de Red (DHCP) asigna dinámicamente la dirección IP, y la red utiliza la Sesión IP para gestionar el acceso del usuario a la red, por ejemplo, registro, etc.

En las técnicas convencionales, el procedimiento para generar la Sesión IP basándose en DHCP se ilustra en la Figura 2. El procedimiento incluye los siguientes pasos.

Paso S201: un cliente DHCP envía un mensaje Discovery (descubrimiento) del DHCP.

Paso s202: un Nodo de Acceso (AN) que incluye una función de transmisión DHCP detecta el mensaje Discovery de

DHCP, inserta en el mensaje la información de localización del acceso y, a continuación, reenvía el mensaje a un equipo final IP que incluye una función de transmisión DHCP/proxy (intermediario) de AAA.

Paso s203: el equipo final IP envía al servidor AAA una petición de acceso.

Paso s204: el servidor AAA envía una confirmación de acceso al equipo final IP.

Paso s205: el equipo final IP autoriza la Sesión IP.

Paso s206: el equipo final IP envía al servidor DHCP el mensaje Discovery del DHCP.

Paso s207: el servidor DHCP devuelve al equipo final IP un mensaje Offer (oferta) del DHCP.

Paso s208: el cliente DHCP envía al servidor DHCP un mensaje Request (petición) del DHCP.

Paso s209: el servidor DHCP devuelve al cliente DHCP un mensaje Ack (de confirmación) del DHCP. Esto es, se establece la sesión IP.

También se proporcionan otras técnicas convencionales relacionadas. Por ejemplo, el documento EP 1628458A1 está orientado a un método para la transmisión de paquetes IP entre redes del cliente y redes del proveedor IP utilizando una red de acceso. En particular, un elemento de red de la red de acceso realiza los siguientes pasos: creación de una conexión de capa 2 entre una red del proveedor y una red del cliente utilizando una dirección IP del cliente; creación de una conexión de servicio; asignación de una sesión IP activa y; transmisión de paquetes IP entre las sesiones IP activas de las conexiones de servicio. El documento WO 2002/078253A2 está orientado a una red de acceso que utiliza el protocolo de transmisión de Capa 2 entre un LAC y un LSN. El documento “Migration to Ethernet-Based DSL Aggregation” (migración a agregación DSL basada en Ethernet) del Forum DSL, publicado en abril de 2006, trata de un método para permitir un proceso de migración tan fácil como sea posible desde una red de agregación basada en ATM a una red de agregación basada en Ethernet.

En la implementación de la presente invención, el inventor descubre que las técnicas convencionales tienen los siguientes problemas: no se propone ningún método de acceso VPDN en función de la sesión IP de acceso.

Resumen

Se proporciona un método, un sistema y un equipo para acceder a una sesión de Capa 3 de acuerdo con algunos modos de realización de la presente invención, en los que se propone una sesión unificada de Capa 3 para el acceso para tratar la cuestión de una interconexión entre la técnica de enlace de Capa 2 de la red de acceso y aquella de la red de origen del usuario.

De acuerdo con un aspecto de la presente invención se proporciona un método de acceso de sesión basado en Capa 3 para una Red Privada Virtual a través de Teléfono, VPDN. El método incluye los siguientes pasos:

establecer, por parte de un concentrador de sesiones de acceso (SAC) en una red de acceso de un usuario, una sesión de acceso con un sistema remoto;

establecer, por parte del SAC, una sesión del Protocolo de Transporte de Sesión (STP) con un servidor de sesión de red (SNS) en la red de origen del usuario;

establecer, por parte del SAC, una relación de correspondencia entre la sesión de acceso del sistema remoto y la sesión STP, en donde la relación de correspondencia que establece el paso comprende, además, el establecimiento de la relación de correspondencia de un ID de sesión de acceso del sistema remoto, y/o un ID de la capa física o de la capa de enlace de la sesión de acceso, con un túnel STP, y un ID de la sesión STP; y reenviar, por parte del SAC, mensajes entre el sistema remoto y el SNS de acuerdo con la relación de correspondencia.

También se proporciona un sistema para acceder a una sesión de Capa 3 de acuerdo con otro aspecto de la presente invención. El sistema incluye un sistema remoto y un concentrador de sesiones de acceso (SAC):

el sistema remoto se encuentra en una red de acceso de un usuario, y se configura para establecer una sesión de acceso con un sistema remoto; establecer una sesión del Protocolo de Transporte de Sesión (STP) con un servidor de sesión de red (SNS) en la red de origen del usuario; establecer una relación de correspondencia entre la sesión de acceso del sistema remoto y la sesión STP, y reenviar mensajes entre el sistema remoto y el SNS de acuerdo con la relación de correspondencia.

Comparados con la técnica convencional, los modos de realización de la presente invención disfrutan, al menos, de las ventajas que se presentan a continuación.

De acuerdo con los modos de realización de la presente invención, los escenarios de aplicación de la sesión IP se amplían de modo que se resuelve el problema de las limitaciones técnicas de la sesión IP en relación con una VPDN y un escenario mayorista.

Breve descripción de los dibujos

La Figura 1 ilustra una vista esquemática de un procedimiento de las técnicas convencionales para el acceso mediante PPP utilizando L2TP;

la Figura 2 ilustra una vista esquemática de un procedimiento para generar una sesión IP basada en DHCP;

la Figura 3 ilustra una arquitectura de sistema de un mecanismo del STP para implementar un acceso de sesión de Capa 3 de acuerdo con un modo de realización de la presente invención;

la Figura 4 ilustra una vista esquemática de una estructura del protocolo STP de acuerdo con un modo de realización de la presente invención;

la Figura 5 ilustra una vista esquemática de las pilas del protocolo en la VPDN o el mecanismo mayorista con respecto a una sesión de un método de acceso de sesión de Capa 3 de acuerdo con un modo de realización de la presente invención;

la Figura 6 ilustra una vista esquemática de un formato de encapsulación de una pila del protocolo STP de acuerdo con un modo de realización de la presente invención;

la Figura 7 ilustra una vista esquemática de otro formato de encapsulación de una pila del protocolo STP de acuerdo con un modo de realización de la presente invención;

la Figura 8 ilustra un diagrama de flujo para establecer una sesión IP que utiliza el STP mediante un concentrador de sesiones de acceso (SAC) que actúa en modo PROXY (intermediario) de acuerdo con un primer modo de realización de la presente invención;

la Figura 9 ilustra un diagrama de flujo para establecer una sesión IP que utiliza el STP mediante un SAC que actúa en modo RELAY (retransmisión) de acuerdo con un primer modo de realización de la presente invención;

la Figura 10 ilustra un diagrama de flujo para establecer una sesión IP a través de una red de acceso utilizando DHCP;

la Figura 11 ilustra un diagrama de flujo de procesamiento en el que el STP soporta una ampliación en una asignación de una dirección IP de sesión de acuerdo con un modo de realización de la presente invención;

la Figura 12 ilustra un diagrama de flujo para procesar una petición ARP mediante el SAC y el SNS, respectivamente;

la Figura 13 ilustra un diagrama de flujo en el que el SNS envía periódicamente un mensaje de detección;

la Figura 14 ilustra un diagrama de flujo en el que el SAC envía periódicamente un mensaje de detección;

la Figura 15 ilustra un diagrama de flujo para el procesamiento por parte del SAC de un mensaje recibido del sistema remoto; y

la Figura 16 ilustra un diagrama de flujo para el procesamiento por parte del SAC de un mensaje recibido del túnel STP.

Descripción detallada

De acuerdo con los modos de realización de la presente invención, el usuario puede atravesar una red de acceso utilizando una sesión de acceso de Capa 3 y, de este modo, acceder a una red de origen (de pago) del usuario utilizando un mecanismo del Protocolo de Transporte de Sesión (STP). En la Figura 3 se ilustra una arquitectura del sistema del mecanismo del STP para implementar un acceso de sesión de Capa 3 de acuerdo con un modo de realización de la presente invención. La arquitectura del sistema incluye, al menos, un Sistema Host (Central), un Concentrador de Sesiones de Acceso (SAC), un servidor de sesiones de red (SNS).

El sistema central incluye, al menos uno de los siguientes: un Sistema Remoto, un Sistema Final y un servidor de red. El Sistema Remoto incluye un equipo terminal de un usuario remoto, incluyendo equipos como, por ejemplo, un CPE, una Pasarela Residencial (RG), un ordenador personal, un terminal inalámbrico, etc. El Sistema Final incluye un equipo terminal de un usuario local (dentro de una red de origen, por ejemplo), incluyendo: un CPE, una RG, etc. El servidor de red incluye un servidor de Autorización, Autenticación y Registro (AAA), un servidor del Protocolo de Configuración Dinámica de Equipos de Red (DHCP), etc.

El SAC es un equipo final de la red de acceso, por ejemplo, un servidor de acceso de la red (NAS) o un equipo final IP, incluyendo equipos como, por ejemplo, un router de servicios de red, una pasarela de la red de acceso, una BNG, un BRAS, un LAC, etc. El SAC pertenece a la red de acceso. El SAC y el sistema remoto se pueden conectar entre sí utilizando la tecnología de enlace de Capa 2 (L2), por ejemplo, tecnología Ethernet, tecnología de Transporte de Proveedores de Redes Troncales/Redes de Retorno (PBT), tecnologías de Conmutación

Multiprotocolo mediante Etiquetas (MPLS), etc. El SAC es responsable del establecimiento de un Túnel con el SNS de la red de origen del usuario, y de reenviar los mensajes (incluyendo mensajes de datos y mensajes de control) transmitidos entre el SNS y el sistema remoto del usuario, por ejemplo, mapeando y encapsulando un mensaje recibido desde el sistema remoto basado en el protocolo STP y enviándolo al SNS, mapeando un mensaje recibido del SNS y enviándolo al sistema remoto.

El SNS es un equipo final homólogo del SAC, incluyendo equipos de red como, por ejemplo, un router de servicios de red, una pasarela de de acceso a la red, un BNG, un BRAS, un LNS, etc., y es un extremo lógico en la parte de red de una sesión de acceso (por ejemplo, una sesión IP) del sistema remoto. Más aún, el SNS es responsable del control y de la gestión de una sesión de acceso del usuario, y también es responsable del establecimiento de un túnel con la red de acceso para transmitir los datos del usuario.

El SAC y el SNS se conectan a través de una red de transmisión, siendo cada uno de ellos un extremo STP homólogo del otro. En otras palabras, si el SAC es un equipo final local del STP, el SNS es, por tanto, un equipo final homólogo del STP, y viceversa. El protocolo STP se ejecuta entre el SAC y el SNS. Se establece un túnel de servicio emulado en la red de transmisión, donde la red de transmisión incluye una red IP, una red Ethernet, una red del Modo de Transferencia Asíncrono (ATM), una red de la Jerarquía Digital Síncrona (SDH), una red de Multiplexación por División de Longitud de Onda (WDM), una red MPLS, etc. El túnel de servicio emulado entre el SAC y el SNS se puede poner en funcionamiento de forma estática, o también se puede activar en función de una indicación de la sesión de acceso y, por lo tanto, se puede establecer de forma dinámica.

De acuerdo con el modo de realización de la presente invención, el mecanismo del STP se ejecuta entre el SAC y el SNS, y se pueden utilizar los protocolos especificados por una Petición de Comentarios (RFC) para una implementación específica del STP, por ejemplo, un protocolo L2TP, un protocolo LDP, un protocolo de señalización PW, etc.

Existen dos tipos de conexiones entre una pareja de SNS y SAC. Uno de ellos es una conexión de túnel, en la que se define una pareja de SNS y SAC. La otra es una conexión de Sesión, que se multiplexa sobre la conexión de túnel y se configura para representar cada procedimiento de sesión de Capa 3 (por ejemplo, una sesión IP) transportada sobre la conexión de túnel. Se puede establecer una pluralidad de túneles STP entre una pareja de SAC y SNS, donde el túnel se forma mediante una conexión de control y una o una pluralidad de sesiones. La sesión se debería conectar después que se haya establecido satisfactoriamente el túnel (incluyendo un intercambio de información como, por ejemplo, seguridad de ID, versión, tipo de trama, tipo de transmisión hardware, etc.), donde cada conexión de sesión se corresponde con un flujo de datos del protocolo (IP) de Capa 3 entre el SAC y el SNS: a través del túnel se transmiten todos los mensajes de control y paquetes de datos (IP) de la Capa 3. Para la detección de la conectividad del túnel el STP utiliza el mensaje Hello (Hola). El SAC y el SNS envían periódicamente el mensaje Hello al otro extremo homólogo. Si durante un período de tiempo no se ha recibido una confirmación sobre el mensaje Hello, se habría interrumpido el túnel.

En el STP existen dos tipos de mensajes, es decir, mensaje de control y mensaje de datos. El mensaje de control se utiliza para el establecimiento, el mantenimiento del túnel y/o la conexión de la sesión así como para el control de la transmisión; mientras que el mensaje de datos se configura para encapsular paquetes de datos o tramas de la Capa 3 (cargas de datos, por ejemplo paquetes IP para la comunicación entre el sistema remoto y el sistema final dentro de la red de origen), y para transmitir sobre el túnel. La transmisión del mensaje de control puede ser una transmisión fiable y puede soportar un control de flujo y un control de congestión del mensaje de control; mientras que la transmisión del mensaje de datos puede ser una transmisión no fiable, por ejemplo, no se lleva a cabo ninguna retransmisión cuando se descarta el mensaje de datos y puede no soportar un control de flujo ni un control de la congestión del mensaje de datos. Los datos del STP y el canal de control se refieren a un concepto lógico, no siempre a un túnel o ruta de transmisión real, sino a un mecanismo de transmisión de la información, por ejemplo, indicativo de un canal fiable o no fiable.

Haciendo referencia a la Figura 4, se ilustra una estructura del protocolo STP de acuerdo con un modo de realización de la presente invención. El mensaje STP de control y el mensaje STP de datos pueden utilizar un encabezado del mensaje parecido, por ejemplo, un encabezado de datos del STP o un encabezado de control del STP, donde el mensaje de control y el mensaje de datos se identifican mediante el encabezado del mensaje. El encabezado de datos del STP o el encabezado de control del STP pueden contener información de un ID del Túnel o un ID de la Sesión para identificar diferentes túneles y sesiones. Los mensajes con un mismo ID de Túnel pero un diferente ID de Sesión se multiplexarán sobre un túnel. El encabezado de datos del STP o el encabezado de control del STP pueden ser un encabezado lógico, es decir puede no existir realmente un campo de datos entre un paquete de datos de sesión (trama) o un mensaje STP de control y el túnel; por el contrario, los datos de información real pueden estar contenidos en un paquete de datos de sesión (trama) o en un mensaje STP de control.

Haciendo referencia a la Figura 5, se proporciona una vista esquemática de las pilas del protocolo en la VPDN o el mecanismo mayorista con respecto a una sesión de un método de acceso de sesión de Capa 3 de acuerdo con un modo de realización de la presente invención, donde se ilustran las pilas de protocolo de cada equipo central de la VPDN o del mecanismo mayorista del método de acceso de la sesión de la Capa 3. El segmento de la red de acceso entre el sistema remoto y el SAC, el segmento de red del túnel de transmisión entre el SAC y el SNS, y el

segmento de red de origen entre el SNS y el sistema final pueden utilizar un enlace de Capa 2 o enlace de la capa física distintos, pero utilizan una misma red de Capa 3, por ejemplo, una red IP.

El sistema remoto puede transportar los datos (cargas de paquetes IP) de la sesión de Capa 3 (sesión IP) utilizando una tecnología de enlace de la Capa 2 o los puede transportar directamente sobre el enlace físico, por ejemplo, IP sobre Ethernet (IPoE) o IP sobre mensajes WDM (IPoWDM) y, a continuación, enviarlos al SAC a través del enlace físico; o se reciben los datos de la sesión de Capa 3 desde el SAC, por ejemplo, mensajes IPoE que contienen las cargas de los paquetes IP.

El SAC recibe un mensaje del sistema remoto, y lleva a cabo un proceso de terminación en relación con la capa de enlace o la capa física, que incluye: obtener un ID del enlace de la capa 2 o del enlace físico, eliminar del mensaje de datos un encabezado de la Capa 2 de enlace, extraer el paquete o la trama de datos de la sesión de Capa 3 (cargas del paquete IP) del sistema remoto. A continuación, el SAC lo mapea (lo hace corresponder) con un túnel STP y/o una conexión de sesión STP en función de la información del encabezado del paquete o trama de datos de la sesión de la Capa 3, y/o el ID del enlace de la Capa 2 o del enlace físico. Después, se lleva a cabo un mapeo y una adaptación del STP (por ejemplo, una clasificación del mensaje de control o el mensaje de datos, y la adaptación del STP) sobre el paquete o trama de datos de la sesión de Capa 3 (cargas del paquete IP), incluyendo la incorporación de un encabezado del mensaje STP, y el envío a través del túnel STP, donde el envío a través del túnel STP incluye la adaptación del encabezado del túnel de transmisión y, a continuación, el envío a través de la capa física. El túnel de transmisión del STP incluye un túnel IP, un túnel PBT, un túnel MPLS, un túnel SDH, etc.

El SAC recibe del SNS un mensaje STP a través del túnel STP, y primero lleva a cabo un proceso de terminación del túnel, que incluye la obtención de la información de conexión del túnel y/o de la sesión. A continuación, el SAC elimina el encabezado del túnel del mensaje; después, el mensaje STP se clasifica en función del encabezado del mensaje STP. Si es un mensaje STP de control, el mensaje STP de control se procesa localmente en el SAC, o se transfiere a un equipo dedicado para procesar el mensaje STP de control o al sistema remoto para procesar el mensaje STP de control. Si es un mensaje STP de datos, el SAC puede obtener los paquetes de datos (paquetes IP de la carga de datos) de la sesión de Capa 3 (sesión IP), a continuación, obtiene un ID del enlace de la Capa 2 o del enlace físico conectado entre el SAC y el sistema remoto en función del ID de la sesión STP (por ejemplo, una dirección IP de destino para los paquetes IP de la carga de datos) y, a continuación, lleva a cabo una adaptación y encapsulado en relación con la capa física o la capa de enlace, y posteriormente lo envía al sistema remoto.

El SNS recibe del SAC un mensaje a través del túnel STP, y primero lleva a cabo un proceso de terminación del túnel, que incluye la obtención de la información de conexión del túnel y/o la sesión. A continuación, el SNS elimina el encabezado del túnel del mensaje; después, el mensaje se clasifica en función del encabezado del mensaje STP. Si es un mensaje STP de datos, por ejemplo, un mensaje en el que está presente un encabezado del mensaje STP de datos, se elimina el encabezado del mensaje y se obtienen las cargas de datos. A continuación, se envía el mensaje STP de datos en función de la dirección de destino (una dirección IP de destino) de las cargas de datos. Si es un mensaje STP de control, el mensaje STP de control se envía, en función del tipo de mensaje, a un equipo correspondiente para su procesamiento, por ejemplo, se envía a un servidor AAA a través de RADIUS para su procesamiento, o se envía a un servidor de direcciones (servidor DHCP) a través de un mensaje DHCP para su procesamiento.

El SNS recibe un mensaje desde otros sistemas finales dentro de la red, obtiene las cargas de los paquetes IP del mensaje y mapea (hace corresponder) una dirección de destino (por ejemplo, una dirección IP) de las cargas del paquete IP al túnel STP, a continuación, lleva a cabo una adaptación del STP para el paquete o trama de datos de la Capa 3 (cargas del paquete IP), incluyendo la incorporación de un encabezado del mensaje STP y el envío a través del túnel STP.

Haciendo referencia a la Figura 6, se ilustra un formato de encapsulación de una pila del protocolo STP de acuerdo con un modo de realización de la presente invención. El presente modo de realización ilustra una encapsulación realizada por el STP utilizando las versiones V2 y V3 actuales del L2TP. El mensaje de Capa 3 de la sesión es un mensaje IP, y el usuario puede acceder a través de una sesión IP. El mensaje de control y el mensaje de datos del STP se pueden encapsular en un formato L2TP parecido o idéntico. Se puede identificar el tipo del mensaje STP en función de un encabezado L2TP, en el que se puede utilizar como referencia la RFC 2661 y la RFC 3931 para una descripción detallada del encabezado L2TP. El mensaje de control y las cargas de datos se encapsulan directamente en el encabezado L2TP, en el que las cargas de datos incluyen un mensaje IP. Un dominio del encabezado UDP y un dominio del encabezado IP (de la red pública) se refieren al encabezado del túnel de acuerdo con la V2 del L2TP, mientras que un dominio del encabezado IP (de la red pública) o un dominio del encabezado del PW del mensaje se refiere al encabezado del túnel de acuerdo con la V3 del L2TP.

Para la encapsulación de acuerdo con la V3 del L2TP, el mensaje de datos se puede almacenar no explícitamente en el encabezado L2TP. En otras palabras, no existe realmente ningún campo de datos entre el mensaje de Capa 3 y el encabezado del túnel. El mensaje de datos y el mensaje de control se identifican en función de un encabezado del mensaje de control predeterminado. Por ejemplo, en el encabezado L2TP del mensaje de control pueden ser cero los primeros 32 bits de datos (4 bytes sucesivos). Esto es, el mensaje es un mensaje de control cuando son cero los primeros 32 bits de datos del mensaje después de haber eliminado el encabezado del túnel; en caso

contrario, el mensaje es un mensaje de datos cuando no son cero los primeros 32 bits de datos del mensaje. Debido a que el mensaje de Capa 3 se encapsula directamente en el encabezado L2TP del encabezado del túnel, esto puede acelerar de forma significativa la eficiencia del mensaje y puede soportar una red heterogénea de la red de acceso y de la red de origen.

Haciendo referencia a la Figura 7, se ilustra otro formato de encapsulación de una pila del protocolo STP de acuerdo con un modo de realización de la presente invención. Debido a que las cargas de datos del mensaje de datos pueden incluir un ID de sesión, por ejemplo, una dirección IP para las cargas de datos de la sesión IP, el mensaje de datos es, de este modo, encapsulado directamente en el túnel de transmisión, y el mensaje STP de control se transmite sobre el túnel después de haber añadido y encapsulado en él el encabezado del mensaje STP de control.

El mensaje de control y el mensaje de datos se pueden identificar en función del dominio asociado del encabezado del túnel, por ejemplo, un campo de protocolo en el encabezado IP del túnel IP (un número de protocolo del encabezado IP), un campo de tipo y/o un campo de la etiqueta de servicio en un encabezado PBT de un túnel PBT, una etiqueta del encabezado PW y/o un campo con la palabra de Control del túnel PW. El mensaje de datos y el mensaje de control del STP también se pueden identificar en función de un encabezado de control del STP predeterminado. Por ejemplo, en el encabezado del mensaje STP de control pueden ser cero los primeros 32 bits de datos. Esto es, el mensaje es un mensaje de control cuando son cero los primeros 32 bits de datos del mensaje después de haber eliminado el encabezado del túnel; en caso contrario, el mensaje es un mensaje de datos cuando no son cero los primeros 32 bits de datos del mensaje (ya que los primeros 32 bits de datos de un mensaje IP normal no serán cero). Un encabezado del mensaje STP de control puede tener un formato similar al encabezado del mensaje L2TP de control, lo cual dependerá de una implementación específica.

De acuerdo con el modo de realización de la presente invención, en el transcurso del establecimiento de una sesión IP por parte del STP, el SAC puede funcionar en dos modos, es decir, un modo PROXY, o un modo RELAY. El modo PROXY se aplica, en general, tanto en un escenario para el establecimiento de una VPN dinámica (VPDN) como en un escenario mayorista, mientras que el modo RELAY se aplica, en general, en un escenario mayorista. La diferencia entre el modo PROXY y el modo RELAY radica en que, el mensaje se procesa de manera diferente durante una etapa de descubrimiento del acceso de sesión asociado con él mismo. Para el modo PROXY, durante el procedimiento de establecimiento de la sesión de acceso, el SAC actúa como un intermediario del SNS para llevar a cabo una negociación de interacción con el sistema remoto en la etapa de descubrimiento, de este modo, el SAC lleva a cabo algunas de las funciones del SNS. Para el modo RELAY, en una etapa de descubrimiento del procedimiento de establecimiento, el SAC reenvía directamente para su procesamiento un mensaje de interacción desde el sistema remoto al SNS y, a continuación, el SAC reenvía al sistema remoto un mensaje desde el SNS como respuesta al sistema remoto. Cuando el acceso de la sesión IP se utiliza en combinación con un PANA, se debe de tener en cuenta un procedimiento para configurar una primera dirección como etapa de descubrimiento cuando se accede al PANA. Cuando el sistema remoto adopta el PANA, el SAC en el modo PROXY es responsable de la asignación de una dirección temporal al sistema remoto.

El primer modo de realización de la presente invención incluye un procedimiento para el establecimiento de una sesión IP que utiliza el STP por parte del SAC que actúa en el modo PROXY. Haciendo referencia a la Figura 8, se incluyen los siguientes pasos.

Paso s801: el sistema remoto negocia con el SAC para descubrir una sesión de acceso. El sistema remoto descubre un servidor de acceso de la red mediante el procedimiento de negociación del descubrimiento, en el que el servidor de acceso de la red proporciona al sistema remoto un servicio de acceso. En el modo PROXY, el SAC actúa haciendo las veces de SNS para llevar a cabo una negociación con el sistema remoto para el descubrimiento de una sesión de acceso, es decir, el SAC puede actuar haciendo las veces de SNS para responder a un mensaje de negociación del descubrimiento de acceso enviado por el sistema remoto. Por ejemplo, el sistema remoto envía un mensaje Discovery/Solicit (solicitud) del DHCP, y el SAC puede responder con un mensaje Offer/Advertise (oferta/anuncio) del DHCP. El sistema remoto envía un mensaje PANA-Client-Initiation (inicio del cliente PANA) del PANA, y el SAC puede responder con un mensaje PANA-Auth-Request (petición de autorización de PANA) del PANA. El sistema remoto envía un mensaje Start (inicio) del EAPoL sobre 802.1x. El SAC puede responder con un mensaje Request/ID del EAPoL. El procedimiento de negociación de descubrimiento para la sesión de acceso es opcional y también se asocia con un mecanismo de negociación específico. Por ejemplo, cuando el sistema remoto está accediendo a través del PANA, el procedimiento de adquisición de la dirección temporal en relación con el sistema remoto puede ser el procedimiento de negociación de descubrimiento de la sesión de acceso, es decir, el SAC puede asignar una dirección temporal al sistema remoto sobre el DCHP.

Paso s802: el sistema remoto negocia con el SAC para establecer una sesión de acceso. El sistema remoto negocia con el servidor de acceso de la red para establecer una sesión de acceso, es decir, el sistema remoto negocia con el SNS para establecer una sesión de acceso. Debido a que el sistema remoto y el SNS se encuentran en diferentes redes donde no se puede realizar ninguna interconexión directa, es necesaria una retransmisión del SAC para la negociación entre el sistema remoto y el servidor de acceso de red. La negociación para establecer la sesión de acceso incluye una autenticación de ID, una asignación de dirección, una negociación del enlace, un establecimiento de la sesión, etc. El sistema remoto envía un mensaje de negociación para establecer una sesión de acceso. El mensaje incluye un mensaje Request/Auth (autenticación) del DHCP, o un mensaje PANA-Auth-Request/ PANA-

Auth-Answer del PANA, o un mensaje Response de EAPoL sobre 802.1x, etc.

Paso s803: el SAC obtiene la información de ID del sistema remoto, por ejemplo, un nombre de cuenta, un ID de enlace, etc., en función del mensaje de negociación enviado por el sistema remoto para establecer la sesión de acceso. A continuación, el SAC lleva a cabo una autenticación y autorización del ID en el sistema remoto en función de la información de ID. Por ejemplo, se envía un mensaje Radius a un servidor AAA de la red de acceso, el servidor AAA de la red de acceso puede llevar a cabo la autenticación y autorización con éxito, y responder al SAC, un mensaje de respuesta que puede incluir información de la red de origen, por ejemplo, información del túnel (por ejemplo, una dirección IP para el extremo homólogo).

Paso s804: el SAC negocia con el SNS para establecer un túnel STP. Si no existe ningún túnel establecido o no existe un túnel inactivo entre el SAC y el SNS, el SAC puede negociar con el SNS el establecimiento de un túnel STP, por ejemplo, estableciendo un túnel L2TP a través del L2TP, estableciendo un túnel MPLS o PW a través del LDP, estableciendo un túnel PBT a través de la señalización PBT, o estableciendo un túnel IPSec, etc. El túnel se puede establecer mediante un mecanismo dedicado que puede no pertenecer a un protocolo STP. El túnel STP se puede configurar de forma estática, por ejemplo, el SAC se puede configurar sobre el túnel STP del SNS a través de la gestión de red.

Paso s805: el SAC negocia con el SNS para establecer una sesión. El SAC negocia con el SNS para el establecimiento, mantenimiento y terminación de la sesión STP a través de un mensaje de control para negociar la sesión STP. El SAC es responsable del mapeo del mensaje de negociación para establecer la sesión de acceso enviado desde el sistema remoto con un mensaje de control de la negociación de la sesión STP y, a continuación, enviarlo al SNS sobre el túnel STP. El mensaje de control para negociar la sesión STP incluye un mensaje Incoming-Call-Request (petición de llamada entrante) (ICRQ), un mensaje Incoming-Call-Reply (respuesta a la llamada entrante) (ICRP), un mensaje Incoming-Call-Connected (conexión de la llamada entrante) (ICCN), un mensaje Outgoing-Call-Request (petición de llamada saliente) (OCRQ), un mensaje Outgoing-Call-Reply (respuesta de la llamada saliente) (OCRP), un mensaje Outgoing-Call-Connected (conexión de la llamada saliente) (OCCN) sobre el protocolo L2TP.

Paso s806: el SNS lleva a cabo una autenticación y autorización de ID en el sistema remoto. El SNS obtiene la información de ID del mensaje de control para negociar la sesión STP desde el sistema remoto, y lleva a cabo una autenticación y autorización de ID en el sistema remoto en función de la información de ID. Cuando se supera la autenticación y autorización que lleva a cabo el servidor AAA, se envía una respuesta al SNS, donde el mensaje de respuesta puede incluir un ID de sesión, por ejemplo, una dirección IP, de la sesión de acceso de la Capa 3 del sistema remoto.

El SNS especifica un ID de la sesión STP y un ID de la sesión de acceso del sistema remoto, y también establece una relación de correspondencia entre el ID de la sesión de acceso del sistema remoto, el túnel y el ID de la sesión STP, y responde, a continuación, al SAC utilizando un mensaje de control de la negociación de la sesión STP. Preferiblemente, el ID de la sesión STP puede utilizar el mismo ID que la sesión de acceso del sistema remoto, por ejemplo, una dirección IP. El SAC establece una sesión STP en función del mensaje de control de la negociación de la sesión STP recibido, y también establece una relación de correspondencia entre la sesión STP y el sistema remoto, por ejemplo, estableciendo una relación de correspondencia del ID de la sesión de acceso del sistema remoto (por ejemplo, una dirección IP) y/o un ID de la capa de enlace o de la capa física de la sesión de acceso, con el túnel y el ID de la sesión STP. El ID de la capa de enlace o de la capa física de la sesión de acceso incluye un ID de la interfaz, un ID de VLAN, un PVC, una dirección MAC, un enlace PBT, etc. El SAC responde al sistema remoto a través de un mensaje de negociación para establecer la sesión de acceso indicando que se ha establecido la sesión de acceso, por ejemplo, el SAC puede responder al sistema remoto a través de un mensaje ACK del DHCP.

Paso s807: se lleva a cabo una comunicación de datos (se transmiten datos a través de la sesión de acceso) entre el sistema remoto y el equipo dentro de la red de origen. El SAC es responsable de reenviar un mensaje entre el SNS y el sistema remoto del usuario, encapsulando el mensaje recibido desde el sistema remoto en función del protocolo STP y enviándolo al SNS, y desencapsulando el mensaje recibido desde el SNS y enviándolo al sistema remoto. El SNS recibe un mensaje de datos de Capa 3 desde otros sistemas finales dentro de la red. A continuación, el SNS mapea una dirección de destino (por ejemplo, una dirección IP) del mensaje al túnel STP, lleva a cabo una adaptación del STP de los paquetes (tramas) de datos de la Capa 3, incluyendo la incorporación de un encabezado del mensaje STP y el envío al sistema remoto a través del túnel STP.

Paso s808 y paso s809: se termina la sesión. La terminación de la sesión incluye una terminación de la sesión de acceso iniciada por el sistema remoto, y una terminación de la sesión provocada por el SNS o el SAC. Por ejemplo, el sistema remoto puede enviar un mensaje de liberación del DHCP, un mensaje de finalización de sesión de EAPOL de 802.1x, etc. El SAC y el SNS terminan la sesión STP, y eliminan la relación de correspondencia entre la sesión de acceso y la sesión STP. Si la sesión terminada es la última sesión sobre el túnel STP, el SAC y el SNS pueden terminar el túnel STP que se ha establecido dinámicamente.

El segundo modo de realización de la presente invención ilustra un procedimiento para establecer una sesión IP utilizando el STP por parte del SAC que actúa en modo RELAY. Haciendo referencia a la Figura 9, se incluyen los

siguientes pasos.

Paso s901: se lleva a cabo una negociación para descubrir una sesión de acceso. El sistema remoto descubre un servidor de acceso de red mediante un procedimiento de negociación de descubrimiento, en el que el servidor de acceso de red proporciona un servicio de acceso al sistema remoto. En modo RELAY, el SAC reenvía un mensaje de la negociación de descubrimiento de acceso enviado al SNS por parte del sistema remoto. El SAC convierte el mensaje de negociación para descubrir la sesión de acceso enviada por el sistema remoto en un mensaje de negociación para descubrir un acceso STP, y convierte el mensaje de negociación para descubrir un acceso STP en un mensaje de negociación para descubrir la sesión de acceso. El mensaje de una negociación de descubrimiento de acceso STP incluye un mensaje Incoming-Call-Request (ICRQ), un mensaje Incoming-Call-Reply (ICRP), un mensaje Incoming-Call-Connected (ICCN), un mensaje de Outgoing-Call-Request (OCRQ), un mensaje Outgoing-Call-Reply (OCRP), un mensaje Outgoing-Call-Connected (OCCN), y un mensaje Set-Link-Info (información de configuración de enlace) (SLI) sobre el protocolo L2TP.

Paso s902: si entre el SAC y el SNS no existe ningún túnel establecido ni ningún túnel inactivo, el SAC puede negociar con el SNS el establecimiento de un túnel STP.

Paso s903: el SAC negocia con el SNS un descubrimiento de acceso.

Paso s904: el sistema remoto inicia una negociación con el SAC para establecer una sesión de acceso. El sistema remoto negocia con el servidor de acceso de red para establecer una sesión de acceso, donde la negociación para el establecimiento de la sesión de acceso incluye una autenticación de ID, una asignación de dirección, una negociación del enlace, un establecimiento de sesión, etc.

Paso s905: el SAC lleva a cabo una autenticación y autorización de ID en el sistema remoto a través de un servidor AAA o de un servidor de políticas de la red de acceso.

Paso s906: el SAC negocia con el SNS el establecimiento de una sesión STP.

Paso s907: el SNS lleva a cabo una autenticación y autorización de ID en el sistema remoto a través de un servidor AAA o de un servidor de políticas de la red de origen. El paso s905 y el paso s907 anteriores son opcionales.

Paso s908: se lleva a cabo una comunicación de datos (los datos se transmiten a través de una sesión de acceso) entre el sistema remoto y el equipo dentro de la red de origen. El SAC es responsable de reenviar un mensaje entre el SNS y el sistema remoto del usuario.

Paso s909 y paso s910: se termina la sesión. La terminación de la sesión incluye una terminación de la sesión de acceso iniciada por el sistema remoto y una terminación de la sesión provocada por el SNS o el SAC.

El tercer modo de realización de la presente invención ilustra un diagrama de flujo para el establecimiento de una sesión IP a través de una red de acceso mediante DHCP, donde el STP utiliza el protocolo L2TP actual. Haciendo referencia a la Figura 10, se incluyen los siguientes pasos.

Paso s1001: el sistema remoto inicia un establecimiento de una sesión IP. El sistema remoto puede, de este modo, acceder a la red de origen mediante la sesión IP a través de la red de acceso. A continuación, el sistema remoto inicia un mensaje Discovery del DHCP, donde el mensaje Discovery del DHCP puede incluir información de ID (UserID) del sistema remoto. La información de ID incluye identificaciones del equipo y puertos conectados con el sistema remoto e incluidos en la Opción 82. La información de ID también puede incluir un nombre de cuenta de usuario o una dirección MAC de un servidor en el sistema remoto, etc.

Paso s1002: en el modo PROXY el SAC recibe un mensaje Discovery del DHCP desde el sistema remoto, identifica un ID de enlace del mensaje Discovery del DHCP, que incluye un ID de interfaz, un ID de VLAN, un ID de PVC del mensaje, etc., y también analiza estos mensajes para obtener la información de ID. A continuación, basándose en el ID de enlace y/o en la información de ID, el SAC determina que la red de origen de la sesión de acceso a establecer por el sistema remoto no es la red local y, después obtiene información de la red de origen a la que acceder por parte del sistema remoto (por ejemplo, una dirección del servidor del DHCP de la red de origen a la que acceder por parte del sistema remoto), responde a un mensaje Offer del DHCP o a un mensaje AUTH (autenticación) procedente del sistema remoto. Específicamente, la dirección del servidor del DHCP incluida en el mensaje Offer del DHCP puede ser, por ejemplo, la dirección del servidor del DHCP de la red de origen de la sesión de acceso a establecer por parte del sistema remoto. Si en el mensaje Discovery del DHCP recibido se incluye el nombre de una cuenta de usuario, el SAC puede especificar un valor Challenge (Aleatorio) y enviar al sistema remoto el valor Challenge a través del mensaje Offer del DHCP. El SAC especifica una dirección MAC de origen para que el SAC envíe el mensaje Offer del DHCP, donde la dirección MAC puede ser una dirección del equipo SAC o puede ser una dirección MAC virtual especificada por el SAC. El sistema remoto es informado de una autenticación a través de un mensaje AUTH (autenticación) del DHCP, donde, para el mensaje de autenticación, se puede adoptar EAP transportando DHCP.

Paso s1003: el sistema remoto continúa solicitando el establecimiento de una sesión IP. El sistema remoto inicia un

mensaje Request o AUTH (autenticación) del DHCP, donde el mensaje Request o AUTH (autenticación) del DHCP puede incluir información de ID. La información de ID incluye, además, información clave, donde la información clave incluye una clave encriptada con el valor Challenge.

Paso s1004: el SAC recibe el mensaje Request o AUTH (autenticación) del DHCP iniciado por el sistema remoto, obtiene un ID de enlace y la información de ID del mensaje y, a continuación, autentica y autoriza la red de acceso. El SAC envía un mensaje de petición de autenticación (Access Request (Petición de Acceso)) a un servidor AAA de la red de acceso, solicitando una autenticación y autorización, donde el mensaje de petición de autenticación puede incluir la información de ID.

Paso s1005: la autenticación y autorización llevada a cabo por el servidor AAA de la red de acceso se realiza con éxito, a continuación el servidor AAA puede responder al SAC un mensaje de éxito de la autenticación y autorización (Access Accept (Aceptación de Acceso)). El servidor AAA también puede enviar al SAC datos de autorización, incluyendo información de la red de origen, por ejemplo, parámetros del túnel entre el SAC y el SNS, etc.

Paso s1006: el SAC determina que es necesario un establecimiento de un túnel de transmisión (por ejemplo, no existe un túnel hasta el SNS o el túnel existente está saturado de sesiones), y por lo tanto, el SAC inicia una petición para el establecimiento de un túnel hasta el SNS, por ejemplo, el SAC inicia un mensaje Start-Control-Connection-Request (Petición de Inicio de Conexión de Control) (SCCRQ).

Paso s1007: el SNS responde a la petición de establecimiento del túnel y envía un mensaje de respuesta, Start-Control-Connection-Reply (Respuesta de Inicio de Conexión de Control) (SCCRP).

Paso s1008: el SNS confirma que se ha completado el establecimiento del túnel, y envía un mensaje de confirmación, Start-Control-Connection-Connected (Inicio de la Conexión de Control Completado) (SCCCN).

Paso s1009: el SAC pide al SNS que establezca una sesión STP, al mismo tiempo, negocia un formato para el encapsulado de un mensaje de los datos de sesión, e inicia un mensaje Call-Request (Petición de Llamada) (CRQ). Por ejemplo, el SAC puede enviar un mensaje Incoming-Call-Request (ICRQ), donde el mensaje incluye parámetros del mensaje Request o AUTH (autenticación) del DHCP iniciado por el sistema remoto, por ejemplo, el mensaje puede incluir información de ID como, por ejemplo, una clave o un valor Challenge, o un mensaje del Protocolo de Autenticación Ampliable (EAP).

Paso s1010: el SNS recibe le mensaje Call-Request (CRQ) iniciado por el SAC, obtiene información de ID del sistema remoto y lleva a cabo una autenticación y autorización de ID. A continuación, el SNS envía un mensaje de petición de autenticación (Access Request) al servidor AAA de la red de origen, solicitando la autenticación y autorización.

Paso s1011: la autenticación y autorización llevada a cabo por el servidor AAA de la red de origen se realiza con éxito, a continuación el servidor AAA puede responder al SNS con un mensaje de confirmación de la autenticación y autorización (Access Accept (Aceptación de Acceso)). El servidor AAA también puede enviar al SNS datos de autorización, incluyendo parámetros de Calidad de Servicio (QoS) y parámetros de políticas. Si el sistema remoto adopta un mecanismo de autenticación ampliable sobre DHCP, es decir, el DHCP se autentica mediante un mensaje AUTH del DHCP, el SNS puede responder al sistema remoto con un mensaje AUTH del DHCP que contiene un resultado de la autenticación. A continuación, el SAC reenvía al sistema remoto este mensaje recibido. Después de haber recibido el mensaje AUTH del DHCP, el sistema remoto continúa con el inicio de una petición de dirección (por ejemplo, envía un Request del DHCP). A continuación, el SAC reenvía al SNS el mensaje de petición de dirección.

Paso s1012: el SNS inicia una petición para asignar una dirección, por ejemplo, envía un mensaje Request del DHCP a un servidor de direcciones (un servidor del DHCP).

Paso s1013: el servidor de direcciones asigna una dirección al sistema remoto y especifica una asignación de dirección IP. A continuación, el servidor de direcciones responde a la petición de asignación de una dirección y envía un mensaje ACK del DHCP.

Paso s1014: el SNS recibe el mensaje ACK del DHCP, obtiene del mensaje la dirección IP y la asignación de dirección realizada por el servidor de direcciones, y establece una sesión de acceso del sistema remoto identificada mediante la dirección IP asignada por el servidor de direcciones (configurando los parámetros de QoS, iniciando la gestión del mantenimiento de la sesión de acceso). El SNS especifica un ID de la sesión STP (L2TP), donde el ID de la sesión STP (L2TP) puede ser la dirección IP asignada por el servidor de direcciones, es decir, el ID de la sesión de acceso del sistema remoto puede utilizar la misma ID de la dirección IP que la ID de la sesión STP (L2TP). También, el SNS establece una relación de correspondencia entre la sesión de acceso del sistema remoto y la sesión STP (L2TP) para reenviar posteriormente un mensaje de datos. El SNS responde a la petición del SAC para establecer una sesión, por ejemplo, envía un mensaje Incoming-Call-Reply (ICRP), donde el mensaje incluye parámetros de la sesión de acceso del sistema remoto y la sesión STP (L2TP), por ejemplo, parámetros de autorización de la red de origen, y parámetros de dirección o un mensaje EAP.

Paso s1015 y paso s1016: el SAC recibe desde el SNS el mensaje de respuesta, obtiene los parámetros de la sesión de acceso del sistema remoto y la sesión STP (L2TP), y establece una relación de correspondencia entre la sesión de acceso del sistema remoto y la sesión STP (L2TP) para reenviar posteriormente un mensaje de datos. La relación de correspondencia incluye una asociación entre la dirección IP de la sesión de acceso y la sesión STP (L2TP), y también incluye un formato para encapsular un mensaje de datos STP (L2TP). Si la dirección IP de la sesión de acceso es una dirección privada, el SAC puede asociar el ID del sistema remoto o el enlace conectado entre el sistema remoto y el SAC con la sesión STP (L2TP), donde el enlace conectado entre el sistema remoto y el SAC incluye un ID de interfaz, un ID de VLAN, un ID de PVC, un ID de la ruta PBT, una etiqueta LSP de MPLS, etc. A continuación, el SAC responde con un mensaje de aceptación, confirmando que se ha establecido la sesión STP (L2TP), por ejemplo, envía un mensaje Incoming-Call-Connected (ICCN).

Paso s1017: el SAC responde al mensaje de aceptación confirmando que se ha establecido la sesión de acceso del sistema remoto, por ejemplo, envía un mensaje ACK del DHCP. A continuación, el SAC obtiene los parámetros asociados, por ejemplo, parámetros de dirección en función del menaje de respuesta (mensaje Incoming-Call-Reply (ICRP)) que recibe el SAC desde el SNS y, de este modo, construye un mensaje ACK del DHCP o extrae el mensaje ACK del DHCP directamente a partir del mensaje de respuesta enviado desde el SNS. El sistema remoto recibe desde el SAC el mensaje para confirmar la sesión de acceso. De este modo, se completa el establecimiento de la sesión de acceso y, en consecuencia, el sistema remoto puede acceder a los recursos de la red de acceso a través de la sesión de acceso establecida. El SAC es responsable de reenviar un mensaje entre el SNS y el sistema remoto del usuario, en función de la relación de correspondencia entre la sesión de acceso del sistema remoto y la sesión STP (L2TP).

Paso s1018 y paso s1019: el sistema remoto inicia una petición para la terminación de la sesión de acceso, por ejemplo, el sistema remoto envía un mensaje Release (Liberación) del DHCP. A continuación, el SAC y el SNS terminan la sesión STP (por ejemplo, utilizando una notificación CDN). Si la sesión STP es la última sesión del túnel STP, el SAC y el SNS pueden terminar el túnel STP que se ha establecido dinámicamente.

De acuerdo con el modo de realización de la presente invención, la sesión establecida por el sistema remoto es una sesión con una dirección IP dinámica. Debido a que el servidor de direcciones de la red de origen asigna la dirección IP del sistema remoto, normalmente se proporciona una gestión de la asignación de la dirección IP dinámica, es decir cuando se asigna la dirección IP también se especifica, en ese mismo momento, un período de tiempo en el que se puede utilizar la dirección IP. Si el periodo expira, el sistema remoto debería dejar de utilizar la dirección IP. Si el sistema remoto necesita aumentar el tiempo de utilización, el sistema remoto debería solicitar el mantenimiento de la dirección. Más aún, si falla la solicitud del mantenimiento, el sistema remoto puede solicitar reiniciar una petición para establecer una sesión de acceso. Al mismo tiempo, el SNS y el SAC registran y detectan una asignación dinámica de dirección IP de la sesión de acceso. Si la asignación expira o falla la solicitud de mantenimiento, el SNS o el SAN tienen que terminar la sesión STP asociada con la sesión de acceso identificada por la dirección IP y liberar los recursos de red ocupados por la sesión de acceso. Por consiguiente, el sistema remoto no puede seguir utilizando el servicio (red de acceso) a través de esta sesión de acceso.

El cuarto modo de realización de la presente invención ilustra un diagrama de flujo del proceso en el que el STP soporta una ampliación de tiempo de una asignación de una dirección IP de sesión de acuerdo con un modo de realización de la presente invención. Haciendo referencia a la Figura 11, se incluyen los siguientes pasos.

Paso s1101: el sistema remoto inicia una petición para aumentar el tiempo de utilización de una dirección. Por ejemplo, el sistema remoto inicia una petición para aumentar el tiempo de utilización de una dirección cuando ha transcurrido el 50% del tiempo. Un mensaje de petición para aumentar el tiempo de utilización de una dirección puede ser un mensaje Request del DHCP, y la petición para aumentar el tiempo de utilización de una dirección incluye parámetros como, por ejemplo, la dirección IP asociada con la asignación de tiempo a aumentar, un período de aumento del tiempo de utilización (una nuevo tiempo de utilización), etc.

Paso s1102: el SAC reenvía el mensaje de petición recibido para aumentar el tiempo de utilización de una dirección enviado desde el sistema remoto al SNS a través de una petición de asignación de tiempo STP. El mensaje se puede reenviar mediante de un mensaje STP de datos, o mediante un mensaje STP de control. Preferiblemente, el mensaje se reenvía a través de un mensaje STP de control.

El procedimiento de reenvío del mensaje de petición para aumentar el tiempo de utilización de una dirección a través del mensaje de datos por parte del SAC incluye: buscar una relación de correspondencia entre la sesión de acceso y la sesión STP (L2TP) en función de una dirección IP de origen del mensaje Request del DHCP y/o un ID de enlace del mensaje; a continuación, encapsular el mensaje Request del DHCP en el mensaje STP de datos en función de los parámetros de una tabla de la relación de correspondencia; y, a continuación, enviarlo al SNS a través del túnel. En este momento, el mensaje de petición de tiempo de utilización STP es el mensaje Request del DHCP encapsulado en el mensaje STP de datos.

El procedimiento de reenvío del mensaje de petición para aumentar el tiempo de utilización de una dirección a través del mensaje de control por parte del SAC incluye los siguientes pasos. El SAC determina que es necesario enviar el mensaje al SNS a través de un túnel, en función de la dirección IP de origen del mensaje Request del DHCP y/o un

ID de enlace del mensaje, etc. A continuación, el SAC obtiene un ID del túnel, encapsula el mensaje Request del DHCP en un mensaje STP de control de la petición de tiempo de utilización y, a continuación, envía al SNS el mensaje de control. El mensaje STP de control de petición de tiempo de utilización incluye un mensaje Set-Link-Info (SLI), un menaje Incoming-Call-Request (ICRQ), un mensaje Outgoing-Call-Request (OCRQ), un mensaje Explicit-Acknowledgement (Confirmación Explícita) (ACK) del L2TP, etc. El mensaje STP de control de la petición de tiempo de utilización también puede utilizar un nuevo mensaje STP, por ejemplo, redefiniendo un mensaje STP de control de la petición de tiempo de utilización. El procedimiento anterior de encapsulado del mensaje Request del DHCP en un mensaje STP de control de la petición de tiempo de utilización por parte del SAC incluye adaptar parámetros del mensaje Request del DHCP a un dominio de parámetros del mensaje STP de control de la petición de tiempo de utilización o considerar el mensaje Request del DHCP completo como un dominio de parámetros del mensaje STP de control de la petición de tiempo de utilización (AVP: Par Atributo Valor).

Paso s1103: el SNS recibe desde el SAC el mensaje STP de petición de tiempo de utilización y extrae el mensaje Request del DHCP o los parámetros del mensaje Request del DHCP a partir del mensaje STP de petición de tiempo de utilización. A continuación, el SNS envía al servidor de direcciones el mensaje Request del DHCP o un mensaje Request del DHCP construido de nuevo a partir de los parámetros del mensaje Request del DHCP para solicitar un aumento del tiempo de utilización de la dirección.

Paso s1104: el servidor de direcciones confirma la petición para solicitar un aumento del tiempo de utilización de la dirección y envía al SNS un mensaje de confirmación, ACK del DHCP.

Paso s1105: el SNS reenvía al SAC el mensaje de petición para solicitar un aumento del tiempo de utilización de la dirección a través de una confirmación STP del tiempo de utilización, y también puede actualizar al mismo tiempo el tiempo de utilización de la dirección IP para la sesión.

Paso s1106: el SAC recibe el mensaje STP de confirmación de tiempo de utilización, y extrae el mensaje Ack del DHCP o los parámetros del mensaje Ack del DHCP a partir del mensaje STP de confirmación del tiempo de utilización. A continuación, el SNS envía al sistema remoto el mensaje Ack del DHCP o un mensaje Ack del DHCP construido de nuevo a partir de los parámetros del mensaje Ack del DHCP. Al mismo tiempo, también se puede actualizar el tiempo de utilización de la dirección IP para la sesión. El sistema remoto recibe el mensaje Ack del DHCP y actualiza el tiempo de utilización de la dirección IP.

De acuerdo con el quinto modo de realización de la presente invención, cuando se establece una sesión IP de acceso a través de la red utilizando el STP, el túnel cubre la tecnología de enlace de la Capa 2 de la red de acceso y de la red de origen. Sin embargo, si la red de acceso se conecta con el sistema remoto utilizando una tecnología Ethernet, es decir, el SAC se conecta con el sistema remoto a través de una Ethernet, el SAC se puede comportar como un PROXY ARP; si la red de origen utiliza una tecnología Ethernet, es decir, el SNS se conecta con un sistema final dentro de la red de origen utilizando una Ethernet, el SNS se puede comportar como un PROXY ARP. El procedimiento específico, como se ilustra en la Figura 12, incluye los siguientes pasos.

Paso s1201a: el sistema remoto envía un mensaje Request del ARP solicitando una dirección MAC de cierto servidor del sistema.

Paso s1202a: el SAC recibe el mensaje Request del ARP y actúa para que el servidor solicitado responda con un mensaje Reply del ARP en función de una dirección (una dirección IP o una dirección MAC) o un ID de enlace incluido en el mensaje. La dirección MAC del mensaje Reply del ARP con el que responde el SAC puede ser la dirección MAC del SAC, o una dirección MAC especificada, por ejemplo, una dirección MAC virtual. El SAC puede devolver una dirección MAC en relación con todas las Peticiones APR de los sistemas remotos, y también puede devolver una dirección MAC especificada en relación con cada sistema remoto especificado. De este modo, una MAC se puede corresponder con una sesión de acceso.

Cuando el SAC actúa como PROXY ARP, se puede utilizar una dirección MAC virtual. De acuerdo con un ID de dirección (segmento) MAC específica y la sesión IP de acceso establecida por el sistema remoto, el SAC puede identificar si el mensaje de datos recibido es un mensaje de la red local o un mensaje de datos para ser enviado al SNS a través del túnel STP que ha establecido el sistema remoto.

Los pasos para procesar el mensaje Request del ARP por parte del SNS, básicamente parecido al realizado por el SAC, incluyen los siguientes pasos.

Paso s1201b: el SNS recibe un mensaje Request del ARP del sistema final.

Paso s1202b: el SNS determina, en función de la dirección IP que solicita el mensaje ARP, que la dirección IP pertenece a un servidor (una dirección IP de un servidor del sistema remoto) de la sesión (la sesión de acceso a través de la red) establecida a través del STP. De este modo, el SNS actúa como un intermediario para que el sistema remoto responda con un mensaje Reply del ARP.

De acuerdo con el modo de realización de la presente invención, para optimizar la utilización de los recursos de red y satisfacer los requisitos como, por ejemplo, registro, en general, la red necesita llevar a cabo una gestión del

mantenimiento de la sesión de acceso, monitorizar un estado de la sesión de acceso, es decir, un mecanismo para mantener activa la sesión.

El sexto modo de realización de la presente invención ilustra un método para implementar un mecanismo para mantener activa la sesión IP establecida a través de la red, en el que el mecanismo para mantener activa la sesión IP se adopta directamente por parte del SNS y el sistema remoto y, de este modo, el SAC puede no detectar el mecanismo para mantener activa la sesión de acceso. El sistema remoto o el SNS comprueban el estado del homólogo enviando periódicamente un mensaje de detección del estado. A continuación se describe un ejemplo en el que el SNS envía periódicamente un mensaje de detección. Haciendo referencia a la Figura 13, se incluyen los siguientes pasos.

Paso s1301: después del establecimiento de una sesión de acceso por parte del SNS (el sistema remoto accede a la red), el SNS envía un mensaje de petición de detección de estado (Test Request (Petición de Comprobación)), en el que la entidad que provoca que el SNS envíe el mensaje incluye un temporizador periódico, es decir, un temporizador periódico provoca que el SNS envíe el mensaje. El mensaje de petición de detección de estado (Test Request) incluye un mensaje Request del ARP, o un mensaje de Detección Bidireccional de Reenvío (BFD), o un mensaje DHCP, donde el tipo específico del mensaje depende de la implementación. El SNS envía el mensaje de petición de detección de estado (Test Request) a través de un mensaje STP de datos. El SAC recibe el mensaje de datos y reenvía al sistema remoto el mensaje de petición de detección de estado (Test Request).

Paso s1302: el sistema remoto recibe un mensaje de confirmación de detección de estado (Test Reply (Respuesta de Comprobación)) enviado por el SNS, y responde a la petición de detección de estado del SNS. El mensaje de confirmación de detección de estado (Test Reply) incluye un mensaje Reply del ARP, o un mensaje BFD, o un mensaje DHCP, donde el tipo específico del mensaje depende de la implementación. El sistema remoto puede determinar el estado de la sesión de acceso en función del mensaje de petición de detección de estado (Test Request). Si dentro de un período determinado no se recibe ningún mensaje de petición de detección de estado (Test Request) desde el SNS, se determina que la sesión de acceso es anómala y, por lo tanto, se lleva a cabo un procesamiento para una sesión de acceso anómala, por ejemplo, terminar la sesión de acceso. El SAC recibe el mensaje de confirmación de detección de estado (Test Reply) del sistema remoto y reenvía el mensaje al SNS mediante un mensaje STP de datos.

El SNS recibe el mensaje de confirmación de detección de estado (Test Reply) desde el sistema remoto, determina que el sistema remoto se encuentra en estado normal y, por lo tanto, continúa esperando hasta la próxima detección. Si durante un periodo específico o un número de veces el SNS no recibe ningún mensaje de confirmación de detección de estado (Test Reply) desde el sistema remoto, el SNS puede determinar que el sistema remoto se encuentra en un estado anómalo y, en consecuencia, puede terminar la sesión. El envío activo del mensaje de detección de estado no es responsabilidad del SNS. El sistema remoto también puede enviar el mensaje de petición de detección de estado (Test Request) y, a continuación, determinar el estado de la sesión de acceso en función del mensaje de confirmación de detección de estado (Test Reply) devuelto por parte del SNS.

De acuerdo con el séptimo modo de realización de la presente invención, el SAC y el sistema remoto adoptan directamente un mecanismo para mantener activa la sesión IP, y el SAS actúa para que el SNS detecte el mecanismo para mantener activa la sesión de acceso. El sistema remoto o el SAC comprueban un estado de su homólogo mediante el envío periódico de un mensaje de detección de estado. A continuación se describe un ejemplo en el que el SAC envía periódicamente un mensaje de detección. Haciendo referencia a la Figura 14, se incluyen los siguientes pasos.

Paso s1401: después de que el SAC detecte el establecimiento de una sesión de acceso (el sistema remoto accede a la red), el SAC envía al sistema remoto un mensaje de petición de detección de estado (Test Request), en el que la entidad que provoca que el SAC envíe el mensaje incluye un temporizador periódico, es decir, un temporizador periódico provoca que el SAC envíe el mensaje. El mensaje de petición de detección de estado (Test Request) incluye un mensaje Request del ARP, o un mensaje BFD, o un mensaje DHCP, o un mensaje OAM. El tipo específico del mensaje depende de la implementación.

Paso s1402: el sistema remoto recibe un mensaje de petición de detección de estado (Test Request) enviado por el SAC y responde a la petición de detección de estado del SAC con un mensaje de confirmación de detección de estado (Test Reply). El mensaje de confirmación de detección de estado (Test Reply) incluye un mensaje Reply del ARP, o un mensaje BFD, o un mensaje DHCP, o un mensaje OAM. El tipo específico del mensaje depende de la implementación. El sistema remoto puede determinar el estado de la sesión de acceso en función del mensaje de petición de detección de estado (Test Request). Si dentro de un período determinado no se recibe ningún mensaje de petición de detección de estado (Test Request) del SAC, se determina que la sesión de acceso es anómala y, por lo tanto, se lleva a cabo un procesamiento para una sesión de acceso anómala, por ejemplo, terminar la sesión de acceso.

Paso s1402: el SAC recibe el mensaje de confirmación de detección de estado (Test Reply) del sistema remoto, determina que el sistema remoto se encuentra en estado normal y, por lo tanto, continúa esperando la siguiente detección.

Paso s1403: el SAC envía un mensaje de petición de detección de estado (Test Request) al sistema remoto. Si durante un periodo específico o un número de veces especificado (por ejemplo, dos veces, de acuerdo con el presente modo de realización) el SAC no recibe ningún mensaje de confirmación de detección de estado (Test Reply) desde el sistema remoto, se determina que el sistema remoto se encuentra en estado anómalo y, en consecuencia, se termina la sesión. El procesamiento de terminación de la sesión incluye el envío de un mensaje de notificación de la terminación de la sesión para informar al SNS del procesamiento de la sesión anómala, por ejemplo, enviando al SNS un mensaje Call-Disconnect-Notify (CDN) de control. El mensaje de detección de estado puede no ser enviado únicamente de manera activa por parte del SAC. El sistema remoto también puede enviar el mensaje de petición de detección de estado (Test Request) y, después, determinar el estado de la sesión de acceso en función del mensaje de confirmación de detección de estado (Test Reply) devuelto por el SAC.

El octavo modo de realización de la presente invención ilustra un diagrama de flujo para procesar un mensaje recibido desde el sistema remoto por parte del SAC. Haciendo referencia a la Figura 15, se incluyen los siguientes pasos.

Paso s1501: el SAC recibe un mensaje de comunicación desde el sistema remoto (terminal), por ejemplo, un mensaje TCP, un mensaje UDP, un mensaje DHCP, un mensaje OAM, un mensaje ICMP, un mensaje IP, un mensaje ARP, etc. El formato del mensaje de comunicación incluye un mensaje IPoE, un mensaje IPoWDM, un mensaje IP sobre ATM (IPoA), etc. Preferiblemente, también se pueden incluir los siguientes pasos. El SAC recibe un mensaje desde un terminal e identifica que el mensaje proviene del sistema remoto. Específicamente, se puede llevar a cabo la determinación en función de al menos un parámetro del encabezado del mensaje y/o un ID del enlace del mensaje. El parámetro del encabezado del mensaje incluye, al menos, una dirección IP de origen o destino del mensaje, una dirección MAC de origen o destino del mensaje, una Etiqueta de Servicio de un encabezado Ethernet del mensaje. El ID del enlace del mensaje incluye, al menos, una VLAN o un PVC que transportan el mensaje, o un número de interfaz, por ejemplo, el mensaje, que tiene una dirección IP de origen de un segmento o una dirección MAC de un segmento o en una VLAN, pertenece al sistema remoto. La regla de determinación depende de la implementación específica.

Paso s1502: el SAC determina (o identifica) el tipo del mensaje. El tipo del mensaje incluye, al menos, un mensaje de control y un mensaje de datos. El mensaje de control incluye un mensaje DHCP, un mensaje ARP, un mensaje EAP, un mensaje 802.1x, un mensaje PANA, y un mensaje de Mantenimiento y Administración de la Operación (OAM), etc. El mensaje de datos incluye un mensaje TCP normal (distinto del mensaje de control), un mensaje UDP normal (distinto del mensaje de control), un mensaje IP normal (distinto del mensaje de control), etc. La regla para clasificar un mensaje SAC se puede configurar o modificar de forma dinámica, y la regla o la política pueden depender de la implementación real.

Paso s1503: si un mensaje recibido desde el sistema remoto por parte del SAC es un mensaje de datos, se determina si es necesario reenviarlo sobre el STP. En otras palabras, se determina si es necesario reenviar el mensaje al SNS después de un proceso de mapeo del STP. Si es necesario (o SÍ), el proceso continúa en el paso s1505; si no es necesario (NO), el proceso continúa en el paso s1504. Específicamente, se puede llevar a cabo la determinación en función de, al menos, un parámetro del encabezado del mensaje y/o un ID de enlace del mensaje. Por ejemplo, una dirección IP de destino de un segmento necesita reenviarse sobre el STP, una dirección MAC de destino dentro de un rango necesita reenviarse sobre el STP, un mensaje desde una VLAN necesita reenviarse sobre el STP, etc. El SAC también puede soportar una determinación del reenvío de un mensaje de la sesión de acceso remoto (un mensaje del sistema remoto) directamente a una red pública a través del SAC. Por ejemplo, se determina si es necesario reenviar el mensaje directamente a una red pública (por ejemplo, Internet) a través del SAC. La negociación para establecer la sesión de acceso puede determinar si se permite que un mensaje del sistema remoto se reenvíe a una red pública a través del SAC, es decir, el SNS pide al SAC que lleve a cabo la determinación a través del mensaje STP de control, en el que, por defecto, en general no se permite reenviar un mensaje del sistema remoto a una red pública a través del SAC.

Paso s1504: el SAC reenvía el mensaje de datos, incluyendo el encaminamiento y reenvío del mensaje de datos o el reenvío directo a través de la Capa 2. Si se reenvía directamente el mensaje a la red pública a través del SAC, el SAC puede llevar a cabo un NAT del mensaje y, a continuación, reenviar el mensaje.

Paso s1505: el SAC lleva a cabo un proceso de mapeo del mensaje de datos con el mensaje de datos del sistema remoto (por ejemplo, un mensaje IPoE que contiene las cargas del paquete IP). El mapeo incluye el mapeo con un túnel STP y con una sesión STP en función del parámetro del encabezado del mensaje y/o el ID de enlace del mensaje y, después, coger las cargas de los paquetes IP del mensaje de datos como cargas de datos del mensaje STP de datos y las encapsula en el mensaje STP de datos de acuerdo con parámetros de encapsulado de una tabla de mapeo. Por ejemplo, se busca en una tabla de mapeo de sesiones STP en función de una dirección IP de origen de las cargas de paquetes IP del mensaje de datos. Se obtiene un ID del túnel y un ID de la sesión así como parámetros de un formato de encapsulado del mensaje. Las cargas de los paquetes IP del mensaje de datos se encapsulan en el mensaje STP de datos de acuerdo con el formato de encapsulado. A continuación se notifica al túnel que reenvíe el mensaje. Además, la adaptación incluye un proceso de la Unidad Máxima de Transmisión (MTU), incluyendo una fragmentación del mensaje. Después del proceso de mapeo, el mensaje de datos continúa en el paso s1509 para su proceso.

Paso s1506: si el mensaje recibido por el SAC desde el sistema remoto es un mensaje de control, se determina si el mensaje requiere únicamente ser procesado de forma local (un procesamiento de terminación) por parte del SAC. Si el SAC va a procesar el mensaje de forma local, el procedimiento continúa en el paso s1507 para indicar o notificar al SAC que procese el mensaje de forma local, por ejemplo, para un mensaje ARP, el SAC puede actuar como el SNS para procesar el mensaje ARP. Si es necesario que el SAC transfiera el mensaje al SNS para su procesamiento, el procedimiento continúa en el paso s1508, en el que el SAC notifica al SAC que lleve a cabo un proceso de mapeo sobre los mensajes de control.

Paso s1507: el SAC procesa el mensaje de control procedente del sistema remoto, incluyendo situaciones en las que el SAC puede servir como Proxy ARP para procesar un mensaje ARP, el SAC puede actuar como un nodo para mantener activa una sesión para procesar un mensaje de petición de detección de estado (Test Request), o el SAC puede actuar en modo PROXY para procesar un mensaje de negociación para descubrir la sesión de acceso (mensaje Discovery del DHCP), etc.

Paso s1508: el SAC lleva a cabo un proceso de mapeo sobre el mensaje de control. El SAC lleva a cabo un proceso de mapeo del mensaje STP de control sobre el mensaje de control procedente del sistema remoto y, a continuación, lo envía a través del STP. El mapeo incluye el mapeo del mensaje de control con un túnel STP en función de los contenidos del mensaje y/o el ID de enlace del mensaje, y, a continuación, mapear el mensaje de control con el mensaje STP de datos, o tomar el mensaje de control como el mensaje STP de control y encapsularlo en el mensaje STP de control de acuerdo con los parámetros de encapsulado del túnel para, a continuación, notificar al túnel para que reenvíe el mensaje STP. El proceso de mapeo para el mensaje de control llevado a cabo por parte del SAC puede incluir, además, un proceso del mensaje de control, por ejemplo, obteniendo los contenidos del mensaje (por ejemplo información de ID) y llevando a cabo una autenticación y autorización en función de los contenidos del mensaje, etc. El procedimiento continúa en el paso s1509.

Paso s1509: el SAC reenvía el mensaje STP, donde el mensaje STP incluye un mensaje STP de control y un mensaje STP de datos. El SAC envía el mensaje STP a través de un túnel STP asociado.

El noveno modo de realización de la presente invención ilustra un diagrama de flujo para procesar un mensaje STP por parte del SAC. Haciendo referencia a la Figura 16, se incluyen los siguientes pasos.

Paso s1601: el SAC recibe un mensaje STP (desde su homólogo, el SNS), donde el mensaje STP incluye un mensaje STP de control o un mensaje STP de datos.

Pasos s1602: el SAC obtiene el tipo del mensaje, incluyendo la identificación en función de un dominio asociado del encabezado del túnel o un encabezado del mensaje STP. Si el mensaje es un mensaje STP de datos, el procedimiento continúa en el paso s1603 donde se lleva a cabo un proceso de mapeo del mensaje STP de datos. Si el mensaje es un mensaje STP de control, el procedimiento continúa en el paso s1604 donde se lleva a cabo un procesamiento del mensaje STP de control.

Paso s1603: se lleva a cabo un proceso de mapeo del mensaje STP de datos, incluyendo eliminar del mensaje STP el encabezado del túnel o el encabezado del mensaje STP; extraer paquetes o tramas de datos de sesión de Capa 3 (por ejemplo, paquetes IP de cargas de datos); a continuación, obtener parámetros de la dirección de Capa 2 de los paquetes IP de las cargas de datos en función de una dirección IP de destino de los paquetes IP de las cargas de datos, incluyendo una dirección MAC de origen y una dirección MAC de destino, por ejemplo, obtener una dirección MAC con la que se corresponde la dirección IP a partir de una tabla ARP y obtener un ID de enlace (un enlace o un puerto a través del cual se conecta el sistema remoto) a partir de una tabla de mapeo de sesión; y, a continuación, incorporar un encabezado de Capa 2 (por ejemplo, un encabezado Ethernet) en los paquetes o tramas de datos de sesión de Capa 3 (por ejemplo, paquetes IP de las cargas de datos) para formar un mensaje de comunicación de datos (por ejemplo, un mensaje IP sobre Ethernet, IPoE) entre el SAC y el sistema remoto; a continuación, ordenar el envío a través de un enlace especificado (al sistema remoto).

Paso s1604: el SAC determina si el mensaje STP de control se necesita procesar (terminar) de forma local, es decir, si el mensaje STP de control únicamente necesita un procesamiento local por parte del SAC. Si el SAC va a procesar localmente el mensaje STP de control, el procedimiento continúa en el paso s1605 donde se procesa localmente el mensaje STP de control. Si el SAC necesita transferir el mensaje STP de control al sistema remoto para su procesado, el procedimiento continúa en el paso s1606.

Paso s1605: el SAC procesa el mensaje STP de control, incluyendo la negociación para establecer el túnel STP, el mantenimiento y la terminación de un mensaje de control de la negociación. Si el STP es un protocolo L2TP, el mensaje de control puede incluir un mensaje Start-Control-Connection-Request (SCCRQ), un mensaje Start-Control-Connection-Reply (SCCRP), un mensaje Start-Control-Connection-Connected (SCCCN), un mensaje Stop-Control-Connection-Notification (StopCCN), y un mensaje Hello (HELLO). El SAC puede procesar el mensaje STP de control de acuerdo con el protocolo STP.

Paso s1606: se lleva a cabo un proceso de mapeo sobre el mensaje STP de control. Específicamente, el proceso de mapeo incluye mapear y encapsular el mensaje STP de control en un mensaje de control de la comunicación (por ejemplo, un mensaje DHCP, un mensaje PANA, o un mensaje 802.1x) entre el SAC y el sistema remoto. El mensaje

STP de control incluye un mensaje STP de control para la negociación del establecimiento de la sesión, la negociación del mantenimiento y terminación, por ejemplo, un mensaje Outgoing-Call-Request (OCRQ), un mensaje Incoming-Call-Reply (ICRP), un mensaje Set-Link-Info (SLI), un mensaje Outgoing-Call-Connected (OCCN), etc. El mapeo incluye la extracción de contenidos del mensaje de control a partir del mensaje STP de control y, a continuación, encapsular los contenidos del mensaje de control en un formato del mensaje entre el SAC y el sistema remoto en función de una tabla ARP o una tabla de mapeo de sesiones. El mapeo incluye, además, extraer del mensaje de control parámetros del mensaje de control y, a continuación, convertir los parámetros extraídos en un mensaje de otro protocolo, por ejemplo, extraer parámetros desde un mensaje Incoming-Call-Reply (ICRP) y, después, convertirlo en un mensaje ACK del DHCP en función de los parámetros.

Paso s1607: el SAC reenvía el mensaje, es decir, el SAC envía al sistema remoto el mensaje.

El procedimiento para procesar un mensaje por parte del SNS es parecido al realizado por parte del SAC, donde el procedimiento para procesar un mensaje por parte del SNS incluye procesar un mensaje enviado al sistema remoto y recibido por un sistema final dentro de la red, y procesar un mensaje STP recibido desde el SAC. El procedimiento para procesar un mensaje por parte del SNS se puede asimilar al procedimiento para procesar un mensaje por parte del SAC, por lo que se omite en este punto por brevedad.

De acuerdo con el modo de realización de la presente invención, además se incluye un procesamiento de la Unidad Máxima de Transmisión (MTU) para el mensaje de datos recibido llevado a cabo por el SAC y el SNS, por ejemplo, el proceso de mapeo para el mensaje de datos realizado por el SAC y el proceso de mapeo para el mensaje de datos realizado por el SNS pueden incluir la incorporación de un nuevo encabezado del mensaje, por ejemplo, la incorporación de un encabezado del mensaje STP y un encabezado del túnel. De este modo, la longitud última del mensaje puede, consecuentemente, exceder la Unidad Máxima de Transmisión (MTU) que puede transportar una capa inferior de la red. En consecuencia, en el proceso de mapeo se añade el procesamiento de MTU realizado por el SAC para el mensaje de datos y el proceso de mapeo realizado por el SNS para el mensaje de datos. En otras palabras, se determina si, después del mapeo, la longitud del mensaje excede la MTU que puede transportar una capa inferior de la red. Si la longitud del mensaje excede la MTU, se lleva a cabo el procesamiento de MTU.

El procesamiento de MTU para un mensaje que realiza el SAC o el SNS puede tener distintos mecanismos de procesamiento en función del tipo del mensaje. Para un mensaje IPV4, el SAC o el SNS dividen primero el mensaje de acuerdo con el principio de IP. A continuación, el SAC o el SNS mapean el mensaje dividido y, a continuación, lo envían a través del túnel. Para un mensaje IPV6, el procesamiento de MTU por parte del SAC y del SNS incluye dos métodos. De acuerdo con un método, el SAC o el SNS informan a una fuente que envía el mensaje, a través de un mensaje ICMP, que el mensaje es demasiado largo de modo que es necesario acortar la longitud del mensaje (se avisa de una MTU deseada) y, por lo tanto, el SAC o el SNS descartan el mensaje. De acuerdo con el otro método, el SAC o el SNS primero dividen el mensaje y, a continuación, el homólogo (el SAC y el SNS son homólogos entre sí) ensambla de nuevo el mensaje recibido. En esta situación, debido a que en IPv6 no se proporciona ningún mecanismo de segmentación o reconstrucción, es necesario añadir al encabezado STP la información para identificar una segmentación o un reconstrucción, por ejemplo, un número de secuencia del mensaje así como identificadores de inicio y terminación, de modo que el SAC o el SNS puedan llevar a cabo el proceso de segmentación o de reconstrucción en función de la información de segmentación o reconstrucción.

De acuerdo con el décimo modo de realización, se proporciona un proceso de terminación de la sesión de acceso. La terminación de la sesión de acceso del sistema remoto incluye una terminación de la sesión iniciada de forma activa por parte del sistema remoto, y una terminación pasiva de la sesión de acceso.

La terminación de la sesión iniciada de forma activa por el sistema remoto incluye el inicio de una petición para la terminación de la sesión de acceso por parte del sistema remoto, por ejemplo, enviando un mensaje Release del DHCP, un mensaje Logoff del EAPoL del 802.1x; recibir, por parte del SAC, la petición de terminación de la sesión iniciada por el sistema remoto; notificar al SNS, por parte del SAC, que termine la sesión STP correspondiente, donde la notificación incluye un mensaje Call-Disconnect-Notify (CDN) para el SNS por parte del SAC; terminar la sesión STP por parte del SAC o del SNS; y terminar, por parte del SAC o del SNS, el túnel STP que se establece dinámicamente si la sesión STP es la última sesión sobre el túnel STP.

La terminación pasiva de la sesión de acceso incluye: terminar la sesión STP por parte del SAC o del SNS, por ejemplo, terminar la sesión STP por parte del SAC o del SNS si el SAC o el SNS detectan que la sesión de acceso se encuentra en un estado anormal a través de un mecanismo para mantener activa la sesión; o notificar al SAC o al SNS que terminen la sesión STP a través de órdenes desde un sistema o software de aplicación de gestión de red.

De acuerdo con un modo de realización de la invención, además se proporciona un sistema para acceder a una sesión de Capa 3. El sistema para acceder a una sesión de Capa 3 incluye un equipo en el extremo de la red configurado para recibir un mensaje desde un sistema remoto, realizar un mapeo STP del mensaje y, a continuación, enviarlo a un servidor de sesiones de red (SNS) a través del STP; llevar a cabo una terminación del túnel STP de acuerdo con el mensaje procedente del SNS, llevar a cabo un mapeo de la capa de enlace o un mapeo de la capa física en relación con un mensaje que es necesario reenviar y, después, enviarlo al sistema remoto; un servidor de sesiones de red, configurado para realizar una terminación del túnel de acuerdo con un mensaje

procedente de un SAC y clasificar el mensaje en función del encabezado del mensaje STP; mapear una dirección de destino del mensaje de datos de Capa 3 procedente de un sistema final con un túnel STP, y reenviarlo al sistema remoto a través del SAC sobre el túnel STP.

Específicamente, el equipo en el extremo de la red incluye: una primera unidad de recepción, configurada para recibir un mensaje de un sistema remoto; una primera unidad de procesamiento de mensajes, configurada para mapear el mensaje; una primera unidad de envío, configurada para enviar el mensaje, después de llevar a cabo un mapeo STP, a un servidor de sesiones de acceso (SNS); una segunda unidad de recepción, configurada para recibir un mensaje STP desde el SNS; una segunda unidad de procesamiento de mensajes, configurada para realizar una terminación del túnel STP de acuerdo con el mensaje procedente del SNS y realizar un mapeo con una capa de enlace o una capa física; una segunda unidad de envío, configurada para enviar al sistema remoto el mensaje mapeado; una unidad de establecimiento de túneles STP, configurada para negociar con el SNS el establecimiento de un túnel STP; una unidad de establecimiento de sesiones STP, configurada para negociar con el SNS el establecimiento de una sesión STP; una unidad de detección del tiempo de utilización, configurada para obtener un nuevo tiempo de utilización de la sesión después de recibir del SNS una confirmación del aumento del tiempo de utilización de la sesión y para notificar al sistema remoto; una unidad de detección de sesión activa, configurada para mantener activa una sesión IP mediante un mensaje de detección de estado que interactúa con el sistema remoto. El equipo en el extremo de la red puede incluir, además, una unidad proxy ARP, configurada para actuar como intermediaria para un equipo en la red de origen (por ejemplo, un SNS) para procesar (por ejemplo, para responder a) un mensaje de petición de dirección ARP desde el sistema remoto y mapear una dirección IP con una dirección MAC.

La primera unidad de procesamiento de mensajes incluye, específicamente una subunidad de mapeo, configurada para mapear el mensaje con un túnel STP y una sesión en función de parámetros de un encabezado de mensaje y/o un ID de enlace del mensaje de datos; y una subunidad de encapsulado, configurada para encapsular el paquete IP en un mensaje STP.

La segunda unidad de procesamiento de mensajes incluye, específicamente, una subunidad de extracción de mensajes de Capa 3, configurada para eliminar un encabezado del túnel de los mensajes de datos o un encabezado del mensaje STP, y extraer el mensaje de Capa 3; una subunidad de obtención de direcciones de Capa 2, configurada para obtener una dirección de Capa 2 del mensaje de Capa 3 en función de una dirección IP de destino del mensaje de Capa 3; y una subunidad de adaptación, configurada para adaptar el mensaje de Capa 3 en función de la dirección de Capa 2.

El servidor de sesiones de red incluye, específicamente, una tercera unidad de recepción, configurada para recibir un mensaje desde un SAC; una tercera unidad de procesamiento de mensajes, configurada para realizar una terminación del túnel de acuerdo con el mensaje procedente del SAC, y clasificar el mensaje en función del encabezado del mensaje STP; una tercera unidad de envío configurada para enviar el mensaje en función del resultado del procesamiento de clasificación; una cuarta unidad de recepción, configurada para recibir un mensaje de datos de Capa 3 desde el sistema final; una cuarta unidad de procesamiento de mensajes, configurada para mapear una dirección de destino del mensaje de datos de la Capa 3 procedente del sistema final con el túnel STP, y realizar una adaptación STP de los datos de Capa 3; y una cuarta unidad de envío, configurada para enviar al sistema remoto el mensaje adaptado a través del túnel STP.

La tercera unidad de procesamiento de mensajes incluye, específicamente, una subunidad de terminación de túneles, configurada para obtener información de conexión de un túnel y/o una sesión, y eliminar un encabezado de túnel del mensaje; y una subunidad de procesamiento de clasificación, configurada para eliminar un encabezado de mensajes de acuerdo con un mensaje de datos con el encabezado del mensaje STP de datos, y enviarlo en función de una dirección de destino del mensaje de Capa 3; y configurada para enviarlo a un equipo asociado para el procesado en función de un tipo de mensaje en términos de un mensaje de control.

La cuarta unidad de procesamiento de mensajes incluye, específicamente, una subunidad de mapeo, configurada para mapear una dirección de destino del mensaje de datos de Capa 3 procedente del sistema final con el túnel STP; y una subunidad de adaptación, configurada para incorporar un encabezado del mensaje STP en los datos de Capa 3.

De acuerdo con los modos de realización de la presente invención, un usuario remoto puede atravesar una red de acceso a través de, por ejemplo, una sesión IP de acceso y, de este modo, acceder a una red de origen del usuario utilizando una VPDN o un mecanismo mayorista en relación con un método de acceso de sesión de Capa 3. La red de acceso incluye una red mayorista o una red pública en un escenario mayorista, mientras que la red de origen del usuario se refiere a una red de suscripción del usuario, incluyendo una red minorista, o una Intranet de empresa en un escenario mayorista, o una red de origen en un escenario nómada. Es posible que una tecnología de enlace de capa 2 de la red de acceso sea diferente de la de la red de origen del usuario. En consecuencia, se propone una sesión de Capa 3 unificada para el acceso para abordar el problema de una interconexión entre la tecnología de enlace de Capa 2 de la red de acceso y la de la red de origen del usuario, ya que la sesión de Capa 3 puede recubrir la tecnología de enlace de Capa 2 de la red de acceso y la de la red de origen del usuario.

Con la descripción de los modos de realización anteriores, aquellos experimentados en la técnica observan fácilmente que la presente invención se puede implementar con hardware, y también se puede implementar con software sobre la necesaria plataforma hardware. A partir de esta premisa, algunas soluciones proporcionadas por la presente invención pueden llevarse a la práctica mediante un producto software. El producto software se puede almacenar en un medio de almacenamiento no volátil (puede ser un CD-ROM, un disco flash USB, un disco duro móvil, etc.). El producto software puede incluir un conjunto de instrucciones que permitan a un dispositivo de computación (puede ser un ordenador personal, un servidor, o un dispositivo de red, etc.) poner en práctica métodos de acuerdo con varios modos de realización de la presente invención.

En resumen, lo anterior son únicamente algunos ejemplos de modos de realización de la presente invención y no pretenden limitar el alcance de la presente invención. Cualquier modificación, equivalencia, mejora realizada dentro del principio de la presente invención se debe interpretar que se incluyen dentro del alcance de la presente invención.

REIVINDICACIONES

1. Un método de acceso de sesión basado en Capa 3 para una Red Privada Virtual a través de Teléfono, VPDN, que comprende:

establecer (s802, s904, s1003), por parte de un concentrador de sesiones de acceso, SAC, en una red de acceso de un usuario, una sesión de acceso con un sistema remoto;

establecer (s805, s906, s1009), por parte del SAC, una sesión del Protocolo de Transporte de Sesión, STP, con un servidor de sesiones de red, SNS, en la red de origen del usuario;

establecer (s806, s906, s1016), por parte del SAC, una relación de mapeo entre la sesión de acceso del sistema remoto, y la sesión STP, en donde el paso que establece la relación de mapeo comprende, además, establecer la relación de mapeo de un ID de la sesión de acceso del sistema remoto, y/o un ID de la capa de enlace o de la capa física de la sesión de acceso, con un túnel STP y un ID de la sesión STP; y

reenviar (s807, s908, s1017), por parte del SAC, mensajes entre el sistema remoto y el SNS de acuerdo con la relación de mapeo.

2. El método de la reivindicación 1, que comprende, además:

establecer (s806, s1016), por parte del SNS, la relación de mapeo entre la sesión de acceso del sistema remoto y la sesión STP; y

reenviar (s807, s908, s1017), por parte del SNS, mensajes entre el sistema remoto y la red de origen de acuerdo con la relación de mapeo.

3. El método de la reivindicación 1 ó 2, en donde el proceso de establecimiento de una sesión de acceso con el sistema remoto comprende:

recibir (s802, s1003), por parte del SAC, un mensaje de negociación para establecer una sesión de acceso procedente del sistema remoto;

mapear (s805, s1009), por parte del SAC, el mensaje de negociación con un mensaje de control de la negociación de la sesión STP y enviar (s805) al SNS el mensaje de control de la negociación de la sesión STP;

recibir (s806, s1015) desde el SNS, por parte del SAC, un mensaje de control de la negociación de la sesión STP; y

responder (s806, s1017) al sistema remoto, por parte del SAC, con un mensaje de negociación para establecer una sesión de acceso indicando que se ha establecido la sesión de acceso.

4. El método de la reivindicación 3, que comprende, además:

establecer (s806), por parte del SAC, la sesión STP con el SNS de acuerdo con el mensaje de control de la negociación de la sesión STP recibido desde el SNS.

5. El método de la reivindicación 3, que comprende, además:

reenviar al SNS, por parte del SAC, un mensaje de petición de dirección desde el sistema remoto;

enviar (s1012) a un servidor de direcciones, por parte del SNS, el mensaje de petición de dirección;

recibir (s1013) desde el servidor de direcciones, por parte del SNS, una dirección IP y un tiempo de utilización asignados al sistema remoto;

establecer con el SAC, por parte del SNS, una sesión de acceso del sistema remoto identificado por la dirección IP y una sesión STP; y

enviar (s1014), por parte del SNS, una respuesta al mensaje de control de la negociación de la sesión STP, en donde el mensaje comprende parámetros de la sesión de acceso del sistema remoto y la sesión STP.

6. El método de la reivindicación 5, que comprende, además:

detectar, por parte del SAC o del SNS, el tiempo de utilización de la dirección IP de la sesión de acceso del sistema remoto;

terminar, por parte del SAC o del SNS, la sesión STP si expira el tiempo de utilización de la dirección IP o falla la solicitud de mantenimiento de la dirección IP.

7. El método de la reivindicación 5 ó 6, en donde la relación de mapeo entre la sesión de acceso del sistema

remoto y la sesión STP comprende una vinculación de la dirección IP de la sesión de acceso, la sesión STP y un formato para encapsular un mensaje STP de datos.

8. El método de la reivindicación 1, que comprende, además:

recibir (s1501), por parte del SAC, un mensaje procedente del sistema remoto;

determinar (s1502), por parte del SAC, un tipo del mensaje;

mapear (s1505, s1508), por parte del SAC, el mensaje con un mensaje STP si el mensaje es un mensaje de datos que es necesario reenviar por STP o si es un mensaje de control que no necesita procesamiento local; y

enviar (s1509) al SNS, por parte del SAC, el mensaje STP.

9. El método de la reivindicación 8, que comprende, además:

llevar a cabo (s1507), por parte del SAC, un procesamiento local del mensaje si el mensaje es un mensaje de control que necesita procesamiento local;

en donde el procesamiento local comprende:

responder, por parte del SAC, con un mensaje Reply de ARP en función de una dirección o un ID de enlace incluidos en el mensaje, donde el mensaje de control es un mensaje de petición de Proxy ARP; o

determinar, por parte del SAC, el estado de la sesión de acceso cuando el mensaje es un mensaje de confirmación de detección de estado.

10. El método de la reivindicación 1, que comprende, además:

recibir (s1601), por parte del SAC, un mensaje STP desde el SNS;

determinar (s1602), por parte del SAC, un tipo del mensaje STP;

mapear (s1603, s1606), por parte del SAC, el mensaje STP con un mensaje de comunicación entre el SAC y el sistema remoto si el mensaje es un mensaje de datos o un mensaje de control que no necesita un procesamiento local; y

enviar (s1607) al sistema remoto, por parte del SAC, el mensaje de comunicación.

11. Un sistema de acceso de sesión basado en Capa 3, que comprende: un sistema remoto, un concentrador de sesiones de acceso, SAC, un servidor de sesiones de red, SNS, en donde

el concentrador de sesiones de acceso se encuentra en una red de acceso de un usuario, y se configura para establecer una sesión de acceso con el sistema remoto; establecer una sesión del Protocolo de Transporte de Sesión, STP, con el SNS en la red de origen del usuario; establecer una relación de mapeo entre la sesión de acceso del sistema remoto y la sesión STP y reenviar mensajes entre el sistema remoto y el SNS de acuerdo con la relación de mapeo, en donde el SAC se configura para establecer la relación de mapeo de un ID de la sesión de acceso del sistema remoto y/o un ID de la capa de enlace o de la capa física de la sesión de acceso, con un túnel STP, y un ID de la sesión STP.

12. El sistema de la reivindicación 11, en donde el SNS se configura para establecer una relación de mapeo entre la sesión de acceso del sistema remoto y la sesión STP, y para reenviar mensajes entre el sistema remoto y la red de origen de acuerdo con la relación de mapeo.

13. El sistema de la reivindicación 11 ó 12, en donde el SAC se configura, además, para recibir desde el sistema remoto un mensaje de negociación para establecer una sesión de acceso; mapear el mensaje de negociación con un mensaje de control de la negociación de la sesión STP; enviar al SNS el mensaje de control de la negociación de la sesión STP; recibir desde el SNS un mensaje de control de la negociación de la sesión STP; y responder al sistema remoto con un mensaje de negociación para establecer una sesión de acceso indicando que se ha establecido la sesión de acceso.

14. El sistema de la reivindicación 11 ó 12, en donde el SAC se configura, además, para recibir un mensaje desde el sistema remoto; determinar un tipo del mensaje; mapear el mensaje con un mensaje STP si el mensaje es un mensaje de datos que necesita reenviarse por STP o un mensaje de control que no necesita un procesamiento local; y enviar al SNS el mensaje STP.

15. El sistema de la reivindicación 11 ó 12, en donde el SAC se configura, además, para recibir desde el SNS un mensaje STP; determinar un tipo del mensaje STP; mapear el mensaje STP con un mensaje de comunicación entre el SAC y el sistema remoto si el mensaje es un mensaje de datos o un mensaje de control que no necesitan un procesamiento local; y enviar al sistema remoto un mensaje de comunicación.

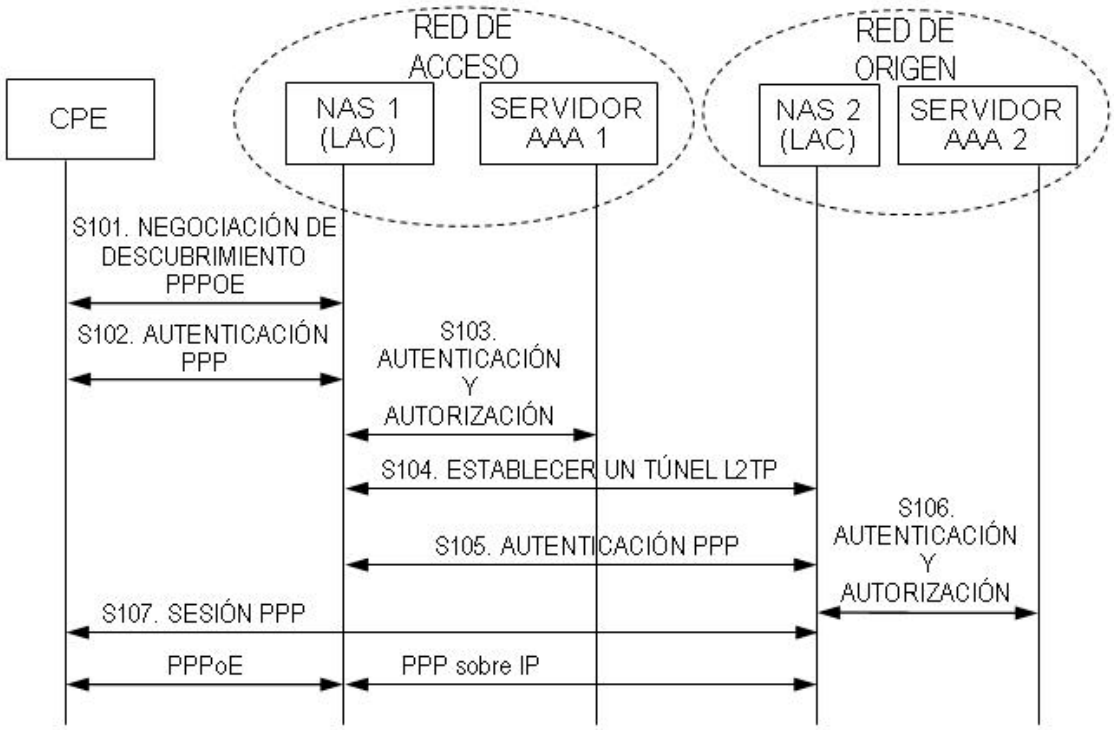
RED DE ACCESO
RED DE ORIGEN
CPE
NAS 1 (LAC)
SERVIDOR AAA 1
NAS 2 (LAC)
SERVIDOR AAA 2
S101. NEGOCIACIÓN DE DESCUBRIMIENTO PPPOE
S102. AUTENTICACIÓN PPP
S103. AUTENTICACIÓN Y AUTORIZACIÓN
S104. ESTABLECER UN TÚNEL L2TP
S105. AUTENTICACIÓN PPP
S106. AUTENTICACIÓN Y AUTORIZACIÓN
S107. SESIÓN PPP
PPPoE
PPP sobre IP

FIG 1

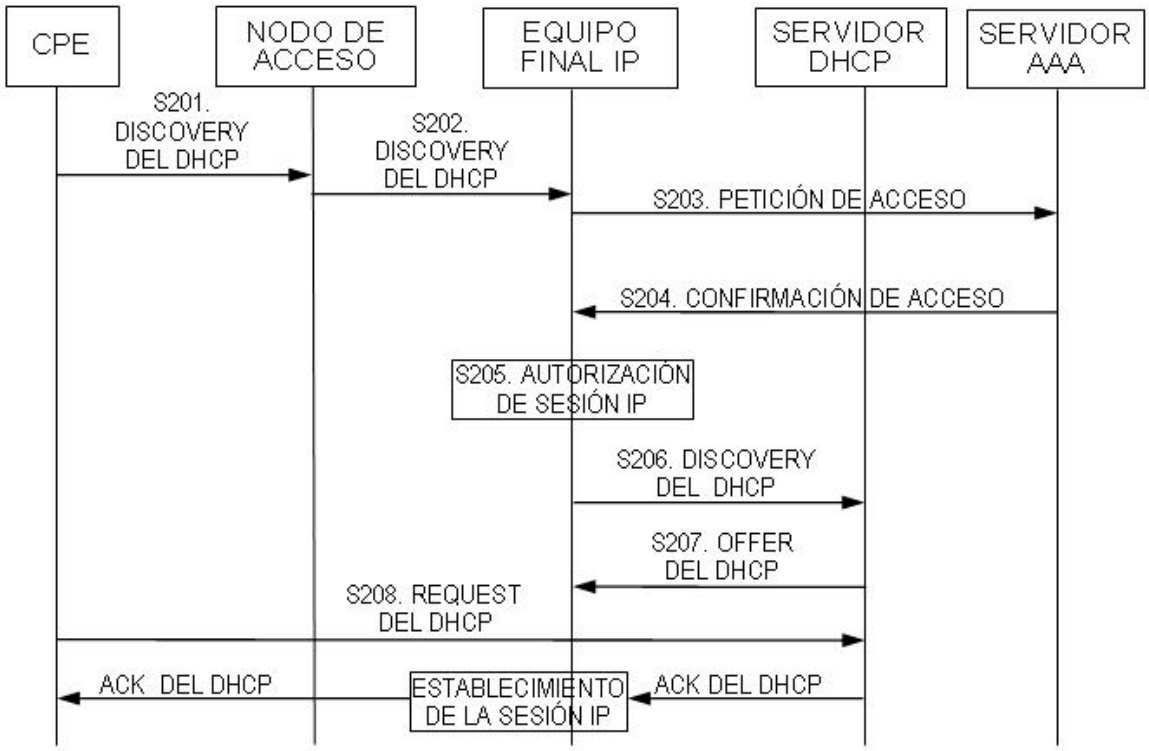
CPE
NODO DE ACCESO
EQUIPO FINAL IP
SERVIDOR DHCP
SERVIDOR AAA
S201. DISCOVERY DEL DHCP
S202. DISCOVERY DEL DHCP
S203. PETICIÓN DE ACCESO
S204. CONFIRMACIÓN DE ACCESO
S205. AUTORIZACIÓN DE SESIÓN IP
S206. DISCOVERY DEL DHCP
S207. OFFER DEL DHCP
S208. REQUEST DEL DHCP
ACK DEL DHCP
ESTABLECIMIENTO DE LA SESIÓN IP
ACK DEL DHCP

FIG 2

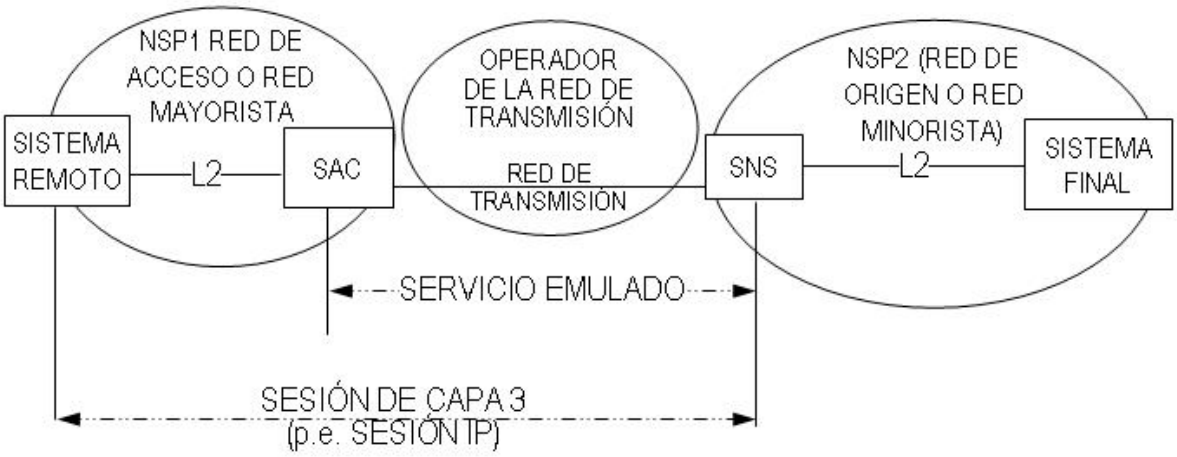
NSP1 RED DE ACCESO O RED MAYORISTA
OPERADOR DE LA RED DE TRANSMISIÓN
NSP2 (RED DE ORIGEN O RED MINORISTA)
SISTEMA REMOTO
L2
SAC
RED DE TRANSMISIÓN
SNS
L2
SISTEMA FINAL
SERVICIO EMULADO
SESIÓN DE CAPA 3
(p.e. SESIÓN TP)

FIG 3

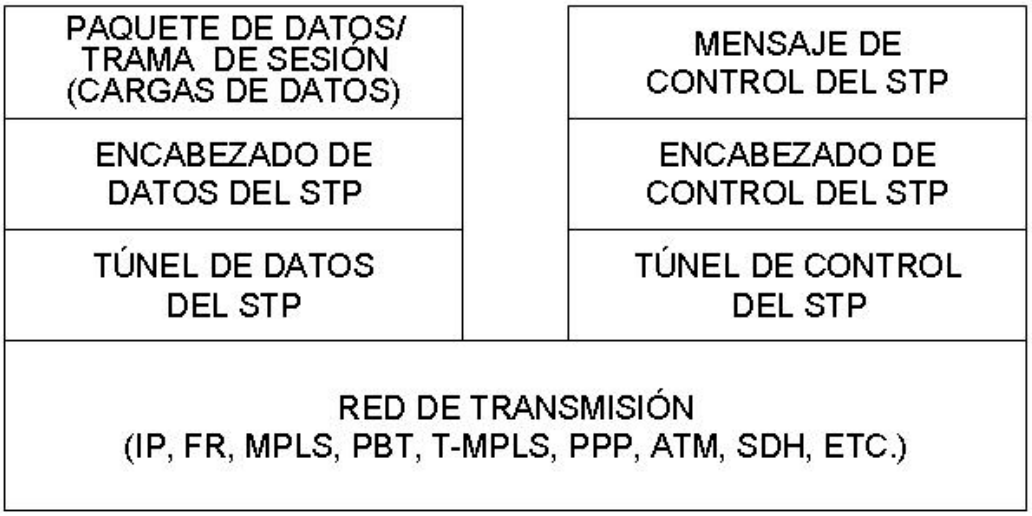
PAQUETE DE DATOS/ TRAMA DE SESIÓN (CARGAS DE DATOS)
ENCABEZADO DE DATOS DEL STP
TÚNEL DE DATOS DEL STP
MENSAJE DE CONTROL DEL STP
ENCABEZADO DE CONTROL DEL STP
TÚNEL DE CONTROL DEL STP
RED DE TRANSMISIÓN
(IP, FR, MPLS, PBT, T-MPLS, PPP, ATM, SDH, ETC.)

FIG 4

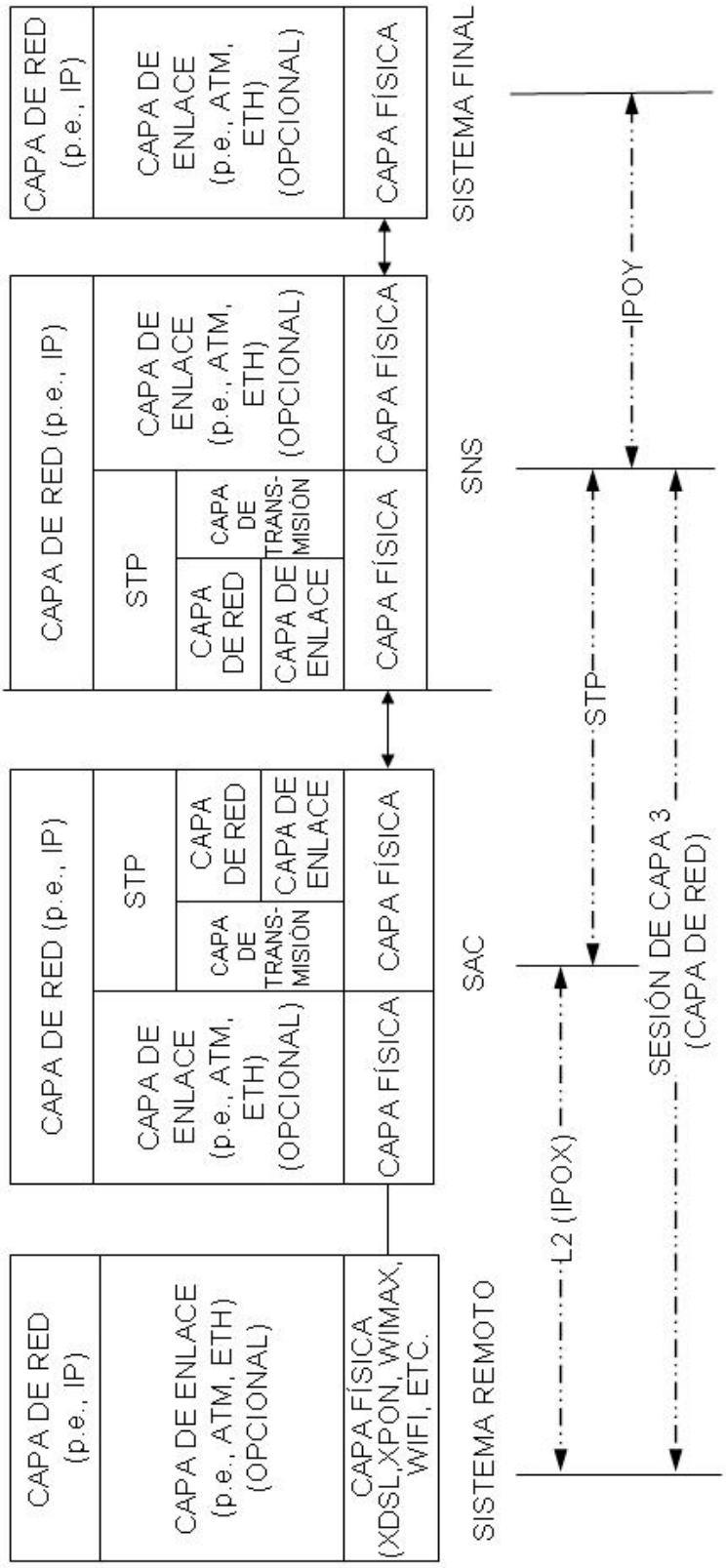
CAPA DE RED (p.e., IP)
CAPA DE ENLACE (p.e., ATM, ETH) (OPCIONAL)
CAPA FÍSICA (XDSL, XPON, WIMAX, WIFI, ETC.
SISTEMA REMOTO
CAPA DE RED (p.e., IP)
CAPA DE ENLACE (p.e., ATM, ETH) (OPCIONAL)
STP
CAPA DE RED
CAPA DE TRANS-MISIÓN
CAPA DE ENLACE
CAPA FÍSICA
CAPA FÍSICA
SAC
CAPA DE RED (p.e., IP)
CAPA DE ENLACE (p.e., ATM, ETH) (OPCIONAL)
STP
CAPA DE RED
CAPA DE TRANS-MISIÓN
CAPA DE ENLACE
CAPA FÍSICA
CAPA FÍSICA
SNS
CAPA DE RED (p.e., IP)
CAPA DE ENLACE (p.e., ATM, ETH) (OPCIONAL)
CAPA FÍSICA
SISTEMA FINAL
L2 (IPOX)
STP
IPOY
SESIÓN DE CAPA 3 (CAPA DE RED)

FIG 5

FIG.6

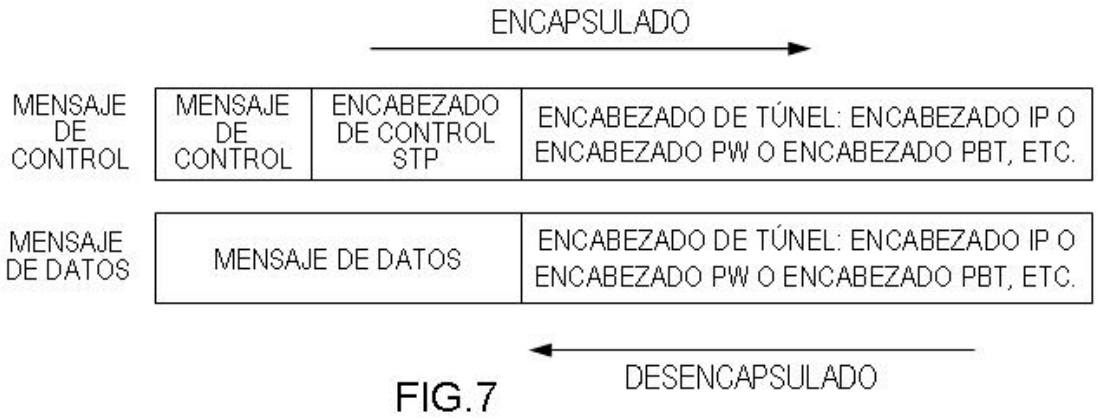

FIG.7

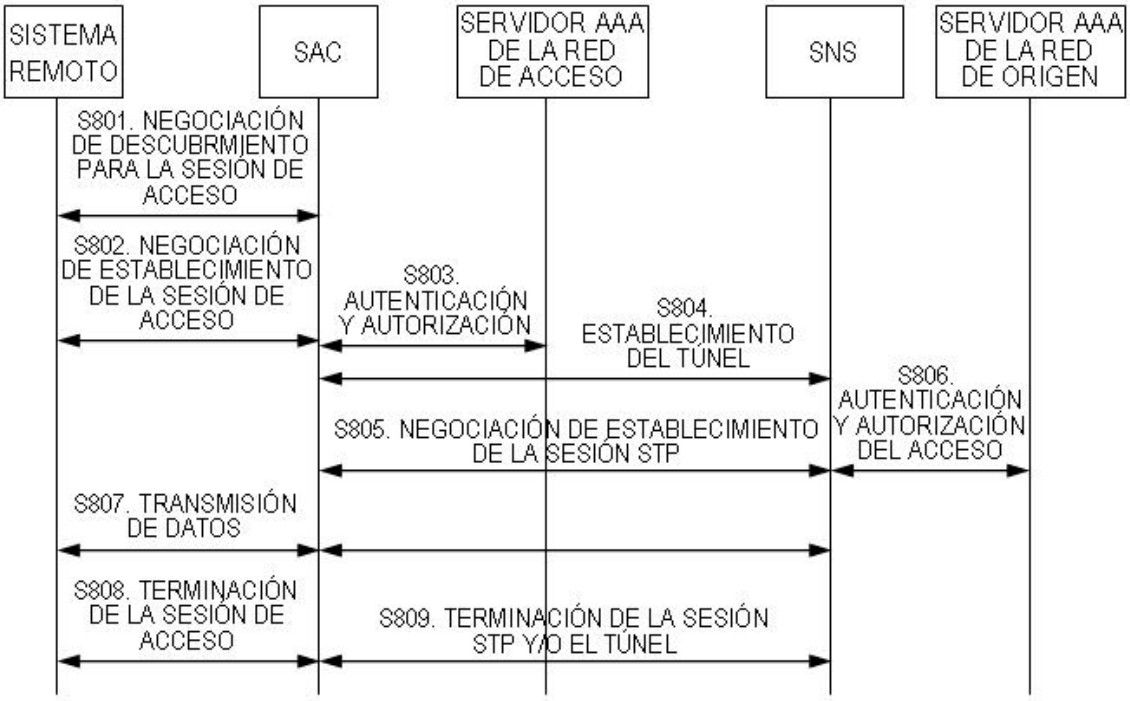

FIG.8

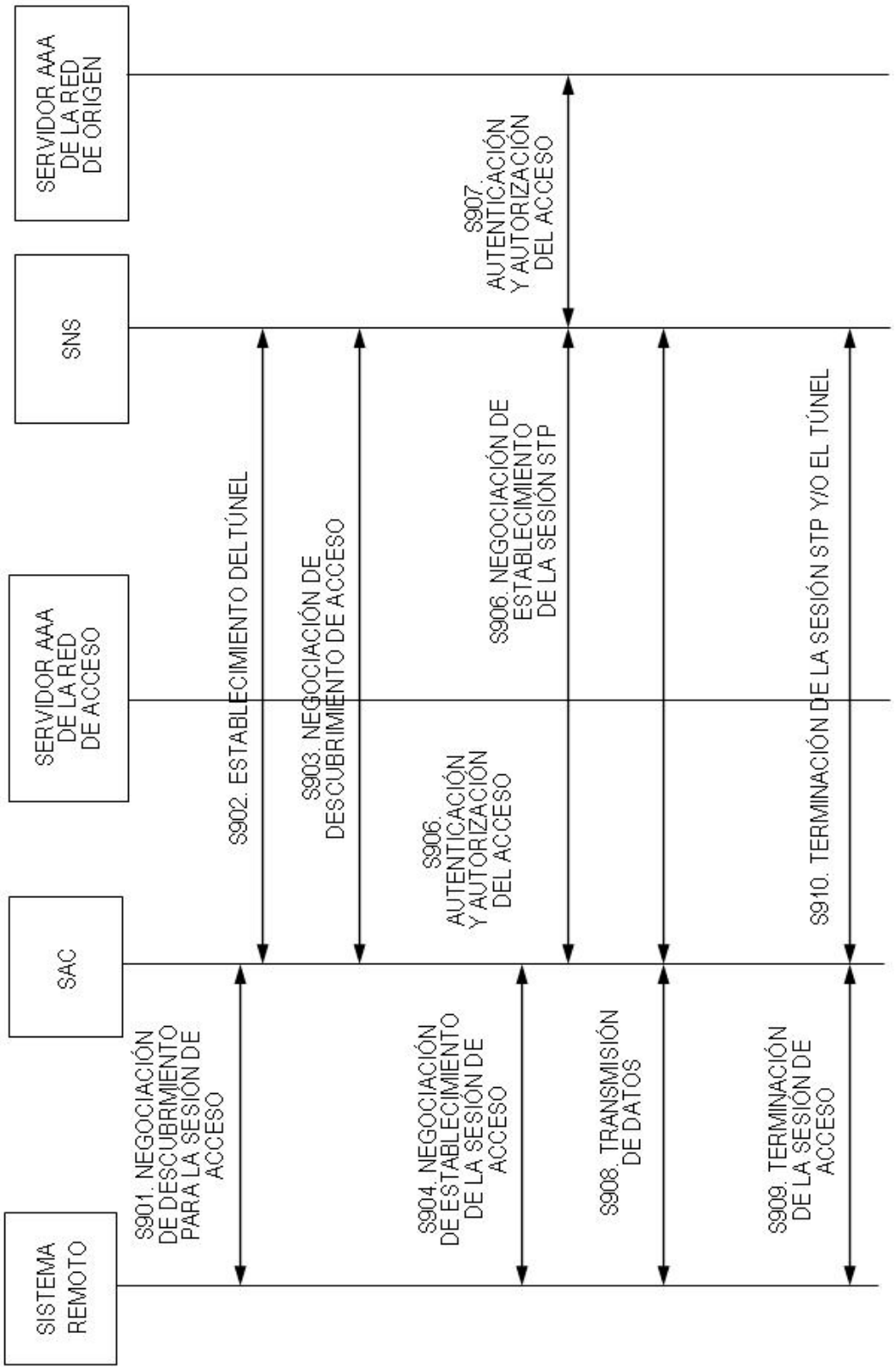
SISTEMA REMOTO
SAC
SERVIDOR AAA DE LA RED DE ACCESO
SNS
SERVIDOR AAA DE LA RED DE ORIGEN
S901. NEGOCIACIÓN DE DESCUBRIMIENTO PARA LA SESIÓN DE ACCESO
S902. ESTABLECIMIENTO DEL TÚNEL
S903. NEGOCIACIÓN DE DESCUBRIMIENTO DE ACCESO
S904. NEGOCIACIÓN DE ESTABLECIMIENTO DE LA SESIÓN DE ACCESO
S906. AUTENTICACIÓN Y AUTORIZACIÓN DEL ACCESO
S906. NEGOCIACIÓN DE ESTABLECIMIENTO DE LA SESIÓN STP
S907. AUTENTICACIÓN Y AUTORIZACIÓN DEL ACCESO
S908. TRANSMISIÓN DE DATOS
S909. TERMINACIÓN DE LA SESIÓN DE ACCESO
S910. TERMINACIÓN DE LA SESIÓN STP Y/O EL TÚNEL

FIG.9

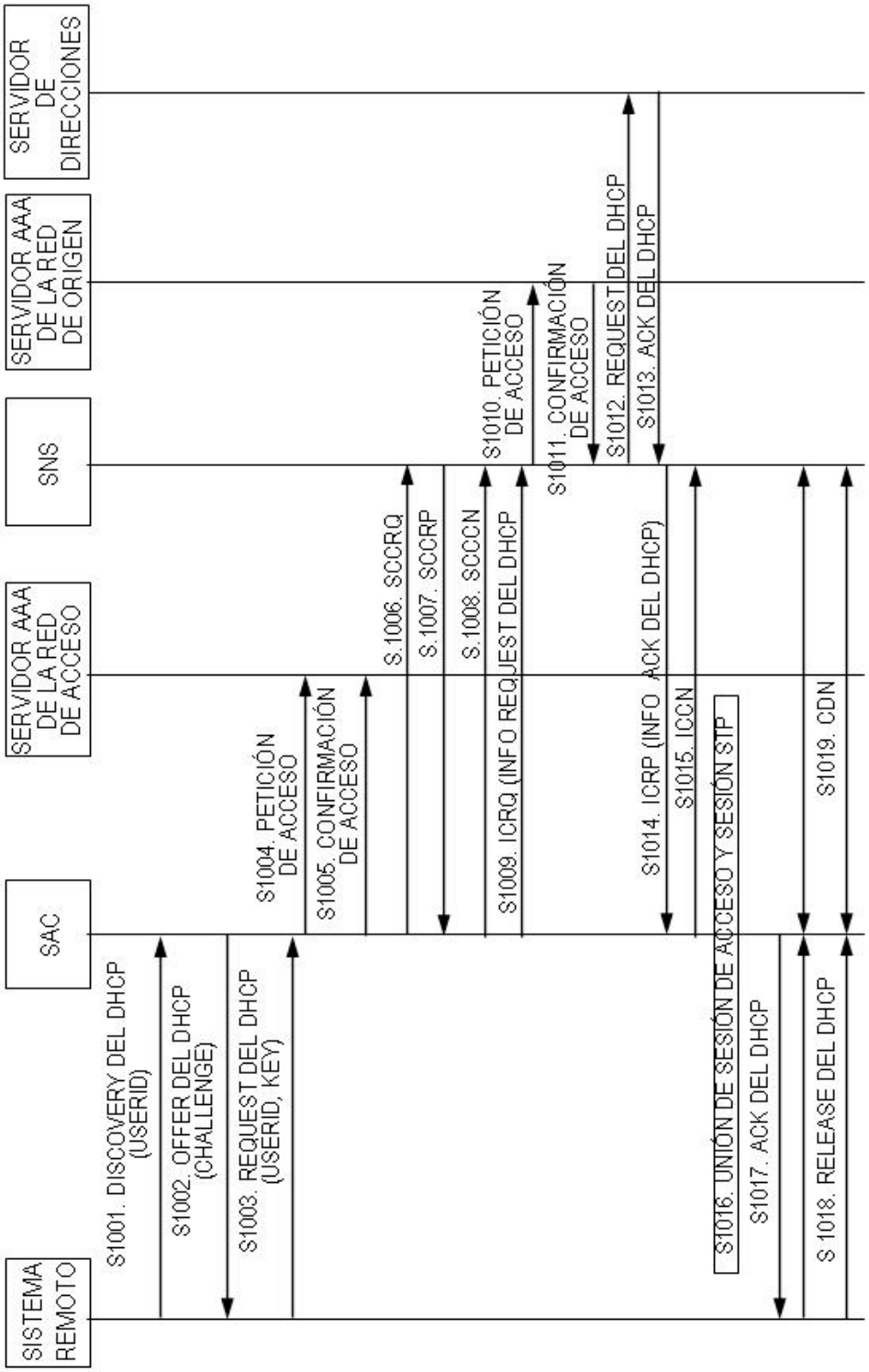
SISTEMA REMOTO
SAC
SERVIDOR AAA DE LA RED DE ACCESO
SNS
SERVIDOR AAA DE LA RED DE ORIGEN
SERVIDOR DE DIRECCIONES
S1001. DISCOVERY DEL DHCP (USERID)
S1002. OFFER DEL DHCP (CHALLENGE)
S1003. REQUEST DEL DHCP (USERID, KEY)
S1004. PETICIÓN DE ACCESO
S1005. CONFIRMACIÓN DE ACCESO
S.1006. SCCRQ
S.1007. SCCRP
S.1008. SCCCN
S1009. ICRQ (INFO REQUEST DEL DHCP
S1010. PETICIÓN DE ACCESO
S1011. CONFIRMACIÓN DE ACCESO
S1012. REQUEST DEL DHCP
S1013. ACK DEL DHCP
S1014. ICRP (INFO ACK DEL DHCP)
S1015. ICCN
S1016. UNIÓN DE SESIÓN DE ACCESO Y SESIÓN STP
S1017. ACK DEL DHCP
S 1018. RELEASE DEL DHCP
S1019. CDN

FIG. 10

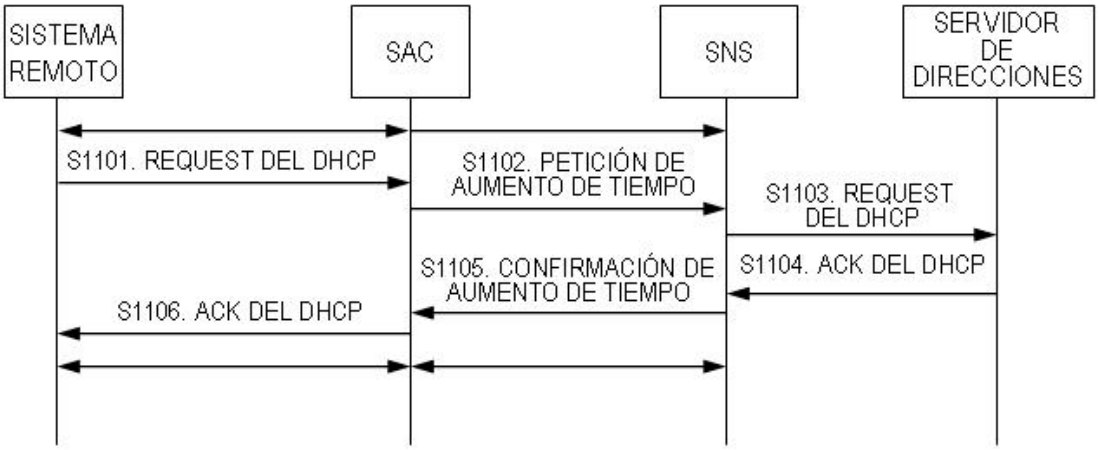

FIG.11

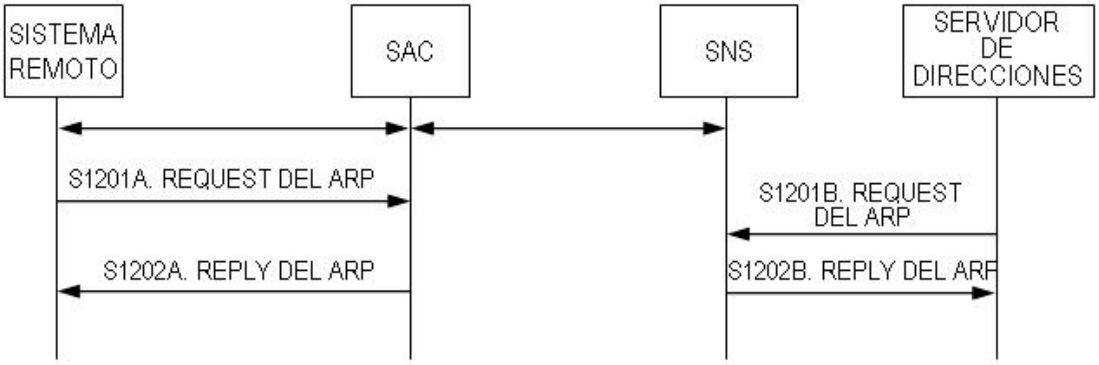

FIG.12

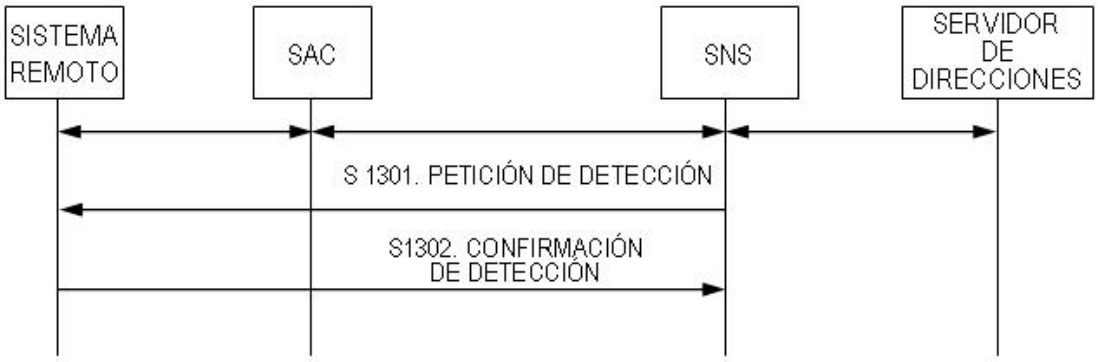

FIG.13

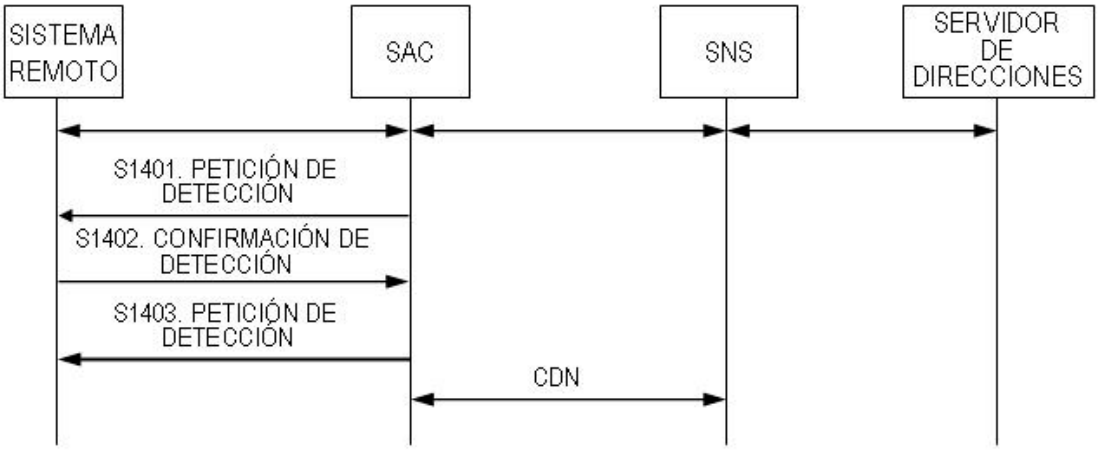
SISTEMA REMOTO
SAC
SNS
SERVIDOR DE DIRECCIONES
S1401. PETICIÓN DE DETECCIÓN
S1402. CONFIRMACIÓN DE DETECCIÓN
S1403. PETICIÓN DE DETECCIÓN
CDN

FIG.14

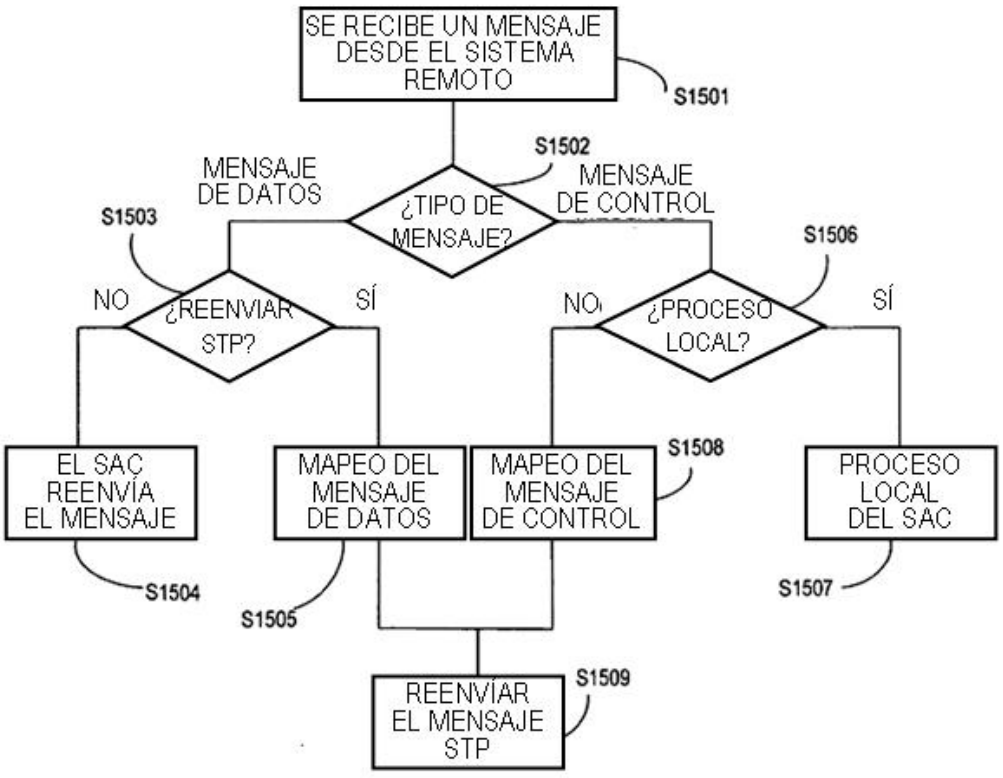
SE RECIBE UN MENSAJE DESDE EL SISTEMA REMOTO
S1501
S1502
MENSAJE DE DATOS
¿TIPO DE MENSAJE?
MENSAJE DE CONTROL
S1503
S1506
NO
¿REENVIAR STP?
SÍ
NO
¿PROCESO LOCAL?
SÍ
EL SAC REENVÍA EL MENSAJE
MAPEO DEL MENSAJE DE DATOS
MAPEO DEL MENSAJE DE CONTROL
S1508
PROCESO LOCAL DEL SAC
S1504
S1505
S1507
REENVIAR EL MENSAJE STP
S1509

FIG.15

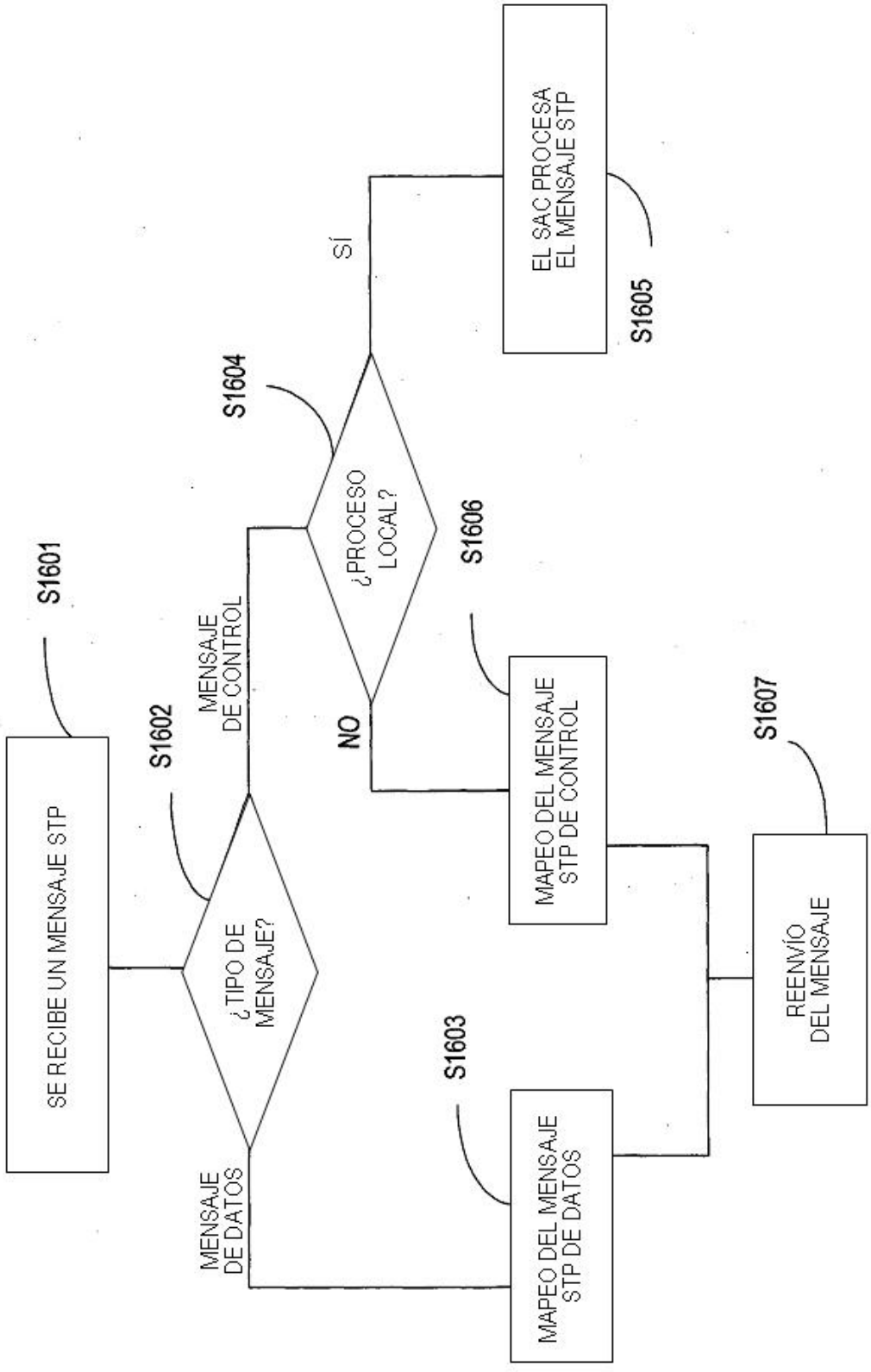
S1601
SE RECIBE UN MENSAJE STP
S1602
¿TIPO DE MENSAJE?
MENSAJE DE CONTROL
MENSAJE DE DATOS
S1603
MAPEO DEL MENSAJE STP DE DATOS
S1604
¿PROCESO LOCAL?
SÍ
NO
S1605
EL SAC PROCESA EL MENSAJE STP
S1606
MAPEO DEL MENSAJE STP DE CONTROL
S1607
REENVÍO DEL MENSAJE

FIG.16