

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 834 031**

51 Int. Cl.:

H04L 12/24 (2006.01)

G06F 16/11 (2009.01)

H03M 13/37 (2006.01)

H04B 3/32 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **28.04.2017 PCT/EP2017/060256**

87 Fecha y número de publicación internacional: **02.11.2017 WO17186938**

96 Fecha de presentación y número de la solicitud europea: **28.04.2017 E 17720483 (1)**

97 Fecha y número de publicación de la concesión europea: **05.08.2020 EP 3449597**

54 Título: **Una red orquestada impulsada por datos mediante un controlador SDN distribuido ligero activado por voz**

30 Prioridad:

29.04.2016 US 201615142748

10.06.2016 US 201615179726

20.12.2016 WO PCT/EP2016/081921

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

16.06.2021

73 Titular/es:

DCB SOLUTIONS LIMITED (100.0%)

**7 Granville Industrial Estate, 90 Dungannon Road
Dungannon, Tyrone BT70 1NJ, GB**

72 Inventor/es:

**SHAIKH, NAZNEEN;
KRISHNAN, MURALI y
GULAWANI, GIRISH**

74 Agente/Representante:

PONS ARIÑO, Ángel

ES 2 834 031 T3

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

DESCRIPCIÓN

Una red orquestada impulsada por datos mediante un controlador SDN distribuido ligero activado por voz

5 Campo de la invención

La presente divulgación se refiere a redes definidas por software (SDN) y un procedimiento para a las mismas. En particular, pero no exclusivamente, la divulgación se refiere a una plataforma SDN y arquitectura relacionada. Además, la descripción se refiere a la privacidad orquestada y la gestión y el control de amenazas mediante el control de reenvío basado en el flujo de SDN. Además, la presente descripción se refiere a un controlador SDN distribuido activado por voz.

ANTECEDENTES

15 Las redes se vuelven cada vez más complicadas a medida que aumentan de tamaño y son mucho más difíciles de administrar y controlar. En una red tradicional, se requieren considerables recursos de TI para implementar procedimientos como la configuración y el aprovisionamiento. Tradicionalmente, estas tareas las implementaba manualmente un administrador de red. La estrategia SDN automatizó estos procedimientos a través de software.

20 Un controlador SDN comprende un repositorio de instrucciones de control y políticas para la red. El controlador SDN tiene una vista de extremo a extremo de toda la red e información de todas las rutas de red y las capacidades del dispositivo. Como consecuencia, el controlador SDN puede calcular rutas basándose tanto en direcciones de origen como de destino; utilizar diferentes rutas de red para diferentes tipos de tráfico y reaccionar a la condición de los cambios de red. Si bien una estrategia de control centralizado permite que una red se gestione de manera más eficiente que la estrategia convencional, pueden producirse retrasos en vista del gran volumen de decisiones de enrutamiento que deben procesarse de forma centralizada. Además, la estrategia de control centralizado no aborda la granularidad individual de establecer políticas específicas para usuarios finales en millones de dispositivos, en cuanto a cómo se deben controlar sus dispositivos. La estrategia centralizada no tiene en cuenta cómo escalar el controlador SDN operado de forma centralizada que controla un gran número de usuarios distribuidos con preferencias granulares y un gran número de dispositivos finales. Estas limitaciones son inherentes a la estrategia totalmente centralizada y son específicamente indeseables cuando el control SDN se utiliza para administrar millones de dispositivos conectados a suscriptores de Internet residencial o empresarial.

Además, esta estrategia centralizada no tiene en cuenta la escala completa y el uso de los análisis que se pueden recopilar. Esta estrategia no aprovecha las valiosas capacidades de referencia histórica de estos datos y su capacidad para ser utilizado para impulsar la gestión y el control de red proactivos, para impulsar aplicaciones de seguridad, para computar aplicaciones de planificación de infraestructura o para crear una resolución automática de fallas.

40 Por tanto, existe la necesidad de un procedimiento para controlar una red definida por software (SDN), y un controlador SDN que aborde al menos algunos de los inconvenientes de la técnica anterior.

Se han creado muchas aplicaciones para violar la seguridad en una red, dañar la conectividad o los sistemas de terceros, robar datos, amenazar o bloquear sistemas e invadir la privacidad de otros. Su evolución comenzó poco después del comienzo de la era de las computadoras e incluye múltiples tipos de virus, malware, adware, troyanos, denegación de servicio (DOS), DOS distribuido, spyware, etc.

Además, los modelos comerciales cambiantes de las empresas ahora significan que cuando un cliente compra un producto de software o incluso usa lo que se considera software legítimo, esto permite que tanto las empresas legítimas como las de malas intenciones recopilen cantidades muy significativas de datos personales del usuario. El consumidor generalmente desconoce el nivel de seguimiento y monitoreo que tiene lugar mediante lo que considera productos legítimos porque el consumidor ha aceptado inadvertidamente términos y condiciones que pueden no ser válidos según las regulaciones locales del país donde reside.

55 La mayoría de estos desarrollos de violación de seguridad y violación de privacidad se están utilizando para algún tipo de propósito malicioso en una escala variable. Los problemas cambiantes y en constante evolución que enfrenta el consumidor en relación tanto con la violación de la seguridad como con la violación de la privacidad se pueden considerar frente a la forma histórica en que evolucionaron los virus. Hace algunos años era obvio cuando estaba presente una infección por virus. Los virus del pasado fueron escritos en gran parte por aficionados y tendían a ser obvios, ya que mostraban comportamientos destructivos o ventanas emergentes. Sin embargo, los virus modernos a menudo están escritos por profesionales y son financiados por organizaciones con malas intenciones. Con estos niveles de actividades de malas intenciones que experimentan los usuarios finales, se requiere una nueva estrategia para abordar las preocupaciones de seguridad y privacidad de los usuarios finales.

65 Por tanto, existe la necesidad de un procedimiento para proporcionar seguridad en una red definida por software (SDN) que aborde al menos algunos de los inconvenientes de la técnica anterior. Además, existe la necesidad de un

controlador de seguridad de red que también supere al menos algunos de los inconvenientes de la técnica anterior.

La solicitud PCT WO 2015/071888 A1 divulga sistemas y procedimientos para garantizar supuestamente el aislamiento de múltiples inquilinos en un centro de datos. Se enseña que se puede utilizar un conmutador, o conmutador virtualizado, para desmultiplexar el tráfico entrante entre varios inquilinos de los centros de datos y para dirigir el tráfico al segmento virtual apropiado para un inquilino identificado. También se enseña que el conmutador puede almacenar información de identificación de inquilinos recibida de un controlador maestro y reglas de reenvío de paquetes recibidas de al menos un controlador de inquilinos. Las reglas de manejo de paquetes están asociadas con un inquilino específico y pueden usarse para reenviar tráfico a su destino.

La solicitud de patente de Estados Unidos US 2014/317261 A1 describe un procedimiento que comprende la identificación, mediante un orquestador ejecutado por una máquina física, de una pluralidad de funciones de red virtualizadas necesarias para la implementación de un servicio de red virtualizado para un cliente, teniendo cada función de red virtualizada un contenedor correspondiente y virtualizado distinto que especifica atributos para definir la ejecución de la función de red virtualizada correspondiente dentro de una o más máquinas físicas; y establecer por parte del orquestador un indicador de interdependencia dentro de cada contenedor virtualizado basado en la asociación con el servicio de red virtualizado, supuestamente permitiendo la identificación de cada una de las funciones de red virtualizada como interdependientes para la ejecución coordinada del servicio de red virtualizado.

La solicitud de patente europea EP 1045374 A1 describe dispositivos de red que pueden controlarse mediante una unidad de voz incluida en la red y pueden enviar un documento de dispositivo que describe su funcionalidad y su interfaz de voz a dicha unidad de voz. La unidad de voz combina esos documentos en un documento general que forma la base para traducir comandos de usuario reconocidos en comandos de red de usuario para controlar los dispositivos de red conectados.

El documento CERF G y col. "Progreso en el despliegue y desarrollo adicional del servicio NYNEX VoiceDialing SM", SPEECH COMMUNICATION, ELSEVIER SCIENCE PUBLISHERS, AMSTERDAM, NL, vol. 23, n. ° 1-2, 1 de octubre de 1997 (01-10-1997), es una publicación científica que informa sobre los desarrollos de investigación de los sistemas y procedimientos de reconocimiento de voz. En particular, analiza una transición de la implementación de hardware de un algoritmo de reconocimiento basado en DTW a la implementación, en un DSP de propósito general, de un algoritmo basado en HMM de mezcla multi-gaussiana de densidad continua. También se analizan las supuestas consecuencias de esto, incluida la posibilidad de expandirse más allá del reconocimiento de nombre dependiente del hablante al reconocimiento continuo de dígitos independiente del hablante (SICDR) y el reconocimiento de comandos de control de red activado por voz (VANC).

RESUMEN

En un aspecto, se proporciona un procedimiento implementado por ordenador para controlar una red definida por software (SDN); el procedimiento comprende:

- proporcionar uno o más portales de clientes configurados para facilitar a los usuarios el control de dispositivos en red; generar datos de configuración basados en la entrada recibida de los usuarios a través de los portales de clientes; proporcionar un controlador SDN maestro para gestionar el control del flujo de datos en la red SDN; siendo operable el controlador SDN maestro para generar datos de enrutamiento para los dispositivos en red;
- generar mediante el controlador SDN maestro una pluralidad de controladores agregados discretos, cada uno asociado con un usuario final particular; cada controlador agregado SDN incluye datos de configuración y datos de enrutamiento para un dispositivo asociado en red;
- enviar el controlador agregado SDN por el controlador SDN maestro a los dispositivos en red asociados con los respectivos usuarios finales para controlarlos;
- instalar los controladores agregados SDN en los dispositivos en red; y
- registrar los controladores agregados SDN instalados con el controlador SDN maestro para controlar el enrutamiento de datos desde los dispositivos en red y para controlar la configuración de los dispositivos en red.

La presente divulgación también se refiere a un procedimiento implementado por ordenador para proporcionar seguridad y privacidad en una red definida por software (SDN); el procedimiento comprende:

- proporcionar un controlador SDN maestro para gestionar el control del flujo de datos en la red SDN; siendo operable el controlador SDN maestro para generar datos de enrutamiento para los dispositivos en red;
- generar mediante el controlador SDN maestro una pluralidad de controladores agregados discretos, cada uno asociado con un usuario final particular; cada controlador agregado SDN incluye datos de enrutamiento para un dispositivo asociado en red;
- enviar el controlador agregado SDN por el controlador SDN maestro a los dispositivos en red asociados con los respectivos usuarios finales para controlarlos;
- solicitar acceso a un destino en la red SDN desde un dispositivo en red solicitante;

En un aspecto adicional, la configuración operativa de los dispositivos en red se actualiza cambiando a un canal de

comunicación alternativo para evitar interferencias de dispositivos vecinos.

En un aspecto, el canal de comunicación incluye un canal WIFI.

- 5 En un aspecto adicional, la configuración operativa del dispositivo en red se cambia para reducir el consumo de energía.

En un aspecto, la configuración operativa del dispositivo en red se cambia reprogramando una interfaz de energía.

- 10 En otro aspecto, la configuración operativa del dispositivo en red se cambia para aumentar la prioridad al ancho de banda disponible.

En un aspecto, la configuración operativa del dispositivo en red se cambia para disminuir la prioridad al ancho de banda disponible.

- 15 En un aspecto adicional, los controladores agregados SDN pueden funcionar para asignar un primer ajuste de prioridad a un primer conjunto de dispositivos de red y asignar un segundo ajuste de prioridad a un segundo conjunto de dispositivos de red.

- 20 En un aspecto, el primer ajuste de prioridad está asociado con un primer límite de ancho de banda, y el segundo ajuste de prioridad está asociado con un segundo límite de ancho de banda.

- 25 En otro aspecto, el controlador SDN maestro implementa la orquestación SDN en respuesta a una solicitud de recursos recibida en los portales del cliente. De manera ventajosa, la orquestación de SDN incluye coordinar los elementos de software y hardware de red requeridos para admitir aplicaciones asociadas con la solicitud de recursos. Preferiblemente, la orquestación de SDN incluye generar una instancia de una o más aplicaciones en la nube. En un ejemplo, la orquestación de SDN genera una instancia de virtualización de funciones de red (NFV).

En un aspecto, se genera un perfil de usuario para cada usuario final.

- 30 En otro aspecto, un usuario está autenticado.

En un aspecto ejemplar, los controladores agregados SDN se instalan en un sistema en chip (SOC) de los respectivos dispositivos en red.

- 35 En otro aspecto, los controladores agregados SDN se cargan en el firmware contenido en los respectivos dispositivos en red.

En un aspecto adicional, los controladores agregados SDN son binarios desplegables.

- 40 En un aspecto, el controlador SDN maestro genera un archivo de configuración para cada recurso seleccionado por el usuario final en el portal del cliente.

- 45 En un aspecto adicional, los controladores agregados SDN se envían a una red doméstica para la recopilación de información relacionada con el protocolo de transporte.

En un aspecto, los dispositivos en red son compatibles con al menos una de las especificaciones de interfaz de servicio de datos por cable (DOCSIS), fibra a la X (FTTx), xDSL, línea de abonado digital asimétrica (DSL) y Wi-Fi.

- 50 En otro aspecto, los portales de clientes son interfaces basadas en web.

La presente enseñanza también se refiere a un controlador de red para una red definida por software (SDN), comprendiendo el controlador de red uno o más módulos operables para:

- 55 proporcionar uno o más portales de clientes configurados para facilitar a los usuarios el control de dispositivos en red; generar datos de configuración basados en la entrada recibida de los usuarios a través de los portales de clientes; proporcionar un controlador SDN maestro para gestionar el control del flujo de datos en la red SDN; siendo operable el controlador SDN maestro para generar datos de enrutamiento para los dispositivos en red; generar mediante el controlador SDN maestro una pluralidad de controladores agregados discretos, cada uno asociado con un usuario final particular; cada controlador agregado SDN incluye datos de configuración y datos de enrutamiento para un dispositivo asociado en red; enviar el controlador agregado SDN por el controlador SDN maestro a los dispositivos en red asociados con los respectivos usuarios finales para controlarlos; instalar el controlador agregado SDN en los dispositivos en red; y
- 65 registrar los controladores agregados SDN instalados con el controlador SDN maestro para controlar el enrutamiento de datos desde los dispositivos en red y para controlar la configuración de los dispositivos en red.

Además, la presente divulgación se refiere a un artículo de fabricación que comprende un medio legible por procesador que tiene incorporado un código de programa ejecutable que, cuando es ejecutado por el dispositivo de procesamiento, hace que el dispositivo de procesamiento realice las siguientes acciones:

- 5 proporcionar uno o más portales de clientes configurados para facilitar a los usuarios el control de dispositivos en red; generar datos de configuración basados en la entrada recibida de los usuarios a través de los portales de clientes; proporcionar un controlador SDN maestro para gestionar el control del flujo de datos en la red SDN; siendo operable el controlador SDN maestro para generar datos de enrutamiento para los dispositivos en red;
- 10 generar mediante el controlador SDN maestro una pluralidad de controladores agregados discretos, cada uno asociado con un usuario final particular; cada controlador agregado SDN incluye datos de configuración y datos de enrutamiento para un dispositivo asociado en red; enviar el controlador agregado SDN por el controlador SDN maestro a los dispositivos en red asociados con los respectivos usuarios finales para controlarlos;
- 15 instalar el controlador agregado SDN en los dispositivos en red; y registrar los controladores agregados SDN instalados con el controlador SDN maestro para controlar el enrutamiento de datos desde los dispositivos en red y para controlar la configuración de los dispositivos en red.

Además, la presente enseñanza se refiere a una red definida por software (SDN); el procedimiento comprende:

- 20 proporcionar uno o más portales de clientes configurados para facilitar a los usuarios el control de dispositivos en red; generar datos de configuración basados en la entrada recibida de los usuarios a través de los portales de clientes; proporcionar un controlador SDN maestro para gestionar el control del flujo de datos en la red SDN; siendo operable el controlador SDN maestro para generar datos de enrutamiento para los dispositivos en red;
- 25 generar mediante el controlador SDN maestro una pluralidad de controladores agregados discretos, cada uno asociado con un usuario final particular; cada controlador agregado SDN incluye datos de configuración y datos de enrutamiento para un dispositivo asociado en red; enviar el controlador agregado SDN por el controlador SDN maestro a los dispositivos en red asociados con los respectivos usuarios finales para controlarlos; y
- 30 instalar el controlador agregado SDN en los dispositivos en red.

En un aspecto, se proporciona un procedimiento implementado por ordenador para controlar una red definida por software (SDN); el procedimiento comprende:

- 35 proporcionar una pluralidad de portales de clientes que están configurados para facilitar a los usuarios finales la selección de recursos a través de interfaces de usuario locales; proporcionar un módulo de control maestro en comunicación con los portales del cliente y configurado para gestionar el control de flujo en la red SDN; generar mediante el módulo de control maestro una pluralidad de agentes de control discretos cada uno asociado
- 40 con un usuario final particular y configurado en base a los recursos seleccionados por el usuario final particular; y enviar los agentes de control discretos a los dispositivos locales de los respectivos usuarios finales para controlarlos.

En otro aspecto, los usuarios finales se autentican antes del envío de los agentes de control.

- 45 En un aspecto, el agente de control maestro genera un archivo de configuración para cada recurso que forma parte de los servicios seleccionados por el usuario final.

En otro aspecto, el archivo de configuración se incorpora al agente de control.

- 50 En otro aspecto se habilita el control localizado para servicios específicamente en relación con los servicios que el cliente ha seleccionado

En otro aspecto, el dispositivo final no está simplificado, sino que el control programable está habilitado localmente y específicamente habilitado para el cliente individual.

- 55 En otro aspecto, los análisis detallados de bajo nivel se recopilan directamente del dispositivo y se transfieren a la solución de orquestación para respaldar la gestión y el control del cliente.

- 60 En un aspecto, los agentes de control discretos se envían a una red doméstica para la recopilación de información relacionada con el protocolo de transporte para garantizar la entrega precisa de los servicios de acuerdo con los criterios de control seleccionados por el usuario final.

- 65 En otro aspecto, un plano de control unificado se distribuye a través de múltiples tecnologías de acceso, por ejemplo, DOCSIS, FTTx, xDSL, Wi-Fi, etc., pero sin limitarse a las tecnologías que se proporcionan a modo de ejemplo únicamente, lo que permite a los operadores desplegar y controlar servicios de manera unificada.

En un aspecto adicional, el control granular del dispositivo final se proporciona de modo que, a diferencia de vCPE, no se simplifica, sino que el control programable se habilita localmente y específicamente para el dispositivo individual en relación con los requisitos de servicio al cliente.

5 En un aspecto, se crea una instancia de cada recurso en la nube.

En otro aspecto, el recurso solicitado es accesible a través del portal del cliente.

En otro aspecto, se configura una instancia de virtualización de funciones de red (NFV).

10

La presente divulgación también se refiere a un controlador de red para una red definida por software (SDN), comprendiendo el controlador de red:

- 15 una pluralidad de portales de clientes configurados para facilitar a los usuarios finales la selección de recursos de red a través de interfaces de usuario locales;
- un módulo de control maestro en comunicación con los portales del cliente y configurado para gestionar el control de flujo en la red SDN; siendo operable el módulo de control maestro para generar una pluralidad de agentes de control discretos, cada uno asociado con un usuario final particular y configurado en base a los recursos de red seleccionados por el usuario final particular; y
- 20 un módulo de comunicación configurado para enviar o controlar agentes de control discretos integrados a uno o más dispositivos locales del respectivo usuario final para controlarlos.

Además, la presente divulgación se refiere a un procedimiento implementado por ordenador para controlar una red SDN; el procedimiento comprende:

25

- proporcionar una pluralidad de portales de clientes que están configurados para facilitar a los usuarios finales la selección de recursos de red de la red SDN a través de interfaces de usuario locales;
- proporcionar un módulo de control maestro en comunicación con los portales del cliente y configurado para gestionar el control de flujo en la red SDN;
- 30 generar una pluralidad de agentes de control discretos, cada uno asociado con un usuario final particular y configurado en base a los recursos de red seleccionados por el usuario final particular; y
- enviar los agentes de control discretos a uno o más dispositivos locales del respectivo usuario final para controlarlo localmente.

35 Además, la presente divulgación se refiere a un medio legible por ordenador que comprende instrucciones no transitorias que, cuando se ejecutan, hacen que un procesador lleve un procedimiento para controlar una red SDN; el procedimiento comprende:

- proporcionar una pluralidad de portales de clientes que están configurados para facilitar a los usuarios finales la selección de recursos de red de la red SDN a través de interfaces de usuario locales;
- 40 proporcionar un módulo de control maestro en comunicación con los portales del cliente y configurado para gestionar el control de flujo en la red SDN;
- generar una pluralidad de agentes de control discretos, cada uno asociado con un usuario final particular y configurado en base a los recursos de red seleccionados por el usuario final particular; y
- 45 enviar los agentes de control discretos a uno o más dispositivos locales del respectivo usuario final para controlarlo localmente.

La presente divulgación también se refiere a un procedimiento implementado por ordenador para controlar una red definida por software (SDN); el procedimiento comprende:

50

- proporcionar una pluralidad de portales de clientes que están configurados para facilitar a los usuarios finales la selección de recursos a través de interfaces de usuario locales;
- proporcionar un módulo de control maestro en comunicación con los portales del cliente y configurado para gestionar el control de flujo en la red SDN;
- 55 generar mediante el módulo de control maestro una pluralidad de agentes de control discretos cada uno asociado con un usuario final particular y configurado en base a los recursos seleccionados por el usuario final particular; y
- enviar los agentes de control discretos a los dispositivos locales de los respectivos usuarios finales para controlarlos.

Además, la divulgación se refiere a un procedimiento implementado por ordenador para controlar el acceso en una red definida por software (SDN); el procedimiento comprende:

60

- proporcionar un módulo de control maestro configurado para gestionar el control de flujo en la red SDN;
- generar mediante el módulo de control maestro una pluralidad de agentes de control de acceso discretos, cada uno asociado con nodos particulares del nodo de red SDN para controlar el acceso al mismo; y
- 65 enviar los agentes de control de acceso discretos a dispositivos asociados con los nodos respectivos para programar dinámicamente los dispositivos con criterios de control de acceso.

La presente divulgación también se refiere a un procedimiento implementado por ordenador para controlar una red doméstica en comunicación con una red definida por software (SDN); el procedimiento comprende:

- 5 suministrar un portal de cliente para facilitar a un usuario final la interfaz con la red doméstica para seleccionar criterios de control local;
proporcionar un módulo de control maestro asociado con la red SDN que está en comunicación con la red doméstica y está configurado para gestionar el control de flujo;
generar mediante el módulo de control maestro una pluralidad de agentes de control discretos cada uno asociado
10 con un usuario final particular y configurado en base a los criterios de control seleccionados por el usuario final en el portal del cliente; y
enviar los agentes de control discretos a la red doméstica para controlar los dispositivos de la red doméstica de acuerdo con los criterios de control seleccionados por el usuario final.
- 15 En un aspecto, los agentes de control, discretos se envían a la red doméstica para la recopilación de información relacionada con el protocolo de transporte para garantizar la entrega precisa de los servicios de acuerdo con los criterios de control seleccionados por el usuario final.

La presente divulgación permite abordar las amenazas a la seguridad y las violaciones a la privacidad aprovechando
20 la capacidad de programación del control de flujo en los dispositivos SDN para identificar y no reenviar el tráfico identificado que contiene amenazas o violaciones a la privacidad. El reenvío basado en flujo está programado en el dispositivo del usuario final para limitar el reenvío de tráfico de amenazas o tráfico de violación de privacidad.

Por consiguiente, la presente divulgación se refiere a un procedimiento implementado por ordenador para
25 proporcionar seguridad en una red definida por software (SDN); el procedimiento comprende:

- proporcionar un controlador SDN maestro para gestionar el control del flujo de datos en la red SDN; siendo operable el controlador SDN maestro para generar datos de enrutamiento para los dispositivos en red;
generar mediante el controlador SDN maestro una pluralidad de controladores agregados discretos, cada uno
30 asociado con un usuario final particular; cada controlador agregado SDN incluye datos de enrutamiento para un dispositivo asociado en red;
enviar el controlador agregado SDN por el controlador SDN maestro a los dispositivos en red asociados con los respectivos usuarios finales para controlarlos;
solicitar acceso a un destino en la red SDN desde un dispositivo en red solicitante;
35 iniciar una interacción del sistema de nombres de dominio (DNS) con el dispositivo en red solicitante;
retransmitir los datos de DNS asociados con el destino solicitado a un sistema de control de gestión de amenazas (TMCS);
determinar por el TMCS si el destino solicitado tiene un criterio de seguridad asociado;
comunicar un estado de amenaza por parte del TMCS al controlador agregado SDN asociado con el dispositivo en
40 red solicitante; y
generar datos de enrutamiento por parte del controlador agregado SDN asociado con el dispositivo en red solicitante en función del estado de amenaza para permitir o denegar el acceso al destino solicitado.

Además, la presente divulgación se refiere a un procedimiento implementado por ordenador para proporcionar
45 seguridad en una red definida por software (SDN); el procedimiento comprende:

- proporcionar un controlador SDN maestro para gestionar el control del flujo de datos en la red SDN; siendo operable el controlador SDN maestro para generar datos de enrutamiento para los dispositivos en red;
generar mediante el controlador SDN maestro una pluralidad de controladores agregados discretos, cada uno
50 asociado con un usuario final particular; cada controlador agregado SDN incluye datos de enrutamiento para un dispositivo asociado en red;
enviar el controlador agregado SDN por el controlador SDN maestro a los dispositivos en red asociados con los respectivos usuarios finales para controlarlos;
solicitar acceso a un localizador uniforme de recursos (URL) desde un dispositivo en red solicitante;
55 iniciar una interacción del sistema de nombres de dominio (DNS) con el dispositivo en red solicitante;
retransmitir los datos de DNS asociados con la URL solicitada a un sistema de control de gestión de amenazas (TMCS);
determinar por el TMCS si la URL solicitada tiene un criterio de seguridad asociado;
comunicar un estado de amenaza por parte del TMCS al controlador agregado SDN asociado con el dispositivo en
60 red solicitante; y
generar datos de enrutamiento por parte del controlador agregado SDN asociado con el dispositivo en red solicitante en función del estado de amenaza para permitir o denegar el acceso a la URL solicitada.

En un aspecto, el TMCS está en comunicación con al menos un repositorio de datos que contiene detalles de URL
65 que tienen criterios de seguridad predeterminados asociados con ellos.

En otro aspecto, el al menos un repositorio de datos se actualiza una vez que se sabe que una URL tiene un criterio de seguridad malicioso.

En otro aspecto, el al menos un repositorio de datos está alojado por una entidad de terceros. De manera ventajosa, el al menos un repositorio de datos comprende una clasificación de múltiples tipos de riesgo. En un ejemplo, el al menos un repositorio de datos comprende una clasificación de múltiples perfiles de usuario. Preferiblemente, cada perfil de usuario tiene una acción de enrutamiento asociada basada en su clasificación. En una disposición ejemplar, el al menos un repositorio de datos comprende un primer conjunto de datos asociado con destinos que tienen amenazas de seguridad identificadas previamente. En un ejemplo adicional, el al menos un repositorio de datos comprende un segundo conjunto de datos asociado con destinos que se sabe que recogen datos relacionados con la privacidad de los usuarios.

En un aspecto, el primer conjunto de datos se almacena en un primer repositorio de datos; y el segundo conjunto de datos se almacena en un segundo repositorio de datos.

En otro aspecto, cada controlador agregado SDN tiene un módulo de coincidencia de seguridad asociado que puede funcionar para definir una decisión de reenvío apropiada basada en el estado de amenaza recibido del TMCS. En un ejemplo, la decisión de reenvío se basa en un perfil de usuario asociado con el dispositivo en red solicitante. En otro aspecto, la decisión de reenvío se basa en una clasificación de riesgo. De manera ventajosa, la decisión de reenvío da como resultado que el tráfico se envíe a un destino de cuarentena. En un ejemplo, la decisión de reenvío da como resultado que el tráfico se reenvíe a la URL solicitada.

En un aspecto adicional, el controlador agregado SDN en el dispositivo de red solicitante ingresa una entrada de reenvío en una tabla de enrutamiento de flujo en base a la decisión de reenvío del módulo de coincidencia de seguridad.

En un aspecto, el TMCS puede funcionar para completar una base de datos abierta accesible por un orquestador SDN. De manera ventajosa, el TMCS puede funcionar para completar la base de datos abierta con el estado de las amenazas identificadas.

En otro aspecto, la base de datos abierta es accesible desde al menos un portal remoto. De manera ventajosa, el estado de las amenazas identificadas se puede ver desde al menos un portal remoto.

En otro aspecto, el TMCS puede funcionar para retransmitir una dirección IP de un usuario; un identificador de perfil de usuario y un identificador de clasificación de riesgo para la base de datos abierta. De manera ventajosa, la dirección IP del usuario se utiliza para mapear un informe de alerta de seguridad con un registro de cliente. En un aspecto, el informe de alerta de seguridad detalla las acciones que debe realizar el usuario para aliviar la amenaza.

En otro aspecto, el usuario selecciona una configuración de seguridad de una pluralidad de configuraciones de seguridad disponibles. De manera ventajosa, se genera una política de seguridad basada en la configuración de seguridad seleccionada. En un aspecto, se extrae un identificador del dispositivo en red solicitante de la base de datos abierta. Preferiblemente, una lista de sitios comúnmente utilizados por el usuario se extrae de la base de datos abierta.

En un aspecto adicional, el procedimiento comprende además extraer datos analíticos por parte de los controladores agregados SDN de los dispositivos en red. De manera ventajosa, el procedimiento incluye enrutar los datos analíticos extraídos a una base de datos abierta.

En un aspecto, los datos analíticos extraídos son enrutados por los controladores agregados SDN a la base de datos abierta a través del controlador SDN maestro.

En un aspecto adicional, un motor de análisis está en comunicación con la base de datos abierta y para analizar los análisis extraídos para generar una salida de análisis.

En otro aspecto, la salida de análisis es accesible a través de uno o más portales de clientes.

En una disposición ejemplar, una o más opciones de mejora del rendimiento se ponen a disposición del usuario final a través de los portales del cliente para su selección en función de la salida de análisis. De manera ventajosa, los datos de configuración se actualizan en respuesta a que el usuario final seleccione una o más opciones de mejora del rendimiento.

En un aspecto, el procedimiento comprende además actualizar el controlador agregado SDN instalado con los datos de configuración actualizados para modificar la configuración operativa de los dispositivos en red.

En otro aspecto, se modifica la configuración operativa de los dispositivos en red para incrementar un parámetro de calidad de servicio. De manera ventajosa, los ajustes operativos de los dispositivos en red se actualizan en tiempo

real mientras están en línea. En un ejemplo, la configuración operativa de los dispositivos en red se actualiza mientras está en modo de suspensión.

En otro ejemplo, los controladores agregados SDN se instalan en un sistema en chip (SOC) de los respectivos dispositivos en red. De manera ventajosa, los controladores agregados SDN se cargan en el firmware contenido en los respectivos dispositivos en red. En un aspecto ejemplar, los controladores agregados SDN son desplegables binariamente.

En un aspecto, los controladores agregados SDN se registran con el controlador SDN maestro después de ser instalados en los respectivos dispositivos en red para controlar el enrutamiento de datos desde los dispositivos en red y para controlar la configuración de los dispositivos en red.

La presente divulgación también se refiere a un controlador de seguridad de red para una red definida por software (SDN), el controlador de seguridad de red comprende uno o más módulos que pueden funcionar para:

- 15 proporcionar un controlador SDN maestro para gestionar el control del flujo de datos en la red SDN; siendo operable el controlador SDN maestro para generar datos de enrutamiento para los dispositivos en red;
generar mediante el controlador SDN maestro una pluralidad de controladores agregados discretos, cada uno asociado con un usuario final particular; cada controlador agregado SDN incluye datos de enrutamiento para un dispositivo asociado en red;
20 enviar el controlador agregado SDN por el controlador SDN maestro a los dispositivos en red asociados con los respectivos usuarios finales para controlarlos;
solicitar acceso a un localizador uniforme de recursos (URL) desde un dispositivo en red solicitante;
iniciar una interacción del sistema de nombres de dominio (DNS) con el dispositivo en red solicitante;
25 retransmitir los datos de DNS asociados con la URL solicitada a un sistema de control de gestión de amenazas (TMCS);
determinar por el TMCS si la URL solicitada tiene un criterio de seguridad asociado;
comunicar un estado de amenaza por parte del TMCS al controlador agregado SDN asociado con el dispositivo en red solicitante; y
30 generar datos de enrutamiento por parte del controlador agregado SDN asociado con el dispositivo en red solicitante en función del estado de amenaza para permitir o denegar el acceso a la URL solicitada.

Además, la presente divulgación se refiere a un medio legible por ordenador que comprende instrucciones no transitorias que, cuando se ejecutan, hacen que un procesador lleve a cabo un procedimiento de acuerdo con cualquiera de las etapas descritas anteriormente. Por ejemplo; las instrucciones no transitorias que, cuando se ejecutan, hacen que un procesador lleve a cabo un procedimiento que comprende:

- 40 proporcionar un controlador SDN maestro para gestionar el control del flujo de datos en la red SDN; siendo operable el controlador SDN maestro para generar datos de enrutamiento para los dispositivos en red;
generar mediante el controlador SDN maestro una pluralidad de controladores agregados discretos, cada uno asociado con un usuario final particular; cada controlador agregado SDN incluye datos de enrutamiento para un dispositivo asociado en red;
enviar el controlador agregado SDN por el controlador SDN maestro a los dispositivos en red asociados con los respectivos usuarios finales para controlarlos;
45 solicitar acceso a un localizador uniforme de recursos (URL) desde un dispositivo en red solicitante;
iniciar una interacción del sistema de nombres de dominio (DNS) con el dispositivo en red solicitante;
retransmitir los datos de DNS asociados con la URL solicitada a un sistema de control de gestión de amenazas (TMCS);
determinar por el TMCS si la URL solicitada tiene un criterio de seguridad asociado;
50 comunicar un estado de amenaza por parte del TMCS al controlador agregado SDN asociado con el dispositivo en red solicitante; y
generar datos de enrutamiento por parte del controlador agregado SDN asociado con el dispositivo en red solicitante en función del estado de amenaza para permitir o denegar el acceso a la URL solicitada.

La presente divulgación también se refiere a un procedimiento implementado por ordenador para controlar una red compatible con DOCSIS; el procedimiento comprende:

- 55 proporcionar un módulo de control maestro en un sistema de terminación de cable módem (CMTS) que está configurado para controlar cable módems DOCSIS;
generar mediante el módulo de control maestro una pluralidad de agentes de control discretos, cada uno asociado con un cable módem DOCSIS particular; y
60 enviar los agentes de control discretos a los cables módems DOCSIS para programar dinámicamente el cable módem DOCSIS con un archivo de arranque del CMTS sin tener que leer un kernel daemon.

Además, la presente divulgación se refiere a un procedimiento implementado por ordenador para controlar una red definida por software (SDN); el procedimiento comprende:

- 65 proporcionar una o más interfaces de usuario de vox que están configuradas para facilitar a los usuarios el control de

dispositivos en red;

generar datos de control basados en la entrada de voz recibida de los usuarios a través de las interfaces de usuario de voz;

proporcionar un controlador SDN maestro para gestionar el control del flujo de datos en la red SDN; siendo operable

5 el controlador SDN maestro para generar datos de control para los dispositivos en red;

generar mediante el controlador SDN maestro una pluralidad de controladores agregados discretos, cada uno asociado con un usuario final particular; cada controlador agregado SDN incluye al menos uno de datos de control y datos de enrutamiento para un dispositivo asociado en red;

10 enviar el controlador agregado SDN por el controlador SDN maestro a los dispositivos en red asociados con los respectivos usuarios finales para controlarlos;

instalar los controladores agregados SDN en los dispositivos en red; y

registrar los controladores agregados SDN instalados con el controlador SDN maestro para controlar los dispositivos en red.

15 En un aspecto, se puede acceder a la salida de análisis a través de las interfaces de usuario de voz.

En un aspecto adicional, se ponen a disposición del usuario final una o más opciones de mejora del rendimiento a través de las interfaces de usuario de voz para su selección en función de la salida de análisis.

20 En otro aspecto, el controlador SDN maestro implementa la orquestación SDN en respuesta a una solicitud de recursos recibida en las interfaces de usuario de voz.

En un aspecto ejemplar, el controlador SDN maestro genera un archivo de configuración para cada recurso seleccionado por el usuario final en las interfaces de usuario de voz.

25 En otro aspecto, las interfaces de usuario de voz son interfaces basadas en web.

La presente divulgación también se refiere a un controlador de red para una red definida por software (SDN), comprendiendo el controlador de red uno o más módulos operables para:

30 proporcionar una o más interfaces de usuario de voz que están configuradas para facilitar a los usuarios el control de dispositivos en red;

generar datos de control basados en la entrada de voz recibida de los usuarios a través de los portales de clientes;

proporcionar un controlador SDN maestro para gestionar el control del flujo de datos en la red SDN; siendo operable

35 el controlador SDN maestro para generar datos de control para los dispositivos en red;

generar mediante el controlador SDN maestro una pluralidad de controladores agregados distribuidos discretos cada uno asociado con un usuario final particular; cada controlador agregado SDN incluye al menos uno de datos de control y datos de enrutamiento para un dispositivo asociado en red;

40 enviar el controlador agregado SDN por el controlador SDN maestro a los dispositivos en red asociados con los respectivos usuarios finales para controlarlos;

instalar el controlador agregado SDN en los dispositivos en red; y

registrar los controladores agregados SDN instalados con el controlador SDN maestro para controlar los dispositivos en red.

45 Además la presente divulgación se refiere a un artículo de fabricación que comprende un medio legible por procesador que tiene incorporado un código de programa ejecutable que, cuando es ejecutado por el dispositivo de procesamiento, hace que el dispositivo de procesamiento realice las siguientes acciones:

50 proporcionar una o más interfaces de usuario de voz que están configuradas para facilitar a los usuarios el control de dispositivos en red;

generar datos de control basados en la entrada de voz recibida de los usuarios a través de los portales de clientes;

proporcionar un controlador SDN maestro para gestionar el control del flujo de datos en la red SDN; siendo operable el controlador SDN maestro para generar datos de control para los dispositivos en red;

55 generar mediante el controlador SDN maestro una pluralidad de controladores agregados discretos, cada uno asociado con un usuario final particular; cada controlador agregado SDN incluye al menos uno de datos de control y datos de enrutamiento para un dispositivo asociado en red;

enviar el controlador agregado SDN por el controlador SDN maestro a los dispositivos en red asociados con los respectivos usuarios finales para controlarlos;

instalar los controladores agregados SDN en los dispositivos en red; y

60 registrar los controladores agregados SDN instalados con el controlador SDN maestro para controlar los dispositivos en red.

Además, la presente divulgación se refiere a un procedimiento implementado por ordenador para controlar una red definida por software (SDN); el procedimiento comprende:

65 proporcionar una o más interfaces configuradas para facilitar a los usuarios el control de dispositivos en red;

generar datos de control basados en la entrada recibida de los usuarios a través de las interfaces de usuario de voz; proporcionar un controlador SDN maestro para gestionar el control del flujo de datos en la red SDN; siendo operable el controlador SDN maestro para generar datos de control para los dispositivos en red; generar mediante el controlador SDN maestro una pluralidad de controladores agregados discretos, cada uno asociado con un usuario final particular; cada controlador agregado SDN incluye al menos uno de datos de control y datos de enrutamiento para un dispositivo asociado en red; enviar el controlador agregado SDN por el controlador SDN maestro a los dispositivos en red asociados con los respectivos usuarios finales para controlarlos; instalar los controladores agregados SDN en los dispositivos en red; y registrar los controladores agregados SDN instalados con el controlador SDN maestro para controlar los dispositivos en red.

Además, la presente descripción se refiere a un procedimiento implementado por ordenador para controlar una red definida por software (SDN); comprendiendo el procedimiento:

- 15 proporcionar una o más interfaces de usuario de voz que están configuradas para facilitar a los usuarios el control de dispositivos en red; generar datos de control basados en la entrada de voz recibida de los usuarios a través de las interfaces de usuario de voz; proporcionar un controlador SDN maestro para gestionar el control del flujo de datos en la red SDN; siendo operable el controlador SDN maestro para generar datos de control para los dispositivos en red; y
- 20 proporcionar una pluralidad de controladores agregados distribuidos asociados con el controlador maestro que cooperan con el controlador maestro para controlar los dispositivos en red.

Además, la presente descripción se refiere a un controlador de red para una red definida por software (SDN),

- 25 comprendiendo el controlador de red uno o más módulos operables para: proporcionar una o más interfaces de usuario de voz que están configuradas para facilitar a los usuarios el control de dispositivos de red; generar datos de control basados en la entrada de voz recibida de los usuarios a través de las interfaces de usuario de voz;
- 30 proporcionar un controlador SDN maestro para gestionar el control del flujo de datos en la red SDN; siendo operable el controlador SDN maestro para generar los datos de control para los dispositivos en red; y proporcionar una pluralidad de controladores agregados distribuidos que cooperan con el controlador maestro para controlar los dispositivos de red.
- 35 Otras características y ventajas de la presente divulgación serán evidentes a partir de la descripción detallada que sigue a continuación. La siguiente descripción detallada se refiere a los dibujos adjuntos.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

- 40 La presente divulgación se describirá ahora con referencia a los dibujos que la acompañan en los que:

La figura 1 es un diagrama de bloques que ilustra una plataforma SDN ejemplar de acuerdo con la presente enseñanza.

- 45 **La figura 2** es un diagrama de bloques que ilustra detalles de la arquitectura de la figura 1.

La figura 3 es un diagrama de bloques que ilustra detalles de la arquitectura de la figura 1.

La figura 4 es un diagrama de bloques que ilustra detalles de la arquitectura de la figura 1.

- 50 **La figura 5** es un diagrama de bloques que ilustra otra plataforma SDN ejemplar de acuerdo con la presente enseñanza.

La figura 6 es un diagrama de bloques que ilustra detalles de la arquitectura de la figura 5.

- 55 **La figura 7** es un diagrama de flujo que ilustra etapas ejemplares durante el funcionamiento de la plataforma SDN de la figura 1 o la figura 5.

- 60 **La figura 8** es un diagrama de flujo que ilustra etapas ejemplares durante el funcionamiento de la plataforma SDN de la figura 1 o la figura 5.

La figura 9 es un diagrama de flujo que ilustra etapas ejemplares durante el funcionamiento de la plataforma SDN de la figura 1 o la figura 5.

- 65 **La figura 10** es un diagrama de bloques que ilustra otra plataforma SDN ejemplar de acuerdo con la presente enseñanza.

La figura 11 es un diagrama de bloques que ilustra otra plataforma SDN ejemplar de acuerdo con la presente enseñanza.

5 **La figura 12A** es un diagrama de bloques que ilustra otra plataforma SDN ejemplar de acuerdo con la presente enseñanza.

La figura 12B es un diagrama de bloques que ilustra otra plataforma SDN ejemplar de acuerdo con la presente enseñanza.

10

La figura 13 es un diagrama de flujo que ilustra etapas ejemplares durante el funcionamiento de la plataforma SDN de la figura 1, figura 5, figura 11, figura 12A o figura 12B.

La figura 14 es un diagrama de flujo que ilustra etapas ejemplares durante el funcionamiento de la plataforma SDN de la figura 1, figura 5, figura 11, figura 12A o figura 12B.

La figura 15 es un diagrama de flujo que ilustra etapas ejemplares durante el funcionamiento de la plataforma SDN de la figura 1, figura 5, figura 11, figura 12A o figura 12B.

20 **Las figuras 16A y 16B** son un diagrama de bloques que ilustra detalles de una arquitectura SDN que también está de acuerdo con la presente enseñanza.

La figura 17 es un diagrama de bloques que ilustra detalles de la arquitectura SDN de la figura 16A y 16B.

25 **La figura 18** es un diagrama de bloques que ilustra detalles de la arquitectura SDN de la figura 16A y 16B.

La figura 19 es un diagrama de flujo que ilustra etapas ejemplares durante el funcionamiento de la plataforma SDN de las figuras 16A-18.

30 **La figura 20** es un diagrama de flujo que ilustra etapas ejemplares durante el funcionamiento de la plataforma SDN de las figuras 16A-18.

La figura 21 es un diagrama de bloques que ilustra detalles de una arquitectura SDN que también está de acuerdo con la presente enseñanza.

35

La figura 22 es un diagrama de flujo que ilustra etapas ejemplares durante el funcionamiento de la plataforma SDN de la figura 16A 16B o la figura 21.

La figura 23 es un diagrama de bloques que ilustra otra plataforma SDN ejemplar de acuerdo con la presente enseñanza.

40

La figura 24 es un diagrama de flujo que ilustra etapas ejemplares implementadas por la plataforma SDN de la figura 23.

45

DESCRIPCIÓN DETALLADA

Las realizaciones de la presente divulgación se describirán ahora con referencia a algunas plataformas SDN ejemplares. Se entenderá que la arquitectura ejemplar se proporciona para ayudar a la comprensión de la presente enseñanza y no debe interpretarse como limitante en modo alguno. Además, los módulos o elementos que se describen con referencia a cualquier figura pueden intercambiarse con los de otras figuras u otros elementos equivalentes sin apartarse del espíritu de la presente enseñanza.

50

Con referencia a los dibujos e inicialmente a las figuras 1 a 3, se ilustra una plataforma SDN 100 de acuerdo con la presente enseñanza. Un controlador SDN maestro 102 está configurado para gestionar el control del flujo de datos en la red SDN 103. El controlador SDN maestro 102 puede funcionar para generar datos de flujo de enrutamiento para una pluralidad de dispositivos en red 104. Los dispositivos en red 104 pueden incluir, entre otros, equipos de infraestructura de red (NIC), amplificadores, servidores, nodos de fibra, sistemas de terminación de módem de cable (CMTS), plataformas de acceso de cable convergente (CCAP), multiplexores de acceso de línea de suscripción digital (DSLAM), terminales de línea óptica (OLT), terminales de red óptica (ONT), puntos de acceso WIFI independientes, dispositivos portátiles o similares. El controlador SDN maestro 102 tiene una vista de extremo a extremo de toda la red SDN 103 e información de todas las rutas de red y capacidades del dispositivo. El controlador SDN maestro 102 puede funcionar para generar una pluralidad de controladores agregados SDN 105, cada uno asociado con un usuario particular. El controlador SDN maestro 102 y la pluralidad de controladores SDN secundarios 105 cooperan para calcular rutas de datos basándose tanto en las direcciones de origen como en las de destino; utilizar diferentes rutas de red para diferentes tipos de tráfico y reaccionar a la condición de los cambios de

60

65

red.

El controlador agregado SDN 105 es distribuido por el controlador SDN maestro 102 a los dispositivos en red 104 asociados con los respectivos usuarios para controlar los dispositivos 104 de manera que los dispositivos 104 puedan funcionar para tomar decisiones de enrutamiento de datos locales. Cada controlador agregado SDN 105 incluye datos de configuración y un motor de enrutamiento. Los controladores agregados distribuidos 105 están instalados en los dispositivos en red 104 asociados con usuarios finales particulares. El controlador agregado discreto SDN 105 está configurado para agregar funciones de red a los dispositivos 105 que pueden incluir enrutamiento distribuido, funciones de calidad de servicio, funciones de listas de control de acceso y funciones de equilibrio de carga. Estas tareas las habría realizado principalmente el controlador SDN central en las redes SDN conocidas hasta ahora.

Una vez instalados en los dispositivos 104, los controladores agregados distribuidos 105 se registran con el controlador SDN maestro 102 y pueden cooperar para controlar el enrutamiento de datos desde los dispositivos en red a través de la red SDN 103. Los controladores agregados distribuidos 105 actúan como un motor de enrutamiento distribuido eliminando de ese modo las limitaciones de hardware tales como las entradas de memoria ternaria direccionable de contenido (TCAM). Debido a su implementación liviana, los controladores agregados distribuidos 105 pueden instalarse en una variedad de dispositivos, desde plataformas de conmutación de bajo / alto nivel hasta Bare Metal, máquinas virtuales e incluso controladores de interfaz de red (NIC). Tanto el controlador SDN maestro 102 como el controlador agregado SDN 105 pueden adaptarse a las necesidades de topología tanto de la LAN (Este Oeste) como de la WAN (Norte Sur) con enrutamiento unificado usando el protocolo de puerta de enlace fronteriza (BGP). La gestión de topología para el enrutamiento consciente del servicio se puede habilitar mediante el descubrimiento de enlaces basado en el protocolo de descubrimiento de la capa de enlace (LLDP) / detección de reenvío bidireccional (BFD). El controlador agregado SDN 105 puede integrarse sin problemas en un sistema operativo de conmutador como LINUX o UNIX. Los controladores agregados distribuidos 105 pueden funcionar para ejecutarse en los dispositivos 104 como instancias de contenedor y proporcionan una integración perfecta con cualquier dispositivo o protocolo de enrutamiento heredado.

La plataforma SDN 100 elimina la complejidad de la red y asegura la máxima QoS (Calidad de servicio) con programación en tiempo real de rutas tanto dentro como entre dominios. El plano de control de la plataforma SDN 100 se basa en los estándares de la industria con el beneficio de eliminar la carga del bloqueo del proveedor. La plataforma SDN 100 está provista de herramientas e interfaces de programación de aplicaciones (API) ricas en funciones para permitir a los usuarios adaptar las aplicaciones SDN y definir políticas, reglas y optimizaciones específicas del usuario para la red SDN 103. La plataforma SDN 100 se integra con configuraciones de nube pública y privada y reduce el tiempo de aprovisionamiento de los servicios con reconocimiento de aplicaciones a minutos en lugar de semanas, lo que proporciona ahorros de costos operativos reales. Un panel de interfaz intuitivo basado en la web permite a los usuarios implementar de forma rápida y sin problemas adiciones, movimientos y cambios a la red 103 mientras combinan el control de red programático con el conocimiento del estado de la red para proporcionar garantía de SLA (Acuerdo de nivel de servicio).

El controlador agregado SDN 105 comprende un repositorio de instrucciones de control y políticas para dispositivos 104 específicos. El controlador agregado SDN distribuido 105 puede funcionar para tomar decisiones de enrutamiento localmente en los dispositivos 104, lo que alivia los retrasos que pueden producirse si estas decisiones de enrutamiento se toman de forma centralizada en lugar de local. Además, el controlador agregado SDN distribuido 105 facilita la granularidad individual de establecer políticas específicas para usuarios finales en un gran número de dispositivos 105, en cuanto a cómo se deben controlar sus dispositivos y optimizar el rendimiento. El controlador agregado SDN 105 también permite recopilar análisis de los dispositivos 104 para determinar si los dispositivos 105 están funcionando de manera óptima. Si se determina que los dispositivos 105 no funcionan de manera eficiente, la plataforma 100 puede modificar dinámicamente la configuración operativa de los dispositivos 104 para mejorar la eficiencia o la calidad del servicio experimentado por el usuario.

La plataforma SDN 100 proporciona visibilidad completa de una topología de red completa a través de un plano de control 107, que a diferencia de las implementaciones SDN tradicionales, está centralizado usando el controlador SDN maestro 102, además de estar completamente distribuido, utilizando controladores agregados SDN distribuidos 105. Los controladores agregados distribuidos 105 son un motor de enrutamiento de peso ligero inteligente que puede enviarse a cualquier CPE habilitado para Openflow, tal como un conmutador, servidor, NIC o similar. El plano de control 107 se puede construir según los estándares de la industria con el beneficio de eliminar la carga del bloqueo al proveedor. La arquitectura 100 proporciona las herramientas para adaptar las aplicaciones SDN y definir las propias políticas, reglas y optimizaciones del usuario para la red 110.

El controlador SDN maestro 102 y el controlador agregado SDN 105 pueden estar basados en protocolos, tales como OpenFlow o NetConf/YANG, que permiten a un servidor decirle a los conmutadores dónde enviar paquetes. En un conmutador compatible con OpenFlow, la ruta de datos está separada de la ruta de control. La ruta de datos reside en el propio conmutador mientras que el controlador SDN maestro 102 proporciona la ruta de control que toma las decisiones de enrutamiento. El protocolo OpenFlow proporciona un medio para que el conmutador y el controlador SDN maestro 102 se comuniquen y proporciona información sobre los flujos que se están programando

en la red. Además, el protocolo NetConf con su uso de modelos YANG también puede usarse para programar funciones de red específicas dentro de los dispositivos en red 105.

El plano de control 107 es altamente resistente, facilitado a través de una federación de controladores agregados distribuidos 105, formando un único punto virtualizado de control SDN. Cada controlador individual federado, a su vez, envía automáticamente un agente de control SDN ligero a cada uno de los dispositivos 104 de red en una capa 109 de infraestructura, proporcionando una visibilidad completa de la red. La plataforma 100 incluye una capa de aplicación 126 que integra la orquestación de la nube Openstack, para gestionar la entrega y configuración de servicios, aplicaciones y funciones de redes virtuales basadas en la nube. También residen en la capa de aplicación 126 una serie de herramientas y sistemas, portales de interfaz que permiten al proveedor de servicios y sus clientes operar, optimizar y realizar autoservicio. La plataforma general 100 se integra a las tres capas del modelo SDN proporcionando un conjunto completo de capacidades como se ilustra gráficamente en la figura 2.

Una arquitectura de ejemplo de acuerdo con la presente enseñanza se ilustra en las figuras 3 y 4. Las interfaces de los portales de la arquitectura de orquestación traen los controles de las pilas de los sistemas de apoyo empresarial (BSS) 110, las aplicaciones de terceros 112, las aplicaciones de control 114 que forman parte de las funciones de un portal de administrador 116 y un portal de clientes 118. Estas aplicaciones se comunican a través de interfaces de programación de aplicaciones (API) admitidas 120, el kit de desarrollo de software (SDK) 122, el bus de mensajes 124 y todas las comunicaciones se identifican y autentican primero para acceder a una capa de orquestación 126 en una capa de autenticación/identidad 128. El protocolo de acceso a directorio ligero (LDAP) puede ejecutarse en la capa de autenticación/identidad 128. Proporciona un mecanismo utilizado para conectarse, buscar y modificar directorios de Internet. El servicio de directorio LDAP se basa en un modelo cliente-servidor. Tras la validación, se genera un token y este token se comunica a través de las capas para identificar la autorización para la configuración de componentes funcionales de la arquitectura.

OpenStack 130 está completamente integrado en la solución y sus API de orquestación se utilizan para recopilar y señalar la conmutación de los tokens de autenticación e identidad a todos los componentes del sistema. A su vez, OpenStack 130 se utiliza para alojar los componentes del sistema de administración dentro de su entorno gestionado y orquestado por hardware. Sus capacidades de nube 132 se utilizan para el alojamiento de servicios al cliente y para la conexión a nubes públicas a través de controles API.

Un motor 135 de control de políticas identifica y mapea los datos de configuración apropiados al dispositivo 104 que está siendo controlado. Esto se logra mediante la consulta de los registros de clientes en vivo dentro de una base de datos 138 que ha recopilado análisis utilizando los controladores agregados distribuidos 105. Estos análisis se recopilan de las estructuras de datos del cliente en vivo, perfiles, etc. en la base de datos de datos abiertos que se ha completado con análisis de los dispositivos controlados por SDN 104 y de datos obtenidos a través del procedimiento de aprovisionamiento basado en perfiles de clientes y perfiles de productos. Todos los datos se mapean en la base de datos 138 en registros estructurados apropiadamente para una lectura y escritura rápidas. El controlador de políticas 135 identifica y mapea el perfil del cliente con las configuraciones apropiadas requeridas para el sistema en chip (SOC) del dispositivo 104 basado en el perfil de producto del cliente y el rol del token de autenticación y administración de identidad asignado por la capa de autenticación/identidad 128.

El controlador SDN maestro 102 puede residir en el plano de control 107. El controlador maestro SDN 102 comprende un componente primario de control/orquestación en comunicación con el portal del cliente 118 a través de las capas de datos y orquestación de nivel superior y está configurado para gestionar el control de flujo en la red SDN 103. El componente de control/orquestación se puede operar para generar una pluralidad de controladores agregados discretos 105, cada uno asociado con un usuario final particular y configurado en base a los recursos de red seleccionados por el usuario final particular a través del portal del cliente 118. El controlador SDN maestro 102 está configurado para enviar el controlador agregado SDN discreto 105 a uno o más dispositivos locales 104 del usuario final respectivo para al mismo. Los controladores agregados discretos SDN 105 se envían a través de la solución de orquestación cuando se identifica la necesidad de una nueva capa de control a través del análisis producido por la orquestación. Los controladores agregados distribuidos 105 son agentes extremadamente livianos y pueden integrarse en el firmware o BIOS de los dispositivos 104. En un ejemplo, los controladores agregados 105 se pueden desplegar de forma binaria.

El control principal lo maneja el plano de orquestación 126 y maneja tareas administrativas como autenticación, registro, descubrimiento y configuración. Los controladores agregados multicapa 105 se proporcionan en las funciones multicomponente de los planos de control multifuncionales 107. Estos controladores agregados distribuidos 105 administran las operaciones internas del dispositivo y proporcionan las instrucciones utilizadas por los motores de enrutamiento para dirigir los paquetes a través de la programación usando NetConf/YANG, OpenFlow/OVSDB o la programación directa a través del kit de desarrollo de software (SDK) del sistema en chip (SOC). También puede ejecutar los protocolos de enrutamiento y conmutación y retroalimenta los datos operativos al plano de orquestación e informa los análisis a través del controlador SDN maestro 102 a la capa de orquestación 126 y la capa de control 107.

Además, los controladores agregados distribuidos 105 construyen una base de datos de topología 142 y la utilizan

- para identificar sus vecinos y rutas relevantes. La base de datos de topología 142 se utiliza para tomar decisiones de reenvío y para definir decisiones de reenvío proactivas y reactivas. Los controladores agregados 105 construyen una base de datos de red 144 y la usan para construir una visibilidad de red completa de todas las rutas conocidas. Esta base de datos de red 144 se utiliza para integrarse en sus vecinos y en rutas relevantes, las interfaces pueden incluir el protocolo de puerta de enlace exterior (EGP) y el protocolo de puerta de enlace interior (IGP). La base de datos de red 144 se usa para construir decisiones de reenvío y para definir controles de reenvío proactivos y reactivos. Además, el controlador agregado SDN 105 puede admitir el Protocolo de puerta de enlace fronteriza (BGP), Open Shortest Path First (OSPF), Application-Layer Traffic Optimization (ALTO) y otros EGP e IGP para completar la conciencia de la red para todas las decisiones de reenvío. Los datos recopilados de estos componentes se evalúan utilizando los datos creados a partir de una base de datos de enlaces 117, la tabla de red 121, la tabla de reenvío de flujo 119 para la creación de un control de reenvío reactivo y proactivo. El control de reenvío para los dispositivos 104 se genera y agrega a la base de información de enrutamiento (RIB) 125 para la programación de los dispositivos 104 con una base de información de reenvío (FIB) 127 a través de interfaces 123 disponibles como SOC SDK, Open vSwitch Database (OVSDb) o Protocolo de configuración de red (NetConf) / Yet Another Next Generation (YANG).
- Un administrador RIB 141 puede funcionar para crear una base de información de reenvío (FIB) en los dispositivos 104 que es utilizada por el sistema operativo del dispositivo 104 para encontrar la interfaz adecuada a la que la interfaz de entrada debe enviar un paquete de datos. Los datos de políticas se almacenan en una base de datos de políticas 129 y los datos de configuración se almacenan en una base de datos de configuración 131. Estos se generan a partir de instrucciones recibidas desde el controlador de políticas 135 desde la orquestación de nivel superior a través de la API de transferencia de estado representacional (REST). El plano de datos 148 es la sala de máquinas que mueve los paquetes a través del dispositivo 104, usando la tabla de enrutamiento de flujo 119 proporcionada por los controladores agregados distribuidos 105 para determinar el puerto de salida. Esto se programa y las instrucciones se envían mediante NetConf/YANG, OpenFlow/OVSDb o programación directa a través del SOC SDK.
- El controlador SDN maestro 102 y los controladores agregados SDN 105 cooperan para operar como un controlador fuera de banda que busca y programa dinámicamente la configuración de los dispositivos 104 que el cliente ha seleccionado usando el portal del cliente 118. Los flujos se controlan desde los dispositivos 104 y se crea un mapa de reenvío topológico a medida para el entorno del cliente para permitir decisiones de reenvío precisas. Los dispositivos 104 están habilitados con este controlador SDN liviano fuera de banda que está integrado con una solución de orquestación remota para recibir conjuntos de instrucciones y entregar automáticamente control de flujo de servicio, recopilación de análisis y activar cambios solicitados por el cliente en los servicios al cliente en tiempo real.
- Los controladores agregados distribuidos 105 pueden distribuirse como un controlador liviano en una gama de CPE de CPU baja y baja energía, equipos de infraestructura de red, NIC, amplificadores, servidores, nodos de fibra, CMTS, CCAP, amplificadores, DSLAM, OLT, ONT, puntos de acceso WIFI independientes, dispositivos portátiles, etc. y proporcionar servicios con una latencia muy reducida para permitir la entrega de acuerdos de nivel de servicio (SLA) de valor agregado y alta calidad, al tiempo que mejora significativamente la capacidad de una organización para adaptarse rápidamente a las demandas cambiantes de los clientes/redes. La plataforma 100 proporciona una visualización completa de un extremo a otro de todos los servicios NFV y SDN que es tanto jerárquica como multicapa. Esta visualización también incluye información integrada sobre alarmas, disponibilidad, rendimiento, calidad del servicio y cumplimiento de SLA, lo que la convierte en una vista única para una evaluación integral del estado del servicio. Esto brinda una vista dinámica y precisa así como accesibilidad de la red y los servicios asociados, una vista consolidada del estado de cada servicio y administración de recursos y la capacidad de solucionar problemas e identificar rápidamente los servicios afectados.
- En una realización ejemplar, la plataforma SDN 100 puede usarse para eliminar la gestión de archivos de arranque de los módems de cable DOCSIS y la automatización de la orquestación del servicio. La plataforma SDN 100 puede configurarse para el aprovisionamiento y la orquestación de la pila de IP y la red distribuida de servicios domésticos en módems DOCSIS. La plataforma 100 funciona como un controlador fuera de banda que busca y programa dinámicamente el archivo de arranque de CMTS al módem de cable sin tener la necesidad de leer como un kernel daemon, lo que reduce los requisitos de procesamiento del módem de cable (CM) y elimina la necesidad de que los operadores mantengan múltiples archivos de arranque. Actualmente, se están aprovisionando millones de módems de cable en todo el mundo, pero una de las debilidades importantes que pueden percibirse en el modelo de aprovisionamiento DOCSIS es la falta de un procedimiento dinámico para actualizar un servicio. Algunas de las cuestiones clave que preocupan a los operadores de múltiples sistemas (MSO) y suscriptores pueden describirse como:
- Compartir contenido personal a través de los límites del enrutador.
 - Optimización de rutas de red domésticas.
 - Visibilidad MSO y gestión de la red doméstica.
 - Administrar y hacer cumplir la política de manera constante - Cortafuegos - Controles parentales.
 - Acceso remoto
 - Nuevos servicios.

Muchos proveedores de servicios operan su red con un control primario pequeño o débil sobre su configuración y administración. Esto significa que la configuración y el estado de la red se almacenan efectivamente en una base de datos distribuida gigante. Esto no es intrínsecamente un mal estado de cosas, pero los operadores de red no siempre son buenos para obtener la información de esa base de datos gigante en una forma que sea utilizable para tomar decisiones comerciales que optimicen el uso de la red y los servicios que la utilizan. El archivo de arranque maneja el ADN de cualquier cable módem DOCSIS dado y esto se puede hacer dinámico y programable utilizando la plataforma SDN 100 de acuerdo con la presente enseñanza que supera los problemas enumerados anteriormente. El operador puede reducir el procedimiento de prestación de servicios a una sola transacción en lugar de una compleja serie de etapas que involucran múltiples sistemas y humanos.

La plataforma SDN 100 se puede utilizar para resumir la definición y las topologías del servicio del acceso físico y los dispositivos utilizados para proporcionar el servicio. Este resumen permite la máxima flexibilidad en la construcción de un sistema de aprovisionamiento que sea independiente de las tecnologías de acceso que se utilizan. Por ejemplo, cuando es necesario ofrecer a los clientes servicios complejos como L3 VPN (red virtual privada enrutada) o una determinada configuración predefinida del protocolo de enrutamiento Provider Edge (PE)-Customer Edge (CE) para garantizar que se anuncien/filtren las rutas correctas. Se requieren servicios complejos y encadenados, como proporcionar servicios de firewall en línea o proporcionar acceso a servicios en la nube desde una VPN. Los servicios de capa superior como estos son ejemplos de servicios en los que la definición del servicio puede extenderse más allá de los circuitos de conexión y los elementos de la red participan en el protocolo de enrutamiento y requieren más intercambio de estado entre el punto final y la red, por lo que en estos el modelo de aprovisionamiento DOCSIS actual puede ser inadecuado y, por lo tanto, nuestra combinación de SDN para administrar dicha orquestación a través de OpenFlow es extremadamente útil para el aprovisionamiento rápido y las actualizaciones de servicios.

El portal de clientes 118 es el centro de información y autoservicio para el cliente. Proporciona acceso rápido a una amplia gama de informes y herramientas, que permiten al cliente seleccionar y comprender sus servicios y, de manera más crítica, cómo se utilizan. A través de un menú intuitivo, el portal 118 del cliente permite al cliente acceder a una amplia cartera de aplicaciones, servicios y actualizaciones, que se pueden comprar, entregar y utilizar en tiempo real en cuestión de minutos. Para los informes, el cliente puede personalizar el acceso al portal individual y la información mostrada, detallando, por ejemplo; uso, hora del día, actividad de navegación y mucho más. El cliente, ahora armado con estos datos, tiene una elección informada sobre lo que luego permite, prohíbe y restringe. El portal 118 del cliente muestra una o más opciones de mejora del rendimiento basadas en análisis recopilados por los controladores agregados SDN 105. Los datos de configuración asociados con los controladores agregados SDN 105 se actualizan en respuesta a que el usuario final seleccione una o más opciones de mejora del rendimiento. Por tanto, el rendimiento de los dispositivos 104 y la red general 103 pueden optimizarse basándose en la información recibida del usuario final a través de su portal de clientes 118. La función de mapeo permite al cliente tener visibilidad de todos los dispositivos conectados en su hogar, a través de una topología simple con estadísticas de clic hacia abajo en cada usuario. El portal 118 también proporciona notificaciones y recomendaciones en tiempo real que pueden ser de interés, basadas en el perfil del cliente y el uso del servicio. Ampliando el alcance del portal, estas notificaciones también se pueden vincular simplemente a dispositivos móviles para acceder fuera de línea a las alertas.

El controlador agregado SDN instalado 105 puede usar los datos de configuración actualizados para modificar la configuración operativa de los dispositivos en red 104. Por ejemplo, la configuración operativa de los dispositivos en red puede modificarse para aumentar un parámetro de calidad de servicio. Los ajustes operativos de los dispositivos en red pueden actualizarse en tiempo real mientras los dispositivos 105 están en línea. Alternativamente, la configuración operativa de los dispositivos 105 conectados en red puede actualizarse mientras los dispositivos 105 están en modo de suspensión. En una disposición ejemplar, la configuración operativa de los dispositivos en red 105 se actualiza cambiando a un canal de comunicación alternativo para evitar la intercomunicación de los dispositivos vecinos. El canal de comunicación puede ser un canal WIFI, por ejemplo. En otro ejemplo, la configuración operativa del dispositivo en red puede cambiarse para reducir el consumo de energía de los dispositivos 105. De esta manera, la configuración operativa del dispositivo en red 105 puede cambiarse reprogramando una interfaz de energía. En otro ejemplo, la configuración operativa del dispositivo en red 105 puede cambiarse para aumentar la prioridad al ancho de banda disponible o disminuir la prioridad al ancho de banda disponible. Se prevé que los controladores agregados SDN 105 pueden configurarse para asignar un primer ajuste de prioridad a un primer conjunto de dispositivos de red 104 y asignar un segundo ajuste de prioridad a un segundo conjunto de dispositivos de red 104. La primera configuración de prioridad puede estar asociada con un primer límite de ancho de banda, y la segunda configuración de prioridad puede estar asociada con un segundo límite de ancho de banda.

El portal de clientes 118 puede generar datos en tiempo real sobre el uso de la red, el rendimiento y la selección de servicios, utilizando el flujo integral de información y control entre el orquestador, la nube y el agente. Con un conjunto de herramientas, API, datos e idiomas, el portal del cliente 118 puede integrarse e interactuar con la inteligencia de un orquestador OpenFlow SDN para permitir el aprovisionamiento de autoservicio bajo demanda y en tiempo real desde la nube al dispositivo 104. La creciente demanda de los clientes de calidad de servicio, alta disponibilidad, opciones y atención al cliente está colocando al Centro de Operaciones de Red (NOC), con sus

herramientas, procedimientos y recursos asociados bajo una presión abrumadora. Con la migración de los servicios de la oferta a la demanda, nunca ha habido tal enfoque en la excelencia operativa. Se acabaron los días en los que las operaciones se eliminaban por completo de la experiencia del cliente. La migración de dichas herramientas al centro de llamadas para estar a la vanguardia de la tecnología del cliente está evolucionando a un ritmo, SDN desafia las normas del plano de control/datos integrado en la red, con Cloud y NFV resumiendo las topologías físicas. Mientras tanto, se espera que las operaciones, como mínimo, se mantengan al día, pero se mantengan por delante de la curva.

El portal de administración 116 ha sido diseñado para proporcionar un conjunto de herramientas e informes que permiten información e intervención desde el nivel físico hasta el de aplicación. Solidario con la capacidad de aplicar aplicaciones para detectar y reaccionar dinámicamente a eventos de red, abordando así los problemas en tiempo real, mucho más rápido de lo que ha sido posible con herramientas y procedimientos heredados. Operaciones a través de varios niveles de acceso desde el supervisor al usuario una selección de ventanas, que brindan el conjunto completo de FCAPS (el modelo y marco estándar reconocido) de herramientas de administración de red e informes. También permite la aplicación de reglas automatizadas simples para reconfigurar proactivamente la red 103 y los servicios virtuales, minimizando las interrupciones y fallas del servicio que se derivan de ciertas condiciones que se recopilan desde la red/dispositivos.

Haciendo referencia ahora a las Figuras 5-7 que ilustran una plataforma SDN ejemplar 200 que también está de acuerdo con la presente enseñanza. La plataforma SDN 200 es sustancialmente similar a la plataforma SDN 100 y los elementos similares se indican mediante números de referencia similares. El sistema BSS 204 recibe un nuevo pedido de cliente, etapa 220. Un nuevo perfil de cliente es creado por el administrador de perfiles de cliente 206, etapa 221. Un dispositivo 104 de equipo en las instalaciones del cliente (CPE) entra en línea, etapa 222. El CPE 104 está habilitado y aislado, etapa 223. El CPE 104 es validado por el módulo de autenticación 203, etapa 224. El nuevo perfil de cliente se almacena en una base de datos abierta 138, etapa 224. El cliente es identificado y autenticado por el módulo de autenticación 203, etapa 225. El controlador de políticas 135 se comunica con un administrador de perfiles de clientes 206, un controlador de recursos 205 y un módulo de orquestación 207 y resume una política de configuración para el nuevo cliente, etapa 226. Un controlador SDN maestro 102 genera controladores agregados distribuidos apropiados 105A-105H y envía los controladores agregados distribuidos 105A-105H a los dispositivos CPE 104 asociados con el nuevo cliente, etapa 227. El controlador agregado SDN 105 se instancia en los CPE 105A-105H, etapa 228. Los controladores agregados distribuidos una vez instalados en los CPE 104A-104H se registran con el controlador SDN maestro 102, etapa 229. El controlador SDN maestro 102 programa los recursos apropiados y las tablas de enrutamiento en el sistema en los chips 212A-212H de cada CPE 211A-211H usando los controladores agregados distribuidos 105A-105, etapa 230. Una vez instalados los controladores agregados, funcionan como motores de enrutamiento local en los CPE 104. La configuración de los CPE 104A-104H está finalizada, etapa 232. El controlador agregado SDN distribuido 105A-105H envía análisis sobre sus respectivos CPE 104A-104H a la base de datos abierta 138 a través del controlador SDN maestro 102. Los análisis de clientes de cada CPE 104A-104H son accesibles para el cliente desde la base de datos abierta 138 a través de su portal de clientes 118, etapa 237. El análisis operativo de cada CPE 104A-104H es accesible al portal de administración 116 desde la base de datos abierta 138, etapa 238. El controlador de recursos 236 puede funcionar para enviar datos de recursos a la base de datos abierta, etapa 235. Además, el controlador de recursos 236 puede funcionar para enviar datos de políticas a la base de datos abierta 211, etapa 234. Un motor de análisis 205 puede funcionar para analizar los datos en la base de datos 138 y modificar la política y los datos de control para los respectivos CPE 104. La política modificada y los datos de control son enviados a los controladores agregados distribuidos 105 por el controlador SDN maestro 102 con el fin de reconfigurar los ajustes operativos en los CPE 104 para mejorar el rendimiento de los dispositivos 104. Mejorar el rendimiento de los CPE 104 puede incluir, a modo de ejemplo, mejorar la calidad del servicio experimentado por el usuario final. De esta manera, los expertos en la técnica apreciarán que el estado de los CPE 104 está siendo monitoreado continuamente por los controladores agregados 105, y si se detecta un problema, los controladores agregados 105 pueden rectificar el problema mediante reconfigurar los CPE 104 en tiempo real.

Con referencia ahora a la Figura 8, que ilustra un diagrama de flujo que muestra etapas a modo de ejemplo de la plataforma SDN en funcionamiento, que también está de acuerdo con la presente enseñanza. El diagrama de flujo de la figura 8 se corresponde sustancialmente con el diagrama de flujo 7 y los elementos similares se identifican mediante números de referencia similares. La principal diferencia es que las etapas 240-244 de la figura 8 reemplazan las etapas 227-231 de la figura 7 mientras que las etapas restantes son sustancialmente similares. Una vez resumida la política de configuración en la etapa 226, las instrucciones de configuración se envían a una orquestación en la nube, etapa 240. La infraestructura de la nube está orquestada para los servicios de aplicaciones en la nube y el portal, etapa 241. Se inicia una instancia del portal del cliente y se asigna al cliente y al CPE 104, etapa 243. Se abren túneles de comunicación entre el CPE 104 y la instancia del servicio en la nube, etapa 243. El análisis se programa y se recopila de los CPE, etapa 244. El funcionamiento de las etapas restantes es como se describió anteriormente con referencia a la Figura 7.

Con referencia a la Figura 9, que ilustra otro diagrama de flujo que muestra etapas ejemplares de la plataforma SDN en funcionamiento, que también está de acuerdo con la presente enseñanza. El diagrama de flujo de la figura 9 se corresponde sustancialmente con el diagrama de flujo de la figura 7 y los elementos similares se identifican

mediante números de referencia similares. La principal diferencia es que las etapas 250-254 de la figura 9 reemplazan las etapas 227-231 de la figura 7 mientras que las etapas restantes son sustancialmente similares. Una vez resumida la política de configuración en la etapa 226, el control primario identifica el CPE 211A-211H, etapa 250. El controlador SDN maestro 102 inicia la programación de las funciones del sistema, etapa 251. Los componentes
 5 funcionales se programan en el SOC, etapa 252. Los controladores agregados 105 actualizan conjuntos de reglas de reenvío para el respectivo CPE 211A-211H. Los análisis necesarios se programan en el CPE211A-211H y se recopilan. El funcionamiento de las etapas restantes es como se describió anteriormente con referencia a la Figura 7.

Con referencia a la figura 10, se ilustra otra plataforma SDN 300 que también está de acuerdo con la presente
 10 enseñanza. La plataforma SDN 300 es sustancialmente similar a la plataforma SDN 100 y los componentes similares se indican mediante números de referencia similares. La principal diferencia es que solo se proporciona un portal, a saber, el portal del cliente 118, que permite que un cliente active un cambio en la política y/o los datos de control, etapa 310. El cambio de política y/o datos de control se implementan en el CPE 104A-104H por los controladores agregados 105 de la manera descrita anteriormente. De lo contrario, el funcionamiento de la
 15 plataforma SDN 300 funciona de forma similar a la SDN 100.

Con referencia a la figura 11, se ilustra otra plataforma SDN 400 que también está de acuerdo con la presente
 enseñanza. La plataforma SDN 400 es sustancialmente similar a la plataforma SDN 100 y los componentes
 20 similares se indican mediante números de referencia similares. La principal diferencia es que solo se proporciona un portal, a saber, el portal de administración 118, que permite a un operador activar un cambio en la política y/o los datos de control, etapa 410. El cambio de política y/o datos de control se implementan en el CPE 104A-104H por los controladores agregados 105 de la manera descrita anteriormente. De lo contrario, el funcionamiento de la
 plataforma SDN 400 funciona de forma similar a la SDN 100.

Con referencia a la figura 12, se ilustra otra plataforma SDN 500 que también está de acuerdo con la presente
 25 enseñanza. La plataforma SDN 500 es sustancialmente similar a la plataforma SDN 100 y los componentes similares se indican mediante números de referencia similares. La principal diferencia es que los controladores agregados 105 se distribuyen a los CPE 104 en dos redes separadas, a saber, la primera red 510 y la segunda red 520. De lo contrario, el funcionamiento de la plataforma SDN 500 funciona de forma similar a la SDN 100.

Con referencia a la figura 13, que ilustra otro diagrama de flujo que muestra etapas ejemplares de la plataforma SDN
 en funcionamiento, que también está de acuerdo con la presente enseñanza. El diagrama de flujo de la figura 13 se
 corresponde sustancialmente con el diagrama de flujo de la figura 9 y los elementos similares se identifican
 mediante números de referencia similares. En esta realización ejemplar, el motor de análisis 205 escanea los
 35 análisis almacenados en la base de datos 138 que han sido extraídos de los CPE 104 por los controladores
 agregados 105. El motor de análisis puede funcionar para detectar problemas de rendimiento de WIFI en la red
 doméstica de un cliente, etapa 610. Una aplicación de control WIFI está en comunicación con el motor de análisis y
 puede funcionar para interpretar la salida del motor de análisis. En este ejemplo, la aplicación de control WIFI
 40 identifica un solapamiento de canal WIFI con vecinos y desencadena un cambio en la configuración WIFI del hogar
 del cliente en un momento apropiado modificando los datos de política/configuración para el cliente, etapa 620. El
 motor de control de políticas 135 resume datos de configuración para un cambio de canal WIFI, etapa 226. El
 cambio de configuración se implementa en el enrutador WIFI por los controladores agregados apropiados 105 de la
 manera descrita anteriormente. En este ejemplo, la plataforma SDN actualiza sin problemas el canal WIFI sin
 45 requerir ninguna entrada del usuario. Las etapas restantes son similares a las descritas anteriormente con referencia
 a la figura 9.

Con referencia a la figura 14, que ilustra otro diagrama de flujo que muestra etapas ejemplares de la plataforma SDN
 en funcionamiento, que también está de acuerdo con la presente enseñanza. El diagrama de flujo de la figura 14 se
 corresponde sustancialmente con el diagrama de flujo de la figura 9 y los elementos similares se identifican
 50 mediante números de referencia similares. En esta realización ejemplar, el motor de análisis 205 escanea los
 análisis almacenados en la base de datos 138 que han sido extraídos de los CPE 104 por los controladores
 agregados 105. El motor de análisis 205 puede funcionar para detectar servicios prioritarios seleccionados activados
 desde una red doméstica sobre WIFI doméstico general, etapa 710. El servicio de prioridad seleccionado puede
 55 asignar un límite de ancho de banda más alto a ciertos dispositivos sobre otros dispositivos. Una aplicación de
 control WIFI está en comunicación con el motor de análisis y puede funcionar para interpretar la salida del motor de
 análisis 205. En este ejemplo, la aplicación de control de WIFI desencadena cambios en la calidad del servicio en la
 configuración de WIFI doméstico del cliente modificando los datos de política/configuración para el cliente, etapa 720.
 El motor de control de políticas 135 resume datos de configuración para un cambio de QoS, etapa 226. El
 controlador maestro 102 identifica el CPE 104 apropiado que requiere reconfiguración en vista del cambio de QoS,
 60 etapa 250. El cambio de configuración se implementa en el CPE 104 apropiado por los controladores agregados 105
 apropiados de la manera descrita anteriormente. Las etapas restantes son similares a las descritas anteriormente
 con referencia a la figura 9.

Con referencia a la figura 15, que ilustra otro diagrama de flujo que muestra etapas ejemplares de la plataforma SDN
 65 en funcionamiento, que también está de acuerdo con la presente enseñanza. El diagrama de flujo de la figura 15 se
 corresponde sustancialmente con el diagrama de flujo de la figura 9 y los elementos similares se identifican

mediante números de referencia similares. En esta realización ejemplar, el motor de análisis 205 escanea los análisis almacenados en la base de datos 138 que han sido extraídos de los CPE 104 por los controladores agregados 105. El motor de análisis 205 puede funcionar para detectar que el rendimiento de la tasa de error de modulación (MER) de final de línea (EOL) es alto en el segmento de fibra híbrida coaxial (HFC). Una aplicación de gestión DOCSIS está en comunicación con el motor de análisis y puede funcionar para interpretar la salida del motor de análisis 205. En este ejemplo, la aplicación de gestión DOCSIS identifica que la reducción de potencia es factible reprogramando una interfaz de energía de los CPE 104. El motor de control de políticas 135 resume datos de configuración para implementar la reducción de energía, etapa 226. El controlador maestro 102 identifica el amplificador apropiado 104 que requiere reprogramación para implementar la reducción de energía. El cambio de configuración se implementa en el amplificador apropiado por los controladores agregados 105 apropiados de la manera descrita previamente. Las etapas restantes son similares a las descritas anteriormente con referencia a la figura 9.

Una arquitectura ejemplar 1000 de acuerdo con la presente enseñanza se ilustra en las Figuras 16A-B, 17 y 18. La arquitectura 1000 permite abordar las amenazas a la seguridad y las violaciones a la privacidad aprovechando la capacidad de programación del control de flujo en los dispositivos SDN para identificar y no reenviar el tráfico identificado que contiene amenazas o violaciones a la privacidad. El reenvío basado en flujo está programado en el dispositivo del usuario final 104 para limitar el reenvío de tráfico de amenazas o tráfico de violación de privacidad. Las figuras 16A-17 incluyen muchos componentes similares descritos anteriormente con las figuras de referencia 3-5 y los elementos similares se indican mediante números de referencia similares. Estos elementos similares operan de una manera similar a la descrita anteriormente. La arquitectura 1000 incluye un controlador SDN maestro 102 configurado para gestionar el control del flujo de datos en la red SDN. El controlador SDN maestro puede funcionar para generar datos de enrutamiento para los dispositivos en red 104. El controlador SDN maestro 102 está configurado para generar una pluralidad de controladores agregados discretos 105, cada uno asociado con un usuario final particular. Cada controlador agregado SDN 105 incluye datos de enrutamiento para un dispositivo asociado en red 104. El controlador agregado SDN 105 es enviado por el controlador SDN maestro 102 a los dispositivos en red 104 asociados con los respectivos usuarios finales para controlarlos. Los dispositivos en red 104 pueden solicitar acceso a un destino en la red SDN, por ejemplo, un localizador uniforme de recursos (URL). En respuesta, un sistema de nombres de dominio (DNS) 1035 inicia una interacción con el dispositivo en red 104 solicitante. El DNS 1035 retransmite los datos de DNS asociados con la URL solicitada a un sistema de control de gestión de amenazas (TMCS) 1010. El TMCS 1010 está configurado para determinar si la URL solicitada tiene un criterio de seguridad asociado. El TMCS 1010 comunica el estado de amenaza al controlador agregado SDN 105 asociado con el dispositivo en red 104 solicitante. El controlador agregado SDN 105 puede funcionar para generar datos de enrutamiento para el dispositivo en red solicitante 104 en el que está instalado en base al estado de amenaza para permitir o denegar el acceso a la URL solicitada.

En la realización ejemplar, el TMCS 1010 está en comunicación con una base de datos de identificación de amenazas (TIDB) 1020 y una base de datos de identificación de violaciones de privacidad (PVIDB) 1030. El TIDB 1020 almacena detalles de destinos que están clasificados como que tienen un criterio de amenaza malicioso asociado a ellos. El PVIDB 1030 almacena los detalles de los destinos que están clasificados como que tienen una amenaza a la privacidad asociada a ellos. Por ejemplo, se sabe que dichos destinos recopilan datos privados de los usuarios sin que el usuario lo sepa. El TMCS 1010 está configurado para procesar y validar las solicitudes de destino contra la base de datos de identificación de amenazas (TIDB) 1020 y el PVIDB 1030 y puede funcionar para garantizar que los usuarios no se conecten a destinos maliciosos. Por ejemplo, los destinos maliciosos pueden incluir sitios web sospechosos, redes de entrega de contenido (CDN), sitios web y direcciones IP de CDN, dominios, URL, etc. El TMCS 1010 permite la aceptación y las entradas de una consulta de DNS donde luego verifica y valida al usuario y aplica las reglas asociadas a un perfil de usuario. Una vez que se ha consultado al TIDB 1020 para una ruta en particular y se ha validado el perfil de usuario, el TMCS 1010 se comunica con la base de datos 138 del sistema de orquestación SDN. El controlador SDN maestro 102 luego propaga un mensaje al controlador agregado SDN 105 en el CPE 104 con datos de enrutamiento apropiados para el dispositivo solicitante 104. Un módulo de coincidencia de seguridad SDN 1025 dentro del dispositivo 104 valida si se va a aplicar la ruta. Si se va a aplicar, entonces el controlador agregado SDN 105 inserta una entrada de reenvío en la tabla de reenvío; de lo contrario, se incluye una entrada para reenviar el tráfico a un destino de cuarentena. El TMCS 1010 informa a la base de datos 138 de manera que los datos se pueden extraer y utilizar para informar sobre amenazas y/o violaciones de privacidad al portal 118 del cliente y/o al portal 116 de administración.

El TIDB 1020 puede ser la base de datos de una empresa privada de seguridad en Internet que almacena datos sobre sitios web peligrosos y sospechosos, CDN, sitios web y direcciones IP de CDN, dominios, URL, etc. Esta información es recopilada por varias empresas y organizaciones de todo el mundo sobre amenazas conocidas relacionadas con temas de seguridad relacionados con antiphishing, malware y control de dominio, etc. Las agencias de seguridad gubernamentales, las empresas de servicios financieros y las empresas de comercio electrónico, las empresas de tecnología, las redes sociales y los proveedores de servicios de Internet (ISP) ya utilizan estas bases de datos para ayudar a mantenerse en la lucha contra los ataques.

La función del PVIDB 1030 es almacenar datos sobre las empresas de Internet que utilizan sus aplicaciones para recopilar datos privados de los usuarios una vez que las aplicaciones están instaladas en los dispositivos del usuario

final 104. Esto es especialmente relevante cuando un producto o servicio de Internet suministrado por una empresa de Internet no cumple con las regulaciones locales de cada país sobre la recopilación de datos de un suscriptor. El PVIDB 1030 puede ser una extensión del TIDB 1020 o un sistema separado. La función del PVIDB 1030 es garantizar que el consumidor esté protegido contra violaciones de privacidad de empresas que no cumplan con ciertos criterios, por ejemplo, expectativas de decencia y regulaciones locales al bloquear todo el tráfico del suscriptor de la plataforma 1000 a sus sistemas en base al flujo. El PVIDB 1030 permite a los suscriptores decidir qué datos desean enviar a Internet en lugar de que las partes de la red decidan por sí mismos qué tomarán, independientemente de si el cliente lo sabe o no.

- 10 La arquitectura 1000 utiliza una capa de control altamente resistente 107 que facilita la distribución del control a través de una federación de controladores agregados SDN distribuidos 105. Cada cliente puede seleccionar una política de seguridad y/o privacidad seleccionando opciones de configuración a través del portal del cliente 118 y luego esto se transmite usando una API 120 o el SDK 122 a través del plano de control 107 donde el usuario es primero autenticado por el módulo de autenticación 203 antes de que el controlador 135 de políticas aplique una política para la dirección IP y los dispositivos conocidos que se recopilan de las bases de datos 1020, 1030. El controlador de políticas 135 abstrae la política apropiada y aplica la política a los controladores agregados SDN distribuidos 105 que están instalados en los dispositivos 104.

- La figura 19 ilustra un diagrama de flujo que detalla etapas ejemplares implementadas por la arquitectura 1000. En este ejemplo ejemplar, un dispositivo de cliente 104 solicita acceso a una URL. Esta solicitud a una URL puede ser activada por el propio cliente o puede ser provocada por el tráfico generado por Adware, Malware, BotNet, violación de privacidad, tráfico en el dispositivo del usuario 104. En este escenario, se inicia una interacción de consulta/respuesta de DNS entre una aplicación de abonado en el dispositivo 104 y un sistema de nombres de dominio (DNS) 1035 de un operador, etapa 501. El DNS 1035 inicia un procedimiento de búsqueda y también transmite un mensaje que contiene una IP de suscriptor, una IP de destino y una URL a través de una API segura al TMCS 1010, etapa 502.

- La recepción del mensaje del DNS 1035 activa el TMCS 1010 para consultar el PVIDB 1030 y/o TIDB 1020 (o caché) para identificar si la URL contenida en el mensaje tiene un estado de amenaza/privacidad asociado, etapa 503. El TMCS 1030 también puede solicitar la clasificación de identidad del abonado para validar la clasificación del perfil de usuario, etapa 504. Tras la recepción de una respuesta del TIDB 1020 y el PVIDB 1030 (identificación y clasificación de usuario) y (clasificación de seguridad / precio), etapa 503, el TMCS 1010 envía al controlador agregado SDN 105 el estado de amenaza URL y clasificación del cliente, etapa 505. La Tabla 1 y la Tabla 2 definen definiciones ejemplares del usuario y los identificadores de clasificación de riesgo que pueden transmitirse entre los diversos sistemas para ayudar a comprender la naturaleza del tipo de ataque y definir qué expectativas existen para el control del tráfico que pertenece al cliente final. La información proporcionada en la tabla 1 y la tabla 2 se proporciona sólo a modo de ejemplo y no pretende limitar la presente enseñanza a los valores de ejemplo proporcionados.

Tabla 1: Clasificación de infracción de privacidad/amenaza ejemplar

Tipo de riesgo	Definición	Tipo de tráfico	Clasificación
Infección	Virus	Tráfico generado por virus saliente	#A
Usuario bajo ataque	DDOS, BotNet, escaneo de puertos	Tráfico entrante de DOS	#B
Robo de datos de usuario	Adware, malware, etc.	Tráfico saliente	#C
Usuario iniciando ataque	DDOS, escaneo de puertos, BotNet	Tráfico DOS saliente (usuario que se une a BotNet debido a una infección)	#D
Violación de privacidad	Adware, malware, etc.	Tráfico saliente	#E
Sitio web tóxico	Sitio web identificado por TIDB como riesgoso	Tráfico entrante	#F
CDN tóxico	CDN identificado por TIDB como riesgoso	Tráfico entrante	#G
Sitio web fraudulento	Sitio web identificado como secuestrado	El usuario intenta acceder a sitios web que han sido secuestrados.	#H
Infraestructura bajo ataque	Dispositivo del operador bajo ataque	Tráfico entrante	#J
Tráfico de infracción de privacidad	Destino identificado del tráfico de empresas invasoras	Tráfico saliente	#K

Tabla 2: Clasificaciones de perfil de usuario ejemplares

Clasificación de perfil de usuario	Acción	Clasificaciones de flujo
Acceso a Internet muy limitado según la lista blanca generada por TIDB	TMCS aplica el perfil 1	n.º 1
Acceso a Internet medio según la lista blanca generada por TiDB	TMCS aplica el perfil 2	n.º 2
Dominios TOD definidos por el usuario para bloquear	TMCS aplica el perfil 2 con TOD	n.º 3
Adulto con protección de seguridad	TMCS aplica el perfil 4	n.º 4
Sin protección, completamente abierto	TMCS aplica el perfil 5	n.º 5
Se permite comunicar solo con usuarios autenticados	TMCS aplica el perfil 2 + bloqueo de llamadas entrantes en aplicaciones de comunicaciones aprobadas (una para que la analicemos con SKYPE)	n.º 6
Bloqueo de túneles	TMCS aplica el perfil X + perfil 7	n.º 7
Violación de privacidad	TMCS aplica el perfil 8	n.º 8

El controlador agregado SDN 105 tiene un módulo de coincidencia de seguridad 1025 que puede funcionar para definir la decisión de reenvío apropiada en el dispositivo 104 para el perfil de usuario que depende de la clasificación de riesgo, etapa 506. La decisión de reenvío puede ser enviar el tráfico a un destino de cuarentena (con agujeros negros) o permitir que el tráfico se reenvíe al destino según lo solicite el usuario. El controlador agregado SDN 105 establece entonces una entrada de reenvío en la tabla de enrutamiento de flujo 119, etapa 507, contra la dirección IP del abonado solicitante dependiendo de la información recibida de la etapa 506. Si la URL se indica como un sitio de riesgo, el TMCS 1010 genera un informe, etapa 508, que se introduce en la base de datos abierta 138 a la que puede acceder el cliente a través del cliente 118. El informe se puede señalar transmitiendo la dirección IP del abonado, el identificador de perfil de usuario y el identificador de clasificación de riesgo a la base de datos 138. La base de datos 138 usa la dirección IP del abonado para mapear el informe de alerta de seguridad con el registro del cliente. A continuación, estos datos se importan al portal del cliente relevante 118 para indicar un resumen de la acción de seguridad/privacidad necesaria que se puede tomar para aliviar la amenaza.

Además de proporcionar información más completa sobre el riesgo de seguridad/privacidad, la clasificación de riesgo se analiza contra el TIDB 1020, etapa 509, y se puede generar un informe detallado completo sobre el riesgo que se informa al portal del cliente 118. El informe detallado incluye información extraída de la base de datos 138. La base de datos 138 usa la dirección IP del abonado para mapear el informe de alerta de seguridad con el registro del cliente. Además, el informe detallado puede identificar el riesgo, describir los efectos del riesgo y qué medidas se deben tomar para abordarlo.

El portal de administración 116 se puede operar para calcular informes regulares de seguridad/privacidad ejecutando consultas contra la base de datos abierta 138, etapa 510. Los equipos de productos, marketing y ventas de los ISP también pueden acceder a estos informes para permitirles crear nuevos productos, crear promociones sobre los peligros de no estar protegidos y dirigirse a las personas con promociones que estén gravemente infectadas. Para el ISP, se puede utilizar una promoción de ventas para que un cliente limpie sus sistemas, eliminando así la carga innecesaria de la red y para crear una tendencia de marketing sobre el ISP mismo como un proveedor de red seguro.

Un ejemplo de flujo de trabajo de acuerdo con la presente enseñanza se ilustra en la Figura 20A y 20B. El cliente identifica la política por usuario a través de las opciones de configuración proporcionadas en el portal del cliente 118 a través de la capa de control de orquestación 107 donde el usuario se autentica primero y luego se aplica una política, bloque 1053. Para que se aplique esta política, se extraen datos, por ejemplo, dirección IP e ID de dispositivo, política de seguridad o privacidad elegida por el cliente a través del portal del cliente 118 de la base de datos abierta 138. También se extrae de la base de datos abierta 138 una lista de sitios bien conocidos y utilizados comúnmente por el cliente. Estas entradas de reenvío se cotejan, bloque 1055 y clasifican, bloque 1058, antes de ser comunicadas desde el controlador SDN maestro 102 al controlador agregado SDN 105, bloque 1060. El módulo de coincidencia de seguridad SDN 1025 coincide tanto con la privacidad como con las amenazas, bloque 1062. El módulo de coincidencia de seguridad 1025 compara el identificador de perfil de cliente en la tabla de clasificación de flujo de usuarios 1065 contra el riesgo y luego un módulo de control 1067 establece la ruta de reenvío, bloque 1069, según la decisión tomada por el módulo de coincidencia de seguridad SDN 1025. La tabla de clasificación de flujo

1062 almacena la clasificación de amenazas según los ejemplos identificados en la Tabla 1. La tabla de clasificación de flujo de usuarios 1070 almacena la clasificación del perfil de usuario según los ejemplos identificados en la Tabla 2.

- 5 Con referencia a las Figuras 21A y 21B, se ilustra otra plataforma SDN 1200 que también está de acuerdo con la presente enseñanza. La plataforma SDN 1200 es sustancialmente similar a la plataforma SDN 500 de la Figura 12 y los componentes similares se indican mediante números de referencia similares. La principal diferencia es que la plataforma SDN 1200 incluye TMCS 1010, TIDB 1020 y PVIDB 1030 como se describe con referencia a las Figuras 16-21. La plataforma SDN 1200 ilustra el procedimiento de flujo implementado cuando un cliente activa un cambio
10 en el bloque 1205 a la política de amenaza o privacidad que se aplica a la configuración utilizada para proteger su hogar/negocio. Las figuras 21A y 21B ilustran que una solución de plano de control orquestada puede ofrecer un cambio de política para permitir un cambio de política de seguridad o privacidad. En este ejemplo, dicho cambio puede activarse desde el portal de administración 116 para proteger los dispositivos IOT / domésticos a través de redes de acceso que operan en una variedad de tecnologías de acceso diferentes. Cuando el controlador agregado
15 SDN ligero 105 está configurado en el dispositivo IOT, las políticas de seguridad y privacidad pueden aplicarse a estos dispositivos directamente.

Este procedimiento permite a los operadores de red controlar y orquestar entornos de red utilizando controladores agregados SDN orquestados y distribuidos 105 que operan para entornos de clientes ON-Net y OFF-Net. Al reducir
20 la necesidad de que el CPE sea multipropósito y económico, esto permite al operador concentrarse en adquirir un CPE que proporcione reenvío y control de paquetes premium. Al habilitar la verificación contra múltiples TIDB 1020 / PVIDB 1030 de terceros, esto garantiza una mayor conciencia de las amenazas y las violaciones de la privacidad en el momento más temprano. Como TIDB 1020 / PVIDB 1030 se alimenta con las últimas amenazas y datos de privacidad, esto garantiza que los controles aplicados sean los más relevantes. Además, una solución controlada en
25 la nube permite el control total de todos los dispositivos sin causar carga en el dispositivo final y permite que las reglas para todos los dispositivos se apliquen de manera uniforme en todos los dispositivos de las instalaciones del cliente. Esta estrategia de seguridad es particularmente relevante para IOT, ya que permite el control en la nube de todos los datos procedentes de las instalaciones del cliente. Se pueden crear reglas de reenvío basadas en flujo específicas para todos los sistemas IOT, asegurando por tanto que incluso si estos dispositivos son pirateados, el
30 controlador agregado SDN ligero 105 no reenvíe tráfico a ningún otro sistema. Esto brinda control y mejora la protección del usuario final contra la intención maliciosa de algunas organizaciones e individuos. Ayuda al consumidor a lidiar con la complejidad de los problemas de seguridad y privacidad creados en Internet y permite que se creen actualizaciones de políticas generalizadas cuando se identifican y actualizan nuevos vectores de ataque en los TIDB 1020 y PVIDB 1030.

35 Con referencia a la figura 22, que ilustra otro diagrama de flujo que muestra etapas ejemplares de la plataforma SDN en funcionamiento, que también está de acuerdo con la presente enseñanza. El diagrama de flujo de la figura 22 se corresponde sustancialmente con el diagrama de flujo de la figura 9 y los elementos similares se identifican mediante números de referencia similares. En esta realización ejemplar, un cliente desencadena un cambio de
40 configuración de política de privacidad o amenaza desde el portal del cliente 118, etapa 1305. El usuario proporciona detalles de autenticación a través del portal del cliente 118, etapa 1308. El usuario es autenticado por el módulo de autenticación, etapa 1310. El controlador de políticas 135 resume datos de configuración para el cambio de política de amenazas / privacidad, etapa 1312. El controlador SDN maestro 102 identifica el dispositivo apropiado 104, etapa 1214. El controlador maestro SDN 102 señala la programación del cambio de política de amenaza / privacidad al
45 controlador agregado SDN 105, etapa 1316. Las clasificaciones de riesgo / privacidad se programan en el SOC en el CPE 104 para la política del cliente por el controlador agregado SDN 105, etapa 1318. El controlador SDN maestro 102 actualiza los conjuntos de reglas de reenvío, etapa 1320. El módulo de coincidencia de seguridad 1025 procesa las reglas establecidas para los flujos ya existentes consultando el TIDB 1020 y / o PVIDB 1030, etapa 1322. El módulo de coincidencia de seguridad 1025 consulta el TMCS 1010 comparándolo con TIDB / PVIDB para
50 direcciones de riesgo, etapa 1323. El controlador SDN maestro 102 coopera con el controlador agregado SDN 105 para programar un módulo de recopilación de análisis en el CPE 104, etapa 1324. El controlador agregado SDN empuja los análisis a la base de datos abierta 138, etapa 233. Las etapas restantes son similares a las descritas anteriormente con referencia a la figura 9.

55 Las ventajas de la enseñanza actual son muchas. En particular, al pasar a una solución de reenvío de flujo controlado por SDN, esto permite que las nuevas búsquedas de reenvío de un cliente se procesen fuera de línea según las reglas de privacidad / seguridad definidas en la configuración del cliente, utilizando el TMCS 1010. Esto descarga el procesamiento de aplicaciones de seguridad del dispositivo final 104 y reduce la carga de procesamiento en el CPE de múltiples extremos 104. Además, esto reduce la necesidad de ejecutar aplicaciones de
60 seguridad en el CPE 104, lo que reduce los costos. Además, dado que ya no es necesario cargar aplicaciones de seguridad en el CPE 104, esto reduce los recursos de procesamiento y memoria requeridos por el CPE 104.

Cuando la solución CPE controlada por SDN orquesta un entorno residencial, esto permite que los controles se apliquen a un usuario de manera granular para garantizar que los controles se puedan aplicar rápidamente sin la
65 necesidad de volver a escribir primero el software y enviar actualizaciones y parches para sistemas individuales. Un ejemplo de un impulso de política de este tipo es que cuando se identifica un BotNet como disparador, se realiza un

impulso de política a cualquier CPE que solicite una ruta al destino bajo ataque. Esto asegura que el CPE no se una al ataque. Además, el CPE de control de SDN orquestado se identifica como infectado con ese BotNet en particular. A continuación, se envía un informe al consumidor con un informe del dispositivo, su dirección MAC y otra información relevante recopilada. Se les informa de la infección y se les pide que hagan algo al respecto. El mismo mecanismo se utiliza para controlar infecciones como adware o malware, etc., cuando se mantienen destinos conocidos en el TMCS 1010.

Cuando cualquier dispositivo dentro del entorno del consumidor solicita dicho destino, la búsqueda se compara con el TMCS 1010 y cuando una ruta se identifica o se considera cuestionable, la ruta de reenvío basada en flujo no se cumple hasta que se confirma la validación adicional de la ruta solicitada. Se notifica al cliente de la naturaleza de la posible infracción y no se instala ninguna ruta de reenvío hasta que se verifique completamente que la ruta sea segura y cuando el sistema de control esté seguro de que la ruta solicitada no es algo que haya sido generado por una aplicación que podría ocasionar una brecha de seguridad.

Este procedimiento actual utiliza un controlador agregado SDN distribuido y ligero 105 que puede instalarse en cualquier hardware, ya sea mediante la incorporación del controlador SDN ligero dentro del firmware o en un CPE abierto. Esta solución ligera controlada por SDN rompe la naturaleza patentada de CPE y permite que la solución se aplique y controle en las soluciones de CPE de múltiples proveedores. El controlador agregado SDN ligero 105 programa la tabla de reenvío del CPE / dispositivo de consumidor 104 mediante el uso de un componente de orquestación de ruta que está regionalizado o centralizado. Esto se utiliza para establecer una lista definida de reglas de políticas generadas a partir de una base de datos de amenazas única o múltiple que se ha llenado con detalles de las amenazas identificadas. Estas políticas se comunican mediante protocolos estándar abiertos y se establecen dentro de las reglas de reenvío del CPE / dispositivo de consumidor o, cuando el volumen es demasiado grande, residen en la tabla de búsqueda del componente de orquestación de rutas que está regionalizado o centralizado, según la escala de la red. Estas reglas de reenvío iniciadas por la seguridad, luego eliminan el tráfico destinado a estos destinos para los dispositivos que deben protegerse dentro de las instalaciones del consumidor. No es necesario que todas las reglas se almacenen en el dispositivo, ya que cuando se solicita una nueva ruta desde la función de orquestación de ruta central y se puede realizar una verificación en la base de datos de terceros para validar si la ruta es de hecho un destino no tóxico. Esta podría ser una ruta solicitada a través de DNS u otra estrategia basada en otros estándares, por ejemplo, ARP para IPv4.

Un experto en la materia apreciaría que los dispositivos finales distribuidos a los consumidores no tengan la capacidad de analizar o almacenar los grandes volúmenes de datos utilizados necesarios para el procesamiento de las complejas reglas de seguridad. Esta incapacidad para procesar estos complejos conjuntos de reglas y las limitaciones de las aplicaciones basadas en el dispositivo restringen la capacidad de las aplicaciones actuales para proteger mejor al cliente final, dejando al consumidor desprotegido y vulnerable. El cálculo de la base de datos completa del sistema de control de amenazas conocido o de las bases de datos de múltiples sistemas de control de amenazas se realiza fuera de línea. Un ejemplo de dónde se podría procesar la base de datos de amenazas o las bases de datos es dentro de un entorno de nube. Estas bases de datos de terceros contendrían datos conocidos sobre BOTNETS, ADWARE, DDOS, MALWARE, intrusión de privacidad, cortafuegos, control parental, etc. Se identificarán múltiples tuplas de datos coincidentes y se establecerán reglas de reenvío que garantizarán que el tráfico generado dentro del hogar no se envíe a destinos en Internet. Además, el sistema de control de amenazas interactuará con múltiples fuentes de amenazas para garantizar que se mantenga actualizado sobre las últimas materializaciones de amenazas de seguridad que tienen lugar en Internet.

Además, cuando se generan ataques DDOS a un destino conocido en Internet, el control basado en el flujo puede utilizarse para eliminar de forma granular los flujos de ataque del tráfico que atraviesa la red. Hoy en día, los destinos atacados tienden a tener que lidiar con el ataque desconectando el sitio o utilizando hardware costoso y de alta gama que es difícil de escalar de manera efectiva. En efecto, las soluciones conocidas hasta ahora brindan al atacante el efecto deseado, ya que la empresa que aloja el sitio se ve sometida a una presión considerable y, en muchos casos, tiene que retirar la visibilidad del sitio en Internet para evitar el ataque.

Con referencia a la figura 23, se ilustra otra plataforma SDN 1500 que también está de acuerdo con la presente enseñanza. La plataforma SDN 1500 es sustancialmente similar a la plataforma SDN 200 y los componentes similares se indican mediante números de referencia similares. La diferencia principal es que el portal 118 del cliente incluye una interfaz de usuario de voz 1505 que permite a los usuarios interactuar con la plataforma de SDN 1500 utilizando comandos de voz. De esta manera, la plataforma SDN 1500 proporciona una o más interfaces de usuario de voz 1505 que están configuradas para facilitar a los usuarios el control de los dispositivos en red 104. Los datos de control se generan en base a la entrada de voz recibida de los usuarios a través de las interfaces de usuario de voz 1505. Un controlador de SDN maestro 102 está configurado para gestionar el control del flujo de datos en la red SDN. El controlador SDN maestro 102 se puede operar para generar datos de enrutamiento para los dispositivos en red 104. El controlador SDN maestro 102 genera una pluralidad de controladores agregados discretos 105 cada uno asociado con un usuario final particular. Cada controlador agregado SDN 105 incluye al menos uno de datos de control y datos de enrutamiento para un dispositivo en red asociado 104. El controlador agregado SDN 105 es enviado por el controlador SDN maestro 102 a los dispositivos en red 104 asociados con los respectivos usuarios finales para controlar el mismo. Los controladores agregados SDN 105 están instalados en los dispositivos en red

104. Los controladores agregados SDN instalados 105 se registran con el controlador SDN maestro 102 para controlar los dispositivos en red 104. De lo contrario, el funcionamiento de la plataforma SDN 1500 funciona de manera similar al controlador SDN 200. Por ejemplo, la salida de análisis como se describió anteriormente puede ser accesible a través de las interfaces de usuario de voz 1505. La una o más opciones de mejora del rendimiento como se describió anteriormente pueden estar disponibles para el usuario final a través de las interfaces de usuario de voz para selección basada en la salida de análisis. El controlador SDN maestro puede implementar la orquestación de SDN en respuesta a una solicitud de recursos recibida en las interfaces de usuario de voz.

La interfaz de usuario de voz 1505 puede configurarse para facilitar el control principal de la red doméstica, por ejemplo. La interfaz de usuario de voz 1505 se puede operar para comprender comandos de voz tales como "bloquear Youtube durante las próximas dos horas". La interfaz de usuario de voz 1505 también entendería comandos de voz tales como "priorizar todo el tráfico de un dispositivo cliente designado durante las próximas dos horas". La interfaz de usuario de voz 1505 proporciona un modo conveniente para consultar las operaciones de la red SDN. Por ejemplo, el usuario podría introducir un comando de voz en la interfaz de usuario de voz 1505 tal como "por qué mi Internet es lento". El comando de voz se convertiría en una instrucción legible por máquina que el controlador maestro 105 comprende. En respuesta al comando de voz, el controlador maestro 105 se comunica con los controladores agregados instalados 105 para identificar los dispositivos de red 104 que consumen una porción significativa de los recursos disponibles tales como el ancho de banda de Internet. El controlador maestro 102 analiza los datos recibidos de los dispositivos en red 105 a través de los controladores agregados 105 y puede determinar qué dispositivo(s) cliente 104 está(n) haciendo una copia de seguridad, por ejemplo, o está(n) transmitiendo datos de vídeo en vivo. Una vez que el dispositivo maestro 102 ha identificado el dispositivo o los dispositivos 104, el controlador maestro 102 puede informar al usuario enviando un mensaje a la interfaz de usuario de voz 1505 que se traduce en un mensaje de voz. Por ejemplo, la interfaz de usuario de voz 1505 puede emitir un mensaje de audio tal como "Bobs PC está ejecutando una copia de seguridad en iCloud".

Se apreciará que la plataforma SDN 1500 es operativa para implementar un procedimiento implementado por ordenador para controlar una red definida por software (SDN) tal como la ilustrada en el diagrama de flujo de la figura 24. El procedimiento incluye proporcionar una o más interfaces de usuario de voz 1505 que están configuradas para facilitar a los usuarios el control de dispositivos en red; bloque 1550. Los datos de control se generan en base a la entrada de voz recibida de los usuarios a través de las interfaces de usuario de voz; bloque 1555. El controlador SDN maestro 102 gestiona el control del flujo de datos en la red SDN; bloque 1560. El controlador SDN maestro 102 es operativo para generar los datos de control para los dispositivos en red; bloque 1565. Una pluralidad de controladores agregados distribuidos 105 están asociados con el controlador maestro 102; bloque 1570.

La plataforma SDN 1500 puede funcionar como controlador de red para una red definida por software (SDN). El controlador de red puede comprender uno o más módulos operativos para proporcionar una o más interfaces de usuario de voz que están configuradas para facilitar a los usuarios el control de dispositivos en red; generar datos de control basados en la entrada de voz recibida de los usuarios a través de las interfaces de usuario de voz; proporcionar un controlador SDN maestro para gestionar el control del flujo de datos en la red SDN; siendo operativo el controlador SDN maestro para generar los datos de control para los dispositivos en red; y proporcionar una pluralidad de controladores agregados distribuidos que cooperan con el controlador maestro para controlar los dispositivos en red.

Las técnicas introducidas aquí se pueden realizar como hardware de propósito especial (por ejemplo, circuitos), o como circuitos programables programados apropiadamente con software y/o firmware, o como una combinación de circuitos programables y de propósito especial. Por tanto, varias realizaciones pueden incluir un medio legible por máquina que tiene almacenadas instrucciones que pueden usarse para programar una computadora (u otros dispositivos electrónicos) para realizar un procedimiento. El medio legible por máquina puede incluir, entre otros, discos ópticos, memorias de solo lectura de disco compacto (CD-ROM) y disco magnetoóptico, ROM, memorias de solo lectura programables borrables (EPROM), memorias de solo lectura programables y borrables eléctricamente memorias (EEPROM), tarjetas magnéticas u ópticas, memoria flash, unidades de estado sólido (SSD) u otro tipo de medio/medio legible por máquina adecuado para almacenar instrucciones electrónicas.

Se entenderá que lo que se ha descrito en esta invención es un sistema ejemplar para controlar una red SDN.

Se entenderá que aunque se han descrito características ejemplares de un sistema de acuerdo con la presente enseñanza, tal disposición no debe interpretarse como una limitación de la invención a tales características. El procedimiento de la presente enseñanza puede implementarse en software, firmware, hardware o una combinación de los mismos. En un modo, el procedimiento se implementa en software, como un programa ejecutable, y es ejecutado por una o más computadoras digitales de propósito general o especial, como una computadora personal (PC; compatible con IBM, compatible con Apple u otras), asistente digital personal, estación de trabajo, miniordenador u ordenador central. Las etapas del procedimiento pueden implementarse por un servidor u ordenador en el cual los módulos de software residen o residen parcialmente.

Generalmente, en términos de arquitectura de hardware, tal computadora incluirá, como bien entenderá el experto

en la técnica, un procesador, memoria y uno o más dispositivos de entrada y / o salida (E / S) (o periféricos) que están acoplados comunicativamente a través de una interfaz local. La interfaz local puede ser, por ejemplo, pero no se limita a uno o más buses u otras conexiones cableadas o inalámbricas, como se conoce en la técnica. La interfaz local puede tener elementos adicionales, como controladores, memorias intermedias (cachés), drivers, repetidores y receptores, para permitir las comunicaciones. Además, la interfaz local puede incluir conexiones de dirección, control y/o datos para permitir comunicaciones apropiadas entre los componentes mencionados anteriormente.

Los procesadores pueden programarse para realizar las funciones del procedimiento para controlar una red SDN. El/los procesador/es es/son un dispositivo de hardware para ejecutar software, particularmente software almacenado en la memoria. Los procesadores pueden ser cualquier procesador personalizado o disponible comercialmente, una unidad de procesamiento primaria (CPU), un procesador auxiliar entre varios procesadores asociados con una computadora, un microprocesador basado en semiconductores (en forma de microchip o conjunto de chips) MACroprocesador o, en general, cualquier dispositivo para ejecutar instrucciones de software.

La memoria está asociada con los procesadores y puede incluir uno o una combinación de elementos de memoria volátiles (por ejemplo, memoria de acceso aleatorio (RAM, como DRAM, SRAM, SDRAM, etc.)) y elementos de memoria no volátil (por ejemplo, ROM, disco duro, cinta, CDROM, etc.). Además, la memoria puede incorporar medios de almacenamiento electrónicos, magnéticos, ópticos y/o de otro tipo. La memoria puede tener una arquitectura distribuida en la que varios componentes se encuentran alejados entre sí, pero los procesadores aún pueden acceder a ellos.

El software en la memoria puede incluir uno o más programas separados. Los programas separados comprenden listados ordenados de instrucciones ejecutables para implementar funciones lógicas con el fin de implementar las funciones de los módulos. En el ejemplo descrito anteriormente, el software en la memoria incluye uno o más componentes del procedimiento y es ejecutable en un sistema operativo adecuado (S/O).

La presente divulgación puede incluir componentes proporcionados como programa fuente, programa ejecutable (código objeto), secuencia de comandos o cualquier otra entidad que comprenda un conjunto de instrucciones a realizar. Cuando un programa fuente, el programa necesita ser traducido a través de un compilador, ensamblador, intérprete o similar, que puede o no estar incluido dentro de la memoria, para que funcione correctamente en conexión con el S/O. Además, una metodología implementada de acuerdo con la enseñanza puede expresarse como (a) un lenguaje de programación orientado a objetos, que tenga clases de datos y métodos, o (b) un lenguaje de programación procedimental, que tiene rutinas, subrutinas y / o funciones, por ejemplo, pero no limitado a, C, C ++, Pascal, Basic, Fortran, Cobol, Perl, Java y Ada.

Cuando el método se implementa en software, debe tenerse en cuenta que dicho software puede almacenarse en cualquier medio legible por ordenador para su uso por o en conexión con cualquier sistema o método relacionado con el ordenador. En el contexto de esta enseñanza, un medio legible por ordenador puede ser un dispositivo o medio electrónico, magnético, óptico u otro dispositivo físico o un medio que pueda contener o almacenar un programa informático para su uso por o en conexión con un sistema o procedimiento relacionado con el ordenador. Tal disposición se puede realizar en cualquier medio legible por ordenador para su uso por o en conexión con un sistema de ejecución de instrucciones, aparato o dispositivo, como un sistema basado en ordenador, sistema que contiene un procesador u otro sistema que pueda obtener las instrucciones del sistema, aparato o dispositivo de ejecución de instrucciones y ejecutar las instrucciones. En el contexto de este documento, un «medio legible por ordenador» puede ser cualquier medio que pueda almacenar, comunicar, propagar o transportar el programa para su uso por o en conexión con el sistema, aparato o dispositivo de ejecución de instrucciones. El medio legible por ordenador puede ser, por ejemplo, pero no limitado a un sistema, aparato, dispositivo o medio de propagación electrónico, magnético, óptico, electromagnético, infrarrojo o semiconductor. Cualquier descripción de procedimiento o bloque en las Figuras, debe entenderse como la representación de módulos, segmentos o porciones de código que incluyen una o más instrucciones ejecutables para implementar funciones lógicas específicas o etapas en el proceso, como lo entenderían aquellos expertos en la técnica.

La descripción detallada anterior de las realizaciones de la divulgación no pretende ser exhaustiva ni limitar la divulgación a la forma exacta divulgada. Aunque los ejemplos específicos de la divulgación se describen anteriormente con fines ilustrativos, los expertos en la técnica relevante reconocerán que son posibles varias modificaciones dentro del alcance de la divulgación. Por ejemplo, si bien los procesos y bloques se han demostrado en un orden particular, diferentes implementaciones pueden realizar rutinas o emplear sistemas que tienen bloques, en un orden alternativo, y algunos procesos o bloques se pueden eliminar, complementar, agregar, mover, separar, combinar, y/o modificar para proporcionar diferentes combinaciones o subcombinaciones. Cada uno de estos procedimientos o bloques puede implementarse de diversas formas alternativas. Además, mientras que los procedimientos o bloques a veces se muestran como ejecutados en secuencia, estos procedimientos o bloques pueden en cambio ser realizados o implementados en paralelo o pueden realizarse en diferentes momentos. Los resultados de procedimientos o bloques también pueden guardarse en un almacén no persistente como un procedimiento para aumentar el rendimiento y reducir los requisitos de procesamiento.

En general, los términos utilizados en las siguientes reivindicaciones no deben interpretarse para limitar la

divulgación a los ejemplos específicos divulgados en la especificación, a menos que la descripción detallada anterior defina explícitamente dichos términos.

REIVINDICACIONES

1. Un procedimiento implementado por ordenador para controlar una red definida por software, SDN,
5 (103); el procedimiento comprende:

proporcionar una o más interfaces de usuario de voz que están configuradas para facilitar a los usuarios el control de dispositivos en red (104);
generar datos de control basados en la entrada de voz recibida de los usuarios a través de las interfaces de usuario
10 de voz;
proporcionar un controlador SDN maestro (102) para gestionar el control del flujo de datos en la red SDN (103);
siendo operable el controlador SDN maestro (102) para generar datos de control para los dispositivos en red (104);
generar mediante el controlador SDN maestro (102) una pluralidad de controladores agregados discretos (105) cada uno asociado con un usuario final particular; cada controlador agregado SDN (105) incluye al menos un dato de
15 control y datos de enrutamiento para un dispositivo asociado en red (104);
enviar el controlador agregado SDN (105) por el controlador maestro SDN (102) a los dispositivos en red (104) asociados con los respectivos usuarios finales para controlarlos;
instalar los controladores agregados SDN (105) en los dispositivos en red (104); y
registrar los controladores agregados SDN instalados (105) con el controlador SDN maestro (102) para controlar los
20 dispositivos en red (104).
2. Un procedimiento de la reivindicación 1, que comprende además la extracción de datos analíticos por los controladores agregados SDN instalados de los dispositivos en red (104); y/o que comprende además el enrutamiento de los datos analíticos extraídos a un depósito principal.
25
3. Un procedimiento de la reivindicación 2, donde los datos analíticos extraídos son enrutados por los controladores agregados SDN (105) al depósito principal a través del controlador SDN maestro (102); y/o que comprende además el suministro de un motor de análisis en comunicación con el depósito principal que es operable para analizar los análisis extraídos para generar una salida de análisis.
30
4. Un procedimiento de la reivindicación 3; donde la salida de análisis es accesible a través de las interfaces de usuario de voz; y
donde una o más opciones de mejora del rendimiento se ponen a disposición del usuario final a través de las interfaces de usuario de voz para la selección basada en la salida de análisis.
35
5. Un procedimiento de la reivindicación 4; donde los datos de configuración se actualizan en respuesta a que el usuario final seleccione una o más opciones de mejora del rendimiento; y/o que comprende además la actualización del controlador agregado SDN instalado (105) con datos de configuración para modificar la configuración operativa de los dispositivos en red (104).
40
6. Un procedimiento de la reivindicación 5, donde la configuración operativa de los dispositivos en red (104) se modifica para aumentar un parámetro de calidad de servicio; y/o
donde los ajustes operativos de los dispositivos en red (104) se actualizan en tiempo real mientras están en línea; y/o
45 donde la configuración operativa de los dispositivos en red (104) se actualiza mientras está en modo de suspensión; y/o
donde la configuración operativa de los dispositivos en red (104) se actualiza cambiando a un canal de comunicación alternativo para evitar la intercomunicación de dispositivos vecinos.
7. Un procedimiento de la reivindicación 6, donde el canal de comunicación incluye un canal WIFI; y/o donde la configuración operativa del dispositivo en red (104) se cambia para reducir el consumo de energía.
50
8. Un procedimiento de la reivindicación 7, donde la configuración operativa del dispositivo en red (104) se cambia reprogramando una interfaz de energía; y/o
55 donde la configuración operativa del dispositivo en red (104) se cambia para aumentar la prioridad al ancho de banda disponible; y/o
donde la configuración operativa del dispositivo en red (104) se cambia para disminuir la prioridad al ancho de banda disponible.
9. Un procedimiento de cualquiera de las reivindicaciones 1 a 8, donde los controladores agregados SDN (105) pueden funcionar para asignar un primer ajuste de prioridad a un primer conjunto de dispositivos de red (104) y asignar un segundo ajuste de prioridad a un segundo conjunto de dispositivos de red (104);
donde el primer ajuste de prioridad está asociado con un primer límite de ancho de banda y el segundo ajuste de prioridad está asociado con un segundo límite de ancho de banda; y/o
60 donde el controlador SDN maestro (102) implementa la orquestación de SDN en respuesta a una solicitud de recursos recibida en las interfaces de usuario de voz.

10. Un procedimiento de la reivindicación 9, donde la orquestación de SDN incluye la coordinación de los elementos de hardware y software de red necesarios para soportar aplicaciones asociadas con la solicitud de recursos;
- 5 donde la orquestación de SDN incluye generar una instancia de una o más aplicaciones en la nube; y/o donde la orquestación de SDN genera una instancia de virtualización de funciones de red (NFV).
11. Un procedimiento según cualquiera de las reivindicaciones 1 a 10; que comprende además generar un perfil de usuario para cada usuario final; y/o
- 10 que comprende además la autenticación de un usuario.
12. Un procedimiento de cualquiera de las reivindicaciones 1 a 11; donde los controladores agregados SDN (105) están instalados en un sistema en chip (SOC) de los respectivos dispositivos en red (104); y/o donde los controladores agregados SDN (105) se cargan en el firmware contenido en los respectivos dispositivos en red (104); y/o
- 15 donde los controladores agregados SDN (105) son desplegables binariamente; y/o donde el controlador SDN maestro (102) genera un archivo de configuración para cada recurso seleccionado por el usuario final en las interfaces de usuario de voz.
- 20 13. Un procedimiento de una cualquiera de las reivindicaciones 1 a 12, que comprende además enviar los controladores agregados SDN (105) a una red doméstica para la recopilación de información relacionada con el protocolo de transporte.
14. Un controlador de red para una red definida por software, SDN, (103), el controlador de red que
- 25 comprende uno o más módulos que pueden funcionar para:
- proporcionar una o más interfaces de usuario de voz que están configuradas para facilitar a los usuarios el control de dispositivos en red (104);
- generar datos de control basados en la entrada de voz recibida de los usuarios a través de los portales del cliente;
- 30 proporcionar un controlador SDN maestro (102) para gestionar el control del flujo de datos en la red SDN (103); siendo operable el controlador SDN maestro (102) para generar datos de control para los dispositivos en red (104); generar mediante el controlador SDN maestro (102) una pluralidad de controladores agregados distribuidos discretos (105) cada uno asociado con un usuario final particular; cada controlador agregado SDN (105) incluye al menos datos de control y datos de enrutamiento para un dispositivo asociado en red (104);
- 35 enviar los controladores agregados SDN (105) por el controlador maestro SDN (102) a los dispositivos en red (104) asociados con los respectivos usuarios finales para controlarlos;
- instalar los controladores agregados SDN (105) en los dispositivos en red (104); y registrar los controladores agregados SDN instalados (105) con el controlador SDN maestro (102) para controlar los dispositivos en red (104).
- 40 15. Un artículo de fabricación que comprende un medio legible por procesador que tiene incorporado un código de programa ejecutable que, cuando es ejecutado por el dispositivo de procesamiento, hace que el dispositivo de procesamiento realice las siguientes acciones:
- 45 proporcionar una o más interfaces de usuario de voz que están configuradas para facilitar a los usuarios el control de dispositivos en red (104);
- generar datos de control basados en la entrada de voz recibida de los usuarios a través de los portales de clientes;
- proporcionar un controlador SDN maestro (102) para gestionar el control del flujo de datos en la red SDN (103); siendo operable el controlador SDN maestro (102) para generar datos de control para los dispositivos en red (104);
- 50 generar mediante el controlador SDN maestro (102) una pluralidad de controladores agregados discretos (105) cada uno asociado con un usuario final particular; cada controlador agregado SDN (105) incluye al menos datos de control y datos de enrutamiento para un dispositivo asociado en red (104);
- enviar el controlador agregado SDN (105) por el controlador maestro SDN (102) a los dispositivos en red (104) asociados con los respectivos usuarios finales para controlarlos;
- 55 instalar los controladores agregados SDN (105) en los dispositivos en red (104); y registrar los controladores agregados SDN instalados (105) con el controlador SDN maestro (102) para controlar los dispositivos en red (104).

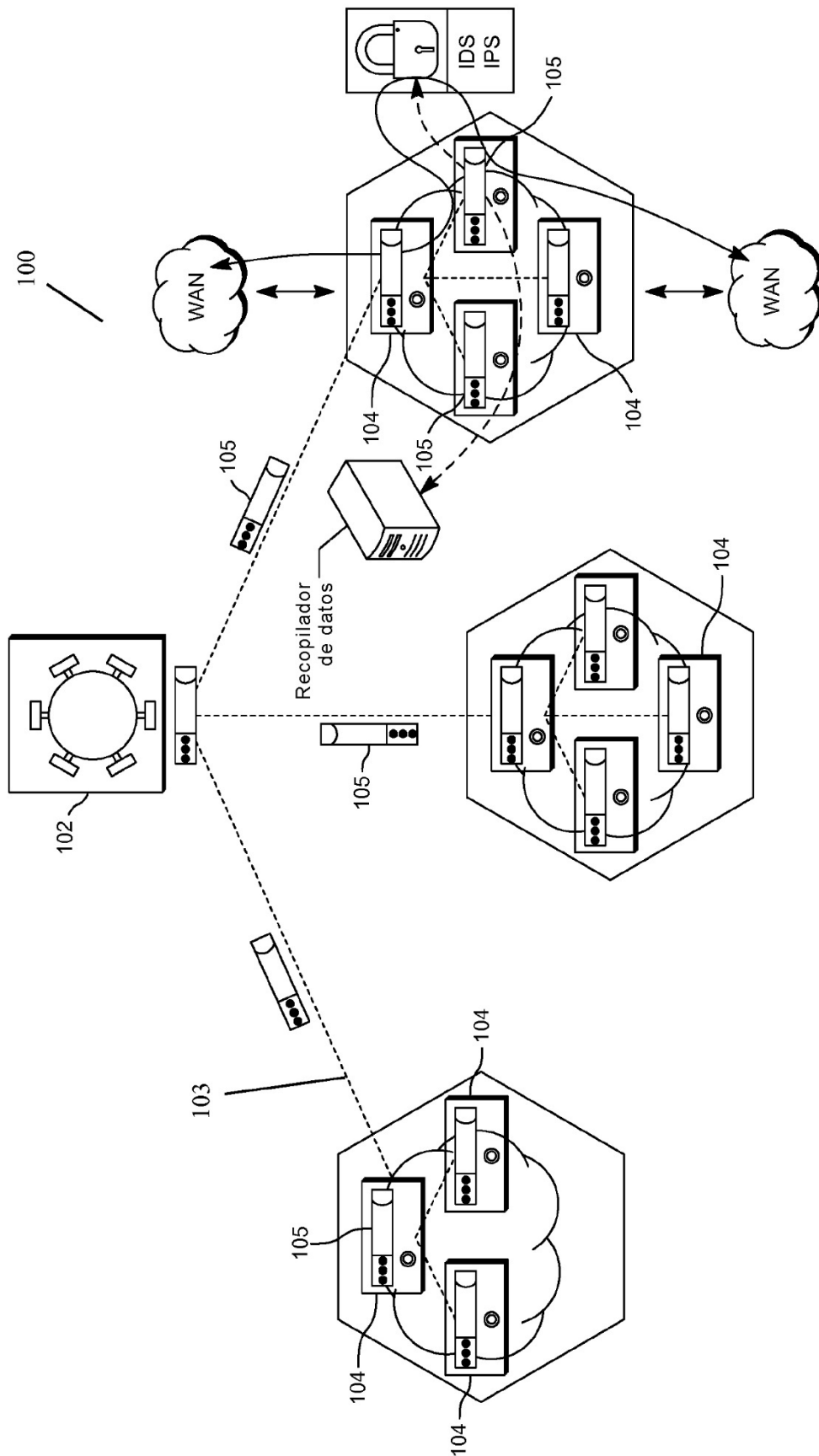


FIG. 1

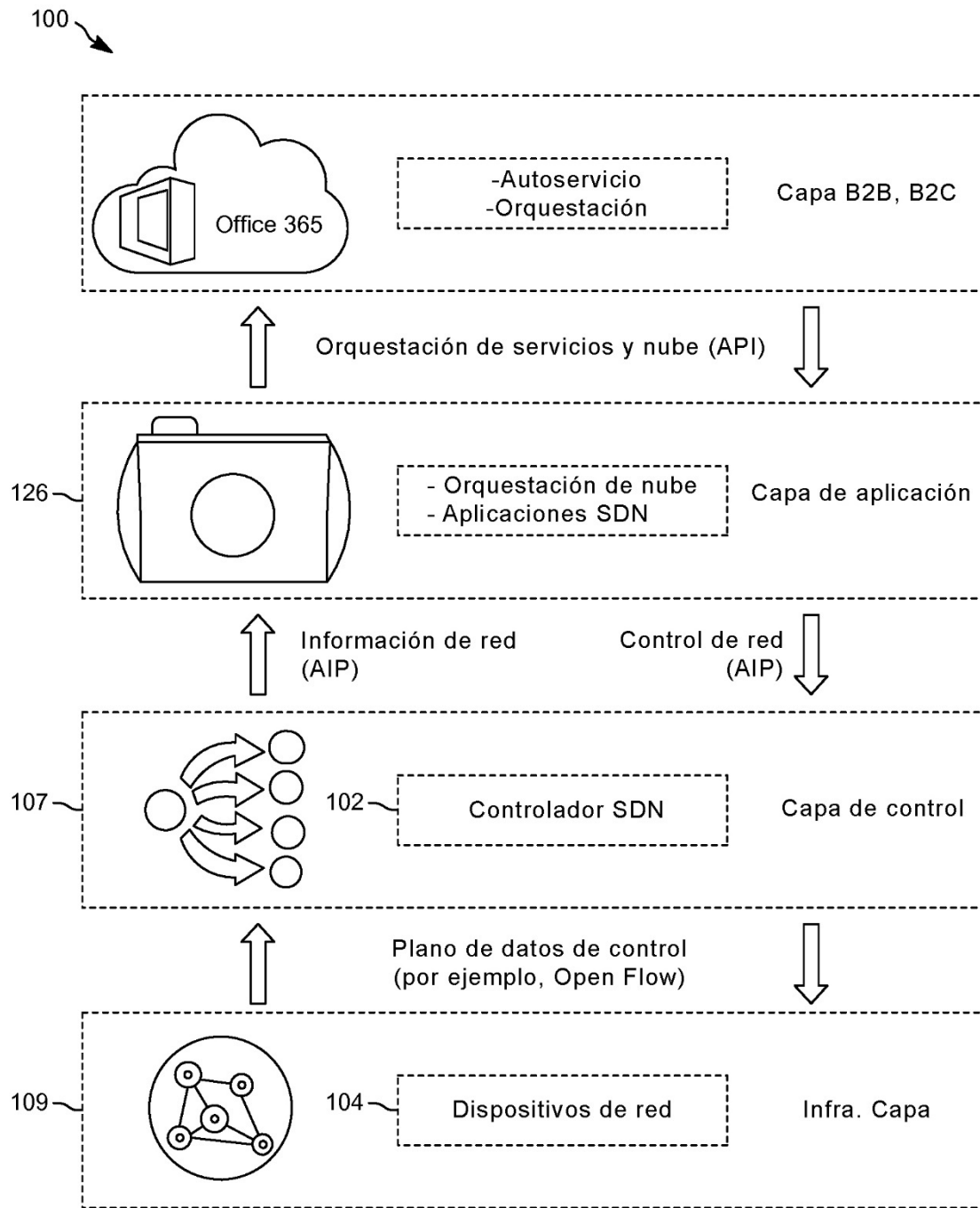


FIG. 2

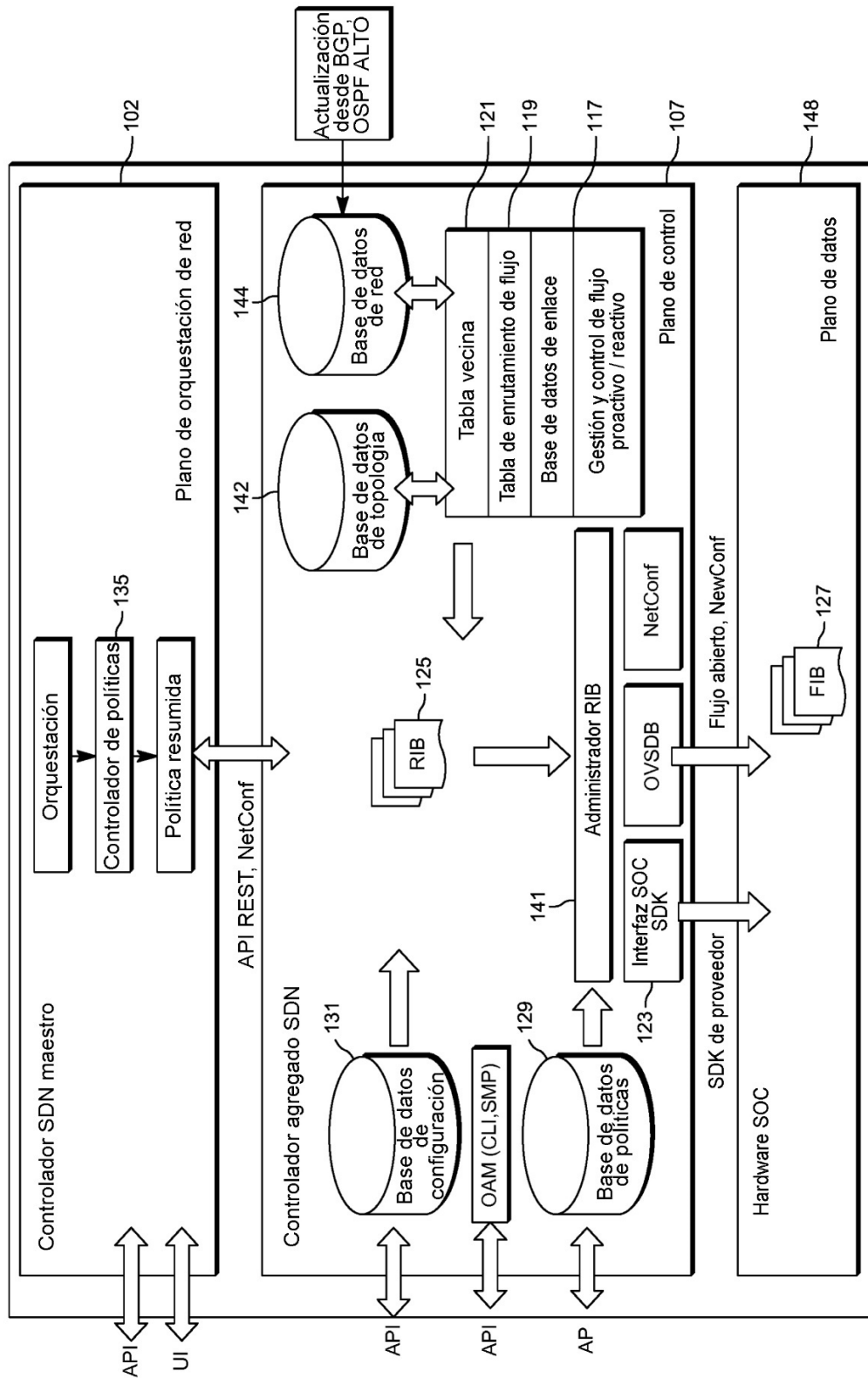


FIG. 3

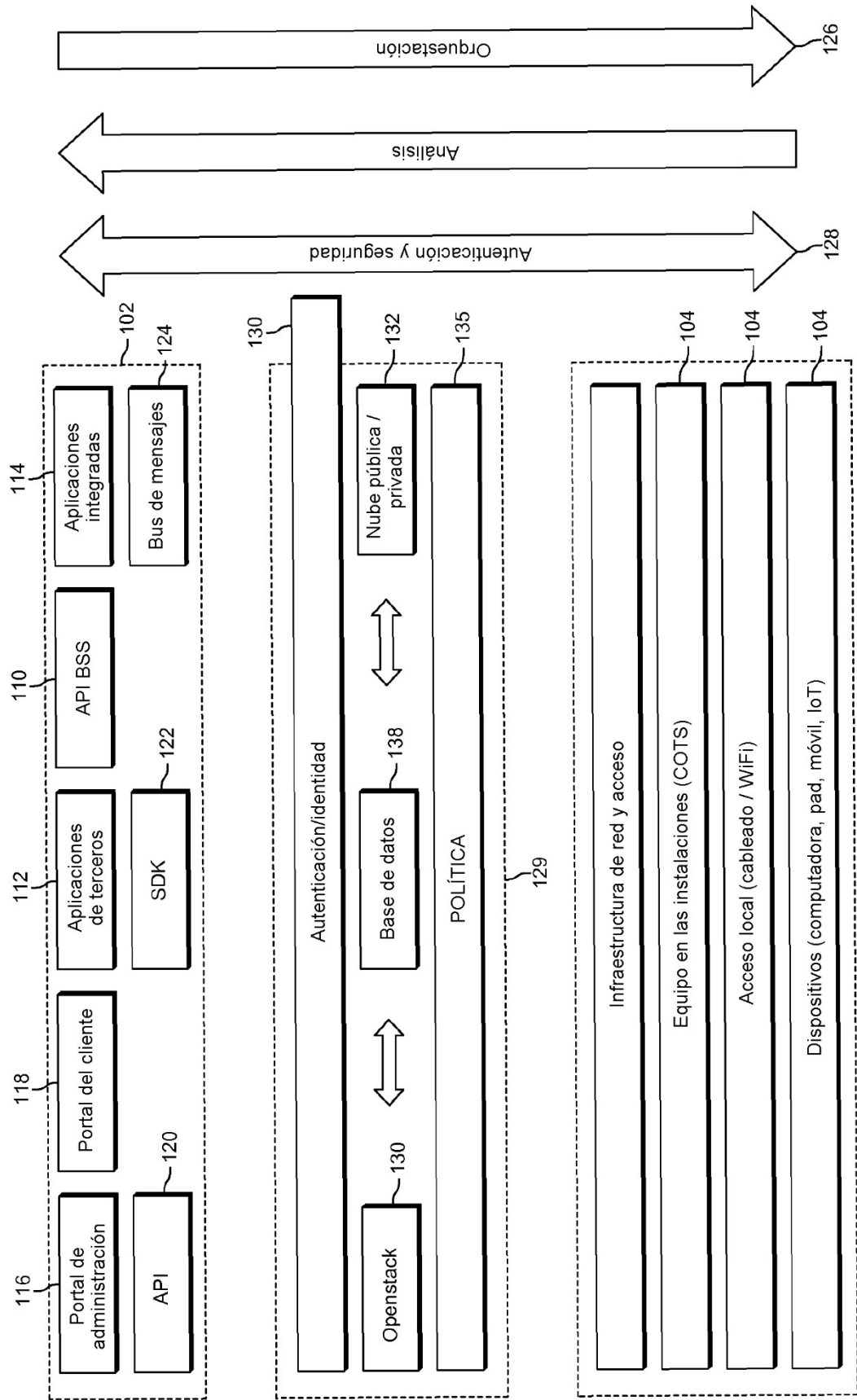


FIG. 4

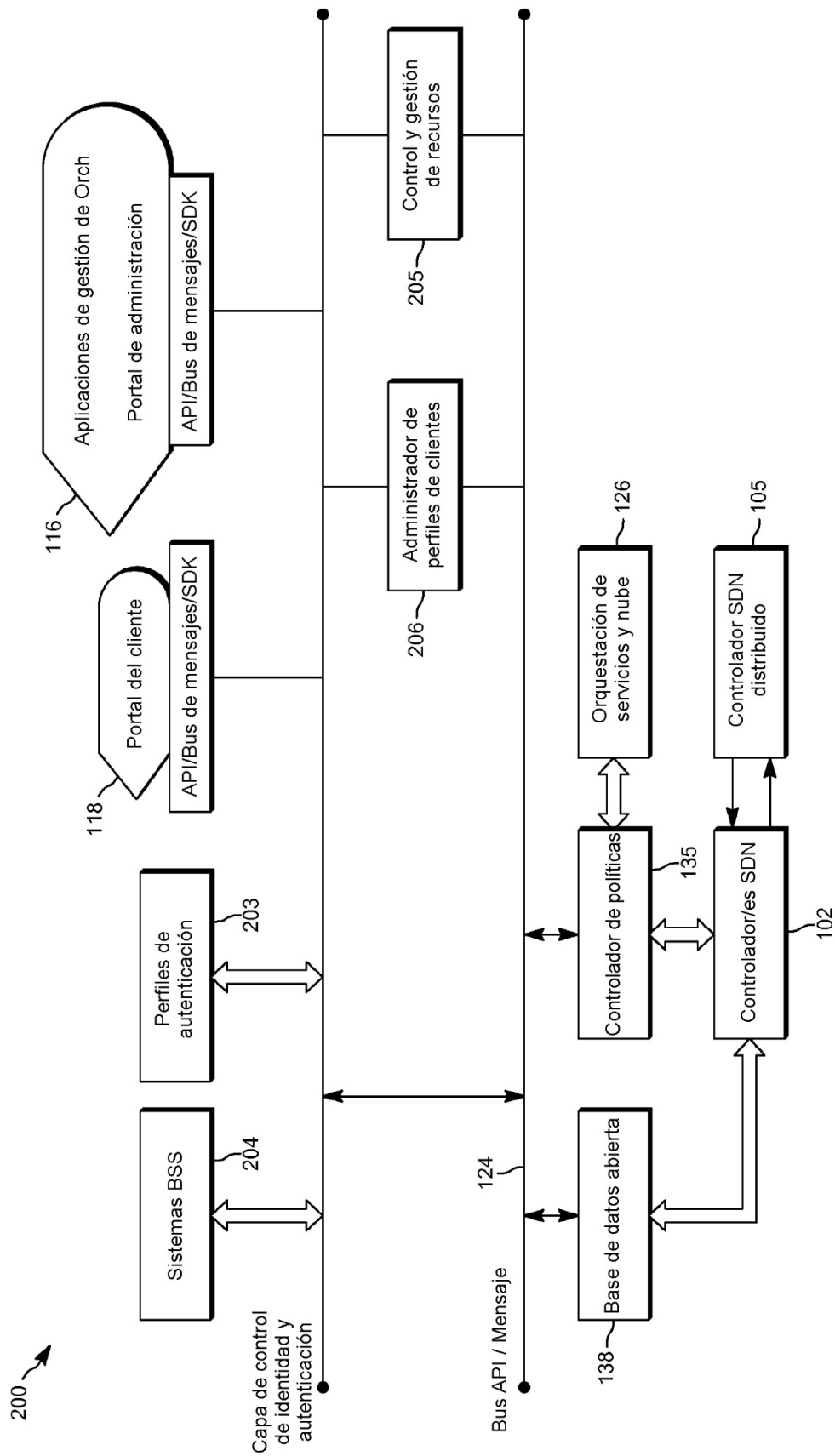


FIG. 5

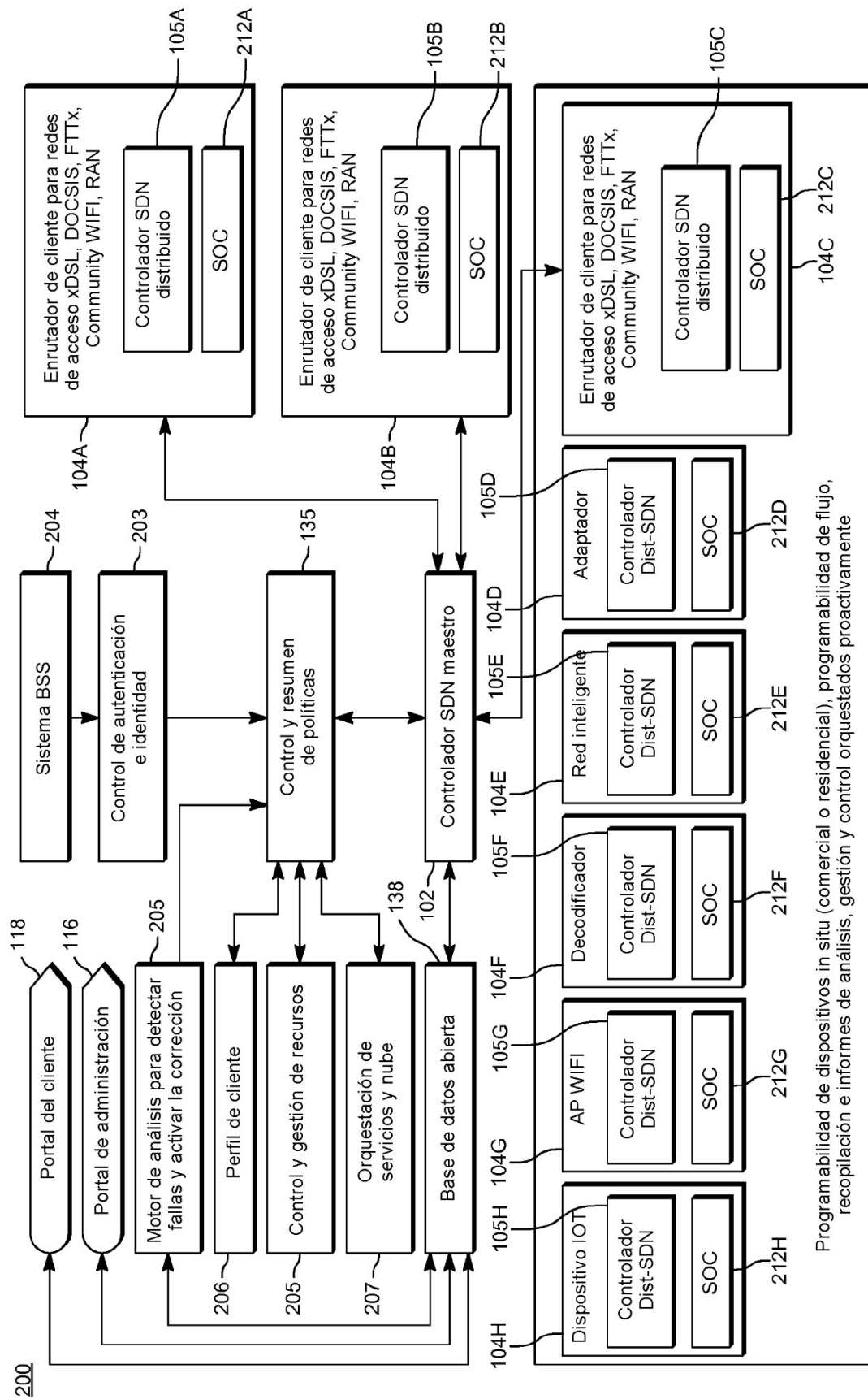


FIG. 6

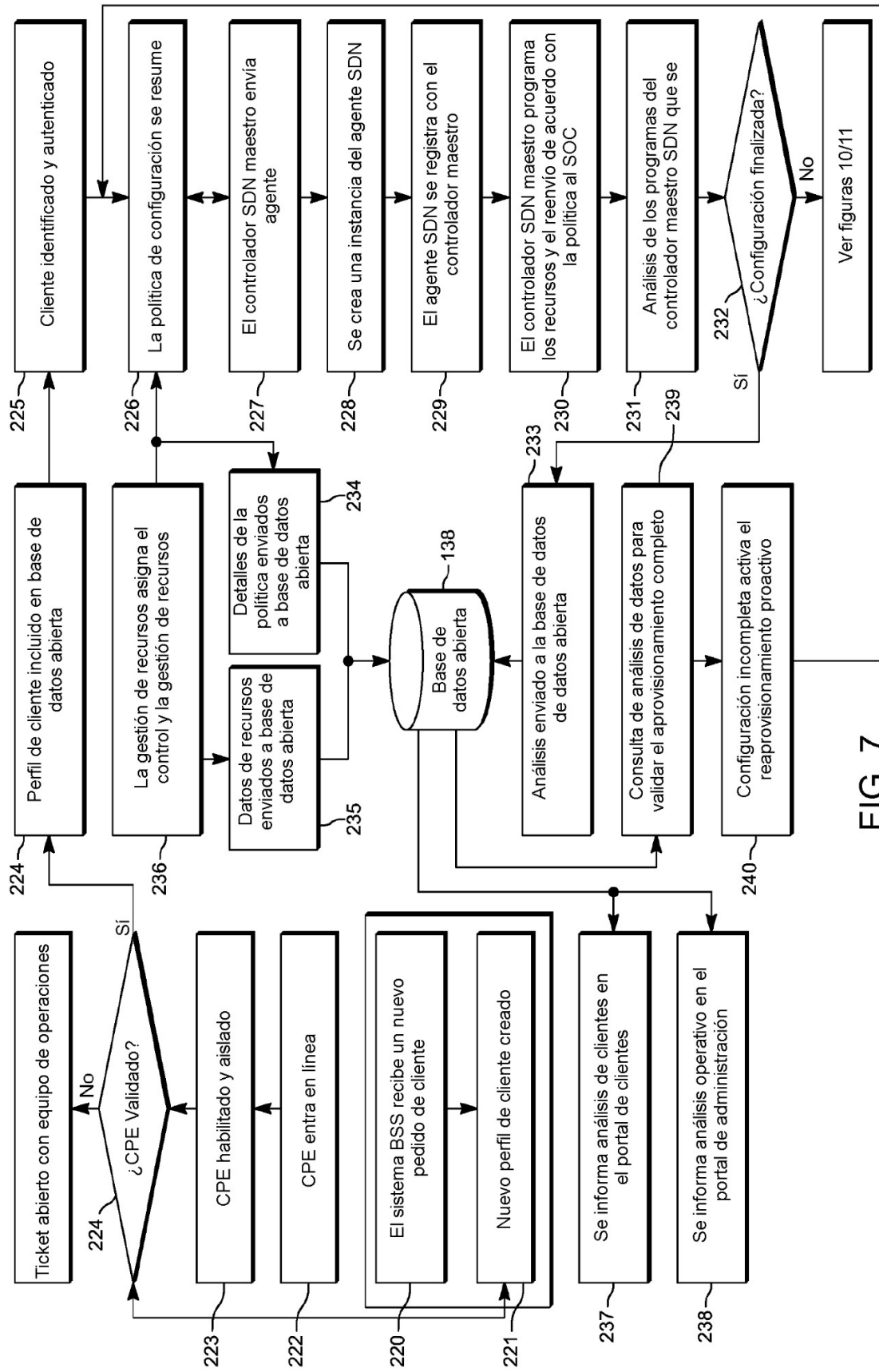


FIG. 7

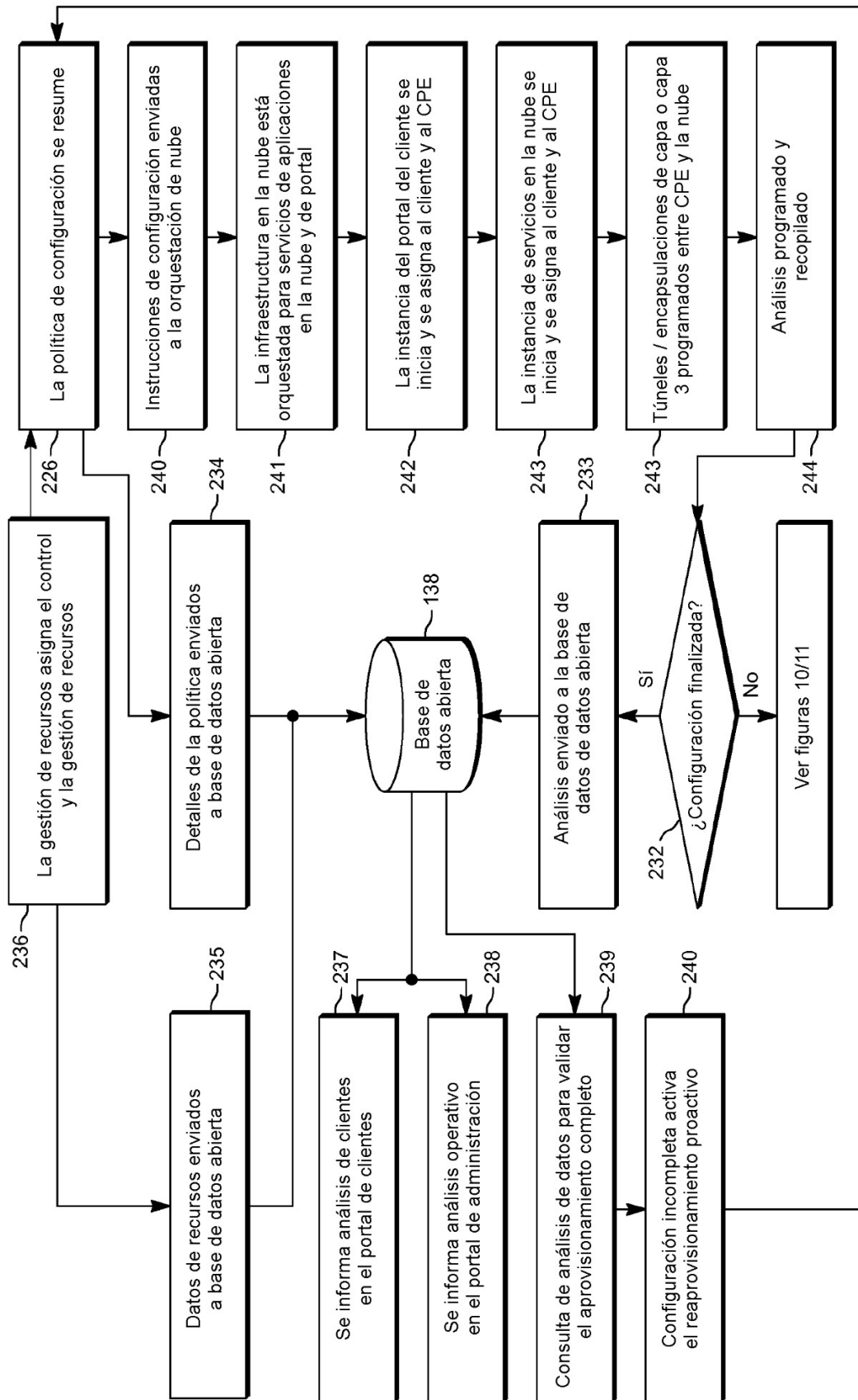


FIG. 8

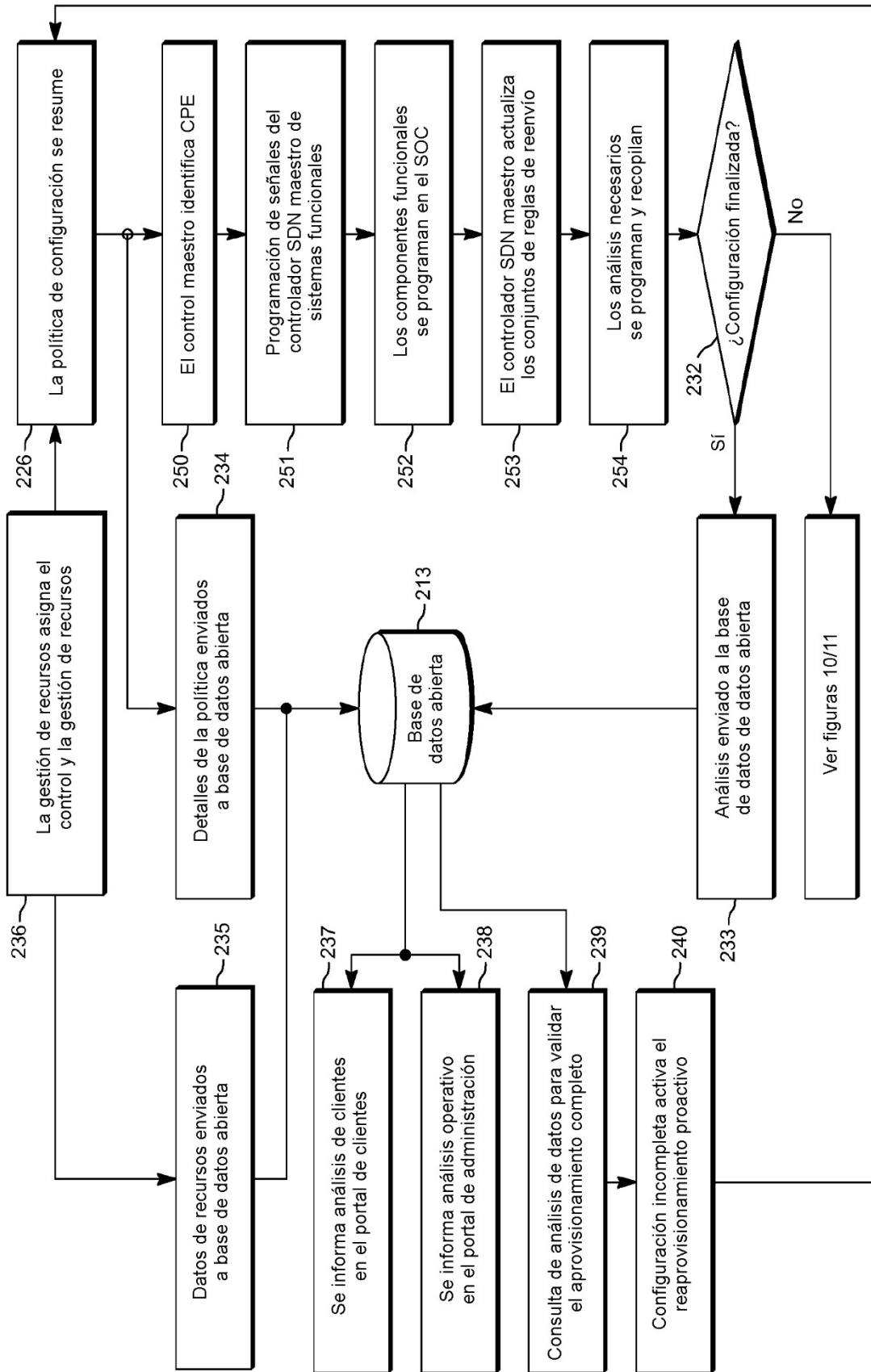


FIG. 9

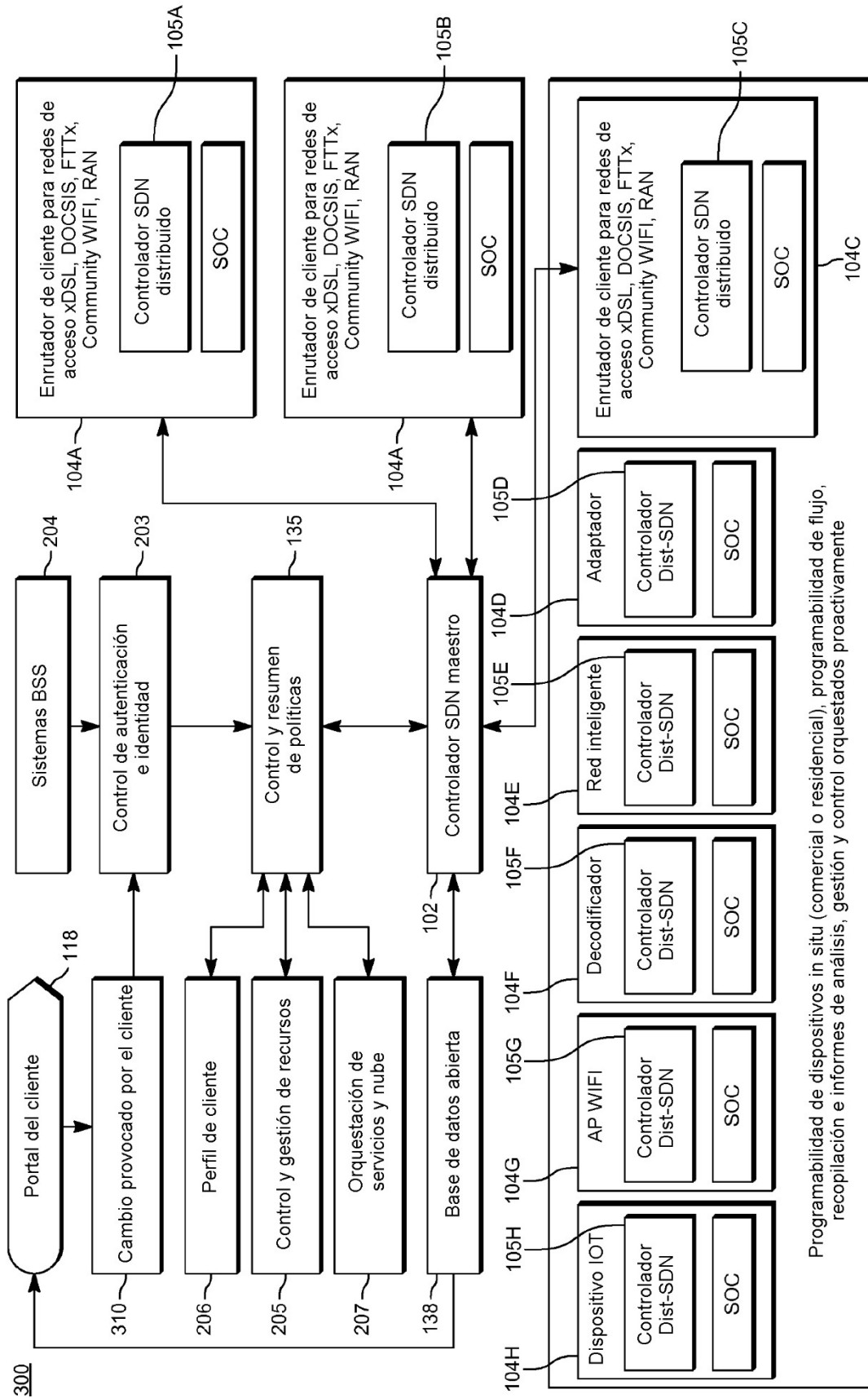


FIG. 10

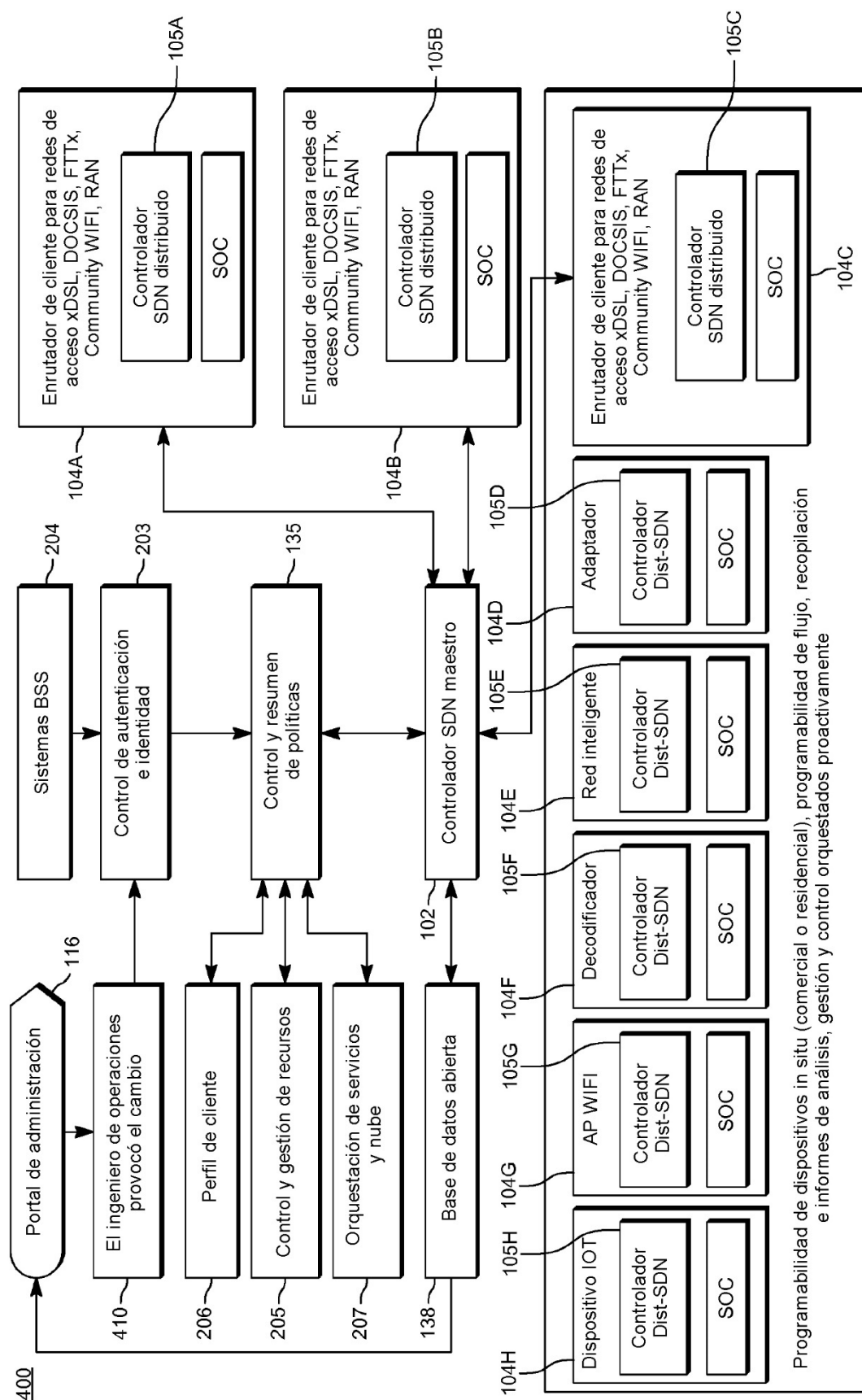


FIG. 11

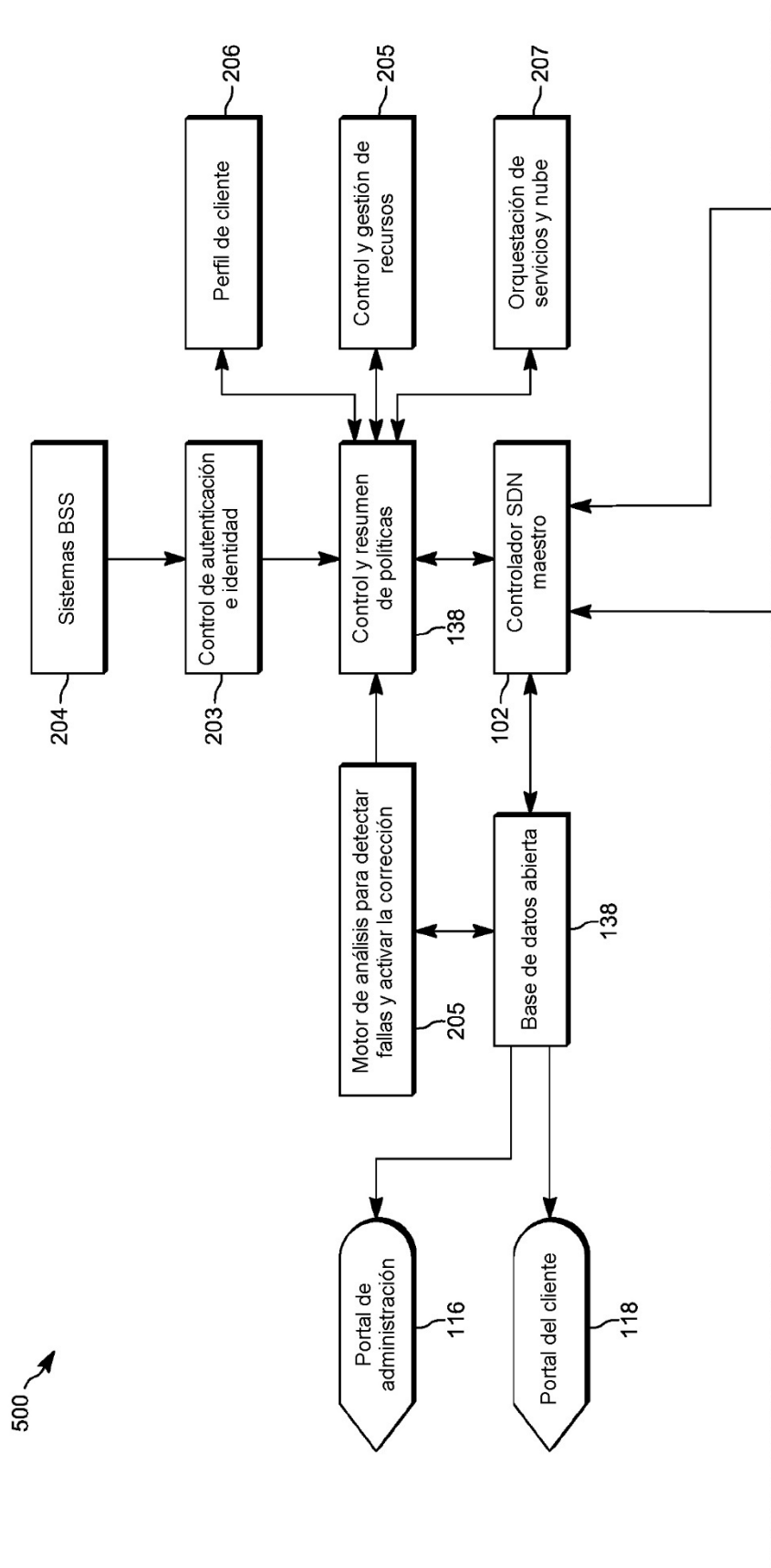


FIG. 12A

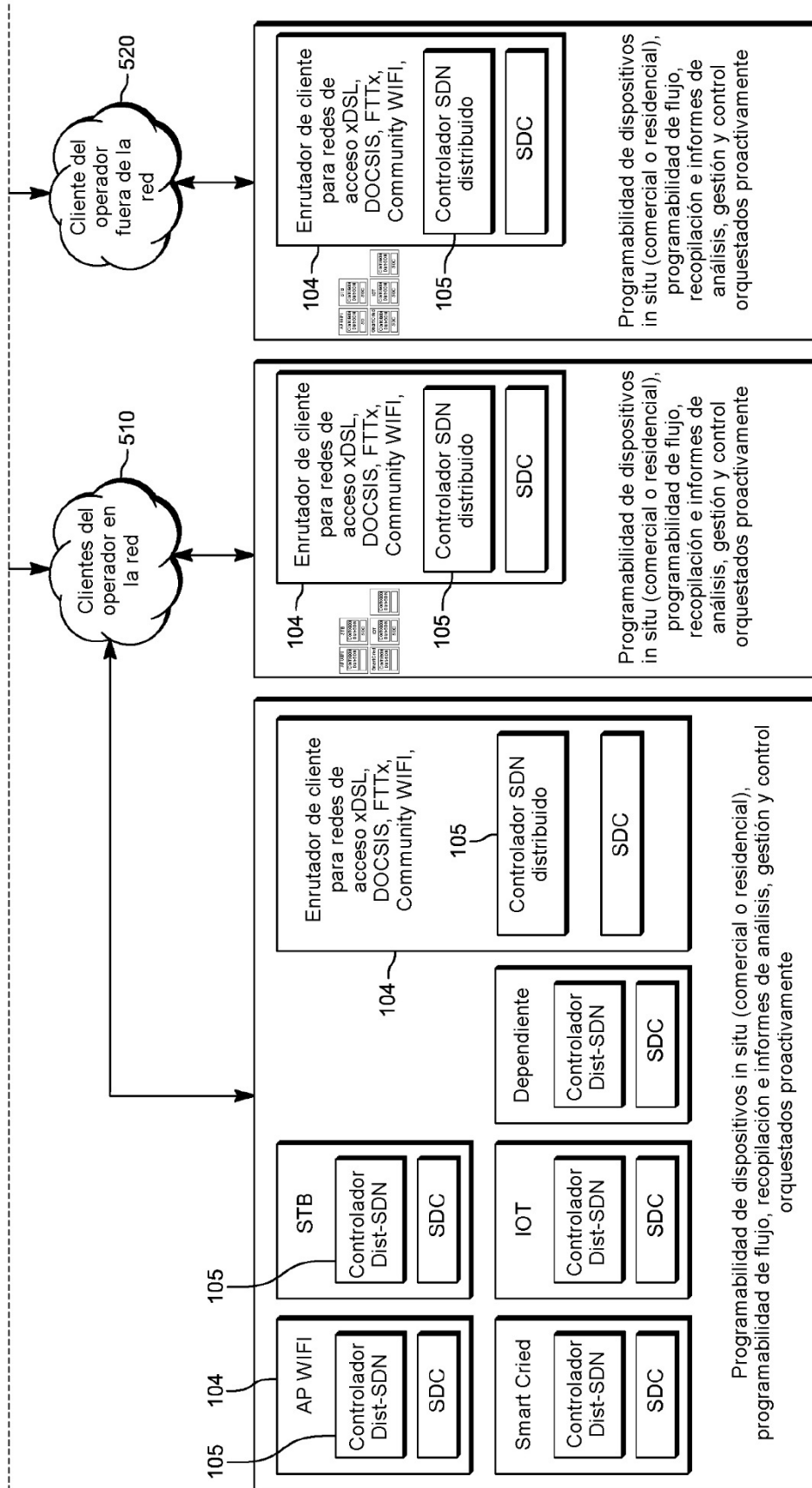


FIG. 12B

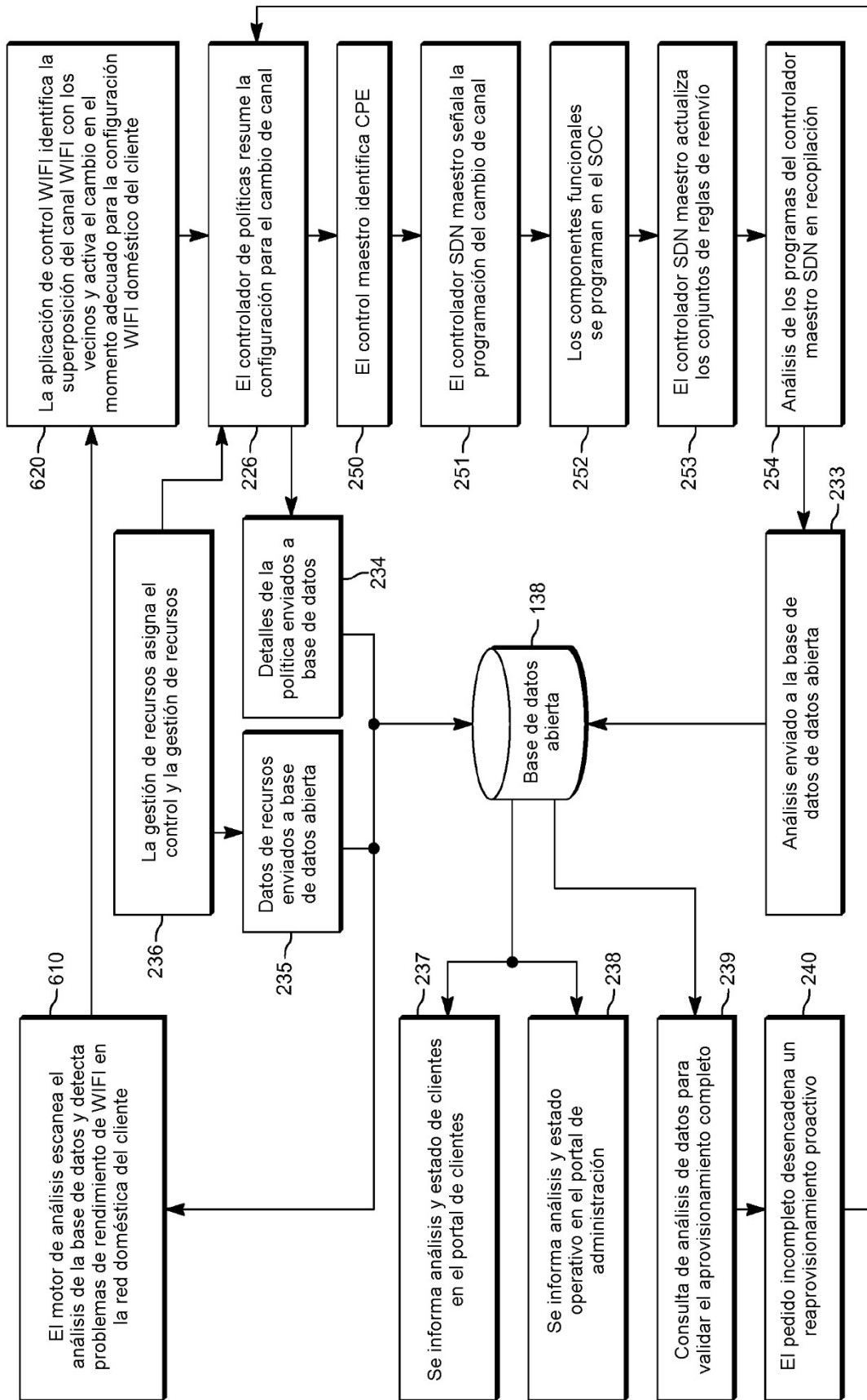


FIG. 13

600

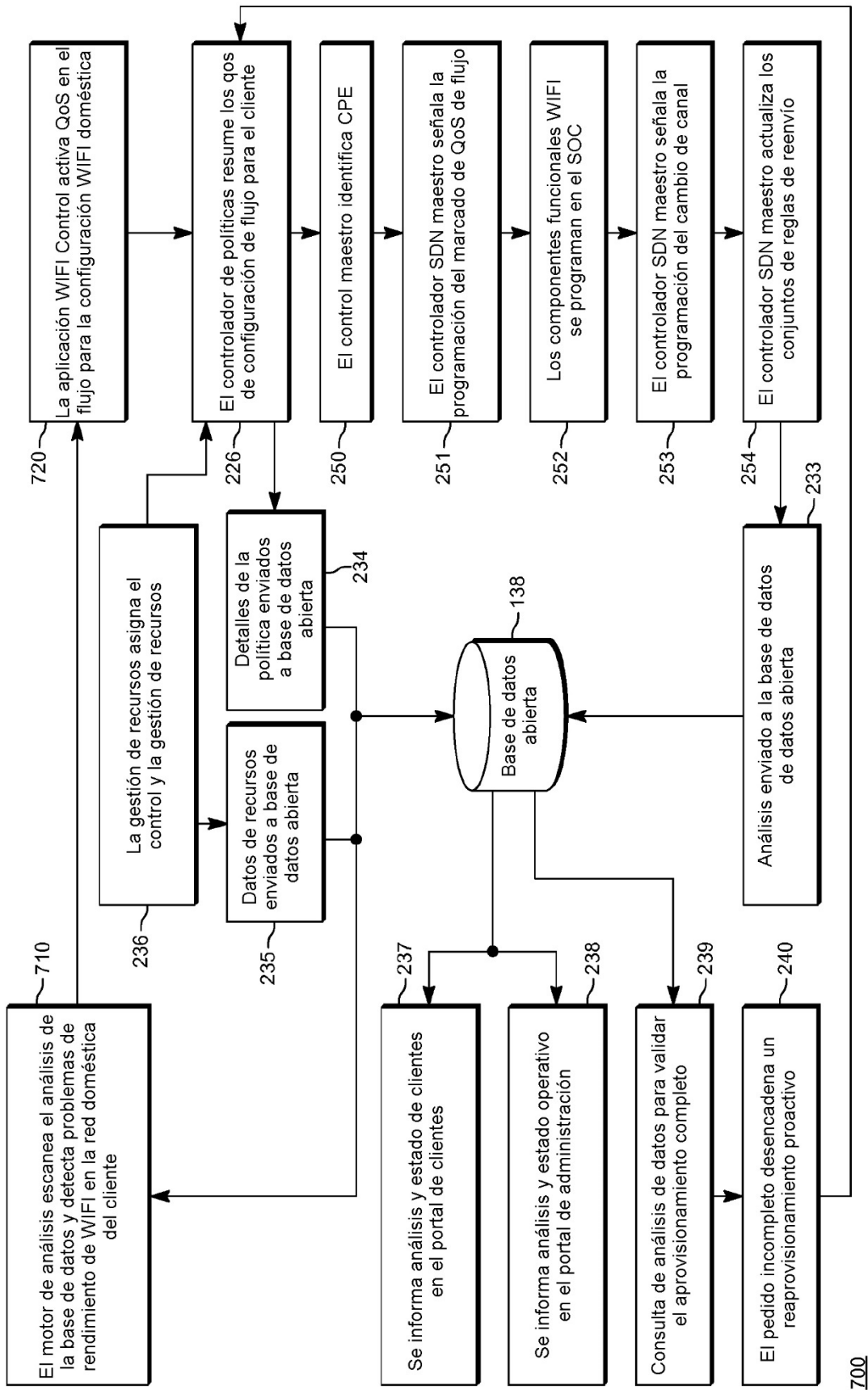


FIG. 14

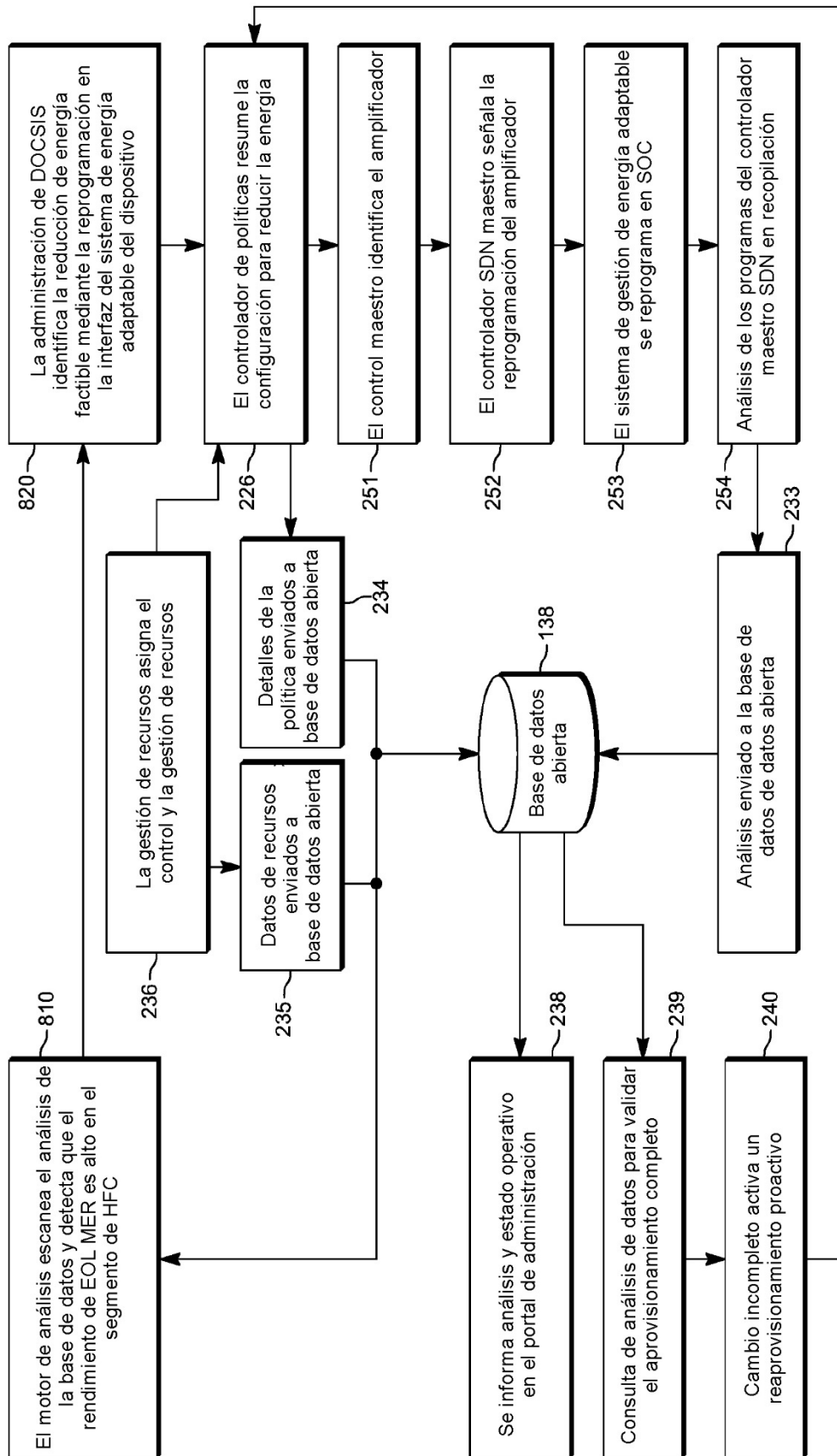


FIG. 15

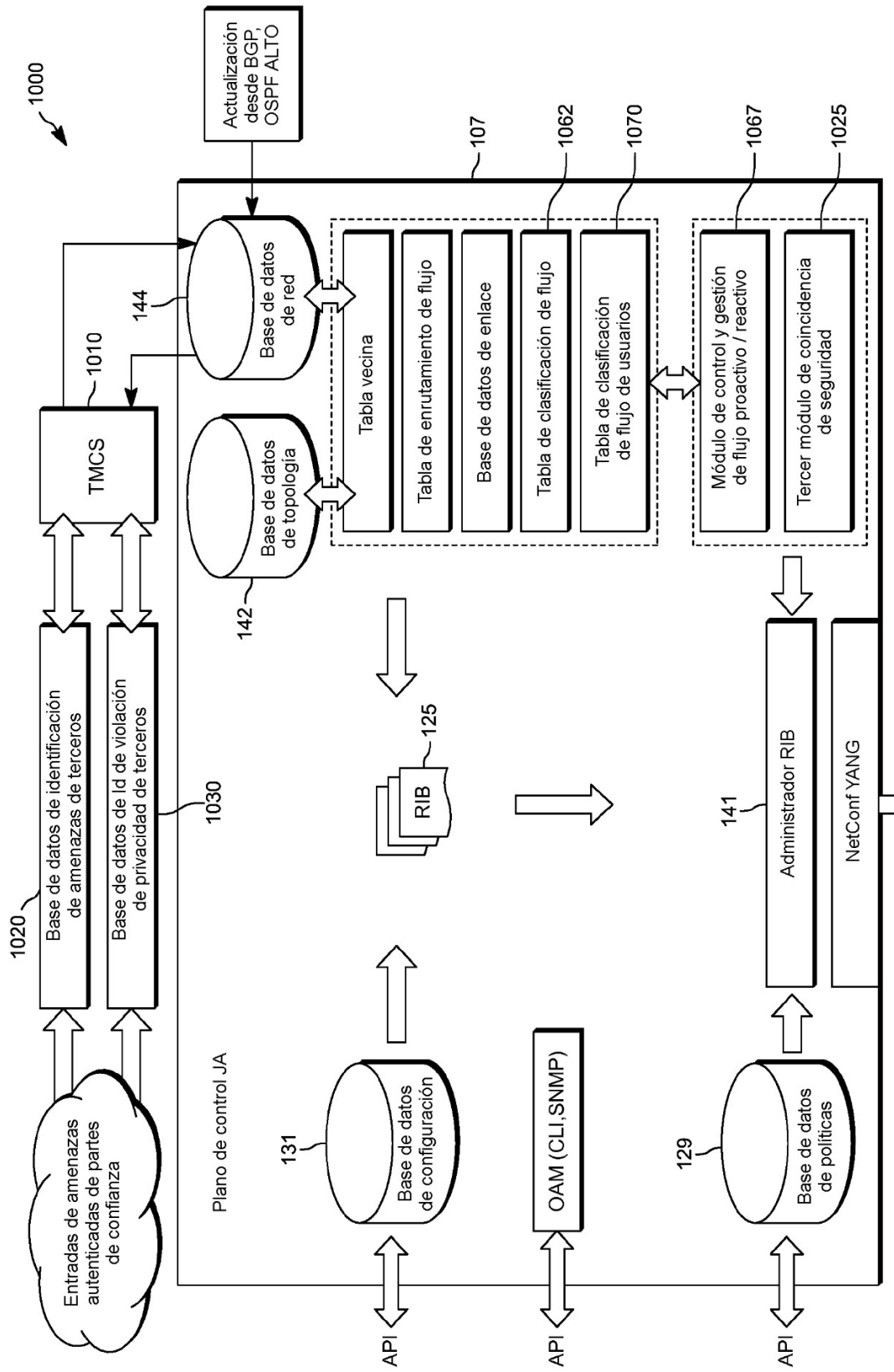


FIG. 16A

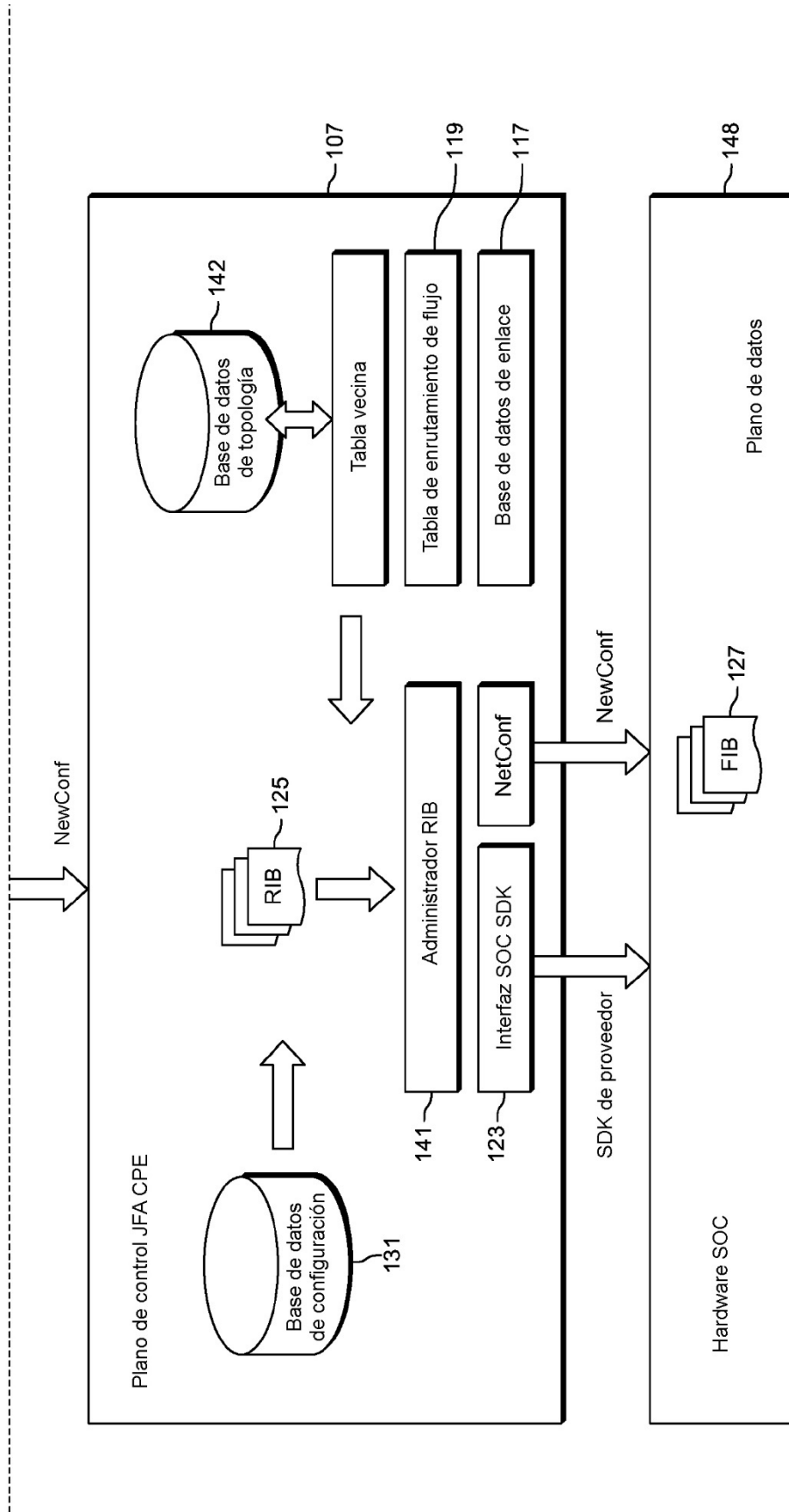


FIG. 16B

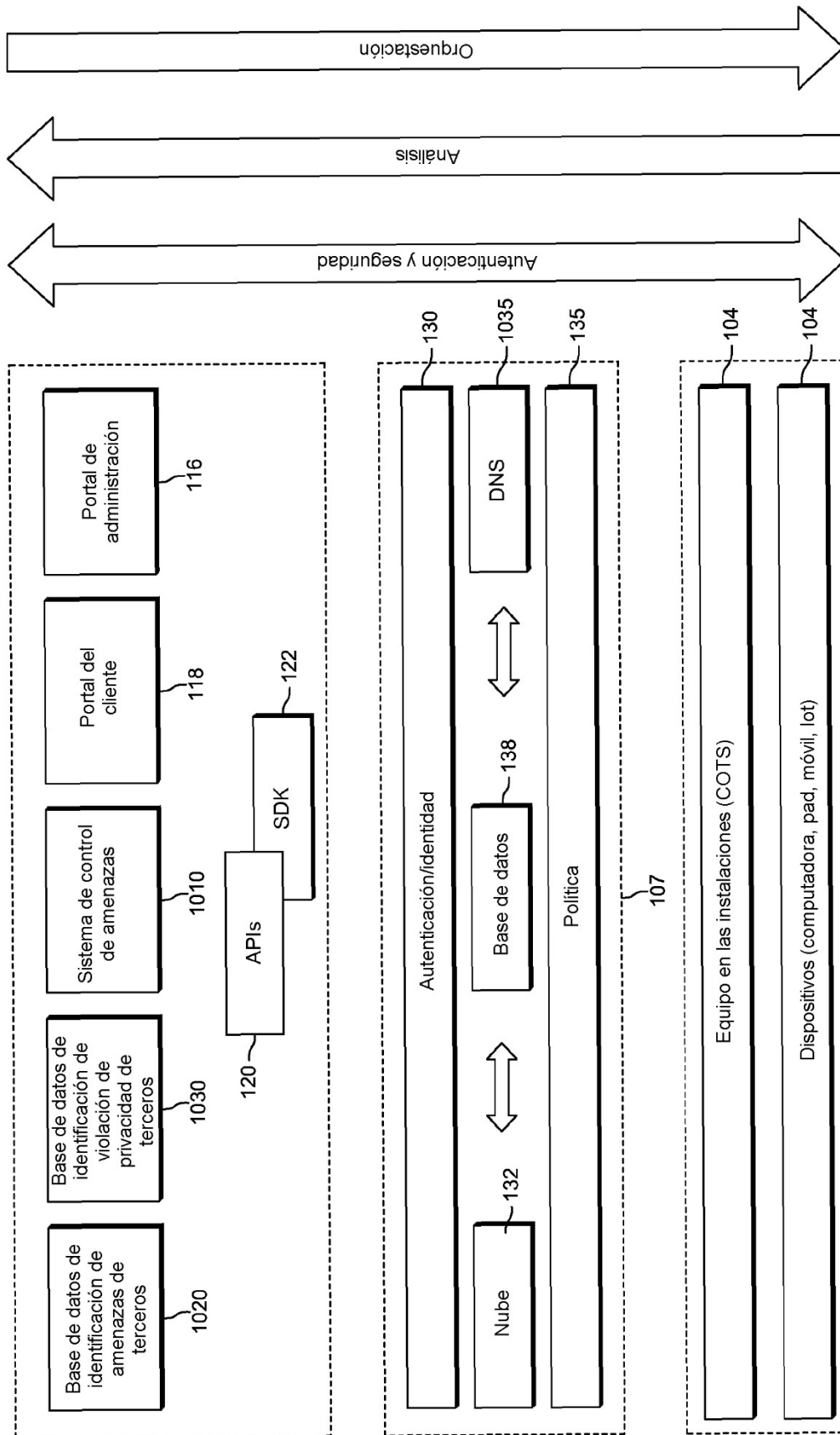


FIG. 17

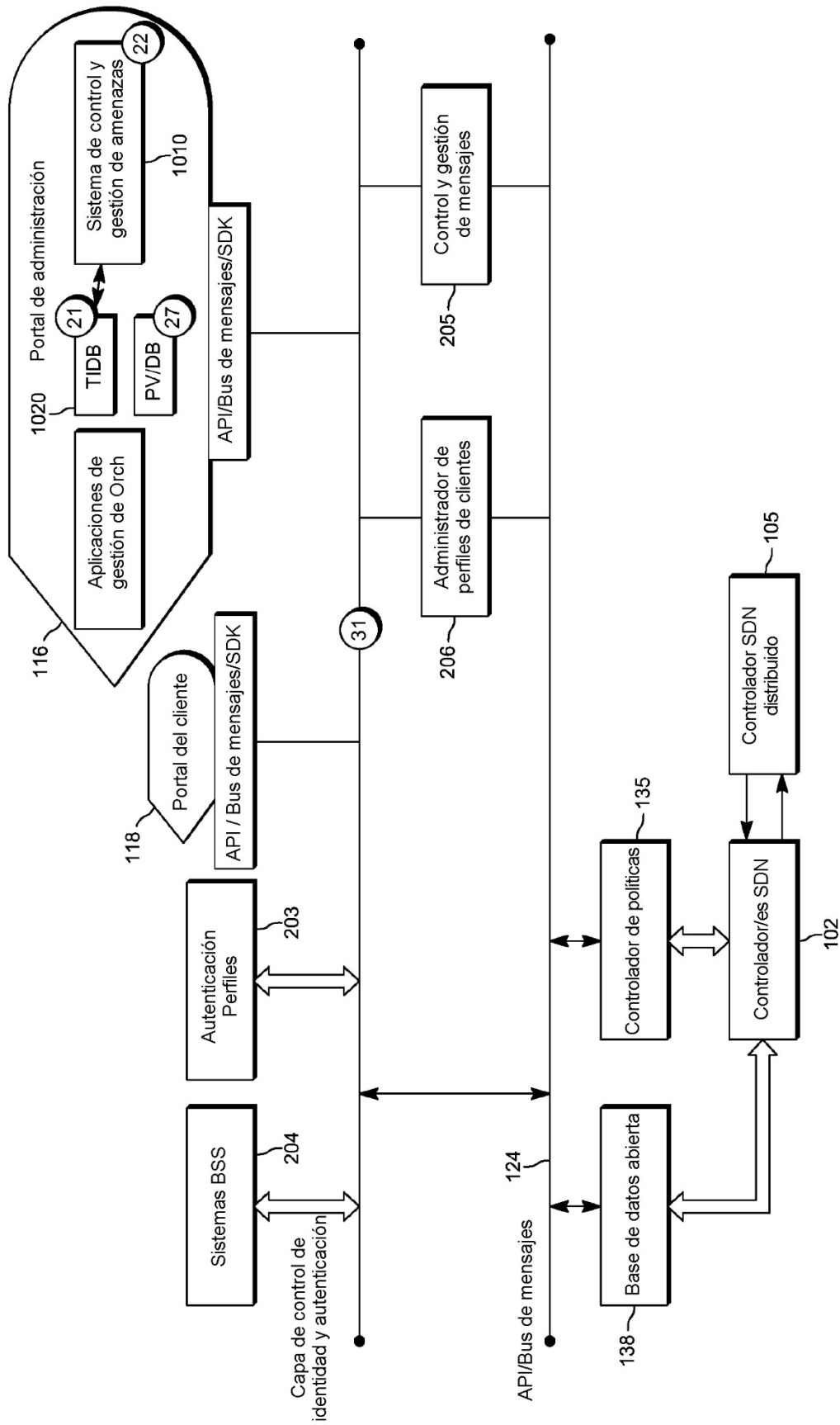


FIG. 18

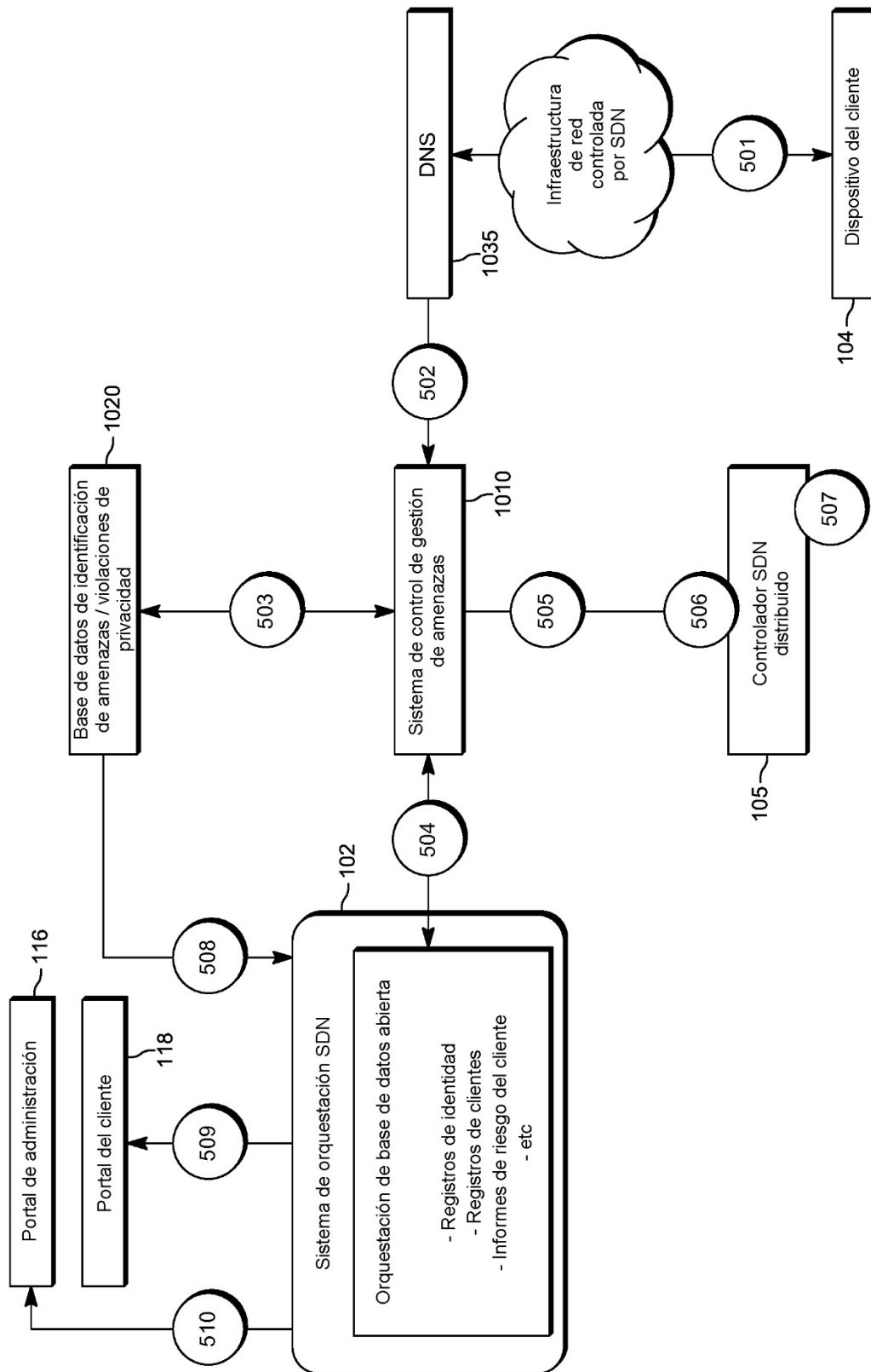


FIG. 19

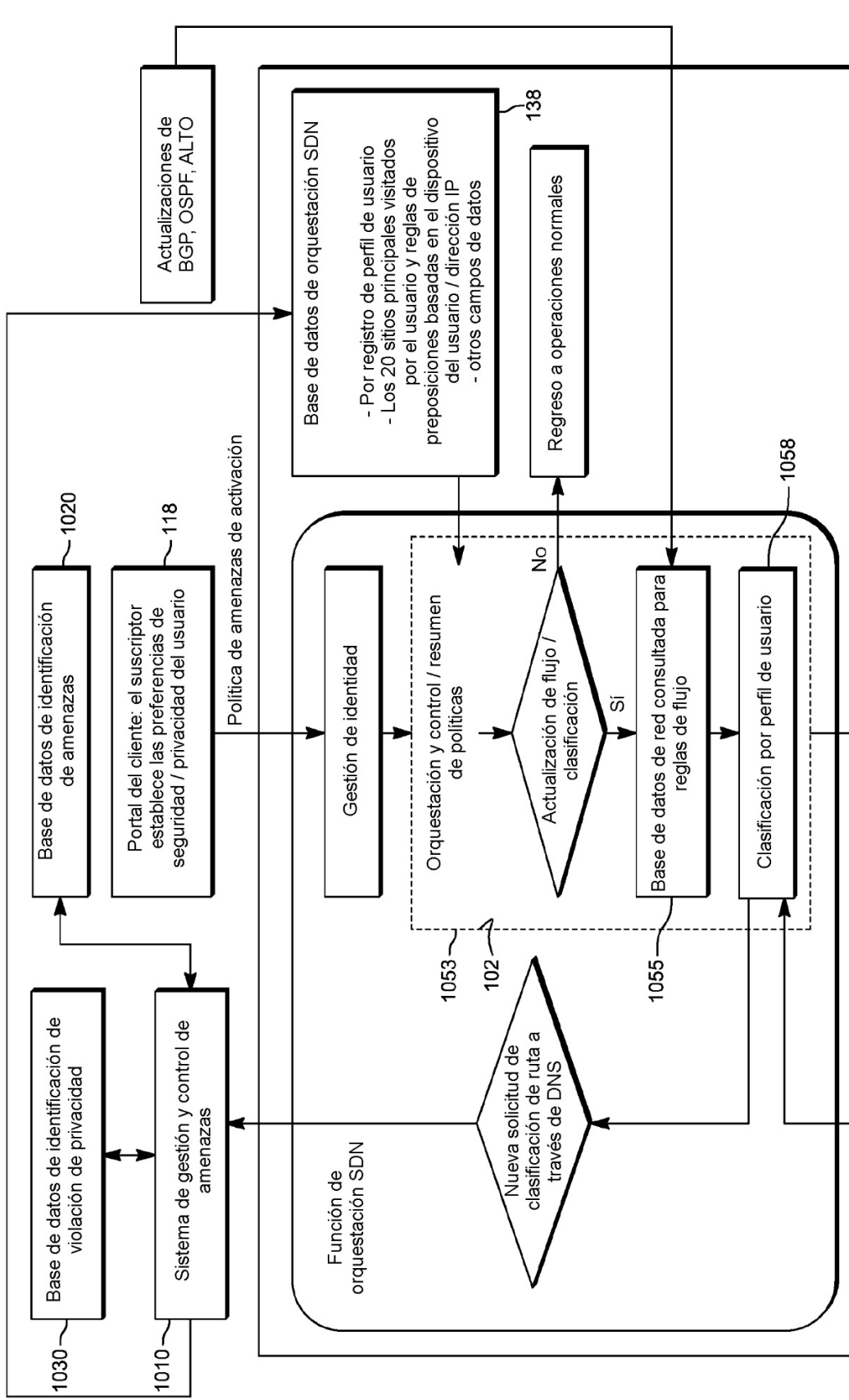


FIG. 20A

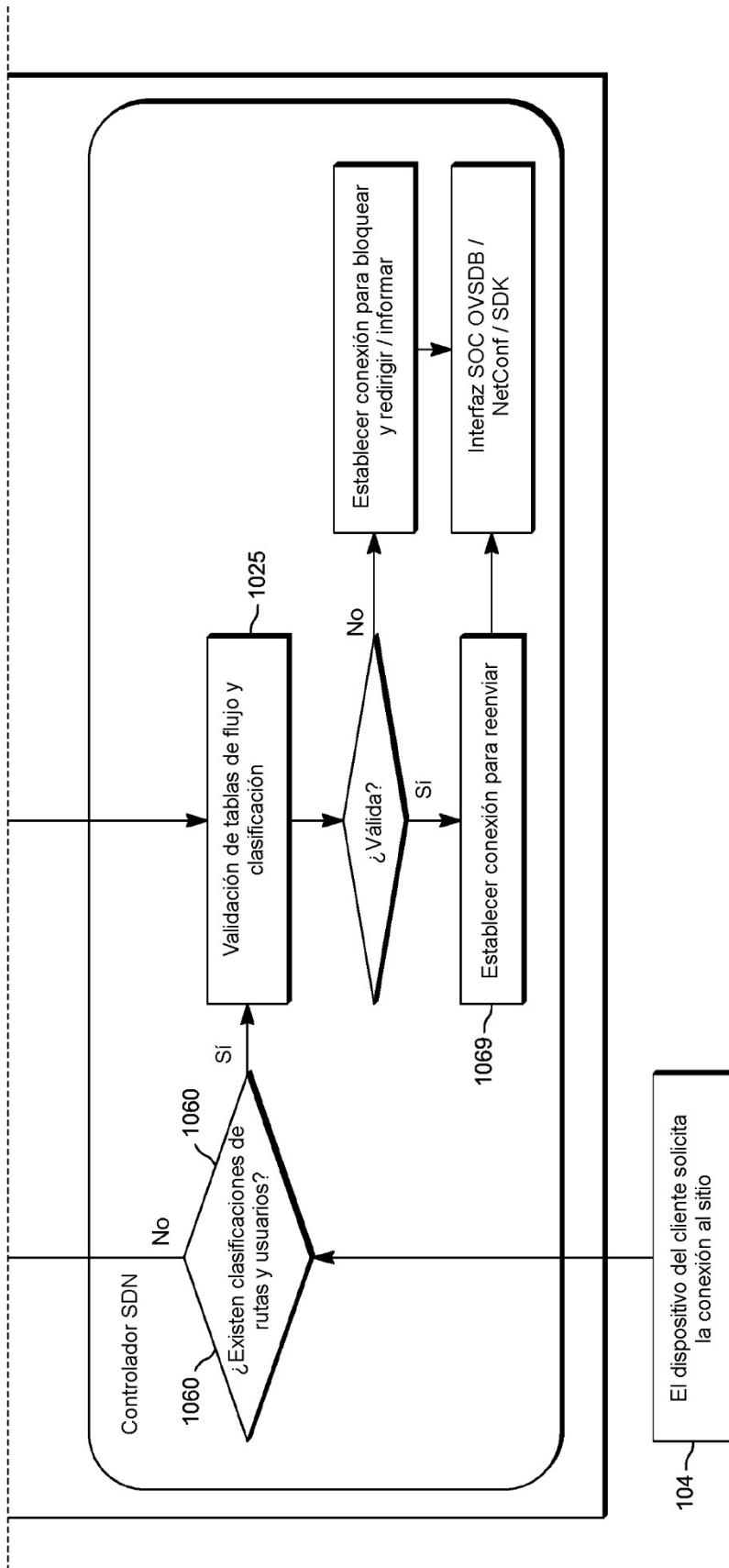


FIG. 20B

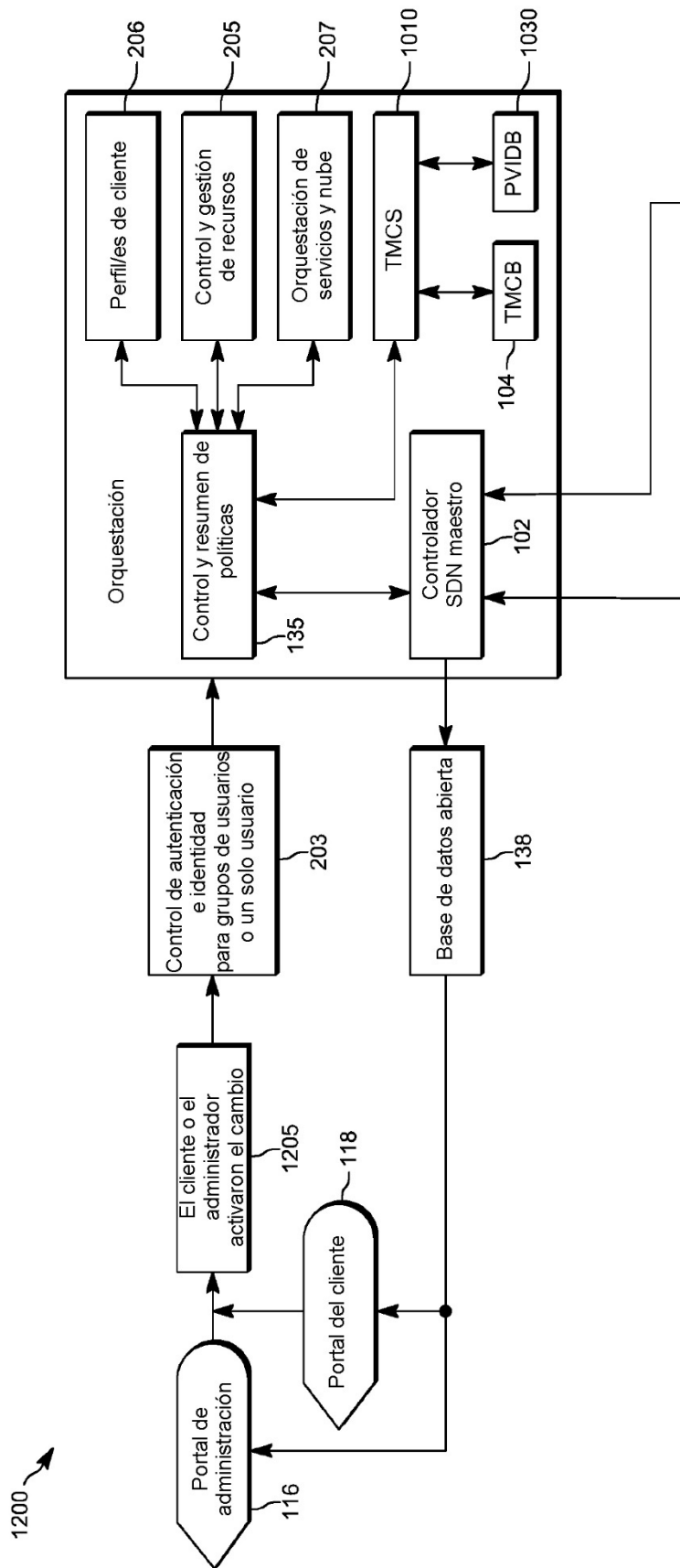


FIG. 21A

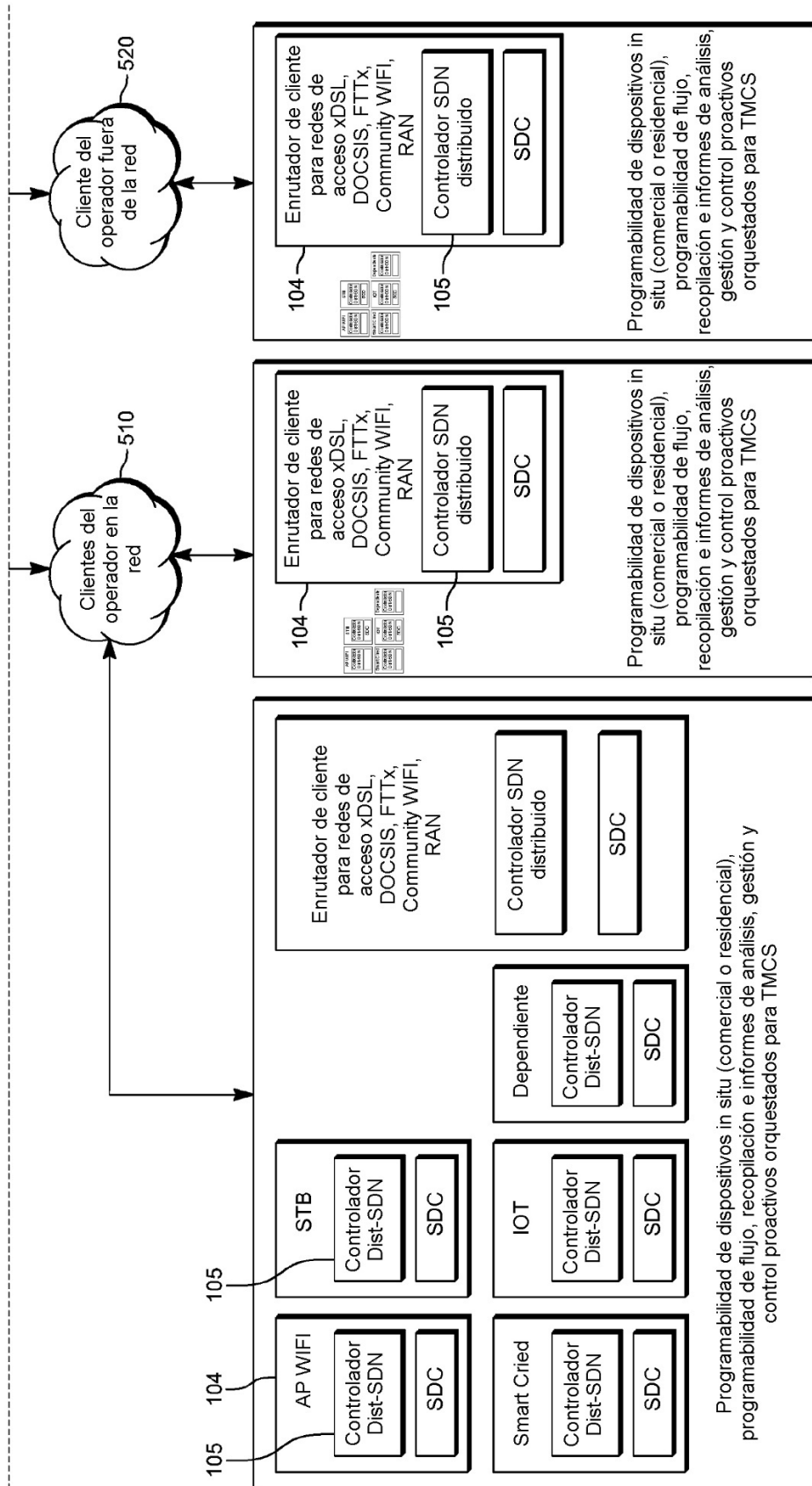


FIG. 21B

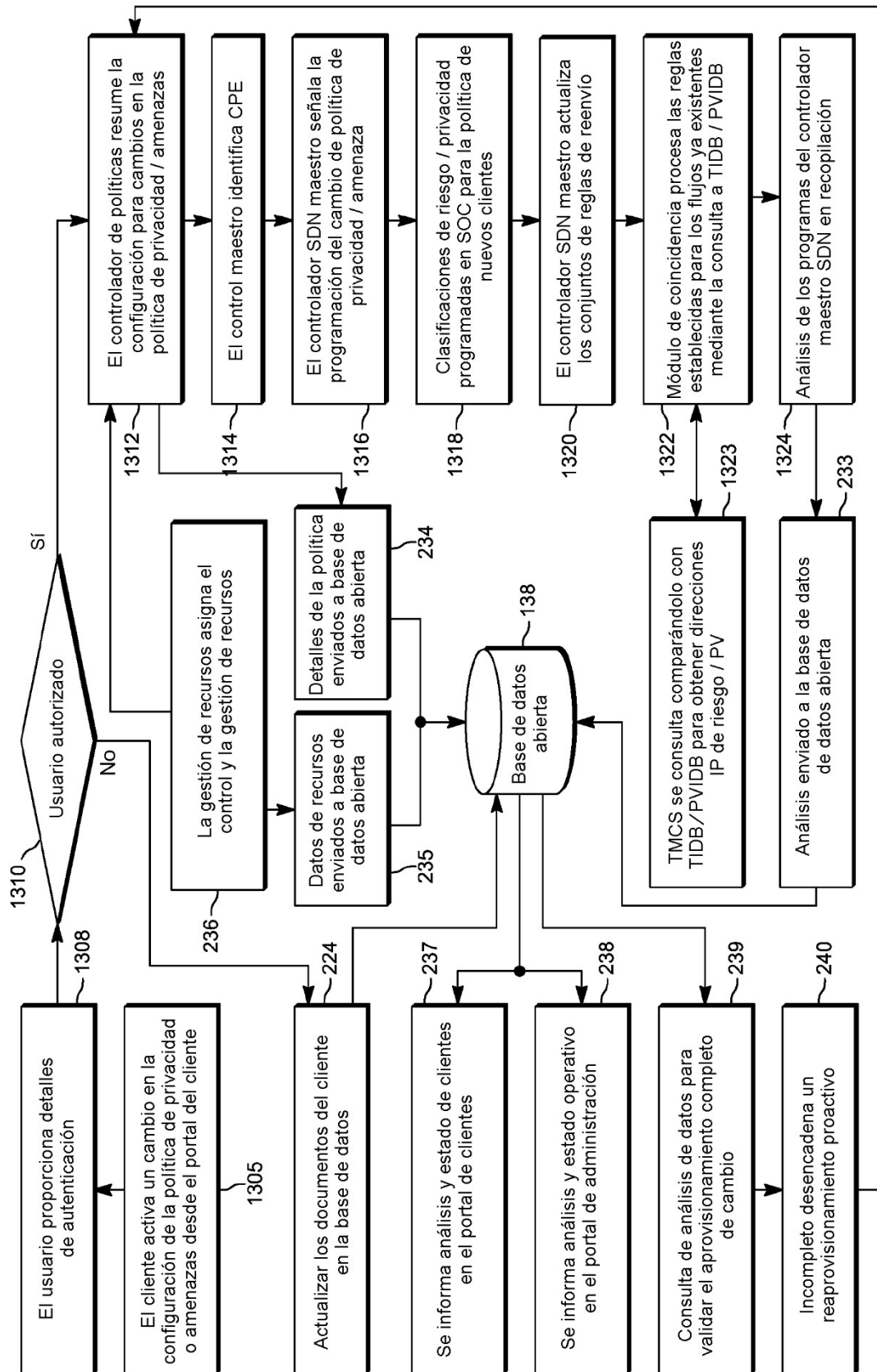


FIG. 22

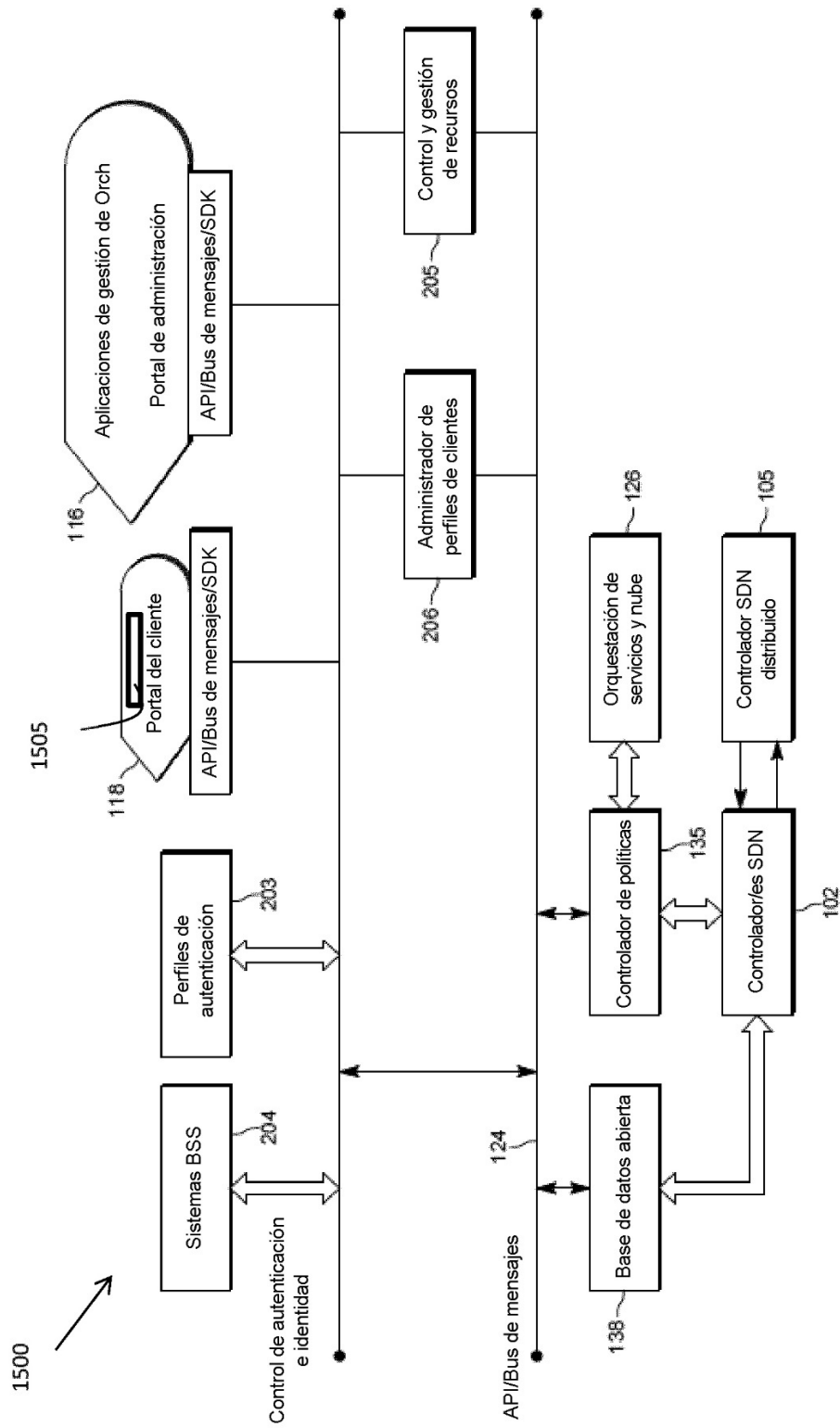


Fig. 23

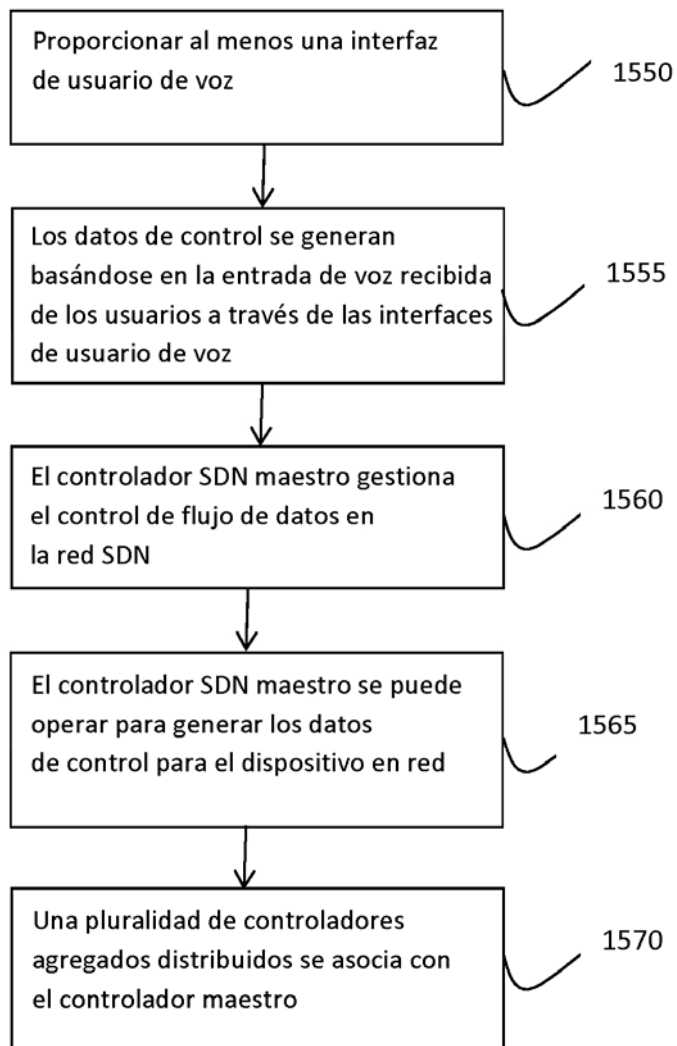


Fig. 24