(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 735 408**

(51) Int. CI.:

H04L 12/24 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.12.2016 PCT/EP2016/081921**

(87) Fecha y número de publicación internacional: **29.06.2017 WO17108790**

(96) Fecha de presentación y número de la solicitud europea: **20.12.2016 E 16816688 (2)**

(97) Fecha y número de publicación de la concesión europea: **13.03.2019 EP 3248328**

(54) Título: **Una red orquestada basada en datos utilizando un controlador SDN distribuido de peso ligero**

(30) Prioridad:

25.12.2015 IN 4857MU2015
29.04.2016 US 201615142748
10.06.2016 US 201615179726

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.12.2019

(73) Titular/es:

KN INSTALL SOLUTIONS (N.IRE) 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

DESCRIPCIÓN

Una red orquestada basada en datos utilizando un controlador SDN distribuido de peso ligero

CAMPO DE LA INVESTIGACIÓN

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

ANTECEDENTES

Las redes se vuelven cada vez más complicadas a medida que se expanden en tamaño y mucho más difíciles de administrar y controlar. En una red tradicional se requieren recursos considerables de TI para implementar procedimientos como la configuración y el aprovisionamiento. Tradicionalmente, estas tareas eran implementadas manualmente por un administrador de red. El enfoque SDN automatizó estos procedimientos a través de software.

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

Además, este enfoque centralizado no tiene en cuenta la escala completa y el uso de los análisis que se pueden recopilar. Este enfoque no hace uso de las valiosas capacidades de referencia histórica de estos datos y de su capacidad para manejar la administración y el control proactivos de la red, para impulsar aplicaciones de seguridad, para computar las aplicaciones de planificación de infraestructura o para crear una resolución automática de fallos.

Por lo tanto, existe la necesidad de un procedimiento para controlar una red definida por software (SDN) y un controlador SDN que resuelva 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 otras partes, robar datos, amenazar o bloquear sistemas e invadir la privacidad de otros. Su evolución comenzó poco después del comienzo de la era de la computadora e incluye múltiples tipos de virus, malware, adware, troyanos, denegación de servicio (DOS), DOS distribuidos, spyware, etc.

Además, los modelos de negocio cambiantes de las empresas ahora significan que cuando un cliente compra un producto de software o incluso utiliza lo que se considera un software legítimo, esto permite que tanto las empresas legítimas como las infames recaben cantidades muy significativas de datos personales sobre el usuario. El consumidor generalmente desconoce el nivel de seguimiento y monitoreo que tienen lugar por lo que consideran productos legítimos porque el consumidor ha aceptado inadvertidamente los términos y condiciones que pueden no ser válidos según las regulaciones del país donde residen.

La mayoría de estos desarrollos de brecha de seguridad y violación de la privacidad se están utilizando para algún tipo de propósito malicioso en una escala variable. Los problemas evolutivos y cambiantes que enfrenta el consumidor en relación con la violación de seguridad y la violación de la privacidad pueden considerarse en contra de la forma histórica en que los virus evolucionaron. Hace algunos años era obvio cuando una infección de virus estaba presente. Los virus del pasado fueron escritos en gran parte por aficionados y tendían a ser obvios, ya que exhibían un comportamiento destructivo o ventanas emergentes. Los virus modernos, sin embargo, a menudo son escritos por profesionales y son financiados por organizaciones infames. Con estos niveles de actividades nefastas experimentadas por los usuarios finales, se requiere un nuevo enfoque para abordar los problemas de seguridad y privacidad de los usuarios finales.

Por lo tanto, existe la necesidad de un procedimiento para proporcionar seguridad en una red definida por software (SDN) que resuelva 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 inconvenientes de la técnica anterior.

La solicitud de patente PCT publicada n.º. WO 2015/071888 se relaciona con los sistemas y procedimientos para asegurar el aislamiento de múltiples inquilinos en un centro de datos. Se puede usar un conmutador o conmutador virtualizado para des-multiplexar el tráfico entrante entre una cantidad de inquilinos de centros de datos y para dirigir el tráfico al segmento virtual apropiado para un inquilino identificado. El conmutador puede almacenar la información de identificación del inquilino recibida de un controlador maestro y las reglas de reenvío de paquetes recibidas de, al menos, un controlador del inquilino. Las reglas de manejo de paquetes están asociadas con un inquilino específico y se pueden usar para reenviar el tráfico a su destino.

La solicitud de patente de Estados Unidos publicada n.º. 2014/317261 se refiere a un procedimiento que comprende la identificación, por un orquestador ejecutado por una máquina física, una pluralidad de funciones de red virtualizadas requeridas para la implementación de un servicio de red virtualizado para un cliente, cada función de red virtualizada tiene un contenedor virtualizado correspondiente y distinto que especifica atributos para definir ejecución de la correspondiente función de red virtualizada dentro de una o más máquinas físicas; y el ajuste por parte del orquestador de un indicador de interdependencia dentro de cada contenedor virtualizado basado en la asociación con el servicio de red virtualizado, que permite la identificación de cada una de las funciones de red virtualizadas como interdependientes para la ejecución coordinada del servicio de red virtualizado.

RESUMEN

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

proporcionar uno o más portales de clientes que están configurados para facilitar a los usuarios el control de dispositivos de 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 de flujo de datos en la red SDN; el controlador SDN maestro es operable para generar datos de enrutamiento para los dispositivos de red;

generar por el controlador SDN maestro una pluralidad de co-controladores discretos, cada uno asociado con un usuario final particular; cada co-controlador SDN, incluyendo datos de configuración y datos de enrutamiento para un dispositivo de red asociado;

enviar el co-controlador SDN por el controlador SDN maestro a los dispositivos de red asociados con los usuarios finales respectivos para el control del mismo;

instalar los co-controladores SDN en los dispositivos de red; y

registrar los co-controladores SDN instalados con el controlador SDN maestro para controlar el enrutamiento de datos desde los dispositivos de red y para controlar la configuración de los dispositivos de red.

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

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

generar por el controlador SDN maestro una pluralidad de co-controladores discretos, cada uno asociado con un usuario final particular; cada co-controlador SDN, incluyendo datos de enrutamiento para un dispositivo de red asociado;

enviar el co-controlador SDN por el controlador SDN maestro a los dispositivos de red asociados con los usuarios finales respectivos para el control del mismo;

solicitar acceso a un destino en la red SDN desde un dispositivo de red solicitante;

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

comunicación alternativo para evitar la interferencia de los dispositivos vecinos.

En un aspecto, el canal de comunicación incluye un canal Wi-Fi.

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

En un aspecto, la configuración de la operación del dispositivo de red se cambia mediante la reprogramación de una interfaz de alimentación.

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

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

En un aspecto adicional, los co-controladores SDN son operables para asignar un ajuste de primera prioridad a un primer conjunto de dispositivos de red y asignar un segundo ajuste de prioridad a un segundo conjunto de dispositivos de red.

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.

En otro aspecto, el controlador SDN maestro implementa la orquestación SDN en respuesta a una solicitud de recurso recibida en los portales del cliente. Ventajosamente, la orquestación SDN incluye la coordinación de los elementos de hardware y software de red necesarios para admitir las aplicaciones asociadas con la solicitud de recursos. Preferiblemente, la orquestación SDN incluye generar una instancia de una o más aplicaciones en la nube. En un ejemplo, la orquestación SDN genera una instancia de virtualización de función de red (NFV).

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

En otro aspecto, un usuario es autenticado.

En un aspecto ejemplar, los co-controladores SDN están instalados en un sistema en chip (SOC) de los dispositivos de red respectivos.

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

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

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.

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

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

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

La presente enseñanza también se relaciona con un controlador de red para una red definida por software (SDN), el controlador de red que comprende uno o más módulos operables para:

proporcionar uno o más portales de clientes que están configurados para facilitar a los usuarios el control de dispositivos de 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 de flujo de datos en la red SDN; el controlador SDN maestro es operable para generar datos de enrutamiento para los dispositivos de red;

generar por el controlador SDN maestro una pluralidad de co-controladores discretos, cada uno asociado con un usuario final particular; cada co-controlador SDN, incluyendo datos de configuración y datos de enrutamiento para un dispositivo de red asociado;

enviar el co-controlador SDN por el controlador SDN maestro a los dispositivos de red asociados con los usuarios finales respectivos para el control del mismo;

instalar el co-controlador SDN en los dispositivos de red; y

registrar los co-controladores SDN instalados con el controlador SDN maestro para controlar el enrutamiento de datos desde los dispositivos de red y para controlar la configuración de los dispositivos de red.

Además, la presente divulgación se refiere a un artículo de fabricación que comprende un medio legible por un procesador que tiene incorporado en él un código de programa ejecutable que cuando se ejecuta mediante el dispositivo de procesamiento hace que el dispositivo de procesamiento realice:

proporcionar uno o más portales de clientes que están configurados para facilitar a los usuarios el control de dispositivos de 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 de flujo de datos en la red SDN; el controlador SDN maestro es operable para generar datos de enrutamiento para los dispositivos de red;

generar por el controlador SDN maestro una pluralidad de co-controladores discretos, cada uno asociado con un usuario final particular; cada co-controlador SDN, incluyendo datos de configuración y datos de enrutamiento para un dispositivo de red asociado;

enviar el co-controlador SDN por el controlador SDN maestro a los dispositivos de red asociados con los usuarios finales respectivos para el control del mismo;

instalar el co-controlador SDN en los dispositivos de red; y

registrar los co-controladores SDN instalados con el controlador SDN maestro para controlar el enrutamiento de datos desde los dispositivos de red y para controlar la configuración de los dispositivos de red.

Además, la presente enseñanza se relaciona con una red definida por software (SDN); el procedimiento que comprende:

proporcionar uno o más portales de clientes que están configurados para facilitar a los usuarios el control de dispositivos de 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 de flujo de datos en la red SDN; el controlador SDN maestro es operable para generar datos de enrutamiento para los dispositivos de red;

generar por el controlador SDN maestro una pluralidad de co-controladores discretos, cada uno asociado con un usuario final particular; cada co-controlador SDN, incluyendo datos de configuración y datos de enrutamiento para un dispositivo de red asociado;

enviar el co-controlador SDN por el controlador SDN maestro a los dispositivos de red asociados con los usuarios finales respectivos para el control del mismo; e

instalar el co-controlador SDN en los dispositivos de red.

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

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 por el módulo de control maestro una pluralidad de agentes de control discretos, cada uno asociado con un usuario final particular y configurado según 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 el control del mismo.

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

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 está incorporado en el agente de control.

En otro aspecto, el control localizado está habilitado para servicios específicamente en relación con los servicios que el cliente ha seleccionado.

En otro aspecto, el dispositivo final no se reduce, sino que es un control programable habilitado localmente y habilitado específicamente para el cliente individual.

En otro aspecto, las analíticas detalladas de nivel bajo se recopilan directamente desde el dispositivo y se transfieren a la solución de orquestación para respaldar la gestión y el control del cliente.

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

En otro aspecto, se distribuye un plano de control unificado a través de tecnologías de acceso múltiple, por ejemplo, DOCSIS, FTTx, xDSL, Wi-Fi, etc., pero no limitado a las tecnologías que se proporcionan solo a modo de ejemplo, lo que permite a los operadores desplegar y controlar particularmente los servicios de una manera unificada.

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

En un aspecto, una instancia de cada recurso creado en la nube.

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

En otro aspecto, una instancia de virtualización de la función de red (NFV) está configurada.

La presente divulgación también se relaciona con un controlador de red para una red definida por software (SDN), el controlador de red que comprende:

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; el módulo de control maestro es operable para generar una pluralidad de agentes de control discretos, cada uno asociado con un usuario final particular y configurado según los recursos de red seleccionados por el usuario final particular; y

un módulo de comunicación configurado para enviar o controlar agentes de control discretos incorporados a uno o más dispositivos locales del usuario final respectivo para el control del mismo.

Además, la presente divulgación se relaciona con un procedimiento implementado por ordenador para controlar una red SDN; el procedimiento que 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;

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

enviar los agentes de control discretos a uno o más dispositivos locales del respectivo usuario final para el control del mismo localmente.

Además, la presente divulgación se relaciona con 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 que 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;

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

enviar los agentes de control discretos a uno o más dispositivos locales del respectivo usuario final para el control del mismo localmente.

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

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 por el módulo de control maestro una pluralidad de agentes de control discretos, cada uno asociado con un usuario final particular y configurado según 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 el control del mismo.

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

proporcionar un módulo de control maestro configurado para gestionar el control de flujo en la red SDN;

generar por el módulo de control maestro una pluralidad de agentes de control de acceso discreto, cada uno asociado con nodos particulares del nodo de red SDN para controlar el acceso a ello; y

enviar los agentes de control de acceso discreto a dispositivos asociados con los nodos respectivos para programar dinámicamente los dispositivos con criterios de control de acceso.

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

proporcionar un portal de clientes para facilitar la interacción de un usuario final con la red doméstica para seleccionar los criterios de control locales;

proporcionar un módulo de control maestro asociado con la red SDN que en comunicación con la red doméstica y configurado para gestionar el control de flujo;

generar por 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 criterios de control seleccionados por el usuario final en el portal de clientes; y

enviar los agentes de control discretos a la red doméstica para controlar los dispositivos de la red doméstica según los criterios de control seleccionados por el usuario final.

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

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

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

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

generar por el controlador SDN maestro una pluralidad de co-controladores discretos, cada uno asociado con un usuario final particular; cada co-controlador SDN, incluyendo datos de enrutamiento para un dispositivo de red asociado;

enviar el co-controlador SDN por el controlador SDN maestro a los dispositivos de red asociados con los usuarios finales respectivos para el control del mismo;

solicitar acceso a un destino en la red SDN desde un dispositivo de red solicitante;

iniciar una interacción del sistema de nombres de dominio (DNS) con el dispositivo de red solicitante;

la transmisión por los datos del 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 unos criterios de seguridad asociados;

comunicar un estado de amenaza por el TMCS al co-controlador SDN asociado con el dispositivo de red solicitante; y

generar datos de enrutamiento por parte del co-controlador SDN asociado con el dispositivo de red solicitante basado en el estado de amenaza para permitir o denegar el acceso al destino solicitado.

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

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

generar por el controlador SDN maestro una pluralidad de co-controladores discretos, cada uno asociado con un usuario final particular; cada co-controlador SDN, incluyendo datos de enrutamiento para un dispositivo de red asociado;

enviar el co-controlador SDN por el controlador SDN maestro a los dispositivos de red asociados con los usuarios finales respectivos para el control del mismo;

solicitar acceso a un localizador de recursos uniforme (URL) desde un dispositivo de red solicitante;

iniciar una interacción del sistema de nombres de dominio (DNS) con el dispositivo de red solicitante;

la transmisión por los datos del DNS asociados con el URL solicitado a un sistema de control de gestión de amenazas (TMCS);

determinar por el TMCS si el URL solicitado tiene unos criterios de seguridad asociados;

comunicar un estado de amenaza por el TMCS al co-controlador SDN asociado con el dispositivo de red solicitante; y

generar datos de enrutamiento por parte del co-controlador SDN asociado con el dispositivo de red solicitante basado en el estado de amenaza para permitir o denegar el acceso al URL solicitado.

En un aspecto, el TMCS está en comunicación con, al menos, un repositorio de datos que contiene detalles de los URL 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 conoce que un URL tiene unos criterios de seguridad maliciosos.

En un aspecto adicional, al menos, un repositorio de datos está alojado por una entidad de terceros. Ventajosamente, al menos, un repositorio de datos comprende una clasificación de múltiples tipos de riesgos. En un ejemplo, al menos, un repositorio de datos comprende una clasificación de múltiples perfiles de usuarios. Preferiblemente, cada perfil de usuario tiene una acción de enrutamiento asociada basada en su clasificación. En una disposición ejemplar, al menos, un repositorio de datos comprende un primer conjunto de datos asociado con destinos que tienen amenazas de seguridad previamente identificadas. En otro ejemplo, al menos, un repositorio de datos comprende un segundo conjunto de datos asociado con destinos que se sabe que recopilan 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 co-controlador SDN tiene un módulo de coincidencia de seguridad asociado que es operable 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 de red solicitante. En otro aspecto, la decisión de reenvío se basa en una clasificación de riesgo. Ventajosamente, la decisión de reenvío hace que el tráfico se envíe a un destino de cuarentena. En un ejemplo, la decisión de reenvío hace que el tráfico se reenvíe al URL solicitado.

En un aspecto adicional, el co-controlador SDN en el dispositivo de red solicitante introduce una entrada de reenvío en una tabla de enrutamiento de flujo basada en la decisión de reenvío del módulo de coincidencia de seguridad.

En un aspecto, el TMCS es operable para llenar una base de datos abierta accesible por un orquestador SDN. Ventajosamente, el TMCS es operable para llenar la base de datos abierta con el estado de las amenazas identificadas.

En otro aspecto, se puede acceder a la base de datos abierta desde, al menos, un portal remoto. Ventajosamente, el estado de las amenazas identificadas se puede ver desde, al menos, un portal remoto.

En un aspecto adicional, el TMCS es operable para transmitir 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. Ventajosamente, la dirección IP del usuario se utiliza para asignar un informe de alerta de seguridad a un registro del 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 un ajuste de seguridad de una pluralidad de ajustes de seguridad disponibles. Ventajosamente, se genera una política de seguridad basada en el ajuste de seguridad seleccionado. En un aspecto, un identificador del dispositivo de red solicitante se extrae de la base de datos abierta. Preferiblemente, una lista de sitios utilizados comúnmente por el usuario se extrae de la base de datos abierta.

En un aspecto adicional, el procedimiento comprende adicionalmente extraer datos analíticos por los co-controladores SDN de los dispositivos de red. Ventajosamente, 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 co-controladores SDN a la base de datos abierta a través del controlador SDN maestro.

En un aspecto adicional, un motor de analítica está en comunicación con la base de datos abierta que se puede operar para analizar la analítica extraída para generar un resultado de analítica.

En otro aspecto, la salida de la analítica 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 de clientes para la selección basada en la salida de la analítica. Ventajosamente, los datos de configuración se actualizan en respuesta al usuario final que selecciona una o más opciones de mejora del rendimiento.

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

En otro aspecto, la configuración operativa de los dispositivos de red se modifica para aumentar una calidad del parámetro del servicio. Ventajosamente, los ajustes operativos de los dispositivos de red se actualizan en tiempo real mientras están en línea. En un ejemplo, la configuración operativa de los dispositivos de red se actualiza mientras está en modo de suspensión.

En un aspecto ejemplar, los co-controladores SDN están instalados en un sistema en chip (SOC) de los dispositivos de red respectivos. Ventajosamente, los co-controladores SDN se cargan en el firmware contenido en los dispositivos de red respectivos. En un aspecto ejemplar, los co-controladores SDN son binarios desplegables.

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

La presente divulgación también se relaciona con un controlador de seguridad de red para una red definida por software (SDN), el controlador de seguridad de red que comprende uno o más módulos operables para:

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

generar por el controlador SDN maestro una pluralidad de co-controladores discretos, cada uno asociado con un usuario final particular; cada co-controlador SDN, incluyendo datos de enrutamiento para un dispositivo de red asociado;

enviar el co-controlador SDN por el controlador SDN maestro a los dispositivos de red asociados con los usuarios finales respectivos para el control del mismo;

solicitar acceso a un localizador de recursos uniforme (URL) desde un dispositivo de red solicitante;

iniciar una interacción del sistema de nombres de dominio (DNS) con el dispositivo de red solicitante;

la transmisión por los datos del DNS asociados con el URL solicitado a un sistema de control de gestión de amenazas (TMCS);

determinar por el TMCS si el URL solicitado tiene unos criterios de seguridad asociados;

comunicar un estado de amenaza por el TMCS al co-controlador SDN asociado con el dispositivo de red solicitante; y

generar datos de enrutamiento por parte del co-controlador SDN asociado con el dispositivo de red solicitante basado en el estado de amenaza para permitir o denegar el acceso al URL solicitado.

Además, la presente divulgación se relaciona con un medio legible por ordenador que comprende instrucciones no transitorias que, cuando se ejecutan, hacen que un procesador lleve a cabo un procedimiento conforme a cualquiera de los pasos previamente descritos. Por ejemplo; las instrucciones no transitorias que, cuando se ejecutan, hacen que un procesador lleve a cabo un procedimiento que comprende:

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

generar por el controlador SDN maestro una pluralidad de co-controladores discretos, cada uno asociado con un usuario final particular; cada co-controlador SDN, incluyendo datos de enrutamiento para un dispositivo de red asociado;

enviar el co-controlador SDN por el controlador SDN maestro a los dispositivos de red asociados con los usuarios finales respectivos para el control del mismo;

solicitar acceso a un localizador de recursos uniforme (URL) desde un dispositivo de red solicitante;

iniciar una interacción del sistema de nombres de dominio (DNS) con el dispositivo de red solicitante;

la transmisión por los datos del DNS asociados con el URL solicitado a un sistema de control de gestión de amenazas (TMCS);

determinar por el TMCS si el URL solicitado tiene unos criterios de seguridad asociados;

comunicar un estado de amenaza por el TMCS al co-controlador SDN asociado con el dispositivo de red solicitante; y

generar datos de enrutamiento por parte del co-controlador SDN asociado con el dispositivo de red solicitante basado en el estado de amenaza para permitir o denegar el acceso al URL solicitado.

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

proporcionar un módulo de control maestro en un sistema de terminación de módem de cable (CMTS) que está configurado para controlar los módems de cable DOCSIS;

generar por el módulo de control maestro una pluralidad de agentes de control discretos, cada uno asociado con un módem de cable DOCSIS particular; y

enviar los agentes de control discretos a los módems de cable DOCSIS para programar dinámicamente el módem de cable DOCSIS con un archivo de arranque desde el CMTS sin tener que leer un demonio del kernel.

La anterior y otras características y ventajas de las realizaciones preferidas de la presente divulgación son más aparentes a partir de la siguiente descripción detallada. La descripción detallada procede con referencia a los dibujos adjuntos.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La presente divulgación se describirá ahora con referencia a los dibujos adjuntos, donde:

Fig. 1 es un diagrama de bloques que ilustra una plataforma SDN ejemplar según la presente enseñanza.

Fig. 2 es un diagrama de bloques que ilustra detalles de la arquitectura de la figura 1.

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

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

Fig. 5 es un diagrama de bloques que ilustra otra plataforma SDN ejemplar según la presente enseñanza.

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

Fig. 7 es un diagrama de flujo que ilustra pasos ejemplares durante la operación de la plataforma SDN de la figura 1 o la figura 5.

Fig. 8 es un diagrama de flujo que ilustra pasos ejemplares durante la operación de la plataforma SDN de la figura 1 o la figura 5.

Fig. 9 es un diagrama de flujo que ilustra pasos ejemplares durante la operación de la plataforma SDN de la figura 1 o la figura 5.

Fig. 10 es un diagrama de bloques que ilustra otra plataforma SDN ejemplar según la presente enseñanza.

Fig. 11 es un diagrama de bloques que ilustra otra plataforma SDN ejemplar según la presente enseñanza.

Fig. 12A es un diagrama de bloques que ilustra otra plataforma SDN ejemplar según la presente enseñanza.

Fig. 12B es un diagrama de bloques que ilustra otra plataforma SDN ejemplar según la presente enseñanza.

Fig. 13 es un diagrama de flujo que ilustra pasos ejemplares durante la operación de la plataforma SDN de la figura 1, la figura 5, la figura 11, la figura 12A o la figura 12B.

Fig. 14 es un diagrama de flujo que ilustra pasos ejemplares durante la operación de la plataforma SDN de la figura 1, la figura 5, la figura 11, la figura 12A o la figura 12B.

Fig. 15 es un diagrama de flujo que ilustra pasos ejemplares durante la operación de la plataforma SDN de la figura 1, la figura 5, la figura 11, la figura 12A o la figura 12B.

Fig. 16A y 16B es un diagrama de bloques que ilustra detalles de una arquitectura SDN que también está según la presente enseñanza.

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

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

Fig. 19 es un diagrama de flujo que ilustra pasos ejemplares durante la operación de la plataforma SDN de las figuras 16A-18.

Fig. 20 es un diagrama de flujo que ilustra pasos ejemplares durante la operación de la plataforma SDN de las figuras 16A-18.

Fig. 21 es un diagrama de bloques que ilustra detalles de una arquitectura SDN que también está según la presente enseñanza.

Fig. 22 es un diagrama de flujo que ilustra pasos ejemplares durante la operación de la plataforma SDN de las figuras 16A y 16B o la figura 21.

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 comprender la enseñanza actual y no debe interpretarse como limitante de ninguna manera. Además, los módulos o elementos que se describen con referencia a una figura pueden intercambiarse con los de otras figuras u otros elementos equivalentes sin apartarse del espíritu de la presente enseñanza.

Con referencia a los dibujos e inicialmente a las figuras 1 a 3, se ilustra una plataforma SDN 100 según la presente enseñanza. Un controlador SDN maestro 102 está configurado para gestionar el control de flujo de datos en la red SDN 103. El controlador SDN maestro 102 es operable para generar datos de flujo de enrutamiento para una pluralidad de dispositivos de red 104. Los dispositivos de red 104 pueden incluir, pero no estar limitado a, equipos de infraestructura de red (NICs), 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 abonado digital (DSLAMs), terminales de línea óptica (OLT), terminales de red óptica (ONT), puntos de acceso Wi-Fi independientes, dispositivos de mano o similares. El controlador SDN maestro 102 tiene una vista completa de toda la red SDN 103, e información de todas las rutas de la red y las capacidades del dispositivo. El controlador SDN maestro 102 es operable para generar una pluralidad de co-controlador 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 basadas tanto en las direcciones de origen y destino; utilizar diferentes rutas de red para diferentes tipos de tráfico y reaccionar a la condición de los cambios de red.

El controlador SDN maestro 102 distribuye el co-controlador SDN 105 a los dispositivos de red 104 asociados con los respectivos usuarios para controlar los dispositivos 104, de modo que los dispositivos 104 son operables para tomar decisiones de enrutamiento de datos locales. Cada co-controlador SDN 105 incluye datos de configuración y un motor de enrutamiento. Los co-controladores distribuidos 105 están instalados en los dispositivos de red 104 asociados con usuarios finales particulares. El co-controlador SDN discreto 105 está configurado para añadir funciones de red a los dispositivos 105 que pueden incluir enrutamiento distribuido, calidad de funciones de servicio, funciones de listas de control de acceso y funciones de equilibrio de carga. Estas tareas habrían sido realizadas principalmente por el controlador SDN central en redes SDN conocidas hasta ahora.

Una vez instalados en los dispositivos 104, los co-controladores distribuidos 105 se registran con el controlador SDN maestro 102 y son co-operables para controlar el enrutamiento de datos desde los dispositivos de red a través de la red SDN 103. Los co-controladores distribuidos 105 actúan como un motor de enrutamiento distribuido, lo que elimina las limitaciones de hardware, como las entradas de memoria direccionables de contenido ternarias (TCAM). Debido a su implementación liviana, los co-controladores distribuidos 105 pueden instalarse en una variedad de dispositivos, desde plataformas de conmutación bajas/altas a metal desnudo, máquinas virtuales e incluso controladores de interfaz de red (NICs). Tanto el controlador SDN maestro 102 como el co-controlador SDN 105 pueden adaptarse a las necesidades de topología tanto de LAN (Este-Oeste) como de WAN (Norte-Sur) con enrutamiento unificado utilizando el protocolo de pasarela de frontera (BGP). La gestión de la topología para el enrutamiento consciente del servicio puede habilitarse mediante el descubrimiento de enlaces basado en el protocolo de descubrimiento de capa de enlace (LLDP)/detección de reenvío bidireccional (BFD). El co-controlador SDN 105 se puede integrar sin problemas en un sistema operativo de conmutador como LINUX o UNIX. Los co-controladores distribuidos 105 pueden 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 calidad de servicio (QoS, Quality of Service) con programación en tiempo real de rutas tanto dentro como entre dominios. El plano de control de la plataforma SDN 100 se basa en estándares de la industria con la ventaja de eliminar la carga del bloqueo de proveedores. La plataforma SDN 100 cuenta con herramientas e Interfaces de Programación de Aplicaciones (API) ricas en características 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 servicios conscientes de la aplicación a minutos en lugar de semanas, lo que proporciona ahorros reales en los costes operativos. Un panel de interfaz intuitivo basado en la web permite a los usuarios implementar de manera rápida y sin problemas agregados, movimientos y cambios a la red 103 mientras combina el control programático de la red con el reconocimiento del estado de la red para proporcionar una garantía de SLA (Acuerdo de Nivel de Servicio).

El controlador SDN 105 comprende un repositorio de instrucciones de control y políticas para dispositivos específicos 104. El co-controlador SDN distribuido 105 es operable para tomar decisiones de enrutamiento localmente en los dispositivos 104, lo que alivia los retrasos que pueden ocurrir si estas decisiones de enrutamiento se tomaran de manera central en lugar de localmente. Además, el co-controlador SDN distribuido 105 facilita la granularidad individual de políticas específicas de ajuste para usuarios finales en una gran cantidad de dispositivos 105, en cuanto a cómo se deben controlar sus dispositivos y optimizar el rendimiento. El co-controlador SDN 105 también permite recopilar analítica 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 una visibilidad completa de toda una topología de red a través de un plano de control 107, que a diferencia de las implementaciones tradicionales de SDN, se centraliza utilizando el controlador SDN maestro 102, además de estar totalmente distribuido, utilizando los co-controladores SDN distribuidos 105. Los co-controladores distribuidos 105 son un motor de enrutamiento inteligente de peso ligero que puede enviarse a cualquier CPE habilitado para Openflow, como un conmutador, servidor, NIC o similar. El plano de control 107 se basa en estándares de la industria con la ventaja de eliminar la carga del bloqueo de proveedores. La arquitectura 100 proporciona las herramientas para adaptar las aplicaciones SDN y definir las políticas, reglas y optimizaciones propias del usuario para la red 110.

El controlador SDN maestro 102 y el co-controlador SDN 105 pueden basarse en protocolos, como OpenFlow o NetConf/YANG, que permiten a un servidor indicar a los conmutadores dónde enviar los 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 se puede utilizar para programar funciones de red específicas dentro de los dispositivos de red 105.

El plano de control 107 es altamente resistente, facilitado a través de una federación de controladores distribuidos 105, formando un punto único virtualizado de control SDN. Cada controlador individual federado a su vez envía automáticamente un agente de control de SDN ligero a cada uno de los dispositivos de red 104 en una capa de infraestructura 109, que proporciona 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 red virtual basada en la nube. También se encuentran en la capa de aplicación 126 una serie de herramientas y sistemas, portales de interfaz que permiten a un proveedor de servicios y a sus clientes operar, optimizar y autoservirse. La plataforma general 100 se integra a las tres capas del modelo SDN, lo que proporciona un conjunto completo de capacidades como se ilustra gráficamente en la figura 2.

Una arquitectura ejemplar según la presente enseñanza se ilustra en las figuras 3 y 4. Las interfaces del portal a la arquitectura de orquestación traen controles de las pilas de sistemas de soporte de negocios (BSS) 110, las aplicaciones de terceros 112, aplicaciones de control 114 que forman parte de las funciones de un portal de administradores 116 y un portal de clientes 118. Estas aplicaciones se comunican a través de las interfaces de programación de aplicaciones soportadas (APIs) 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 ligero de acceso a directorios (LDAP) se puede ejecutar 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 los componentes funcionales de la arquitectura.

OpenStack 130 está totalmente integrado en la solución y sus APIs de orquestación se utilizan para reunir 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 mediante controles API.

Un motor de control de políticas 135 identifica y asigna los datos de configuración adecuados al dispositivo 104 que se está controlando. Esto se logra a través de la consulta de los registros de clientes en vivo dentro de una base de datos 138 que ha recopilado analíticas utilizando los co-controladores distribuidos 105. Estas analíticas se recopilan a partir de las estructuras de datos del cliente en vivo, de los perfiles, etc., en la base de datos de datos abiertos que se ha completado con las analíticas de los dispositivos controlados por SDN 104 y de los datos obtenidos a través del procedimiento de aprovisionamiento en función de los perfiles de los clientes y de los productos. Todos los datos se asignan en la base de datos 138 en registros adecuadamente estructurados para una lectura y escritura rápidas. El controlador de políticas 135 identifica y asigna el perfil del cliente a las configuraciones adecuadas requeridas para el sistema en chip (SOC) del dispositivo 104 según el perfil del producto del cliente y el rol del token de gestión de autenticación e identidad asignado por capa de autenticación / identidad 128.

El controlador SDN maestro 102 puede residir en el plano de control 107. El controlador SDN maestro 102 comprende un componente de control/orquestación primario en comunicación con el portal del cliente 118 a través de las capas de orquestación y capas de nivel superior y está configurado para gestionar el control de flujo en la red SDN 103. Los componentes de control/orquestación son operables para generar una pluralidad de controladores discretos 105, cada uno asociado con un usuario final particular y configurado según 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 co-controlador SDN discreto 105 a uno o más dispositivos locales 104 del usuario final respectivo para el control del mismo. El co-controlador SDN discreto 105 se envía 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 co-controladores distribuidos 105 son agentes extremadamente ligeros y pueden incluirse en el firmware o BIOS de los dispositivos 104. En un ejemplo, los co-controladores 105 son binarios desplegables.

El control primario se maneja con el plano de orquestación 126 y maneja tareas administrativas como autenticación, registro, descubrimiento y configuración. Los co-controladores de múltiples capas 105 se proporcionan en las funciones de múltiples componentes de los planos de control multifuncionales 107. Estos co-controladores 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 utilizando NetConf/YANG, OpenFlow/OVSDB o la programación directa a través del sistema en el kit de desarrollo de software de chip (SOC) (SDK). También puede ejecutar los protocolos de enrutamiento y conmutación y realimenta datos operativos al plano de orquestación e informa de las analíticas a través del controlador SDN maestro 102 a la capa de orquestación 126 y la capa de control 107.

Además, los co-controladores distribuidos 105 construyen una base de datos de topología 142 y la utilizan para identificar sus vecinos y las 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 co-controladores 105 construyen una base de datos de red 144 y utilizan esto 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 para las 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 utiliza para tomar decisiones de reenvío y para definir controles de reenvío proactivos y reactivos. Además, el co-controlador de SDN 105 puede ser compatible con Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Application-Layer Traffic Optimization (ALTO) y otros EGPs e IGP para completar el conocimiento 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, tabla de red 121, tabla de reenvío de flujo 119 para la creación de control de reenvío reactivo y proactivo. El control de reenvío para los dispositivos 104 se genera y añade a la base de información de enrutamiento (RIB) 125 para la programación de dispositivos 104 con una base de información de reenvío (FIB) 127 a través de las interfaces disponibles 123 como SOC SDK, Open vSwitch Database (OVSDB) o Protocolo de configuración de red (NetConf) / Yet Another Next Generation (YANG). Un administrador de RIB 141 es operable para crear una base de información de reenvío (FIB) en los dispositivos 104 que utiliza el sistema operativo del dispositivo 104 para encontrar la interfaz adecuada a la cual la interfaz de entrada debería enviar un paquete de datos. Los datos de política 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, utilizando la tabla de enrutamiento de flujo 119 suministrada por los co-controladores distribuidos 105 para determinar el puerto de salida. Esto se programa y las instrucciones se envían utilizando NetConf/YANG, OpenFlow/OVSDB o la programación directa a través del SDK de SOC.

El controlador SDN maestro 102 y los co-controladores SDN 105 cooperan para funcionar como un controlador fuera de banda que recupera y programa dinámicamente la configuración de los dispositivos 104 que el cliente ha seleccionado usando el portal 118 del cliente. 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 ligero fuera de banda que se integra con una solución de orquestación remota para recibir conjuntos de instrucciones y entregar automáticamente el control de flujo del servicio, la recopilación de analítica y para activar los cambios solicitados por el cliente a los servicios al cliente en tiempo real.

Los co-controladores distribuidos 105 pueden distribuirse como un controlador ligero en un rango de baja potencia, CPE con bajo consumo de CPU, equipo de infraestructura de red, NICs, amplificadores, servidores, nodos de fibra, CMTS, CCAP, amplificadores, DSLAM, OLT, ONT, puntos de acceso Wi-Fi independientes, los dispositivos de mano, etc. y los servicios de aprovisionamiento en una latencia muy reducida para permitir entrega de alta calidad, Acuerdo Nivel de Servicio (SLA) de valor agregado, a la vez que mejoran significativamente la capacidad de una organización para adaptarse rápidamente a las demandas cambiantes del cliente/red. La plataforma 100 proporciona una visualización completa de todos los servicios NFV y SDN que es a la vez jerárquica y de múltiples capas. Esta visualización también incluye información integrada de alarmas, disponibilidad, rendimiento, calidad de servicio y cumplimiento de SLA, lo que la convierte en una vista única para una evaluación integral del servicio de salud. Esto brinda una visión dinámica y precisa y la accesibilidad de la red y los servicios asociados, una visión consolidada de la salud de cada servicio y la gestión de recursos, y la capacidad para resolver problemas e identificar rápidamente los servicios afectados.

En una realización ejemplar, la plataforma SDN 100 se puede utilizar para eliminar la gestión de archivos de los módems de cable DOCSIS y la automatización de la orquestación de servicios. La plataforma SDN 100 puede configurarse para el aprovisionamiento y orquestación de la pila de IP y la red distribuida de servicios en el hogar en módems DOCSIS. La plataforma 100 funciona como un controlador fuera de banda que recupera y programa dinámicamente el archivo de arranque del CMTS al módem por cable sin tener que leerlo como un demonio del kernel, reduciendo así los requisitos de procesamiento del módem por cable (CM), además de la eliminación de operadores hay que mantener múltiples archivos de arranque. Actualmente, millones de módems de cable se aprovisionan a nivel mundial, pero una de las debilidades importantes que se pueden percibir en el modelo de aprovisionamiento de DOCSIS es la falta de un procedimiento dinámico de actualización de un servicio. Algunos de los problemas clave que preocupan a los operadores de sistemas múltiples (MSO) y los suscriptores se pueden describir como:

- Compartir contenido personal a través de los límites del enrutador.
- Optimizar las rutas de la red doméstica.
- Visibilidad MSO y gestión de la red doméstica.
- Gestionar y cumplir consistentemente la política - Cortafuegos - Controles parentales.
- Acceso remoto.
- Servicios nuevos.

Muchos proveedores de servicios operan su red con un control primario poco o débil sobre su configuración y gestión. Esto significa que la configuración y el estado de la red se almacenan efectivamente en una base de datos distribuida gigante. Esto no es inherentemente 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 se ejecutan sobre ella. El archivo de arranque maneja el ADN de cualquier módem de cable DOCSIS dado y esto puede hacerse de forma dinámica y programable utilizando la plataforma SDN 100 según la presente enseñanza que supera los problemas mencionados anteriormente. El operador puede reducir el procedimiento de aprovisionamiento de servicios a una sola transacción en lugar de a una serie de pasos complejos que involucran a múltiples sistemas y personas.

La plataforma SDN 100 puede utilizarse para abstraer la definición de servicio y las topologías del acceso físico y los dispositivos utilizados para proporcionar el servicio. Esta abstracción permite la máxima flexibilidad en la construcción de un sistema de aprovisionamiento que es agnóstico a las tecnologías de acceso que se utilizan. Por ejemplo, cuando los servicios complejos como L3 VPN (red privada virtual enrutada) deben ofrecerse a los clientes o se debe realizar una cierta configuración predefinida del protocolo de enrutamiento del extremo del proveedor (PE) - extremo del cliente (CE) para garantizar que las rutas correctas se anuncian/filtran se requiere que se realicen servicios complejos y encadenados, como proporcionar servicios de cortafuegos en línea o proporcionar acceso a servicios en la nube desde una VPN. Los servicios de capa superior como estos son ejemplos de servicios donde la definición del servicio puede extenderse más allá de los circuitos de conexión y los elementos en 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 este modelo de aprovisionamiento de DOCSIS de hoy en día puede ser inadecuada y, por lo tanto, nuestra combinación de SDN para gestionar dicha organización a través de OpenFlow es extremadamente útil para el rápido aprovisionamiento y las actualizaciones de servicio.

El portal de clientes 118 es el centro de información y autoservicio para el cliente. Proporciona un 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 del cliente 118 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 individual al portal y la información que se muestra, por ejemplo, detalladamente; uso, hora del día, actividad de navegación y mucho más. El cliente, ahora armado con estos datos, tiene una opción informada sobre lo que luego permiten, prohíben y restringen. El portal del cliente 118 muestra una o más opciones de mejora del rendimiento basadas en los análisis recopilados por los co-controladores SDN 105. Los datos de configuración asociados con los co-controladores SDN 105 se actualizan en respuesta al usuario final que selecciona una o más opciones de mejora del rendimiento. Por lo tanto, el rendimiento de los dispositivos 104 y la red global 103 puede optimizarse en función de la entrada recibida del usuario final a través de su portal del cliente 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 en cada usuario. El portal 118 también proporciona notificaciones y recomendaciones en tiempo real que pueden ser de interés, según el perfil del cliente y la utilización del servicio. Al ampliar el alcance del portal, estas notificaciones también se pueden vincular simplemente a dispositivos móviles para el acceso fuera de línea a las alertas.

El co-controlador SDN 105 instalado puede utilizar los datos de configuración actualizados para modificar la configuración operativa de los dispositivos de red 104. Por ejemplo, la configuración operativa de los dispositivos de red se modifica para aumentar el parámetro de calidad del servicio. Los ajustes operativos de los dispositivos de red pueden actualizarse en tiempo real mientras los dispositivos 105 están en línea. Alternativamente, la configuración operativa de los dispositivos de red 105 puede actualizarse mientras los dispositivos 105 están en modo de suspensión. En una disposición ejemplar, la configuración operativa de los dispositivos de red 105 se actualiza cambiando a un canal de comunicación alternativo para evitar la interferencia de los dispositivos vecinos. El canal de comunicación puede ser un canal Wi-Fi, por ejemplo. En otro ejemplo, la configuración operativa del dispositivo de red se puede cambiar para reducir el consumo de energía de los dispositivos 105. De esta forma, la configuración operativa del dispositivo de red 105 se cambia mediante la reprogramación de una interfaz de alimentación. En otro ejemplo, la configuración operativa del dispositivo de red 105 se puede cambiar para aumentar la prioridad al ancho de banda disponible o disminuir la prioridad al ancho de banda disponible. Se prevé que los co-controladores SDN 105 se pueden configurar para asignar un ajuste de primera 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. El primer ajuste de prioridad puede estar asociado con un primer límite de ancho de banda, y el segundo ajuste de prioridad puede estar asociado con un segundo límite de ancho de banda.

El portal del cliente 118 puede procesar datos en tiempo real sobre la utilización de la red, la selección de rendimiento y 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

OpenFlow SDN Orchestrator para permitir el aprovisionamiento de autoservicio bajo demanda y en tiempo real desde la nube al dispositivo 104. La demanda cada vez mayor de los clientes de calidad de servicio, alta disponibilidad, opciones y atención al cliente está colocando el Centro de Operaciones de Red (NOC), con sus herramientas asociadas, procedimientos y recursos bajo una presión abrumadora. Con la migración de los servicios de la oferta a la demanda, nunca se ha prestado tanta atención a la excelencia operativa. Los días de operaciones que se eliminan completamente de la experiencia del cliente se han ido. La migración de estas herramientas al Centro de llamadas para estar a la vanguardia de la Tecnología del cliente está evolucionando a un ritmo acelerado, la SDN desafía las normas de los datos/plano de control integrado, con Cloud y NFV abstrayendo las topologías físicas. Mientras tanto, se espera que las operaciones como mínimo se mantengan al día, pero se mantengan al frente de la curva.

El portal de administración 116 ha sido diseñado para proporcionar un conjunto de herramientas e informes que permiten conocer e intervenir desde la capa física hasta la capa de aplicación. Combine esto con la capacidad de aplicar aplicaciones para detectar y reaccionar dinámicamente a los eventos de la 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 hasta el usuario, una selección de ventanas, que proporcionan el conjunto completo de herramientas e informes de gestión de red (FCAPS) (el modelo y el marco estándar reconocido). También permite la aplicación de reglas automatizadas simples para reconfigurar proactivamente la red 103 y los servicios virtuales, minimizando las interrupciones y los fallos del servicio basados en ciertas condiciones que se recopilan de la red/dispositivos.

Refiriéndose ahora a las figuras 5-7 que ilustran una plataforma SDN ejemplar 200 que también está según 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, paso 220. El nuevo perfil del cliente se crea con un gestor de perfil del cliente 206, paso 221. Un dispositivo de equipo de premisa para el cliente (CPE) 104 se conecta en línea, paso 222. El CPE 104 está habilitado y aislado, paso 223. El CPE 104 es validado por el módulo de autenticación 203, paso 224. El nuevo perfil de cliente se almacena en una base de datos abierta 138, paso 224. El módulo de autenticación 203, paso 225, identifica y autentica al cliente. El controlador de políticas 135 se comunica con un gestor de perfiles de clientes 206, un controlador de recursos 205 y un módulo de orquestación 207 y abstrae una política de configuración para el nuevo cliente, paso 226. Un controlador SDN maestro 102 genera co-controladores distribuidos adecuados 105A-105H y envía los co-controladores distribuidos 105A-105H a los dispositivos CPE 104 asociados con el nuevo cliente, paso 227. El co-controlador SDN 105 se ejemplifica en los CPEs 105A-105H, paso 228. Los co-controladores distribuidos, una vez instalados en los CPEs 104A-104H, se registran con el controlador SDN maestro 102, paso 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 utilizando los co-controladores distribuidos 105A-105, paso 230. Una vez que se han instalado los co-controladores, funcionan como motores de enrutamiento locales en los CPEs 104. La configuración de los CPEs 104A-104H ha finalizado, paso 232. El co-controlador SDN distribuido 105A-105H empuja la analítica sobre sus respectivos CPEs 104A-104H a la base de datos abierta 138 a través del controlador SDN maestro 102. La analítica de clientes de cada CPE 104A-104H son accesibles al cliente desde la base de datos abierta 138 a través de su portal del cliente 118, paso 237. La analítica operativa de cada CPE 104A-104H está accesible al portal de administración 116 desde la base de datos abierta 138, paso 238. El controlador de recursos 236 es operable para enviar datos de recursos a la base de datos abierta, paso 235. Además, el controlador de recursos 236 es operable para enviar datos de política a la base de datos abierta 211, paso 234. Un motor de análisis 205 es operable para analizar los datos en la base de datos 138, y modificar la política y los datos de control para los respectivos CPEs 104. Los datos de política y control modificados se empujan a los co-controladores distribuidos 105 por el controlador SDN maestro 102 con el fin de reconfigurar los ajustes operativos en los CPEs 104 para mejorar el rendimiento de los dispositivos 104. La mejora del rendimiento de los CPEs 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 la salud de los CPEs 104 está siendo monitoreada continuamente por los co-controladores 105, y si se detecta un problema, los co-controladores 105 son capaces de rectificar el problema reconfigurando los CPEs 104 en tiempo real.

Refiriéndonos a la ahora figura 8 que ilustra un diagrama de flujo que muestra pasos ejemplares de la plataforma SDN en operación que también está según la presente enseñanza. El diagrama de flujo de la figura 8 corresponde sustancialmente al diagrama de flujo 7 y los elementos similares se identifican mediante números de referencia similares. La principal diferencia es que los pasos 240-244 de la figura 8 reemplazan los pasos 227-231 de la figura 7, mientras que los pasos restantes son sustancialmente similares. Después de abstraer la política de configuración en el paso 226, las instrucciones de configuración se envían a una organización de la nube, paso 240. La infraestructura de nube se orquesta para servicios de aplicación del portal y de la nube, paso 241. Se inicia una instancia del portal del cliente y se asigna al cliente y al CPE 104, paso 243. Los túneles de comunicación se abren entre el CPE 104 y la instancia de servicio en la nube, paso 243. La analítica se programa y se recopila a partir de los CPEs, paso 244. La operación de los pasos restantes es como se describió anteriormente con referencia a la figura 7.

Refiriéndonos a la figura 9 que ilustra otro diagrama de flujo que muestra pasos ejemplares de la plataforma SDN en operación que también está según la presente enseñanza. El diagrama de flujo de la figura 9 corresponde sustancialmente al diagrama de flujo de la figura 7 y los elementos similares se identifican mediante números de referencia similares. La principal diferencia es que los pasos 250-254 de la figura 9 reemplazan los pasos 227-231 de la figura 7, mientras que los pasos restantes son sustancialmente similares. Después de abstraer la política de configuración en el paso 226, el control primario identifica el CPE 211A-211H, paso 250. El controlador SDN maestro 102 inicia la programación de las funciones del sistema, paso 251. Los componentes funcionales se programan a SOC, paso 252. Los co-controladores 105 actualizan los conjuntos de reglas de reenvío para el CPE 211A-211H respectivo. La analítica necesaria se programa en el CPE211A-211H y se recogen. La operación de los pasos restantes es como se describió anteriormente con referencia a la figura 7.

Refiriéndose a la figura 10 se ilustra otra plataforma SDN 300 que también está según la presente enseñanza. La plataforma SDN 300 es sustancialmente similar a la plataforma SDN 100 y los elementos 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 a un cliente activar un cambio en la política y/o datos de control, paso 310. El cambio de la política y/o los datos de control se implementan en el CPE 104A-104H por los co-controladores 105 de la manera descrita anteriormente. De lo contrario, el funcionamiento de la plataforma SDN 300 funciona de manera similar a la SDN 100.

Refiriéndose a la figura 11 se ilustra otra plataforma SDN 400 que también está según la presente enseñanza. La plataforma SDN 400 es sustancialmente similar a la plataforma SDN 100 y los elementos 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 datos de control, paso 410. El cambio de la política y/o los datos de control se implementan en el CPE 104A-104H por los co-controladores 105 de la manera descrita anteriormente. De lo contrario, el funcionamiento de la plataforma SDN 400 funciona de manera similar a la SDN 100.

Refiriéndose a la figura 12 se ilustra otra plataforma SDN 500 que también está según la presente enseñanza. La plataforma SDN 500 es sustancialmente similar a la plataforma SDN 100 y los elementos similares se indican mediante números de referencia similares. La principal diferencia es que los co-controladores 105 se distribuyen a los CPEs 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 manera similar a la SDN 100.

Refiriéndonos a la figura 13 que ilustra otro diagrama de flujo que muestra pasos ejemplares de la plataforma SDN en operación que también está según la presente enseñanza. El diagrama de flujo de la figura 13 corresponde sustancialmente al 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 la analítica almacenada en la base de datos 138 que han sido recopilados de los CPEs 104 por los co-controladores 105. El motor de análisis es operable para detectar problemas de rendimiento de Wi-Fi en la red doméstica de un cliente, paso 610. Una aplicación de control Wi-Fi está en comunicación con el motor de análisis y es operable para interpretar la salida del motor de análisis. En este ejemplo, la aplicación de control de Wi-Fi identifica un solapamiento de canal Wi-Fi con los vecinos y activa un cambio en la configuración de Wi-Fi en el hogar del cliente en un momento adecuado al modificar los datos de la política/configuración para el cliente, paso 620. El motor de control de políticas 135 extrae datos de configuración para un cambio de canal Wi-Fi, paso 226. El cambio de configuración se implementa en el enrutador Wi-Fi por los co-controladores apropiados 105 de la manera descrita anteriormente. En este ejemplo, la plataforma SDN actualiza sin problemas el canal Wi-Fi sin requerir ninguna entrada por parte del usuario. Los pasos restantes son similares a los descritos anteriormente con referencia a la figura 9.

Refiriéndonos a la figura 14 que ilustra otro diagrama de flujo que muestra pasos ejemplares de la plataforma SDN en operación que también está según la presente enseñanza. El diagrama de flujo de la figura 14 corresponde sustancialmente al 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 la analítica almacenada en la base de datos 138 que han sido recopilados de los CPEs 104 por los co-controladores 105. El motor de análisis 205 es operable para detectar servicios de prioridad seleccionados activados desde una red doméstica a través del Wi-Fi doméstico general, paso 710. El servicio de prioridad seleccionado puede asignar un límite de ancho de banda más alto a ciertos dispositivos sobre otros dispositivos. Una aplicación de control Wi-Fi está en comunicación con el motor de análisis y es operable para interpretar la salida del motor de análisis 205. En este ejemplo, la aplicación de control de Wi-Fi activa cambios en la calidad del servicio a la configuración de Wi-Fi en el hogar del cliente modificando los datos de la política/configuración para el cliente, paso 720. El motor de control de políticas 135 extrae datos de configuración para un cambio de QoS, paso 226. El controlador maestro 102 identifica el CPE 104 apropiado que requiere la reconfiguración en vista del cambio de QoS, paso 250. El cambio de configuración se implementa en el CPE apropiado 104 por los co-controladores apropiados 105 de la manera descrita anteriormente. Los pasos restantes

son similares a los descritos anteriormente con referencia a la figura 9.

Refiriéndonos a la figura 15 que ilustra otro diagrama de flujo que muestra pasos ejemplares de la plataforma SDN en operación que también está según la presente enseñanza. El diagrama de flujo de la figura 15 corresponde sustancialmente al 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 la analítica almacenada en la base de datos 138 que han sido recopilados de los CPEs 104 por los co-controladores 105. El motor de análisis 205 es operable para detectar que el rendimiento de la tasa de error de modulación (MER) de fin 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 es operable para interpretar la salida del motor de análisis 205. En este ejemplo, la aplicación de gestión de DOCSIS identifica que la reducción de potencia es factible reprogramando una interfaz de potencia de los CPEs 104. El motor de control de políticas 135 extrae datos de configuración para implementar la reducción en potencia, paso 226. El controlador maestro 102 identifica el amplificador apropiado 104 que requiere la reprogramación para implementar la reducción de potencia. El cambio de configuración se implementa en el amplificador apropiado por los co-controladores apropiados 105 de la manera descrita anteriormente. Los pasos restantes son similares a los descritos anteriormente con referencia a la figura 9.

Una arquitectura ejemplar 1000 según la presente enseñanza se ilustra en las figuras 16A-B, 17 y 18. La arquitectura 1000 permite abordar las amenazas de seguridad y las violaciones de privacidad al aprovechar la programabilidad del control de flujo en dispositivos SDN para identificar y no reenviar el tráfico identificado que contiene amenazas o violaciones de privacidad. El reenvío basado en flujo está programado en el dispositivo del usuario final 104 para limitar el reenvío del tráfico de amenazas o el tráfico de violación de la privacidad. Las figuras 16A-17 incluyen muchos componentes similares descritos previamente con las figuras de referencia 3-5 y los elementos similares se indican con referencias numéricas similares. Estos elementos similares funcionan de 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 es operable para generar datos de enrutamiento para los dispositivos de red 104. El controlador SDN maestro 102 está configurado para generar una pluralidad de co-controladores discretos 105 cada uno asociado con un usuario final particular. Cada co-controlador SDN 105 incluye datos de enrutamiento para un dispositivo asociado en red 104. El controlador SDN maestro 102 envía el co-controlador SDN 105 a los dispositivos de red 104 asociados con los respectivos usuarios finales para el control del mismo. Los dispositivos de red 104 pueden solicitar acceso a un destino en la red SDN, por ejemplo, un localizador de recursos uniforme (URL). En respuesta, un sistema de nombres de dominio (DNS) 1035 inicia una interacción con el dispositivo de red solicitante 104. El DNS 1035 transmite los datos del DNS asociados con el URL solicitado a un sistema de control de gestión de amenazas (TMCS) 1010. El TMCS 1010 está configurado para determinar si el URL solicitado tiene un criterio de seguridad asociado. El TMCS 1010 comunica el estado de amenaza al co-controlador de SDN 105 asociado con el dispositivo 104 en red solicitante. El co-controlador de SDN 105 es operable para generar datos de enrutamiento para el dispositivo de red solicitante 104 donde se instala en función del estado de amenaza para permitir o denegar el acceso al URL solicitado.

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 se clasifican como que tienen asociados criterios de amenazas maliciosas. El PVIDB 1030 almacena detalles de destinos que se clasifican como que tienen asociados amenazas de privacidad. Por ejemplo, se sabe que tales destinos recopilan datos privados de usuarios sin el conocimiento del usuario. 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 es operativo para garantizar que los usuarios no se conecten a destinos maliciosos. Por ejemplo, los destinos maliciosos pueden incluir sitios web sospechosas, redes de distribución de contenido (CDN), direcciones IP de sitio web y CDN, dominios, URL, etc. El TMCS 1010 permite la aceptación y las entradas de una consulta de DNS donde, a continuación, verifica y valida al usuario y aplica las reglas de asociado con un perfil de usuario. Una vez que el TIDB 1020 ha sido consultado para una ruta en particular y el perfil de usuario validado contra esto, el TMCS 1010 comunicado con la base de datos del sistema de orquestación SDN 138. El controlador SDN maestro 102 propaga, a continuación, un mensaje al co-controlador SDN 105 en el CPE 104 con los datos de enrutamiento apropiados para el dispositivo solicitante 104. Un módulo de coincidencia de seguridad SDN 1025 dentro del dispositivo 104 valida si la ruta se va a aplicar. Si se va a aplicar, el co-controlador SDN 105 inserta una entrada de reenvío en la tabla de reenvíos; 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 amenazas y/o violaciones de privacidad al portal del cliente 118 y/o al portal de administración 116.

El TIDB 1020 puede ser una base de datos de una compañía privada de seguridad de Internet que almacena datos en sitios web, CDN, sitio web y dirección de IP CDN, dominios, URL, etc. peligrosos y sospechosos. Estos datos son recopilados por varias compañías y organizaciones de todo el mundo sobre amenazas conocidas relacionadas con temas de seguridad con la lucha contra el phishing, el malware y el control de dominios, etc. Estas bases de datos ya

están siendo utilizadas por agencias de seguridad del gobierno, firmas de servicios financieros y comercio electrónico, compañías de tecnología, redes sociales y proveedores de servicios de Internet (ISPs) para ayudarse a sí mismos en el luchar contra los ataques.

La función del PVIDB 1030 es almacenar datos en compañías de Internet que utilizan sus aplicaciones para recopilar datos privados de los usuarios una vez que las aplicaciones están instaladas en los dispositivos de usuario final 104. Esto es específicamente relevante cuando un servicio o producto de Internet que está siendo suministrado por una compañía de Internet no cumple con las regulaciones locales para los países individuales en la recopilación de datos de un abonado. 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 las violaciones de privacidad de las compañías que no cumplan con ciertos criterios, por ejemplo, las expectativas de decencia y las regulaciones locales al bloquear todo el tráfico del abonado de la plataforma 1000 a sus sistemas en una base de flujo. El PVIDB 1030 permite a los suscriptores decidir qué datos desean enviar a Internet en lugar de que las partes en la red decidan por sí mismos qué tomarán, independientemente de si el cliente tiene conocimiento o no.

La arquitectura 1000 utiliza una capa de control altamente resistente 107 que facilita la distribución del control a través de una federación de co-controladores de SDN distribuidos 105. Cada cliente puede seleccionar una política de seguridad y/o privacidad seleccionando las opciones de configuración a través del portal del cliente 118 que, a continuación, se transmite mediante una API 120 o el SDK 122 a través del plano de control 107, donde el usuario es autenticado por primera vez por el módulo de autenticación 203 antes de que el controlador de políticas 135 aplique una política para direcciones IP y 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 co-controladores de SDN distribuidos 105 que están instalados en los dispositivos 104.

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

La recepción del mensaje del DNS 1035 hace que el TMCS 1010 consulte el PVIDB 1030 y/o el TIDB 1020 (o caché) para identificar si el URL contenido en el mensaje tiene un estado de amenaza/privacidad asociado con él, paso 503. El TMCS 1030 también puede solicitar la clasificación de identidad del abonado para validar la clasificación del perfil de usuario, paso 504. Al recibir una respuesta del TIDB 1020 y del PVIDB 1030 (identificación y clasificación del usuario) y (clasificación de seguridad/privacidad), el paso 503, el TMCS 1010 envía al co-controlador SDN 105 el estado de amenaza del URL y la clasificación del cliente, paso 505. La tabla 1 y la tabla 2 definen definiciones ejemplares de los identificadores de usuario y de clasificación de riesgo que pueden transmitirse entre los distintos 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 proporcionan solo a modo de ejemplo y no pretende limitar la enseñanza actual a los valores ejemplares proporcionados.

Tabla 1: Amenaza Ejemplar/Clasificación de Violación de Privacidad

Tipo de riesgo	Definición	Tipo de tráfico	Clasificación
Infección	Virus	Tráfico generado por virus saliente	#A
Usuario bajo ataque	ODDS, Botnet, escaneo de puertos	Tráfico DOS entrante	#B
Robo de datos de usuario	Adware, malware, etc.	Tráfico saliente	#C
Usuario iniciando ataque	DDOS, escaneo de puertos, Botnet	Tráfico DOS saliente (el usuario que se une a la Botnet debido a una infección)	#D
Violación de privacidad	Adware, malware, etc.	Tráfico saliente	#E
Sitio web tóxico	Sitio web identificado por	Tráfico entrante	#F

Tipo de riesgo	Definición	Tipo de tráfico	Clasificación
	TIDB como arriesgado		
CDN tóxico	CDN identificado por TIDB como arriesgado	Tráfico entrante	#G
Sitio web phished	Sitio web identificado como secuestrado	Usuario que intenta acceder a sitios web que han sido secuestrados	#H
Infraestructura bajo ataque	Dispositivo de operador bajo ataque	Tráfico entrante	#J
Tráfico de violación de privacidad	Destino identificado para el tráfico de compañías invasivo	Tráfico saliente	#K

Tabla 2: Clasificaciones de perfiles de usuarios ejemplares

Clasificación del perfil de usuario	Acción	Clasificaciones de flujo
Acceso muy limitado a Internet según la lista blanca generada por TIDB	TMCS aplica el perfil 1	#1
Acceso de Internet medio según lista blanca generada por TIDB	TMCS aplica el perfil 2	#2
Dominios TOD definidos por el usuario para ser bloqueados	TMCS aplica el perfil 2 con TOD	#3
Adulto con protección de seguridad	TMCS aplica el perfil 4	#4
Sin protección, completamente abierto	TMCS aplica el perfil 5	#5
Permitido para comunicarse solo con usuarios autenticados	TMCS aplica el perfil 2+biocking de solicitantes de comunicaciones aprobados por callson entrantes (uno para que discutamos con SKYPE)	#6
Bloqueo de túnel	TMCS aplica perfil X + perfil 7	#7
Violación de privacidad	TMCS aplica el perfil 8	#8

El co-controlador SDN 105 tiene un módulo de coincidencia de seguridad 1025 que es operable para definir la decisión de reenvío apropiada en el dispositivo 104 para el perfil de usuario que depende de la clasificación de riesgo, paso 506. La decisión de reenvío puede ser enviar el tráfico a un destino de cuarentena (con agujero negro) o permitir que el tráfico se reenvíe al destino según lo solicite el usuario. El co-controlador SDN 105 establece entonces una entrada de reenvío en la tabla de enrutamiento de flujo 119, paso 507, contra la dirección IP del abonado solicitante que depende de la información recibida desde el paso 506. Si el URL se indica como un sitio de riesgo, el TMCS 1010 genera un informe, paso 508, que se introduce en la base de datos abierta 138, a la que el cliente puede acceder a través del cliente 118. El informe puede ser señalizado 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 utiliza la dirección IP del abonado para asignar el informe de alerta de seguridad al registro del cliente. Luego, estos datos se importan al portal del cliente relevante 118 para indicar un resumen de las acciones de seguridad / privacidad necesarias que se pueden 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, paso 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 utiliza la dirección IP del abonado para asignar el informe de alerta de seguridad al registro del cliente. Además, el informe detallado puede identificar el riesgo, describir los efectos del riesgo y qué medidas deben tomarse para abordarlo.

El portal de administración 116 es operable para calcular informes regulares de seguridad/privacidad mediante la ejecución de consultas contra la base de datos abierta 138, paso 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 personas con promociones que están gravemente infectadas. Para el ISP, se puede utilizar una promoción de ventas para que un cliente limpie sus sistemas, por lo tanto, elimina la carga innecesaria de la red y crea una tendencia de mercadotecnia acerca de que el ISP sea un proveedor de red seguro.

Un flujo de trabajo ejemplar según la presente enseñanza se ilustra en las figuras 20A y 20B. El cliente identifica la política para cada 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 por primera vez y, a continuación, se aplica una política, bloque 1053. Para que esta política se aplique, los datos se extraen, por ejemplo, la dirección IP y la ID del dispositivo, la política de seguridad o privacidad elegida por el cliente a través del portal del cliente 118 desde la base de datos abierta 138. También se extrae de la base de datos abierta 138 una lista de sitios bien conocidos y comúnmente utilizados por el cliente. Estas entradas de reenvío están agrupadas, bloque 1055 y clasificadas, bloque 1058, antes de ser comunicadas desde el controlador SDN maestro 102 al co-controlador SDN 105, bloque 1060. El módulo de coincidencia de seguridad SDN 1025 coincide con la privacidad y las amenazas, bloque 1062. El módulo de coincidencia de seguridad 1025 compara el identificador del perfil del cliente en la tabla de clasificación de flujos de usuarios 1065 con el riesgo y, a continuación, 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 amenaza según los ejemplos identificados en la tabla 1. La tabla de clasificación de flujo de usuario1070 almacena la clasificación de perfil de usuario según los ejemplos identificados en la tabla 2.

Refiriéndose a las figuras 21A y 21B se ilustra otra plataforma SDN 1200 que también está según 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 el TMCS 1010, el TIDB 1020 y el 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 en el bloque 1205 de la política de amenazas o privacidad que se aplica a los ajustes utilizados para proteger su hogar/negocio. La figura 21A y 21B ilustra que una solución de plano de control orquestado pueda ofrecer un cambio de política para permitir un cambio de política de seguridad o privacidad. En este ejemplo, se puede desencadenar un cambio de este tipo desde el portal de administración 116 para proteger los dispositivos domésticos/IOT a través de redes de acceso que operan en una variedad de tecnologías de acceso diferentes. Cuando se configura el co-controlador SDN ligero 105 en las políticas de seguridad y privacidad del dispositivo IOT, se pueden aplicar directamente a estos dispositivos.

Este procedimiento permite a los operadores de red controlar y orquestar entornos de red mediante el uso de co-controladores de SDN orquestados y distribuidos 105 que operan tanto para entornos de clientes ON-Net como OFF-Net. Al reducir la necesidad de que el CPE sea multipropósito y barato, esto permite que el operador se concentre en adquirir un CPE que ofrezca el reenvío y el control de paquetes premium. Al habilitar la verificación contra múltiples TIDB 1020 / PVIDB 1030 de terceros, esto garantiza un mayor conocimiento de las amenazas y las violaciones de la privacidad lo antes posible. Dado que 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 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 consistente en todos los dispositivos de las instalaciones del cliente. Este enfoque de seguridad es particularmente relevante para IOT, ya que permite el control en la nube de todos los datos provenientes de las instalaciones del cliente. Se pueden crear reglas específicas de reenvío basadas en el flujo para todos los sistemas IOT, por lo tanto, se garantiza que incluso si estos dispositivos son pirateados, el co-controlador SDN ligero 105 no reenvía el tráfico a ningún otro sistema. Esto proporciona control y mejora la protección del usuario final frente a la intención maliciosa de algunas organizaciones y personas. Ayuda al consumidor a lidiar con la complejidad de los problemas de seguridad y privacidad creados en Internet y permite que se creen amplias actualizaciones de políticas de difusión cuando se identifiquen y actualicen nuevos vectores de ataque en los TIDB 1020 y PVIDB 1030.

Refiriéndonos a la figura 22 que ilustra otro diagrama de flujo que muestra pasos ejemplares de la plataforma SDN en operación que también está según la presente enseñanza. El diagrama de flujo de la figura 22 corresponde sustancialmente al 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 en el ajuste de la política de amenazas o privacidad desde el portal del cliente 118, paso 1305. El usuario proporciona detalles de autenticación a través del portal del cliente 118, paso 1308. El usuario es autenticado por el módulo de autenticación, paso 1310. El controlador de políticas 135 abstrae los datos de configuración para el cambio de política de amenazas/privacidad, paso 1312. El controlador SDN maestro 102 identifica el dispositivo apropiado 104, paso 1214. El controlador SDN maestro 102 señala la programación del cambio de la política de amenaza/privacidad al co-controlador SDN 105, paso 1316. Las clasificaciones de riesgo/privacidad se programan en el SOC en el CPE 104 para la política del cliente por el co-controlador 105 de SDN, paso 1318. El controlador SDN maestro 102 actualiza los conjuntos de reglas de reenvío, paso 1320. El módulo de coincidencia de seguridad 1025 procesa las reglas establecidas para los flujos ya existentes al consultar el TIDB 1020 y/o PVIDB 1030, paso 1322. El módulo de coincidencia de seguridad 1025 consulta el TMCS 1010 consultado contra TIDB/PVIDB para obtener direcciones de riesgo, paso 1323. El controlador SDN maestro 102 coopera con el co-controlador SDN 105 para programar un módulo de recopilación de análisis en el CPE 104, paso 1324. El co-controlador SDN lleva la analítica a la base de datos abierta 138, paso 233. Los pasos restantes son similares a los descritos anteriormente con referencia a la figura 9.

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 consultas de reenvío de un cliente se procesen fuera de línea según las reglas de privacidad/seguridad definidas en el ajuste del cliente, utilizando el TMCS 1010. Esto descarga el procesamiento de aplicaciones de seguridad desde el dispositivo final 104 y reduce la carga de procesamiento en el CPE 104 de múltiples extremos. Además, esto reduce la necesidad de ejecutar aplicaciones de seguridad en el CPE 104, lo que reduce los costes. Además, como ya no se requiere que las aplicaciones de seguridad se carguen en el CPE 104, esto reduce los recursos de procesamiento y memoria requeridos por el CPE 104.

Cuando la solución de CPE controlada por SDN orquesta un entorno residencial, esto permite que los controles se apliquen contra un usuario de forma granular para garantizar que los controles se puedan aplicar rápidamente sin la necesidad de primero volver a escribir el software y enviar actualizaciones y parches a sistemas individuales. Un ejemplo de un impulso de política de este tipo es que, cuando se identifica una BotNet como habiendo activado un impulso de política a cualquier CPE que solicite una ruta al destino que está siendo atacado. Esto asegura que el CPE no se una al ataque. Además, el CPE de control SDN orquestado se identifica, a continuación, como infectado con esa BotNet en particular. A continuación, se realiza 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 dice que la aborden. El mismo mecanismo se utiliza para controlar infecciones como adware, malware, etc., donde se encuentran los destinos conocidos en el TMCS 1010.

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

Este procedimiento actual utiliza un co-controlador de SDN ligero y distribuido 105 que puede instalarse en cualquier hardware, ya sea incorporando el controlador SDN de peso ligero dentro del firmware o en un CPE abierto. Esta solución de peso ligero controlada por SDN rompe la naturaleza propietaria del CPE y permite que la solución se aplique y controle a través de las soluciones de CPE de múltiples vendedores. El co-controlador de SDN de peso ligero 105 programa la tabla de reenvío del dispositivo de CPE/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 múltiples o únicas que se ha llenado con detalles de amenazas identificadas. Estas políticas se comunican mediante protocolos estándar abiertos y se establecen dentro de las reglas de reenvío del dispositivo de CPE/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, dependiendo de la escala de la red. Estas reglas de seguridad iniciaron el reenvío y, a continuación, eliminan el tráfico destinado a estos destinos para los dispositivos que deben estar protegidos 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 la ruta central y se puede realizar una verificación en la base de datos de terceros para validar si la ruta se encuentra en un destino no tóxico. Esta podría ser una ruta solicitada a través de DNS u otro enfoque basado en estándares, por ejemplo, ARP para IPv4.

Un experto en la materia apreciaría que los dispositivos finales distribuidos a los consumidores no tienen la capacidad de analizar o almacenar los grandes volúmenes de datos 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 dispositivos restringen la capacidad de las aplicaciones actuales para proteger mejor al

cliente final, dejando así 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 del sistema de control de amenazas múltiples se realiza fuera de línea. Un ejemplo de dónde se pueden procesar las bases de datos o las bases de datos de amenazas es en 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 tupels de datos coincidentes y se establecerán reglas de reenvío que garantizan que el tráfico generado dentro de la casa no se envíe a los destinos en Internet. Además, el sistema de control de amenazas se conectará con múltiples fuentes de amenazas para garantizar que se mantenga actualizado sobre las últimas encarnaciones de amenazas de seguridad que se llevan a cabo en Internet.

Además, cuando se están generando ataques DDOS a un destino conocido en el control basado en el flujo de Internet, se puede utilizar para eliminar granularmente los flujos de ataque del tráfico que atraviesa la red. Hoy en día, los destinos bajo ataque tienden a tener que lidiar con el ataque desconectando el sitio o utilizando un hardware costoso y de alta calidad 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 está sometida a una presión considerable y, en muchos casos, debe retirar la visibilidad de la forma del sitio en Internet para liberarse del ataque.

Las técnicas introducidas aquí pueden incorporarse como hardware de propósito especial (por ejemplo, circuitos), o como circuito programable programado adecuadamente con software y/o firmware, o como una combinación de circuito de propósito especial y programable. Por lo tanto, varias realizaciones pueden incluir un medio legible por máquina que tiene almacenadas en él instrucciones que pueden usarse para programar un ordenador (u otros dispositivos electrónicos) para realizar un procedimiento. El medio legible por máquina puede incluir, entre otros, pero no está limitado a, discos ópticos, memorias de solo lectura de discos compactos (CD-ROMs), y discos magnetoópticos, ROMs, memorias de solo lectura programables borrables (EPROMs), memorias solo de lectura programable y borrable eléctricamente (EEPROMs), tarjetas magnéticas u ópticas, memoria flash, unidades de estado sólido (SSD)s u otro tipo de medio/medio legible por máquina adecuado para almacenar instrucciones electrónicas.

Se entenderá que lo que se ha descrito aquí es un sistema ejemplar para controlar una red SDN. Si bien la presente enseñanza se ha descrito con referencia a disposiciones ejemplares, se entenderá que no se pretende limitar la enseñanza a tales disposiciones, ya que se pueden hacer modificaciones sin apartarse del espíritu y el alcance de la presente enseñanza.

Se entenderá que, aunque se han descrito características ejemplares de un sistema según la presente enseñanza, tal disposición no debe interpretarse como limitante 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 se ejecuta en uno o más ordenador(es) digitales de propósito general o especial, como un ordenador personal (PC; IBM compatible, Apple compatible o de lo contrario), asistente digital personal, estación de trabajo, miniordenador u ordenador central. Los pasos del procedimiento pueden implementarse con un servidor u ordenador donde los módulos de software residen o residen parcialmente.

Generalmente, en términos de arquitectura de hardware, tal ordenador incluirá, como será bien entendido por el experto en la materia, un procesador, una 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 limitado 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, buffers (cachés), controladores, repetidores y receptores, para habilitar las comunicaciones. Además, la interfaz local puede incluir dirección, control y/o conexiones de datos para activar las comunicaciones apropiadas entre los otros componentes del ordenador.

El(los) procesador(es) puede(n) programarse para realizar las funciones del procedimiento para controlar una red SDN. El(Los) procesador(es) es un dispositivo de hardware para ejecutar el software, en particular el software almacenado en la memoria. El(los) procesador(es) puede(n) ser cualquier procesador hecho a medida o disponible comercialmente, una unidad de procesamiento primario (CPU), un procesador auxiliar entre varios procesadores asociados con un ordenador, un microprocesador basado en semiconductores (en forma de microchip o conjunto de chips), un macro-procesador o generalmente cualquier dispositivo para ejecutar instrucciones de software.

La memoria está asociada con el procesador(es) y puede incluir uno cualquiera 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 volátiles (por ejemplo, ROM, disco duro, cinta, CDROM, etc.). Además, pueden incorporarse medios de almacenamiento electrónicos, magnéticos, ópticos, y/o de otros tipos. La memoria puede tener una arquitectura distribuida, donde varios componentes se encuentran alejados entre sí pero aún se acceden por el procesador(es).

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

La presente divulgación puede incluir componentes proporcionados como un programa fuente, un programa ejecutable (código de objeto), un script o cualquier otra entidad que comprenda un conjunto de instrucciones a realizar. Cuando se trata de un programa fuente, el programa debe traducirse a través de un compilador, ensamblador, intérprete o similar, que puede o no estar incluido en la memoria, para que funcione correctamente en conexión con el O/S. Además, una metodología implementada según la enseñanza puede expresarse como (a) un lenguaje de programación orientado a objetos, que tiene clases de datos y procedimientos, o (b) un lenguaje de programación de procedimientos, 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 procedimiento se implementa en un software, se debería tener en cuenta que dicho software puede almacenarse en cualquier medio legible por ordenador para su uso o en conexión con cualquier sistema o procedimiento relacionado con el ordenador. En el contexto de esta enseñanza, un medio legible por ordenador es un dispositivo electrónico, magnético, óptico u otro dispositivo físico o medio que puede contener o almacenar un programa de ordenador para ser usado por o en conexión con un sistema o procedimiento relacionado con el ordenador. Dicha disposición se puede realizar en cualquier medio legible por ordenador para su uso por o en conexión con un sistema, aparato o dispositivo de ejecución de instrucciones, como un sistema basado en ordenador, un sistema que contenga un procesador u otro sistema que pueda obtener las instrucciones desde el sistema, aparato o dispositivo de ejecución de instrucciones y ejecute las instrucciones. En el contexto de esta divulgación, 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, debería entenderse como representación de módulos, segmentos o porciones de código que incluyen una o más instrucciones ejecutables para implementar funciones lógicas específicas o pasos en el procedimiento, como entenderán los que tienen experiencia ordinaria 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. Si bien los ejemplos específicos para 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, mientras que los procedimientos y los 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 procedimientos o bloques se pueden eliminar, suplementar, añadir, mover, separar, combinar y/o modificar para proporcionar diferentes combinaciones o sub-combinaciones. Cada uno de estos procedimientos o bloques puede implementarse en una variedad de formas alternativas. Además, mientras que los procedimientos o bloques se muestran a veces como realizados en secuencia, estos procedimientos o bloques pueden realizarse o implementarse en paralelo o pueden realizarse en diferentes momentos. Los resultados de los procedimientos o bloques también se pueden mantener 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 como limitantes de la divulgación a los ejemplos específicos divulgados en la especificación, a menos que la descripción detallada anterior defina explícitamente dichos términos. Por consiguiente, el alcance real de la divulgación abarca no solo los ejemplos divulgados, sino también todas las formas equivalentes de practicar o implementar la divulgación según las reivindicaciones.

De lo que antecede, se apreciará que las realizaciones específicas de la divulgación se han descrito aquí con fines ilustrativos, pero que pueden realizarse diversas modificaciones sin desviarse del espíritu y alcance de la divulgación. En consecuencia, la divulgación no está limitada.

REIVINDICACIONES

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

proporcionar uno o más portales de clientes (118) que están configurados para facilitar a los usuarios el control de dispositivos de red (104);

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

proporcionar un controlador SDN maestro (102) para gestionar el control de flujo de datos en la red SDN (103); el controlador SDN maestro (102) es operable para generar datos de enrutamiento para los dispositivos de red (104);

generar por el controlador SDN maestro (102) una pluralidad de co-controladores discretos (105), cada uno asociado con un usuario final particular; cada co-controlador SDN (105), incluyendo datos de configuración y datos de enrutamiento para un dispositivo de red asociado (104);

enviar el co-controlador SDN (105) por el controlador SDN maestro (102) a los dispositivos de red (104) asociados con los usuarios finales respectivos para el control del mismo;

instalar los co-controladores SDN (105) en los dispositivos de red (104); y

registrar los co-controladores SDN instalados (105) con el controlador SDN maestro (102) para controlar el enrutamiento de datos desde los dispositivos de red (104) y para controlar la configuración de los dispositivos de red (104).

2. Un procedimiento según la reivindicación 1, que comprende además extraer datos analíticos mediante los co-controladores SDN instalados (105) de los dispositivos de red (104).

3. El procedimiento de la reivindicación 1, que además comprende enrutar los datos analíticos extraídos a un repositorio primario; o enrutar los datos analíticos extraídos a un repositorio primario; y donde los datos analíticos extraídos son enrutados por los co-controladores SDN (105) al repositorio primario a través del controlador maestro SDN (102).

4. El procedimiento de la reivindicación 3, que además comprende proporcionar un motor de análisis en comunicación con el repositorio primario que se puede operar para analizar los análisis extraídos para generar un resultado de análisis; o proporcionar un motor de análisis en comunicación con el repositorio primario que se puede operar para analizar los análisis extraídos para generar un resultado de análisis; y donde la salida analítica es accesible a través de los portales del cliente (118).

5. Un procedimiento de reivindicación 4, donde una o más opciones de mejora del rendimiento son puesto a disposición al usuario final a través de los portales del cliente para la selección basada en función de la salida de la analítica; o puesto a disposición del usuario final a través de los portales del cliente para la selección en función de la salida de la analítica; y donde los datos de configuración se actualizan en respuesta al usuario final que selecciona una o más opciones de mejora del rendimiento.

6. Un procedimiento de cualquiera de las reivindicaciones 5, que comprende además actualizar el co-controlador SDN instalado (105) con los datos de configuración actualizados para modificar la configuración operativa de los dispositivos de red (104).

7. Un procedimiento de la reivindicación 6, donde la configuración operativa de los dispositivos de red (104) se modifican para aumentar un parámetro de calidad de servicio; o se actualizan en tiempo real mientras están en línea; o actualizado mientras está en un modo de suspensión; o actualizado cambiando a un canal de comunicación alternativo para evitar interferencias con los dispositivos vecinos; y opcionalmente el canal de comunicación incluye un canal Wi-Fi; o cambiado para reducir el consumo de energía; y opcionalmente la configuración de la operación del dispositivo de red se cambia mediante la reprogramación de una interfaz de alimentación, o se cambia para aumentar la prioridad al ancho de banda disponible; o cambiado para disminuir la prioridad al ancho de banda disponible.

8. Un procedimiento de una cualquiera de las reivindicaciones 1 a 7, donde los co-controladores SDN (105) son operables para asignar un ajuste de primera prioridad a un primer conjunto de dispositivos de red y asignar un segundo ajuste de prioridad a un segundo conjunto de dispositivos de red; o asignar un ajuste de primera prioridad a un primer conjunto de dispositivos de red y asignar un segundo ajuste de prioridad a un segundo conjunto de

dispositivos de red; y 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.

9. Un procedimiento de una cualquiera de las reivindicaciones 1 a 8, donde el co-controlador SDN maestro (102) implementa orquestación SDN en respuesta a una solicitud de recursos recibida en los portales de clientes; u orquestación SDN en respuesta a una solicitud de recursos recibida en los portales de clientes; y donde la orquestación SDN incluye coordinar los elementos de hardware y software de red necesarios para admitir las aplicaciones asociadas con la solicitud de recursos; o incluye generar una instancia de una o más aplicaciones en la nube; o genera una instancia de virtualización de la función de red (NFV).

10. Un procedimiento de una cualquiera de las reivindicaciones 1 a 9, que comprende además generar un perfil de usuario para cada usuario final; o autenticar un usuario.

11. Un procedimiento de una cualquiera de las reivindicaciones 1 a 10, donde los co-controladores SDN (105) están instalados en un sistema en un chip de los respectivos dispositivos de red (104); o cargado en el firmware contenido en los dispositivos de red respectivos (104); o desplegable en binario.

12. Un procedimiento de una cualquiera de las reivindicaciones 1 a 11, donde el controlador SDN maestro (102) genera un archivo de configuración para cada recurso seleccionado por el usuario final en el portal del cliente.

13. Un procedimiento de una cualquiera de las reivindicaciones 1 a 12, que comprende además el envío de los co-controladores SDN (105) a una red doméstica para la recopilación de información relacionada con el protocolo de transporte; y opcionalmente; donde, los dispositivos de red son compatibles con, al menos, uno de DOCSIS, FTTx, xDSL y Wi-Fi.

14. Un controlador de red para una red definida por software (SDN), el controlador de red que comprende uno o más módulos operables para:

proporcionar uno o más portales de clientes (118) que están configurados para facilitar a los usuarios el control de dispositivos de 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 (102) para gestionar el control de flujo de datos en la red SDN; el controlador SDN maestro (102) es operable para generar datos de enrutamiento para los dispositivos de red (104);

generar por el controlador SDN maestro (102) una pluralidad de co-controladores distribuidos discretos (105), cada uno asociado con un usuario final particular; cada co-controlador SDN (105), incluyendo datos de configuración y datos de enrutamiento para un dispositivo de red asociado;

enviar el co-controlador SDN (105) por el controlador SDN maestro (102) a los dispositivos de red (104) asociados con los usuarios finales respectivos para el control del mismo;

instalar el co-controlador SDN (105) en los dispositivos de red (104); y

registrar los co-controladores SDN instalados (105) con el controlador SDN maestro (102) para controlar el enrutamiento de datos desde los dispositivos de red (104) y para controlar la configuración de los dispositivos de red (104).

15. Un artículo de fabricación que comprende un medio legible por un procesador que tiene incorporado en él un código de programa ejecutable que cuando se ejecuta mediante el dispositivo de procesamiento hace que el dispositivo de procesamiento realice:

proporcionar uno o más portales de clientes (118) que están configurados para facilitar a los usuarios el control de dispositivos de red (104);

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

proporcionar un controlador SDN maestro (102) para gestionar el control de flujo de datos en la red SDN; el controlador SDN maestro es operable para generar datos de enrutamiento para los dispositivos de red;

generar por el controlador SDN maestro una pluralidad de co-controladores discretos, cada uno asociado con un

usuario final particular; cada co-controlador SDN, incluyendo datos de configuración y datos de enrutamiento para un dispositivo de red asociado;

enviar el co-controlador SDN (105) por el controlador SDN maestro (102) a los dispositivos de red (104) asociados con los usuarios finales respectivos para el control del mismo;

instalar los co-controladores SDN (105) en los dispositivos de red (104); y

registrar los co-controladores SDN instalados (105) con el controlador SDN maestro (102) para controlar el enrutamiento de datos desde los dispositivos de red (104) y para controlar la configuración de los dispositivos de red (104).

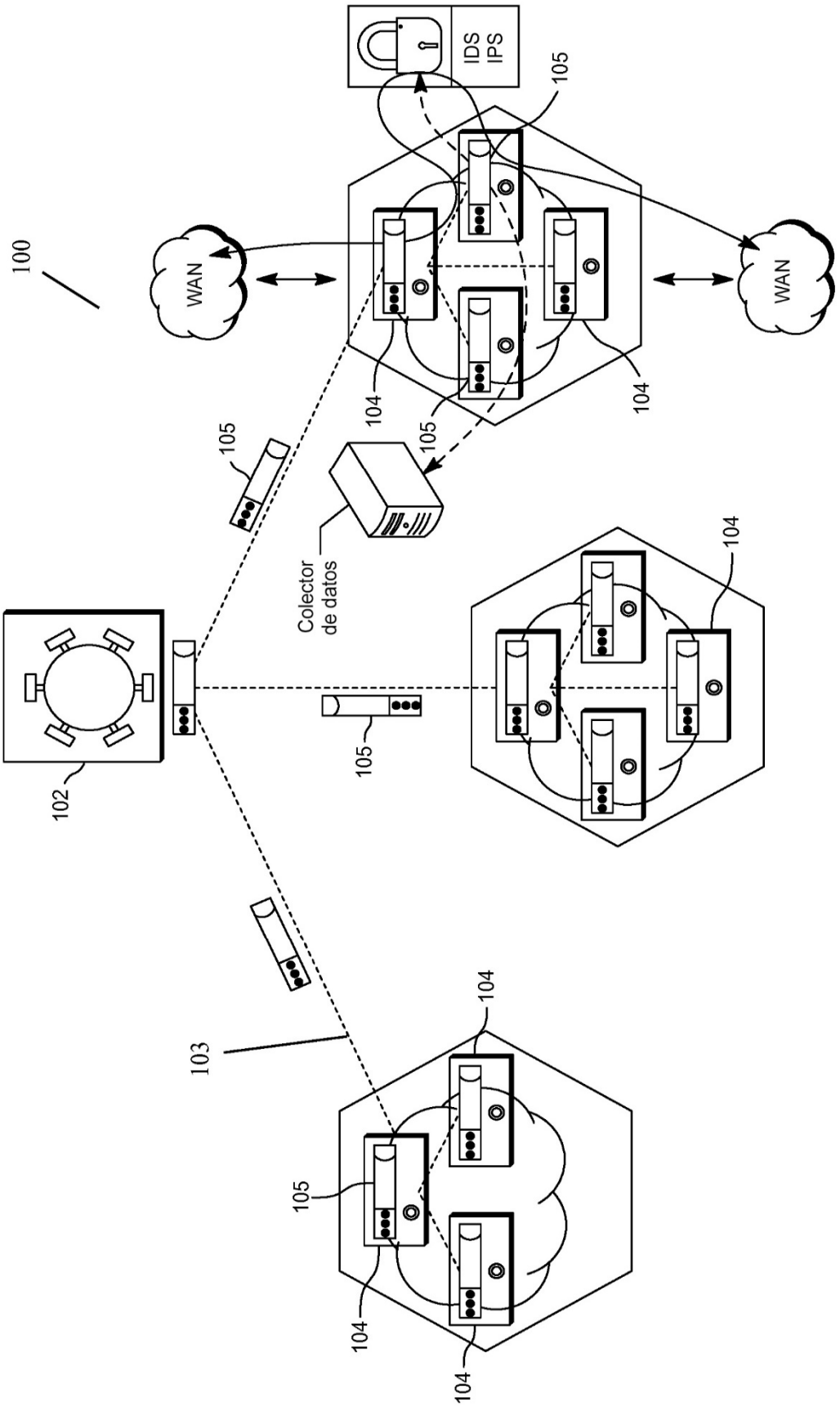

FIG.1

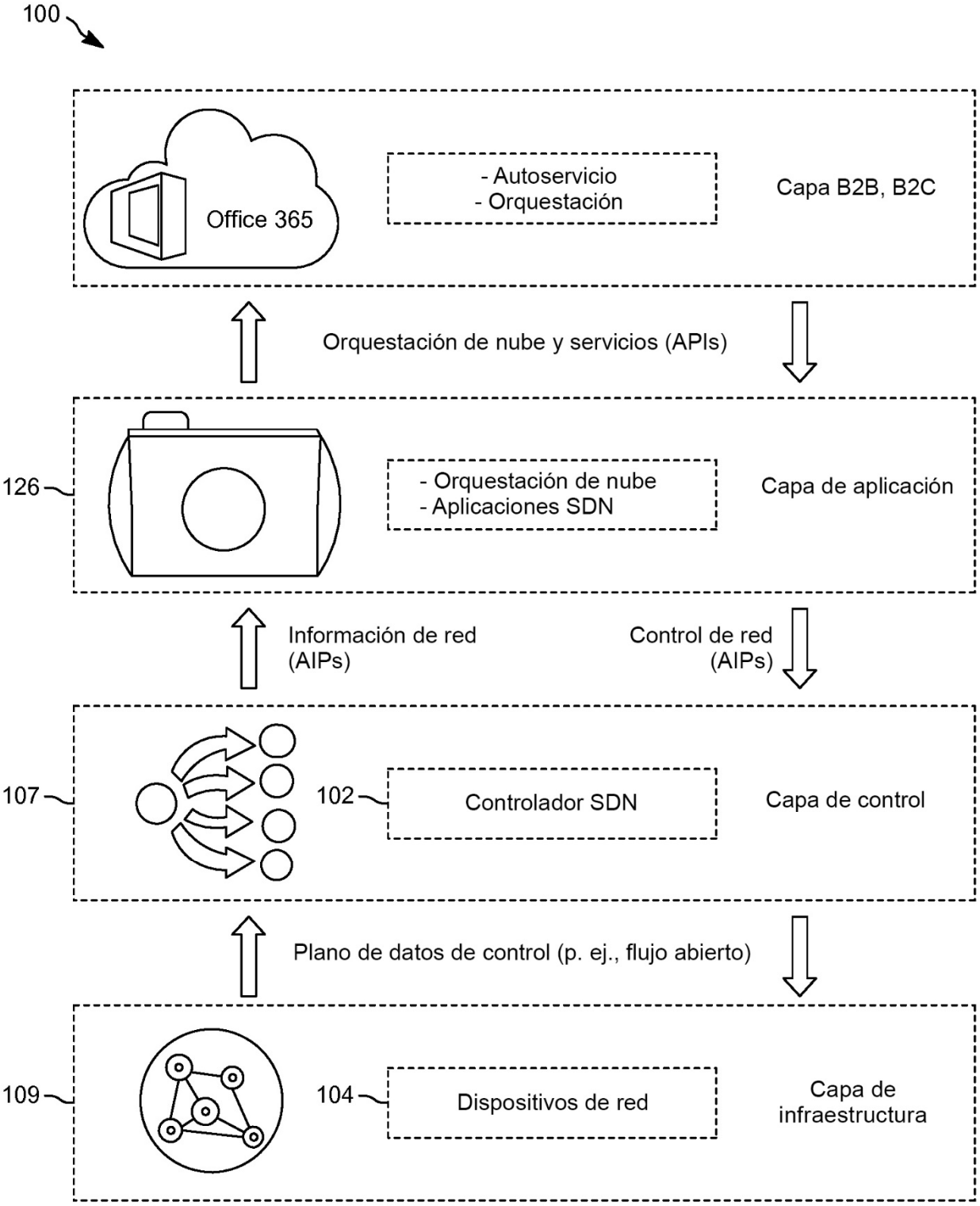
100
Office 365
- Autoservicio
- Orquestación
Capa B2B, B2C
Orquestación de nube y servicios (APIs)
126
- Orquestación de nube
- Aplicaciones SDN
Capa de aplicación
Información de red
(AIPs)
Control de red
(AIPs)
107
102
Controlador SDN
Capa de control
Plano de datos de control (p. ej., flujo abierto)
109
104
Dispositivos de red
Capa de
infraestructura

FIG. 2

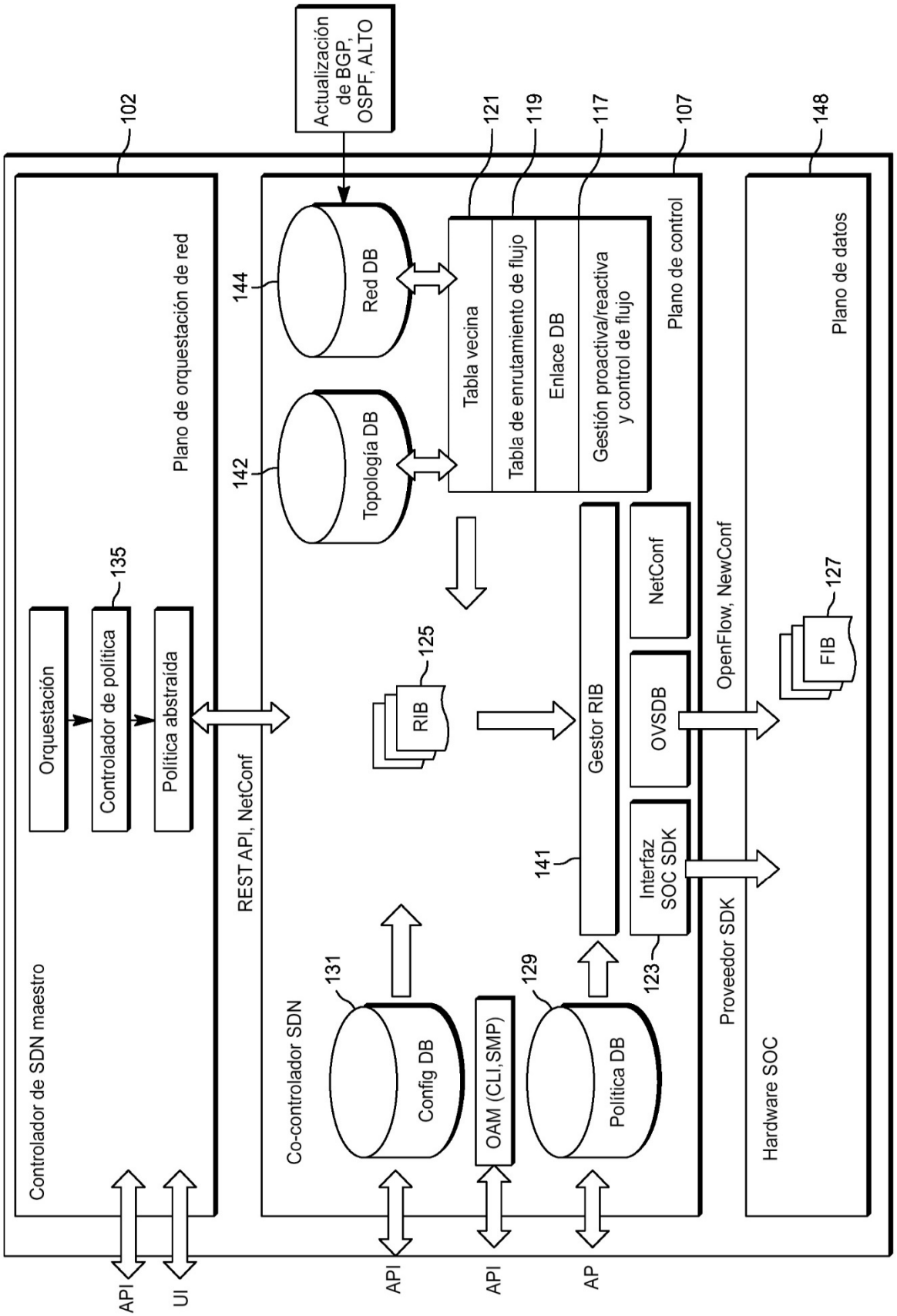
Actualización de BGP, OSPF, ALTO
102
121
119
117
107
148
Controlador de SDN maestro
Plano de orquestación de red
Orquestación
135
Controlador de política
Política abstraída
REST API, NetConf
Co-controlador SDN
144
Red DB
142
Topología DB
Tabla vecina
Tabla de enrutamiento de flujo
Enlace DB
Gestión proactiva/reactiva y control de flujo
Plano de control
Plano de datos
RIB
125
Gestor RIB
NetConf
OVSDB
OpenFlow, NewConf
FIB
127
141
Interfaz SOC SDK
123
Proveedor SDK
Hardware SOC
131
Config DB
OAM (CLI,SMP)
129
Política DB
API
UI
API
API
AP

FIG. 3

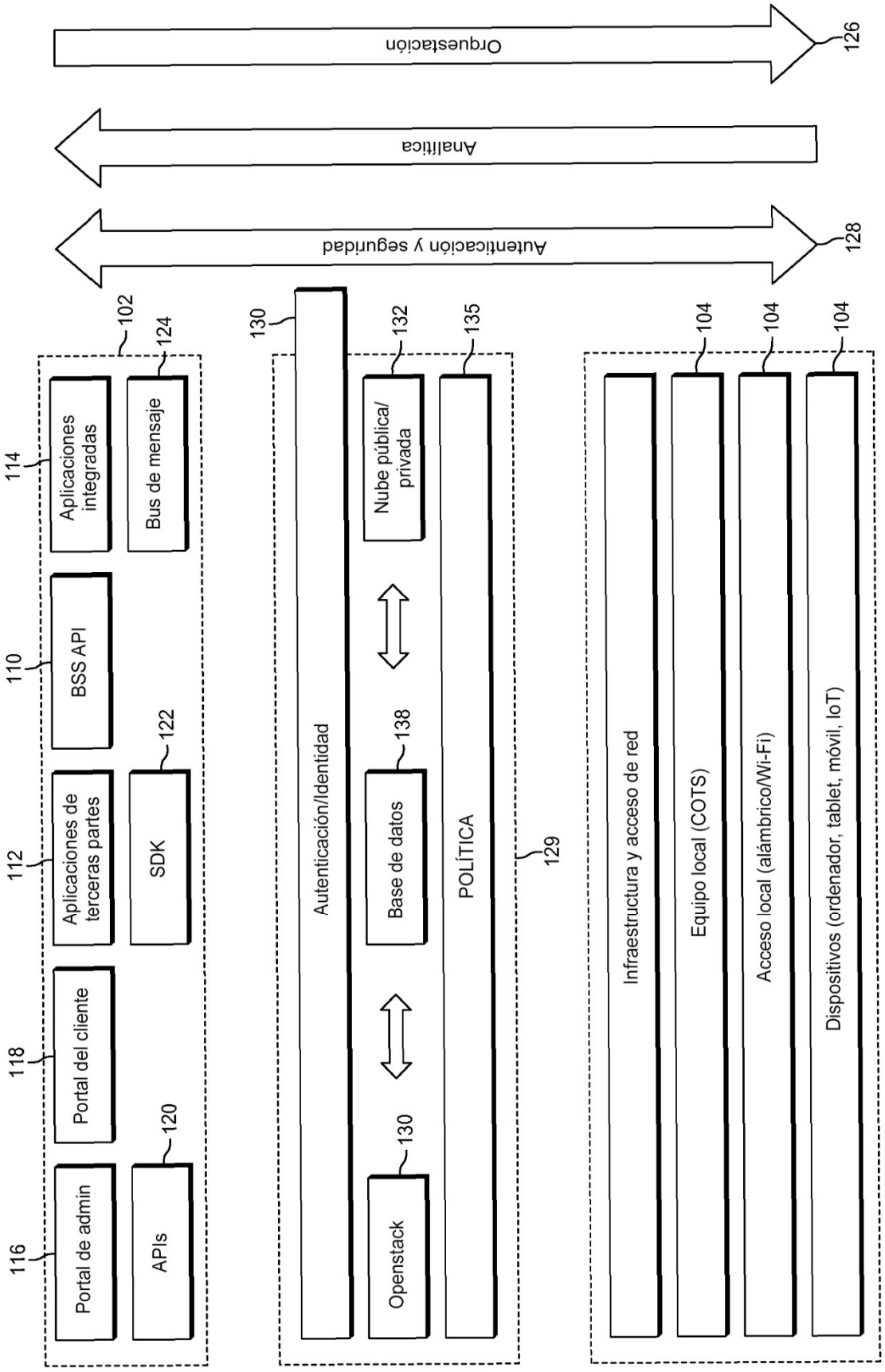
Orquestación
126
Analítica
Autenticación y seguridad
128
102
124
Aplicaciones integradas
Bus de mensaje
114
110
BSS API
112
Aplicaciones de terceras partes
SDK
122
118
Portal del cliente
120
116
Portal de admin
APIs
130
Autenticación/Identidad
132
Nube pública/ privada
135
138
Base de datos
POLÍTICA
129
130
Openstack
104
104
104
Infraestructura y acceso de red
Equipo local (COTS)
Acceso local (alámbrico/Wi-Fi)
Dispositivos (ordenador, tablet, móvil, IoT)

FIG. 4

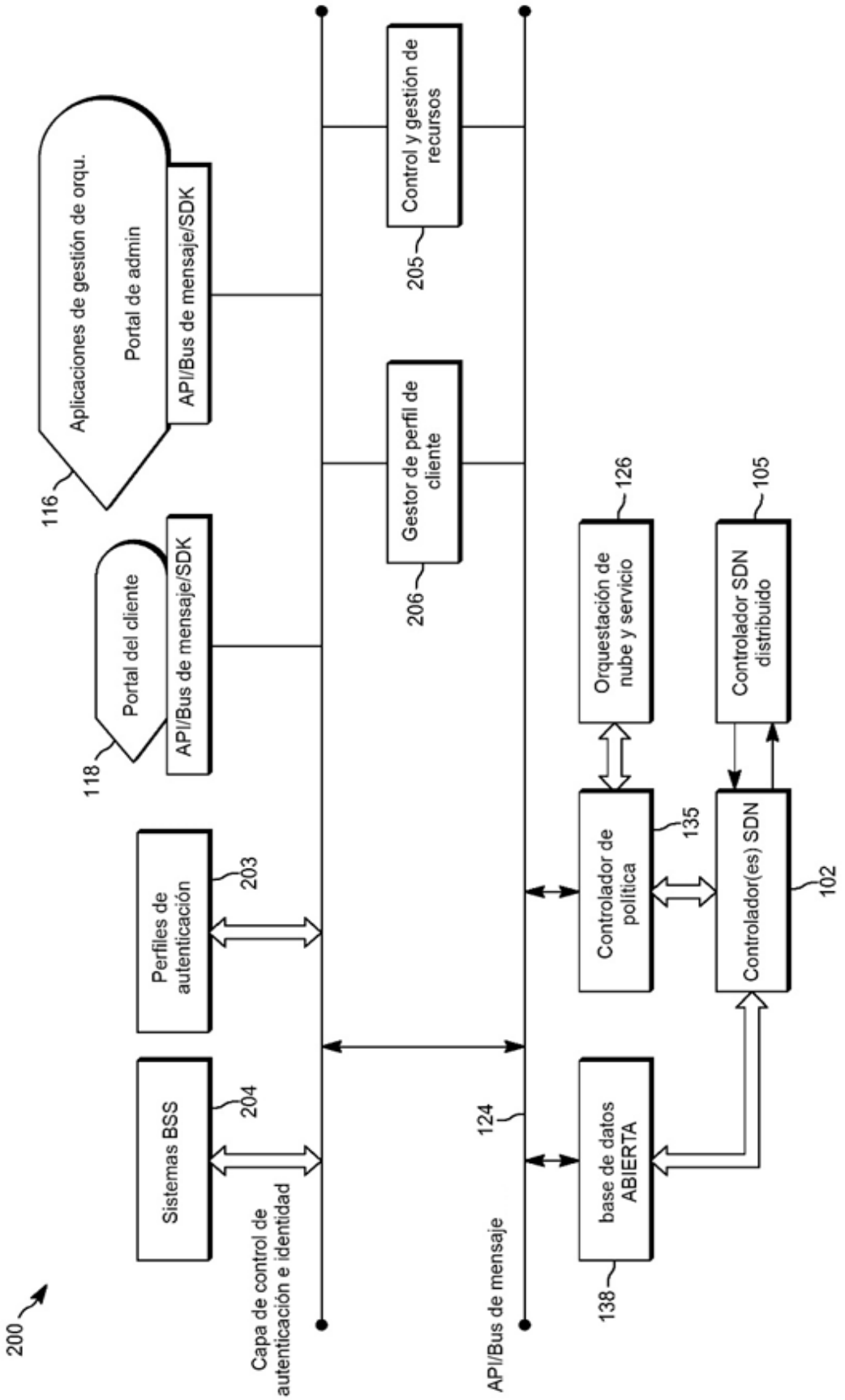
200
Capa de control de autenticación e identidad
API/Bus de mensaje
Sistemas BSS
204
Perfiles de autenticación
203
Portal del cliente
118
API/Bus de mensaje/SDK
Aplicaciones de gestión de orqu.
Portal de admin
116
API/Bus de mensaje/SDK
Gestor de perfil de cliente
206
Control y gestión de recursos
205
124
base de datos ABIERTA
138
Controlador de política
135
Orquestación de nube y servicio
126
Controlador(es) SDN
102
Controlador SDN distribuido
105

FIG. 5

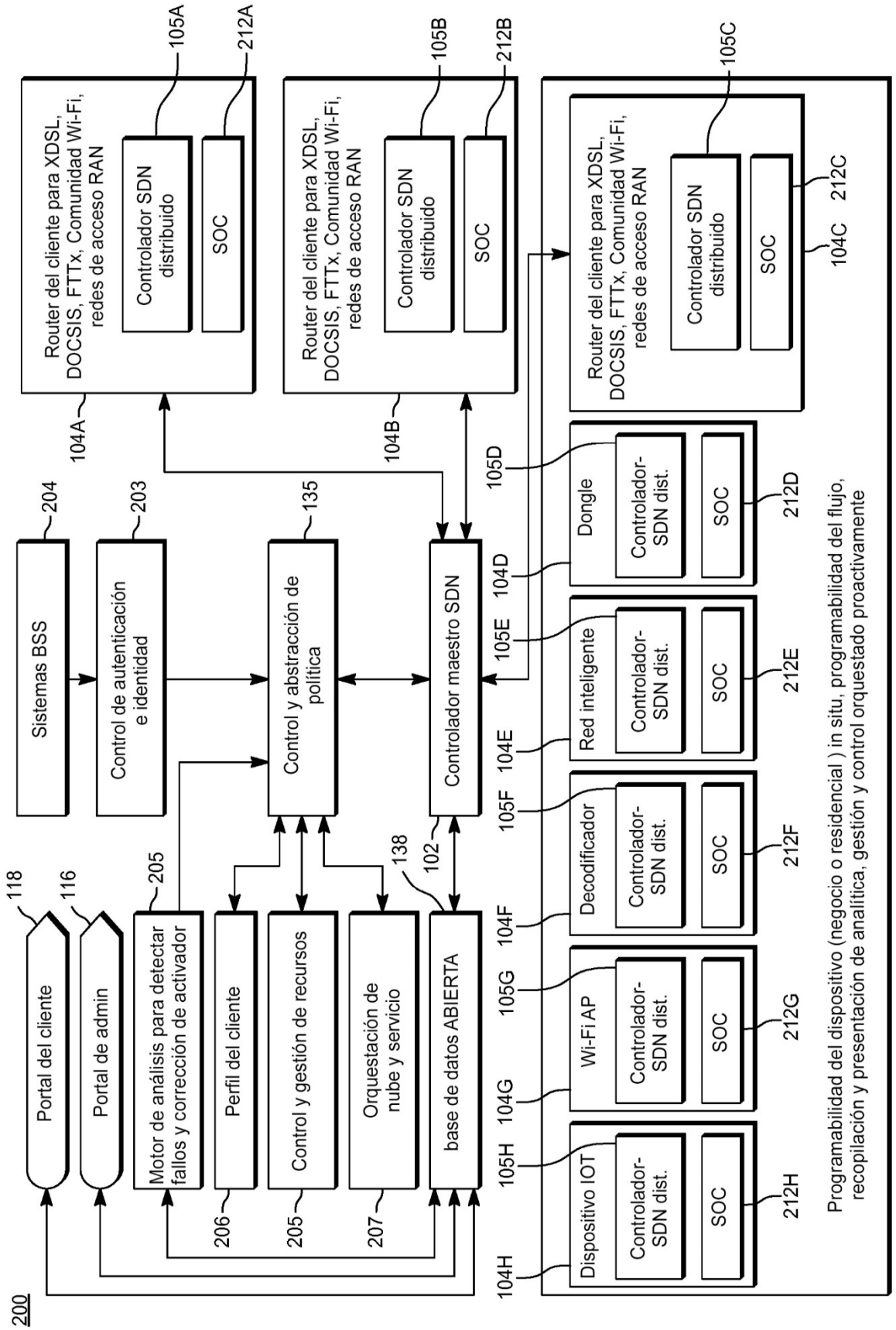
200
Portal del cliente
Portal de admin
Motor de análisis para detectar fallos y corrección de activador
Perfil del cliente
Control y gestión de recursos
Orquestación de nube y servicio
base de datos ABIERTA
Sistemas BSS
Control de autenticación e identidad
Control y abstracción de política
Controlador maestro SDN
Router del cliente para XDSL, DOCSIS, FTTx, Comunidad Wi-Fi, redes de acceso RAN
Controlador SDN distribuido
SOC
Dispositivo IOT
Wi-Fi AP
Dongle
Red inteligente
Decodificador
Controlador-SDN dist.
Programabilidad del dispositivo (negocio o residencial) in situ, programabilidad del flujo, recopilación y presentación de analítica, gestión y control orquestado proactivamente
118
116
205
206
205
207
138
102
204
203
135
104A
105A
212A
104B
105B
212B
105C
212C
104C
105D
104D
105E
104E
105F
104F
105G
104G
105H
104H
212D
212E
212F
212G
212H

FIG. 6

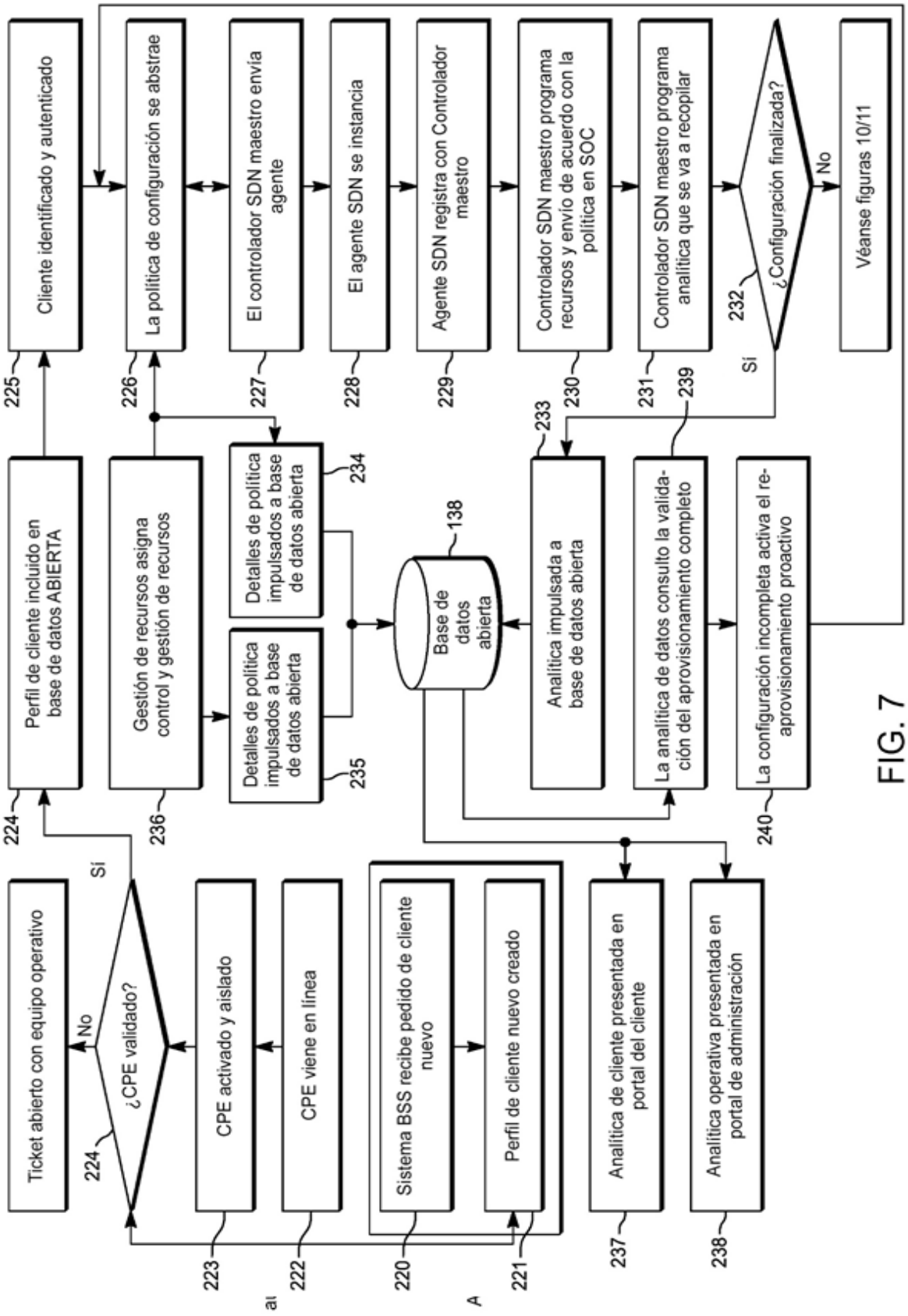
Cliente identificado y autenticado
La política de configuración se abstrae
El controlador SDN maestro envía agente
El agente SDN se instancia
Agente SDN registra con Controlador maestro
Controlador SDN maestro programa recursos y envío de acuerdo con la política en SOC
Controlador SDN maestro programa analítica que se va a recopilar
¿Configuración finalizada?
Sí
No
Véanse figuras 10/11
Perfil de cliente incluido en base de datos ABIERTA
Gestión de recursos asigna control y gestión de recursos
Detalles de política impulsados a base de datos abierta
Detalles de política impulsados a base de datos abierta
Base de datos abierta
Analítica impulsada a base de datos abierta
La analítica de datos consulta la validación del aprovisionamiento completo
La configuración incompleta activa el re-aprovisionamiento proactivo
Ticket abierto con equipo operativo
¿CPE validado?
Sí
No
CPE activado y aislado
CPE viene en línea
Sistema BSS recibe pedido de cliente nuevo
Perfil de cliente nuevo creado
Analítica de cliente presentada en portal del cliente
Analítica operativa presentada en portal de administración
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
138
224
223
222
220
221
A
A

FIG. 7

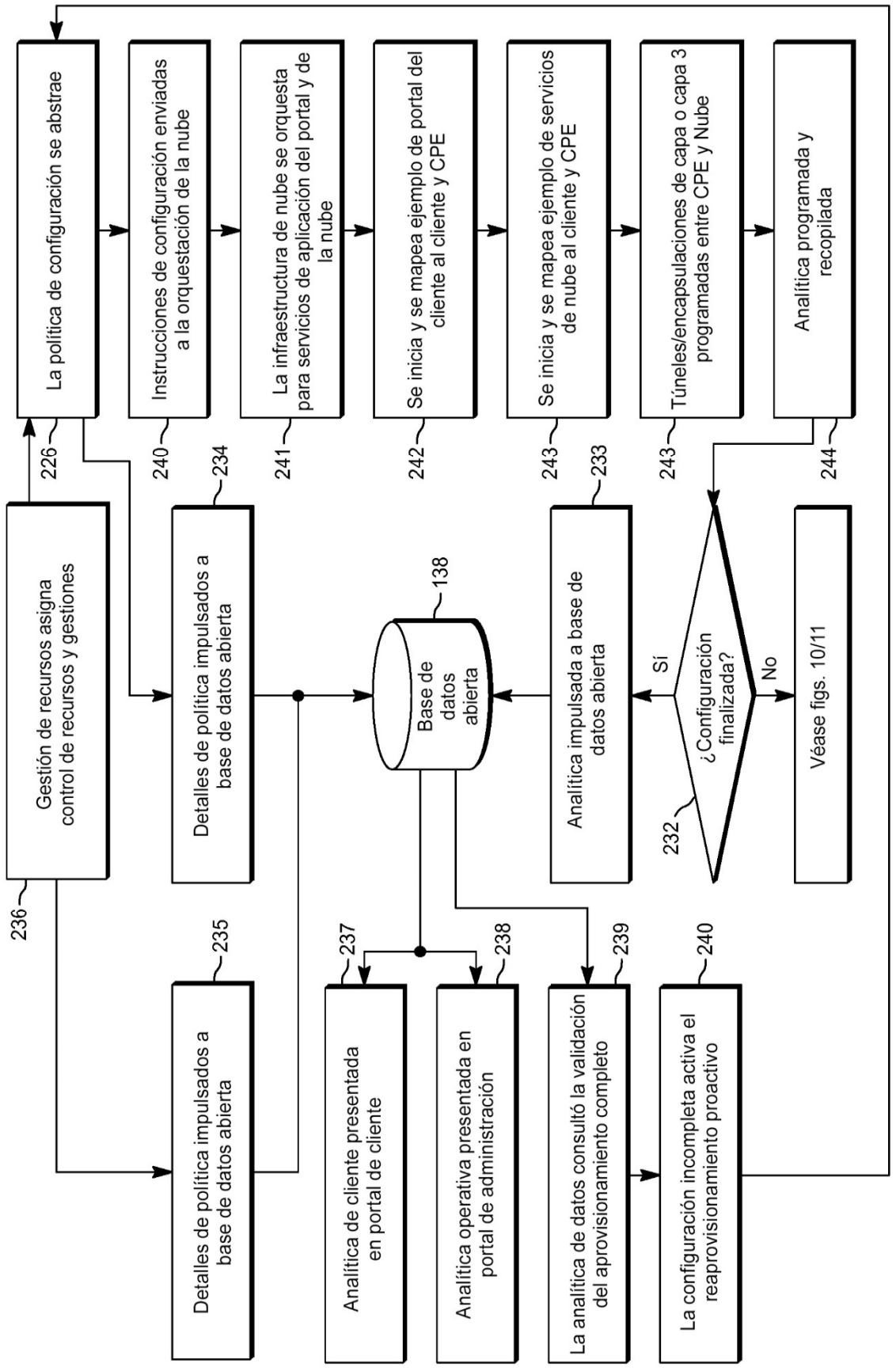
La política de configuración se abstrae
Instrucciones de configuración enviadas a la orquestación de la nube
La infraestructura de nube se orquesta para servicios de aplicación del portal y de la nube
Se inicia y se mapea ejemplo de portal del cliente al cliente y CPE
Se inicia y se mapea ejemplo de servicios de nube al cliente y CPE
Túneles/encapsulaciones de capa o capa 3 programadas entre CPE y Nube
Analítica programada y recopilada
226
240
241
242
243
243
244
Gestión de recursos asigna control de recursos y gestiones
Detalles de política impulsados a base de datos abierta
Base de datos abierta
Analítica impulsada a base de datos abierta
¿Configuración finalizada?
Sí
No
Véase figs. 10/11
232
234
138
233
236
Detalles de política impulsados a base de datos abierta
Analítica de cliente presentada en portal de cliente
Analítica operativa presentada en portal de administración
La analítica de datos consultó la validación del aprovisionamiento completo
La configuración incompleta activa el reaprovisionamiento proactivo
235
237
238
239
240

FIG. 8

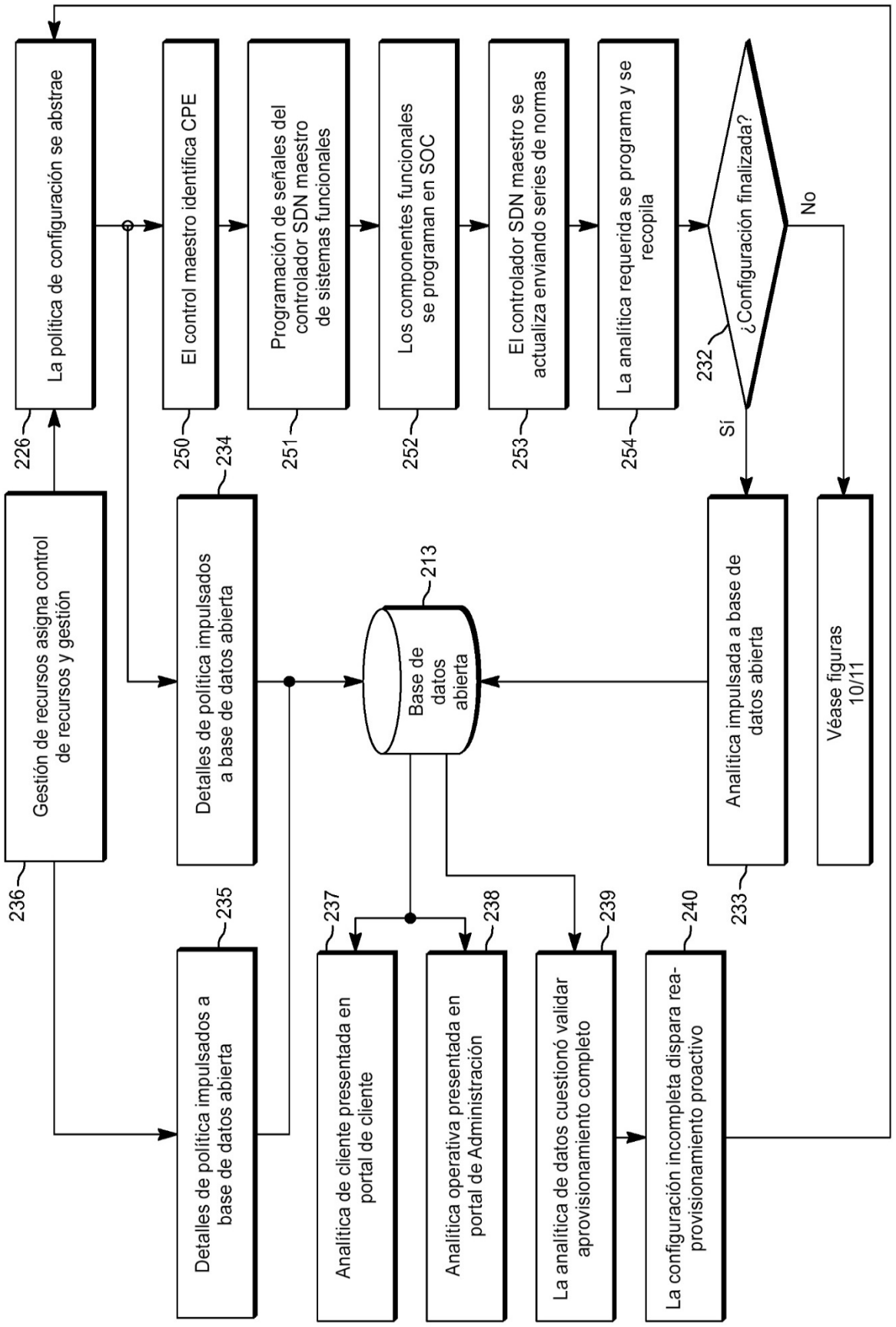
La política de configuración se abstrae
El control maestro identifica CPE
Programación de señales del controlador SDN maestro de sistemas funcionales
Los componentes funcionales se programan en SOC
El controlador SDN maestro se actualiza enviando series de normas
La analítica requerida se programa y se recopila
¿Configuración finalizada?
Sí
No
Gestión de recursos asigna control de recursos y gestión
Detalles de política impulsados a base de datos abierta
Base de datos abierta
Analítica impulsada a base de datos abierta
Véase figuras 10/11
Detalles de política impulsados a base de datos abierta
Analítica de cliente presentada en portal de cliente
Analítica operativa presentada en portal de Administración
La analítica de datos cuestionó validar aprovisionamiento completo
La configuración incompleta dispara rea-provisionamiento proactivo
226
250
251
252
253
254
232
234
213
236
235
237
238
239
240
233

FIG. 9

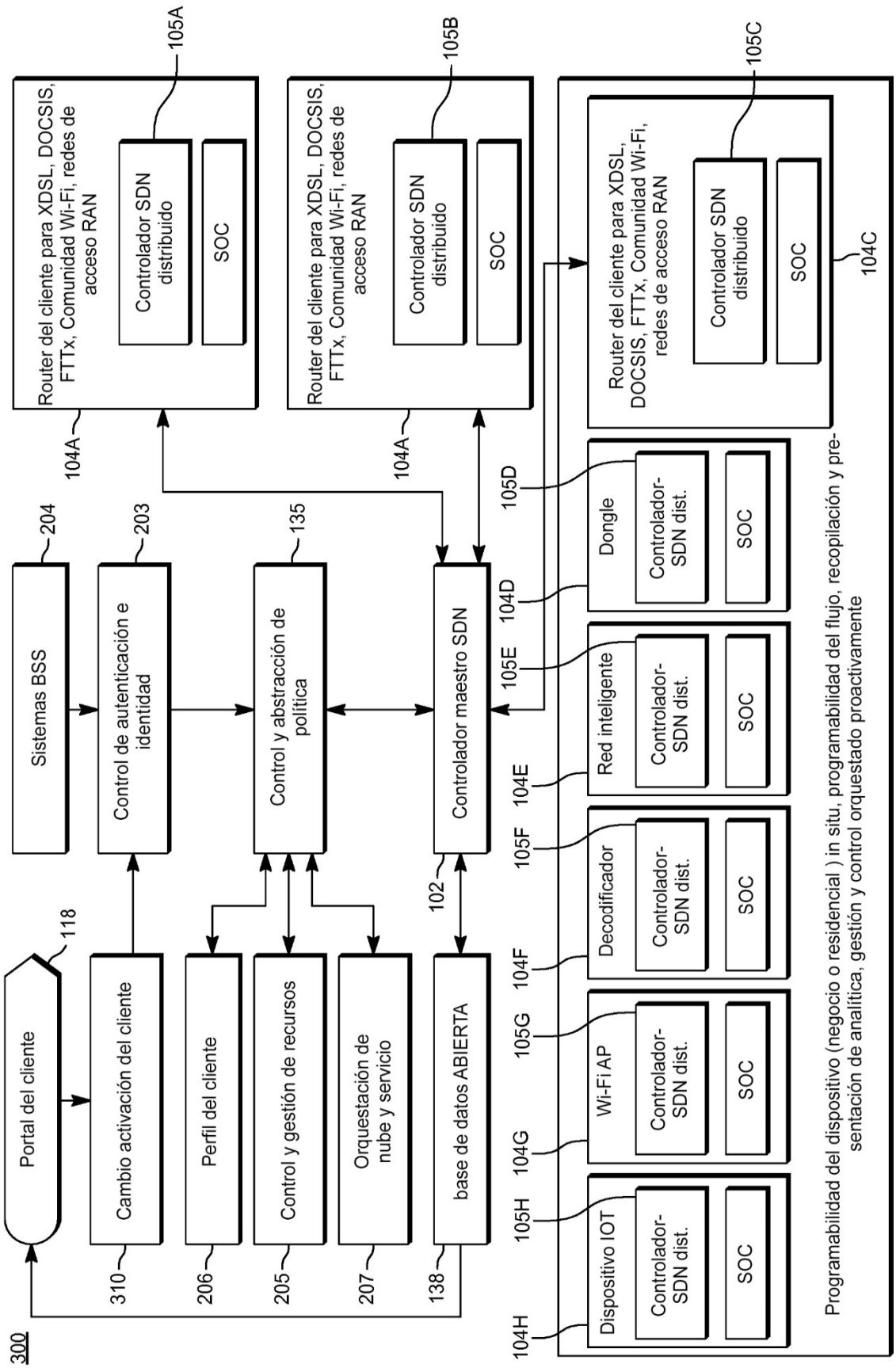
300
Portal del cliente
118
Cambio activación del cliente
310
Perfil del cliente
206
Control y gestión de recursos
205
Orquestación de nube y servicio
207
base de datos ABIERTA
138
Sistemas BSS
204
Control de autenticación e identidad
203
Control y abstracción de política
135
Controlador maestro SDN
102
Router del cliente para XDSL, DOCSIS, FTTx, Comunidad Wi-Fi, redes de acceso RAN
Controlador SDN distribuido
SOC
105A
104A
Router del cliente para XDSL, DOCSIS, FTTx, Comunidad Wi-Fi, redes de acceso RAN
Controlador SDN distribuido
SOC
105B
104A
Router del cliente para XDSL, DOCSIS, FTTx, Comunidad Wi-Fi, redes de acceso RAN
Controlador SDN distribuido
SOC
105C
104C
Programabilidad del dispositivo (negocio o residencial) in situ, programabilidad del flujo, recopilación y presentación de analítica, gestión y control orquestado proactivamente
Dongle
Controlador-SDN dist.
SOC
105D
104D
Red inteligente
Controlador-SDN dist.
SOC
105E
104E
Decodificador
Controlador-SDN dist.
SOC
105F
104F
Wi-Fi AP
Controlador-SDN dist.
SOC
105G
104G
Dispositivo IOT
Controlador-SDN dist.
SOC
105H
104H

FIG. 10

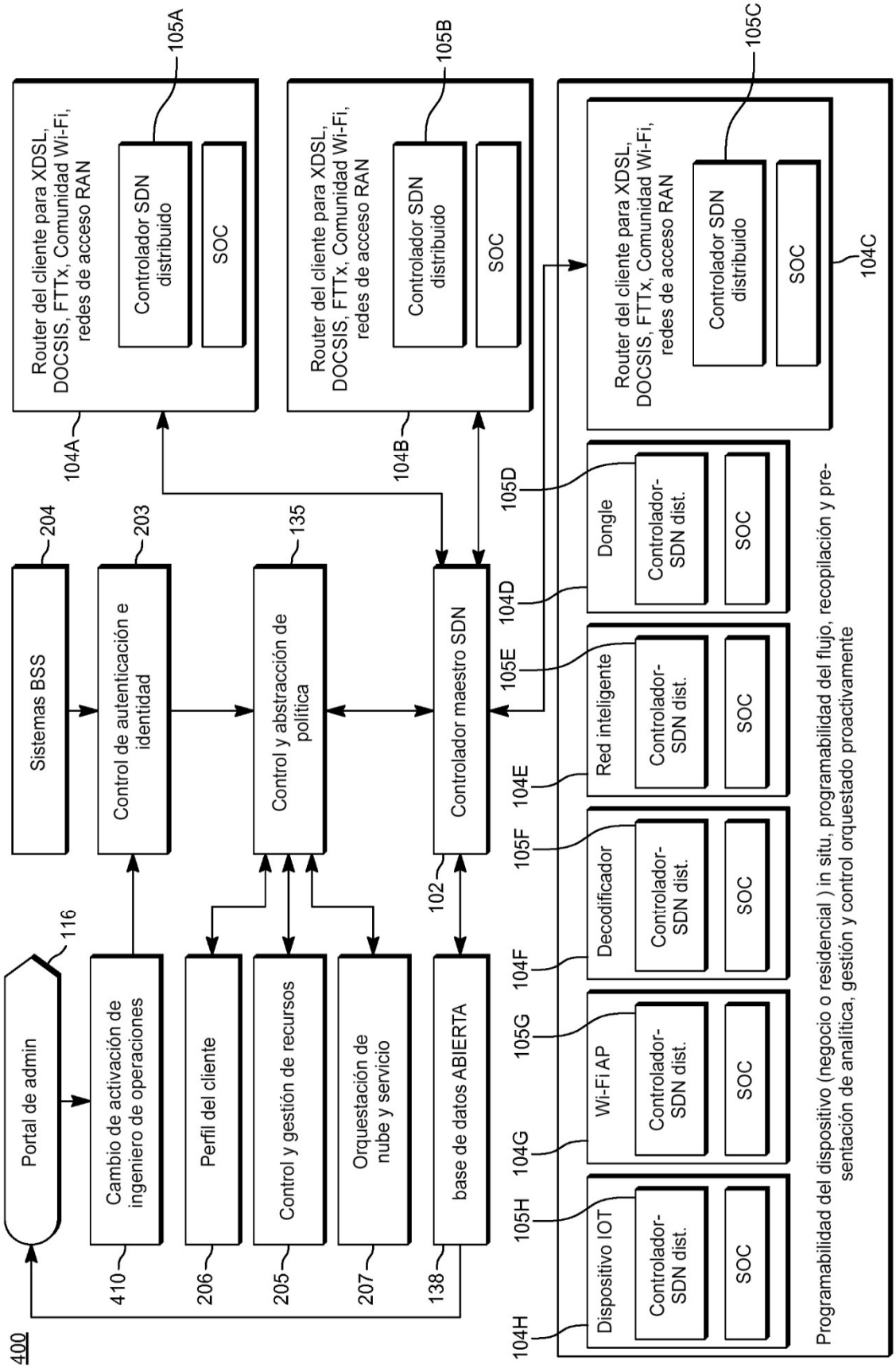
400
Portal de admin
116
Cambio de activación de ingeniero de operaciones
410
Perfil del cliente
206
Control y gestión de recursos
205
Orquestación de nube y servicio
207
base de datos ABIERTA
138
Sistemas BSS
204
Control de autenticación e identidad
203
Control y abstracción de política
135
Controlador maestro SDN
102
Router del cliente para XDSL, DOCSIS, FTTx, Comunidad Wi-Fi, redes de acceso RAN
Controlador SDN distribuido
SOC
104A
105A
104B
105B
104C
105C
Dispositivo IOT
Wi-Fi AP
Decodificador
Red inteligente
Dongle
Controlador-SDN dist.
104H
105H
104G
105G
104F
105F
104E
105E
104D
105D
Programabilidad del dispositivo (negocio o residencial) in situ, programabilidad del flujo, recopilación y presentación de analítica, gestión y control orquestado proactivamente

FIG. 11

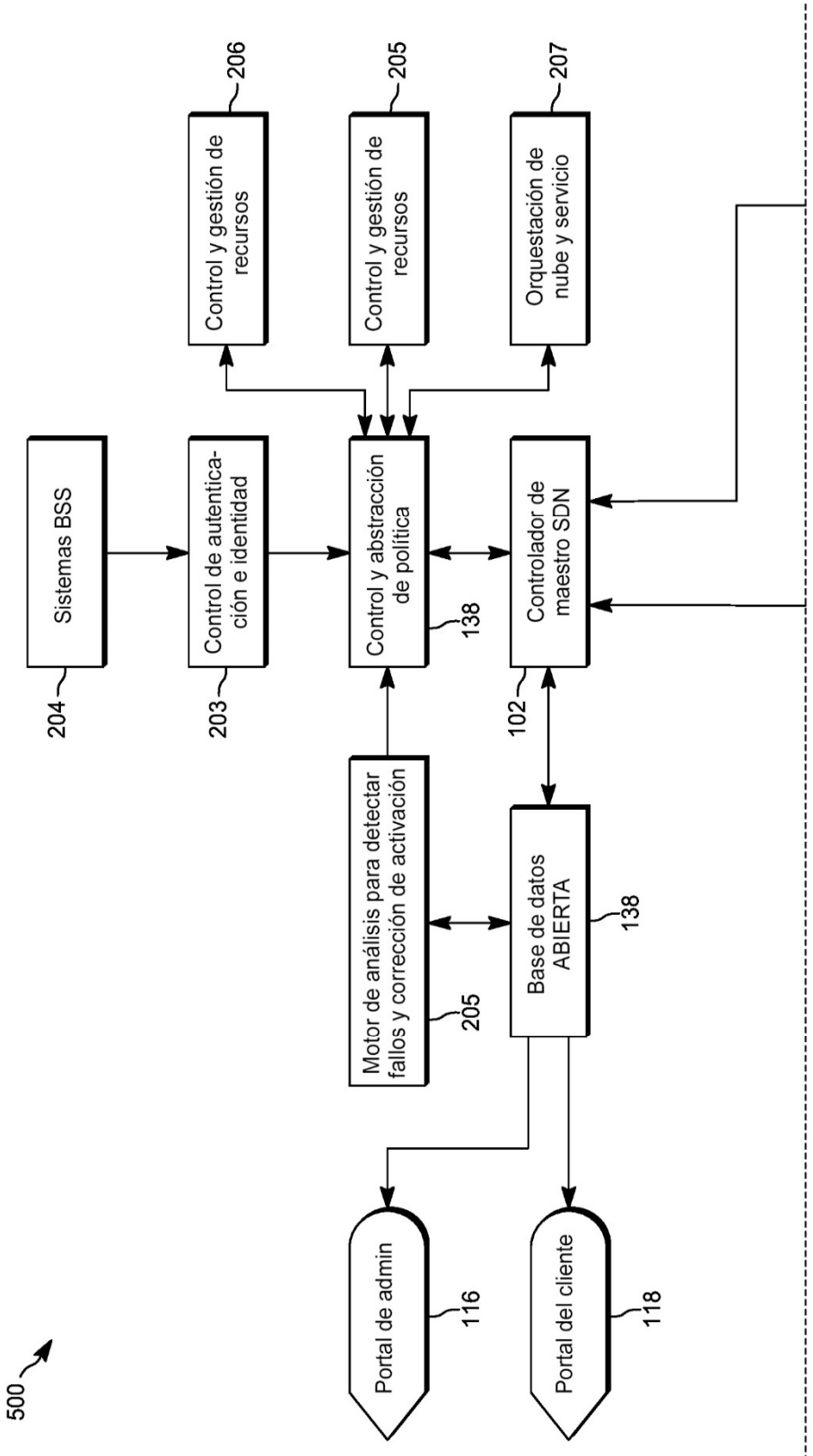
500
Sistemas BSS
204
Control de autentica-ción e identidad
203
Control y abstracción de política
138
Controlador de maestro SDN
102
Control y gestión de recursos
206
Control y gestión de recursos
205
Orquestación de nube y servicio
207
Motor de análisis para detectar fallos y corrección de activación
205
Base de datos ABIERTA
138
Portal de admin
116
Portal del cliente
118

FIG. 12A

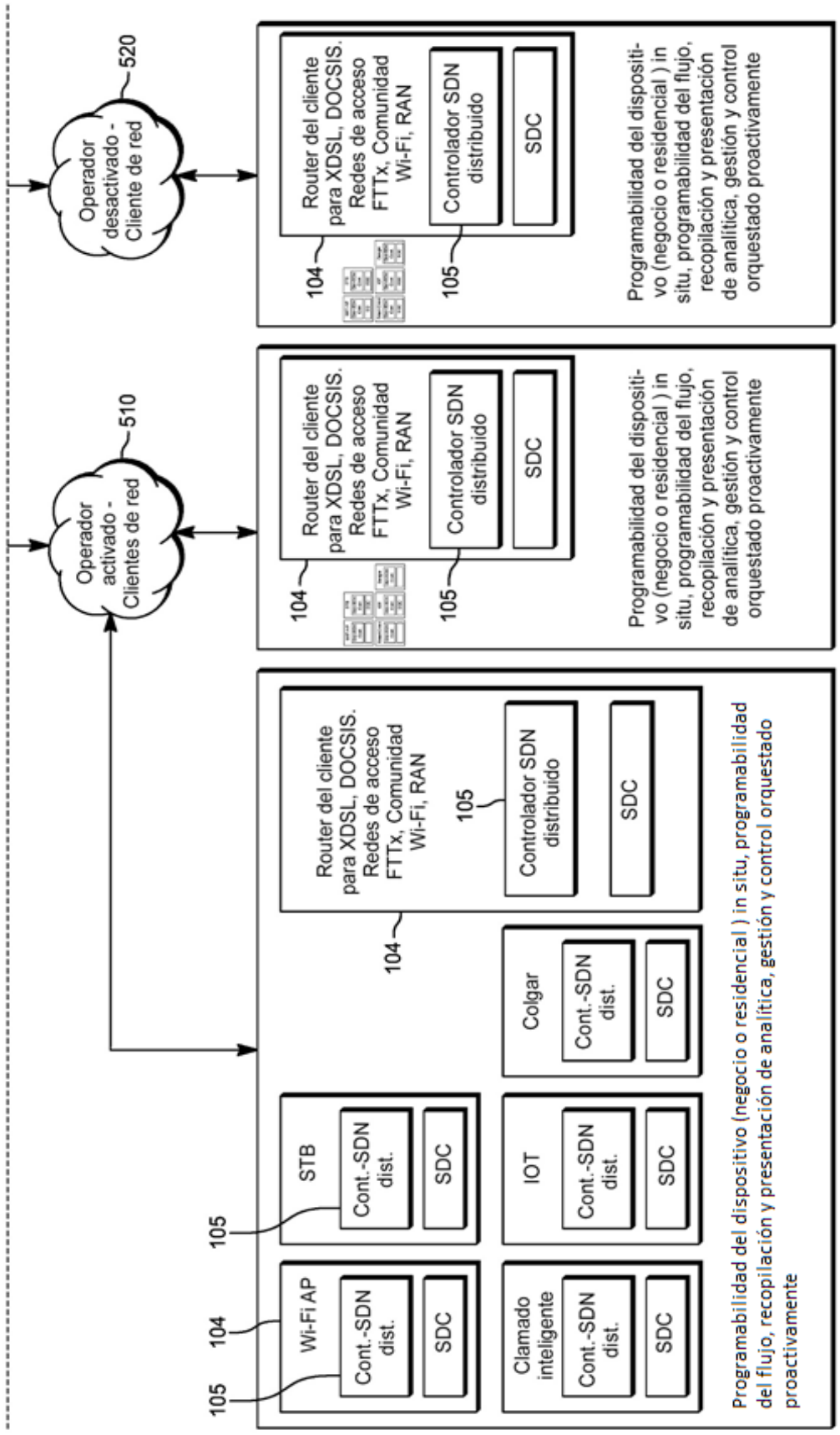
Operador desactivado - Cliente de red
520
Operador activado - Clientes de red
510
Router del cliente para XDSL, DOCSIS. Redes de acceso FTTx, Comunidad Wi-Fi, RAN
Controlador SDN distribuido
SDC
104
105
Programabilidad del dispositivo (negocio o residencial) in situ, programabilidad del flujo, recopilación y presentación de analítica, gestión y control orquestado proactivamente
Wi-Fi AP
STB
IOT
Colgar
Clamado inteligente
Cont.-SDN dist.
Programabilidad del dispositivo (negocio o residencial) in situ, programabilidad del flujo, recopilación y presentación de analítica, gestión y control orquestado proactivamente

FIG. 12B

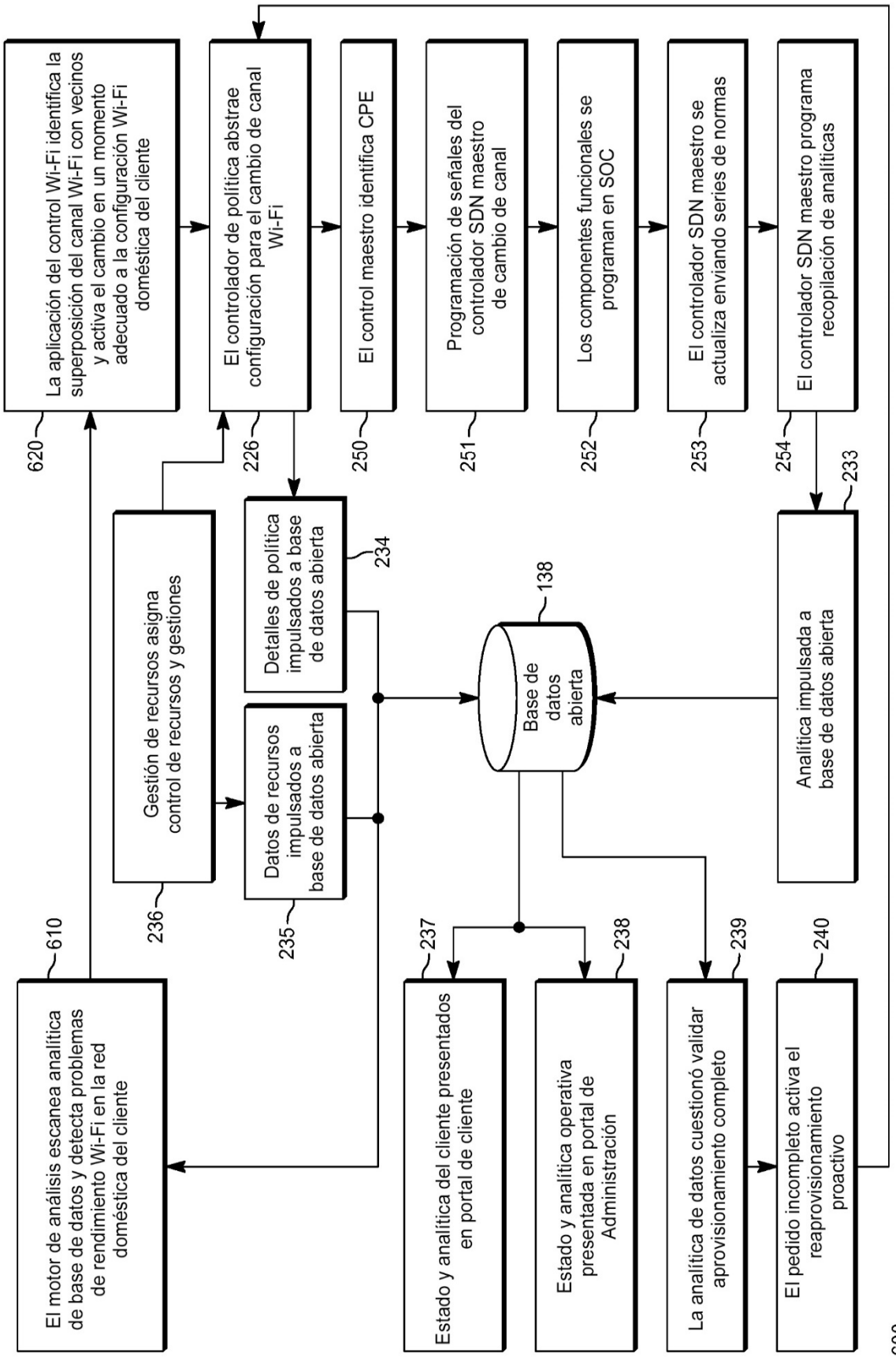
La aplicación del control Wi-Fi identifica la superposición del canal Wi-Fi con vecinos y activa el cambio en un momento adecuado a la configuración Wi-Fi doméstica del cliente
620
El controlador de política abstrae configuración para el cambio de canal Wi-Fi
226
El control maestro identifica CPE
250
Programación de señales del controlador SDN maestro de cambio de canal
251
Los componentes funcionales se programan en SOC
252
El controlador SDN maestro se actualiza enviando series de normas
253
El controlador SDN maestro programa recopilación de analíticas
254
233
Gestión de recursos asigna control de recursos y gestiones
236
Detalles de política impulsados a base de datos abierta
234
Datos de recursos impulsados a base de datos abierta
235
138
Base de datos abierta
Analítica impulsada a base de datos abierta
El motor de análisis escanea analítica de base de datos y detecta problemas de rendimiento Wi-Fi en la red doméstica del cliente
610
237
Estado y analítica del cliente presentados en portal de cliente
238
Estado y analítica operativa presentada en portal de Administración
239
La analítica de datos cuestionó validar aprovisionamiento completo
240
El pedido incompleto activa el reaprovisionamiento proactivo
600

FIG. 13

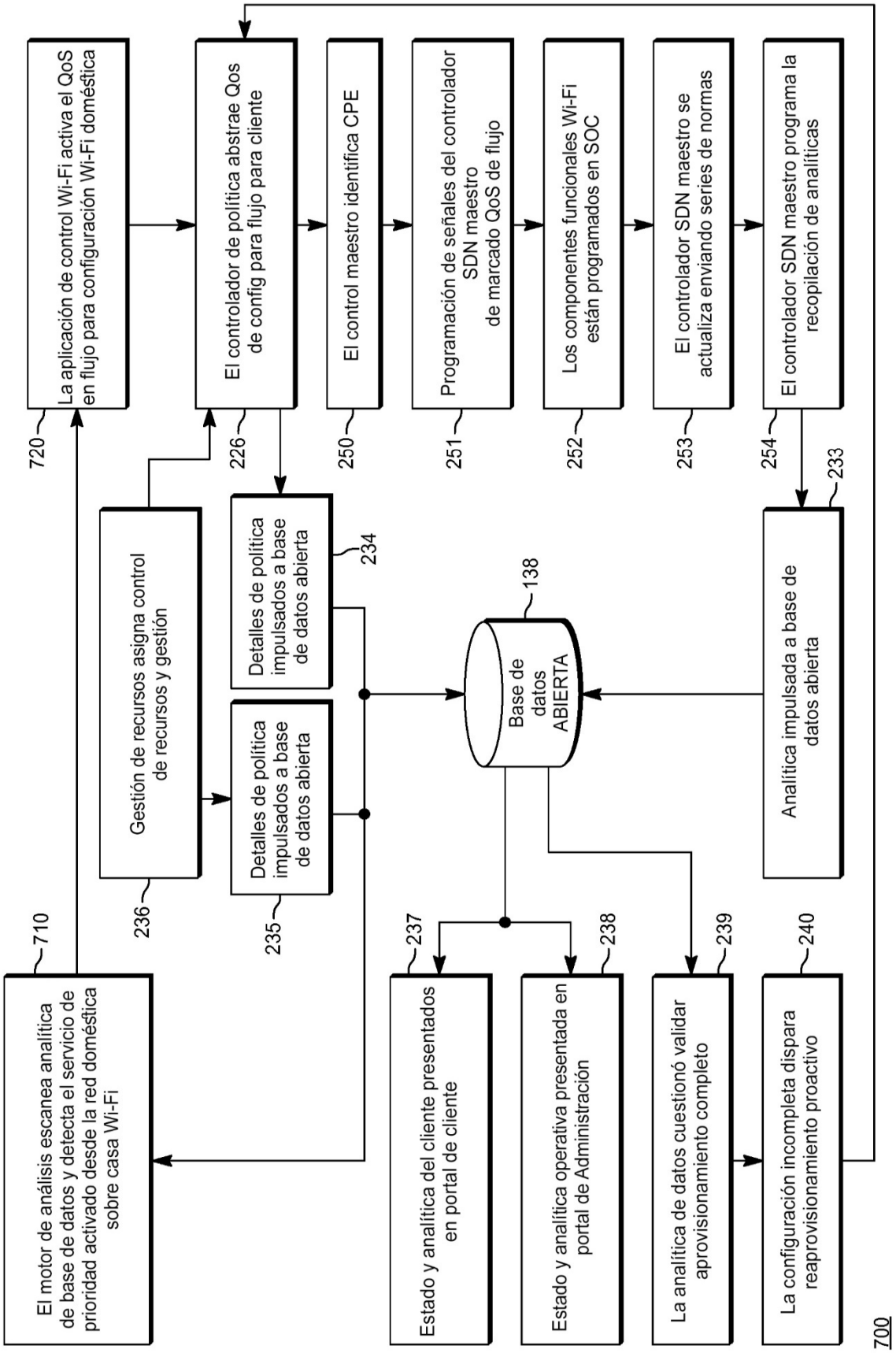
La aplicación de control Wi-Fi activa el QoS en flujo para configuración Wi-Fi doméstica
El controlador de política abstrae Qos de config para flujo para cliente
El control maestro identifica CPE
Programación de señales del controlador SDN maestro de marcado QoS de flujo
Los componentes funcionales Wi-Fi están programados en SOC
El controlador SDN maestro se actualiza enviando series de normas
El controlador SDN maestro programa la recopilación de analíticas
720
226
250
251
252
253
254
233
Gestión de recursos asigna control de recursos y gestión
Detalles de política impulsados a base de datos abierta
Detalles de política impulsados a base de datos abierta
234
138
Base de datos ABIERTA
Analítica impulsada a base de datos abierta
236
235
710
237
238
239
240
El motor de análisis escanea analítica de base de datos y detecta el servicio de prioridad activado desde la red doméstica sobre casa Wi-Fi
Estado y analítica del cliente presentados en portal de cliente
Estado y analítica operativa presentada en portal de Administración
La analítica de datos cuestionó validar aprovisionamiento completo
La configuración incompleta dispara reaprovisionamiento proactivo
700

FIG. 14

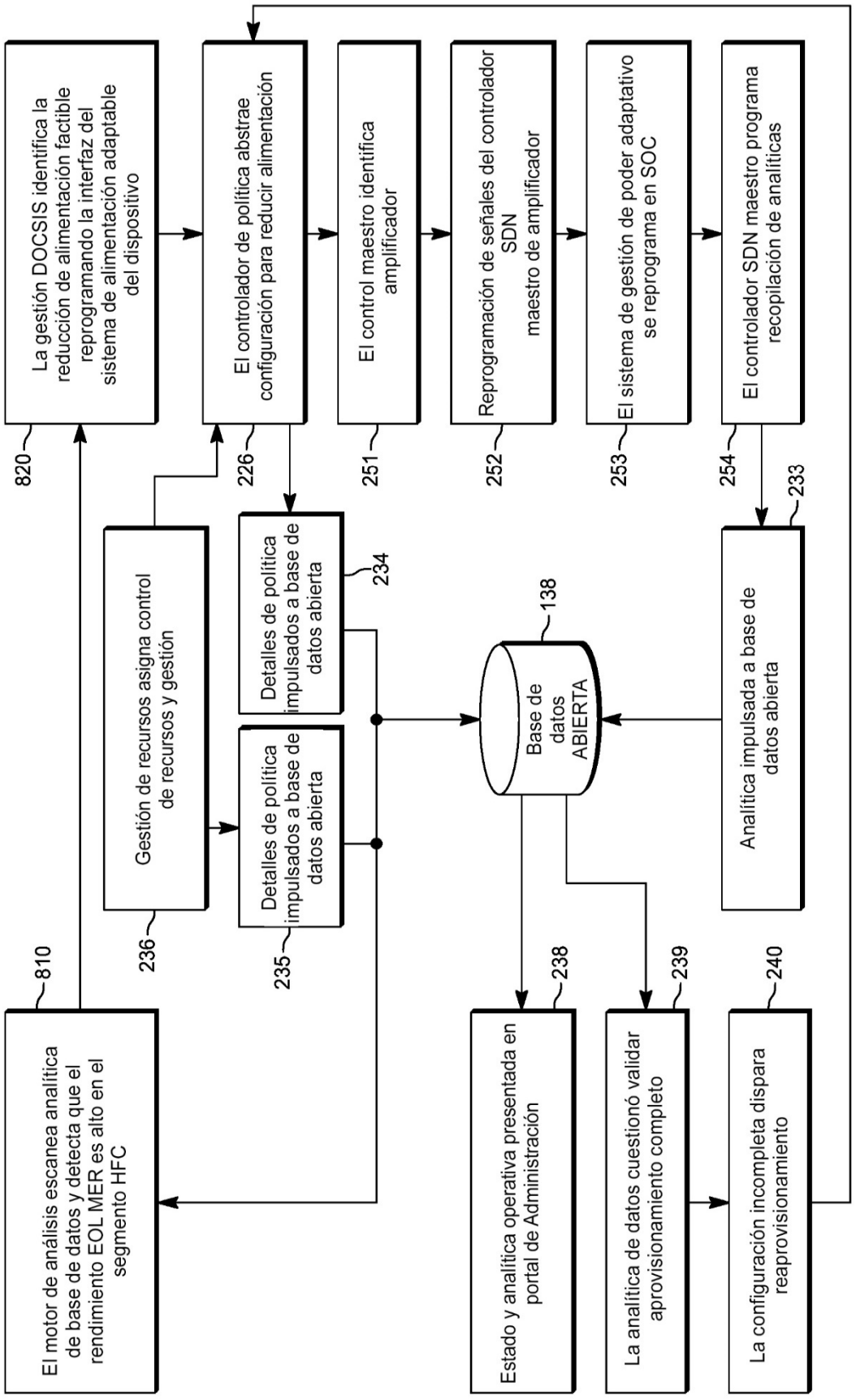
La gestión DOCSIS identifica la reducción de alimentación factible reprogramando la interfaz del sistema de alimentación adaptable del dispositivo
820
El controlador de política abstrae configuración para reducir alimentación
226
El control maestro identifica amplificador
251
Reprogramación de señales del controlador SDN maestro de amplificador
252
El sistema de gestión de poder adaptativo se reprograma en SOC
253
El controlador SDN maestro programa recopilación de analíticas
254
233
Gestión de recursos asigna control de recursos y gestión
236
Detalles de política impulsados a base de datos abierta
234
Detalles de política impulsados a base de datos abierta
235
138
Base de datos ABIERTA
Analítica impulsada a base de datos abierta
El motor de análisis escanea analítica de base de datos y detecta que el rendimiento EOL MER es alto en el segmento HFC
810
Estado y analítica operativa presentada en portal de Administración
238
La analítica de datos cuestionó validar aprovisionamiento completo
239
La configuración incompleta dispara reaprovisionamiento
240
800

FIG. 15

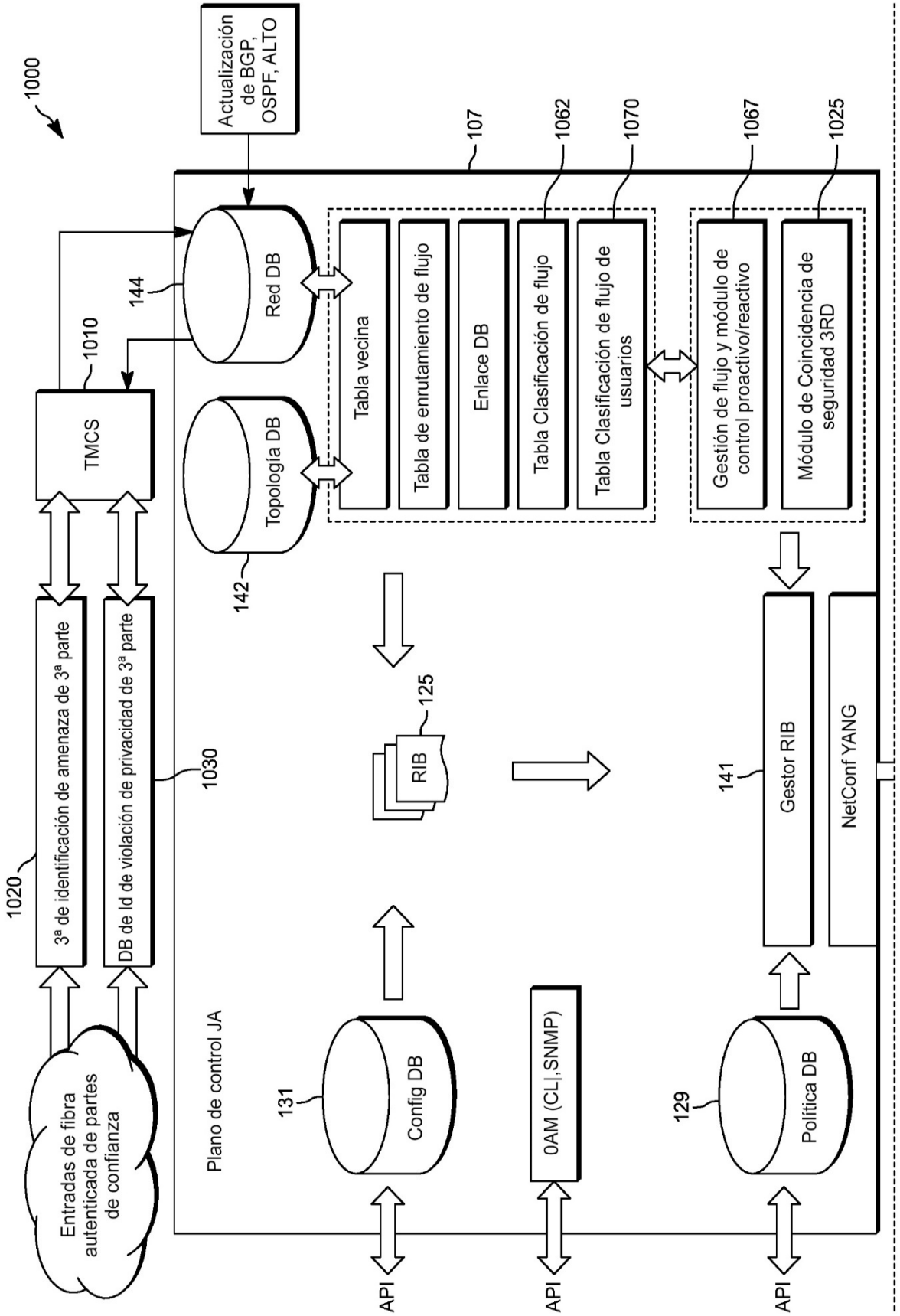
1000
Actualización de BGP, OSPF, ALTO
107
1062
1070
1067
1025
Red DB
144
1010
TMCS
Topología DB
142
Tabla vecina
Tabla de enrutamiento de flujo
Enlace DB
Tabla Clasificación de flujo
Tabla Clasificación de flujo de usuarios
Gestión de flujo y módulo de control proactivo/reactivo
Módulo de Coincidencia de seguridad 3RD
1020
3ª de identificación de amenaza de 3ª parte
DB de Id de violación de privacidad de 3ª parte
1030
125
RIB
141
Gestor RIB
NetConf YANG
Plano de control JA
131
Config DB
0AM (CL|,SNMP)
129
Política DB
Entradas de fibra autenticada de partes de confianza
API
API
API

FIG. 16A

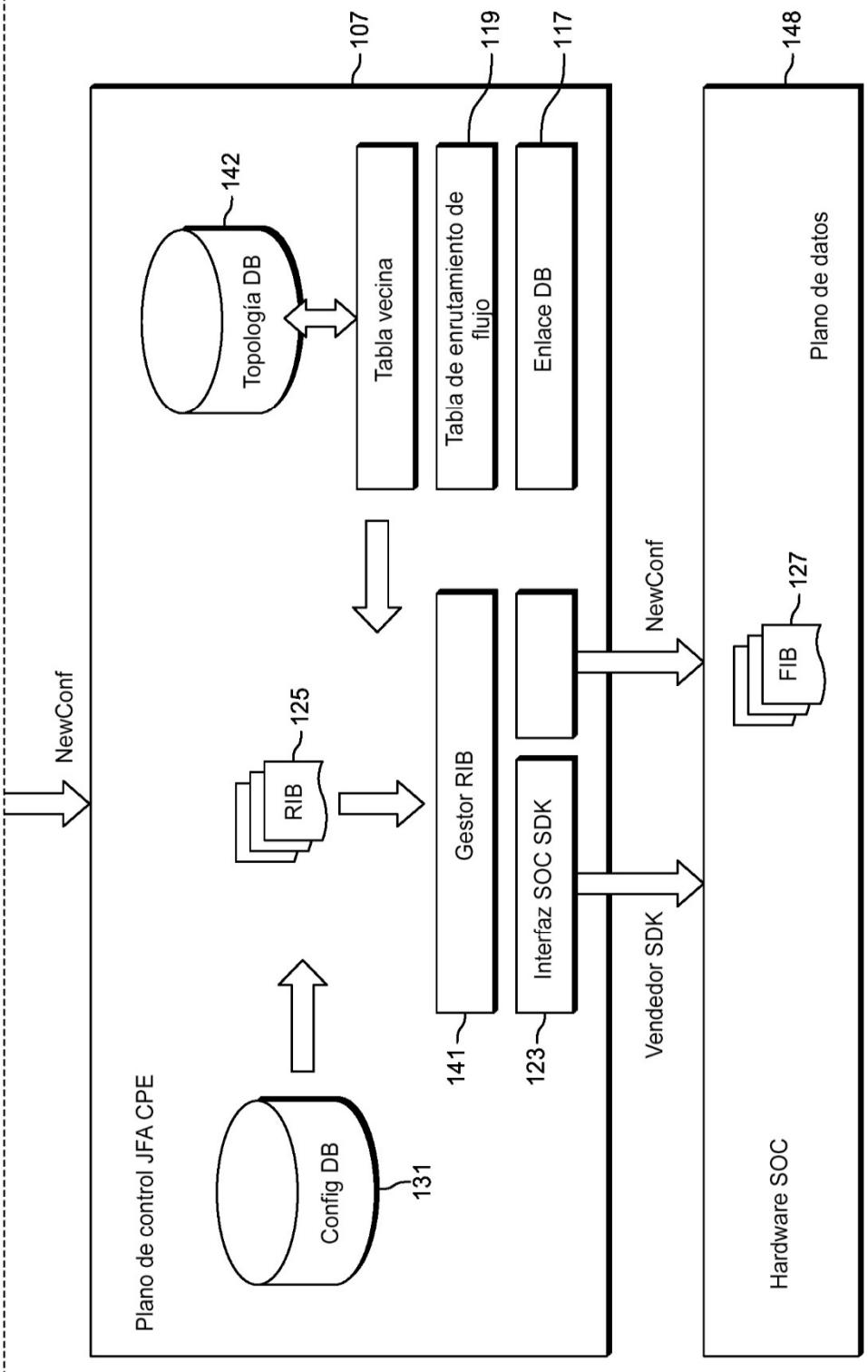
NewConf
Plano de control JFA CPE
107
119
117
148
142
Topología DB
Tabla vecina
Tabla de enrutamiento de flujo
Enlace DB
Plano de datos
125
RIB
Gestor RIB
NewConf
127
FIB
Config DB
131
141
123
Interfaz SOC SDK
Vendedor SDK
Hardware SOC

FIG. 16B

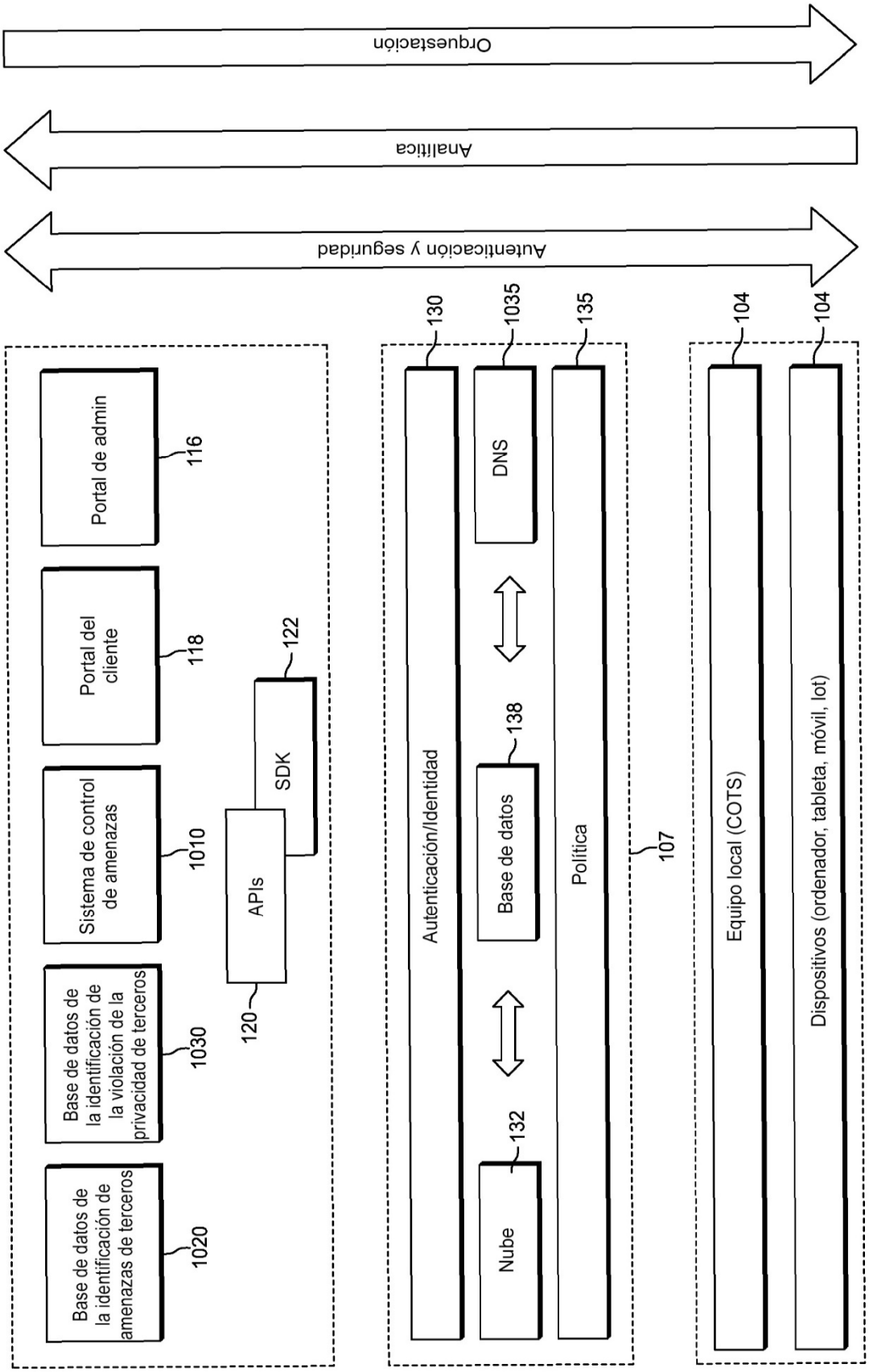
Orquestación
Analítica
Autenticación y seguridad
Portal de admin
116
Portal del cliente
118
Sistema de control de amenazas
1010
Base de datos de la identificación de la violación de la privacidad de terceros
1030
Base de datos de la identificación de amenazas de terceros
1020
APIs
SDK
122
120
Autenticación/Identidad
130
DNS
1035
Base de datos
138
Política
135
Nube
132
107
Equipo local (COTS)
104
Dispositivos (ordenador, tableta, móvil, Iot)
104

FIG. 17

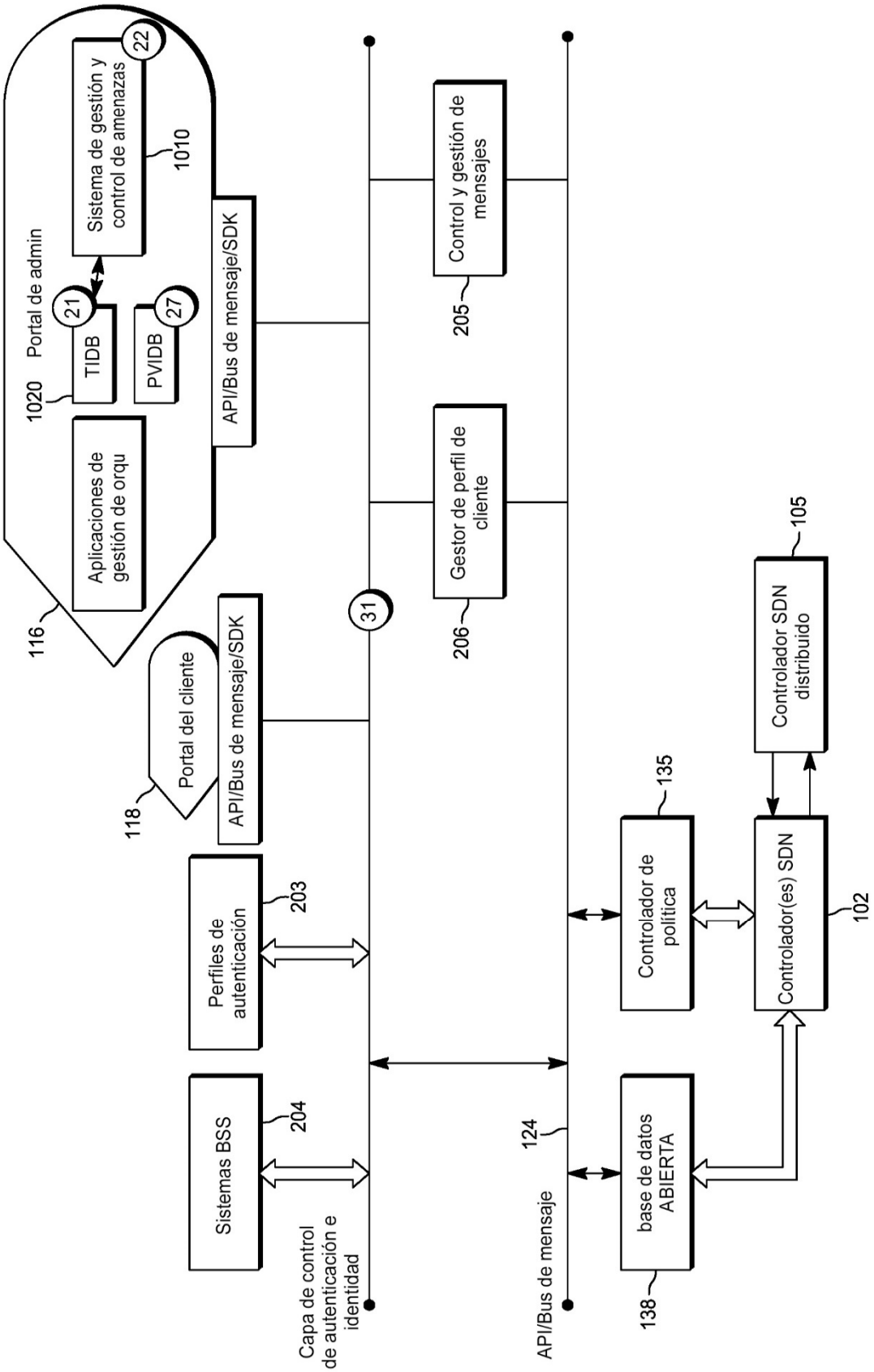
Portal de admin
1020
Sistema de gestión y control de amenazas
22
1010
TIDB
21
PVIDB
27
Aplicaciones de gestión de orqu
116
API/Bus de mensaje/SDK
Control y gestión de mensajes
205
Gestor de perfil de cliente
206
Portal del cliente
118
API/Bus de mensaje/SDK
31
Perfiles de autenticación
203
Sistemas BSS
204
Capa de control de autenticación e identidad
API/Bus de mensaje
124
Controlador de política
135
base de datos ABIERTA
138
Controlador(es) SDN
102
Controlador SDN distribuido
105

FIG. 18

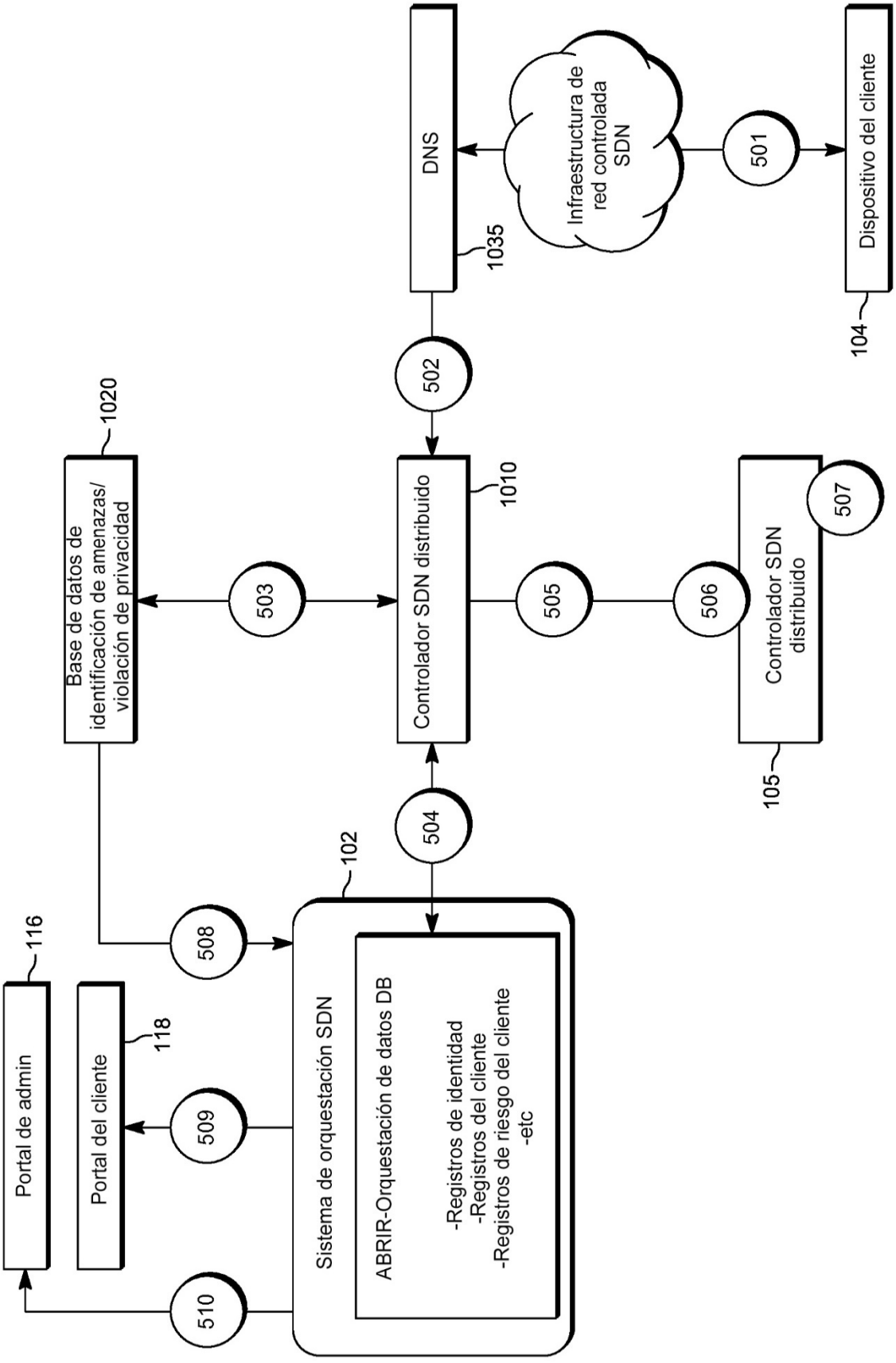
Portal de admin
116
Portal del cliente
118
510
509
508
Sistema de orquestación SDN
102
ABRIR-Orquestación de datos DB
-Registros de identidad
-Registros del cliente
-Registros de riesgo del cliente
-etc
Base de datos de identificación de amenazas/ violación de privacidad
1020
503
504
Controlador SDN distribuido
1010
505
506
Controlador SDN distribuido
507
105
502
DNS
1035
Infraestructura de red controlada SDN
501
Dispositivo del cliente
104

FIG. 19

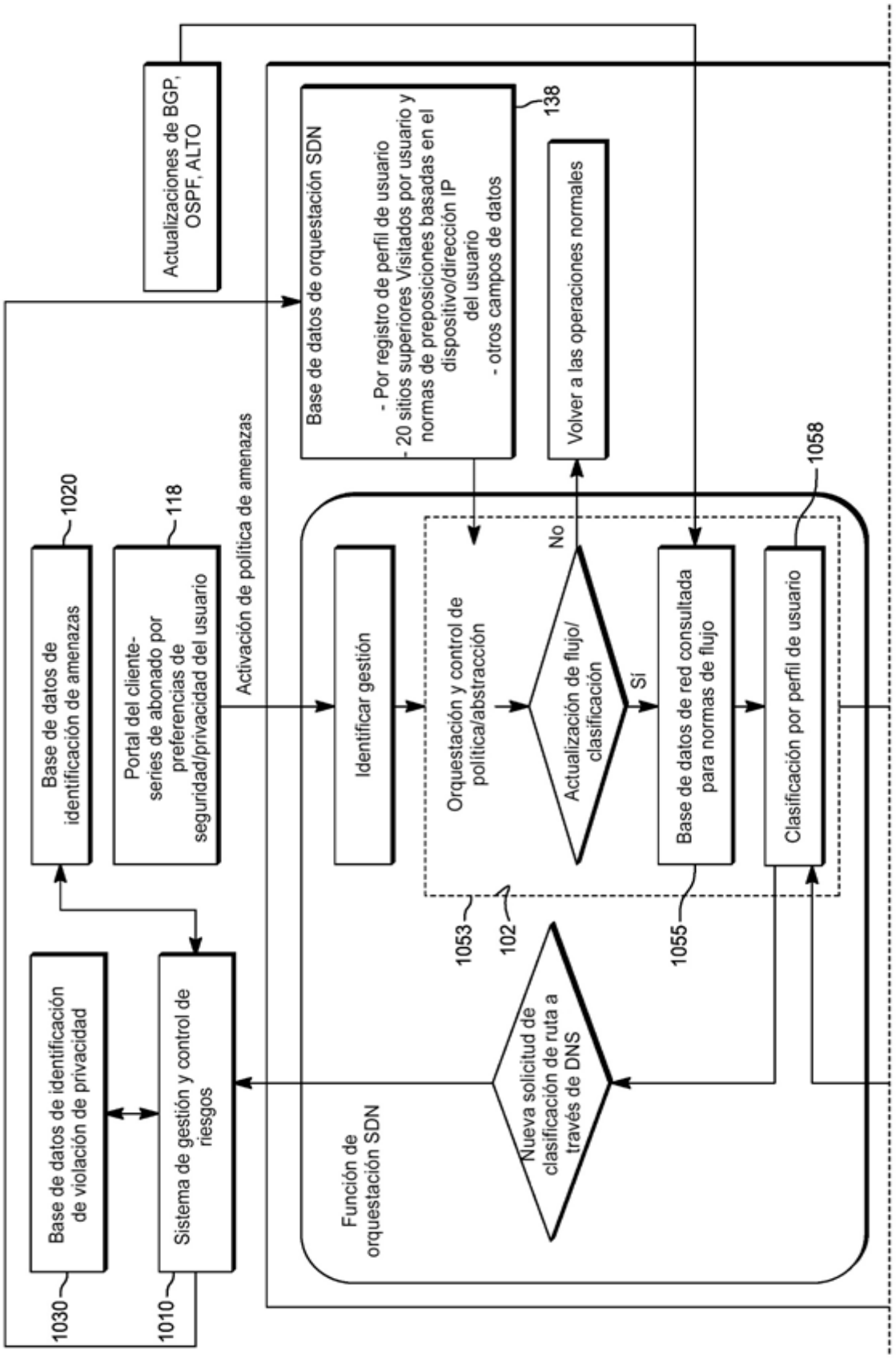
Actualizaciones de BGP, OSPF, ALTO
Base de datos de orquestación SDN
- Por registro de perfil de usuario
- 20 sitios superiores Visitados por usuario y normas de preposiciones basadas en el dispositivo/dirección IP del usuario
- otros campos de datos
138
Volver a las operaciones normales
1020
Base de datos de identificación de amenazas
118
Portal del cliente-series de abonado por preferencias de seguridad/privacidad del usuario
Activación de política de amenazas
Identificar gestión
Orquestación y control de política/abstracción
No
Actualización de flujo/ clasificación
Si
Base de datos de red consultada para normas de flujo
Clasificación por perfil de usuario
1058
1053
102
1055
Nueva solicitud de clasificación de ruta a través de DNS
Función de orquestación SDN
Base de datos de identificación de violación de privacidad
Sistema de gestión y control de riesgos
1030
1010

FIG. 20A

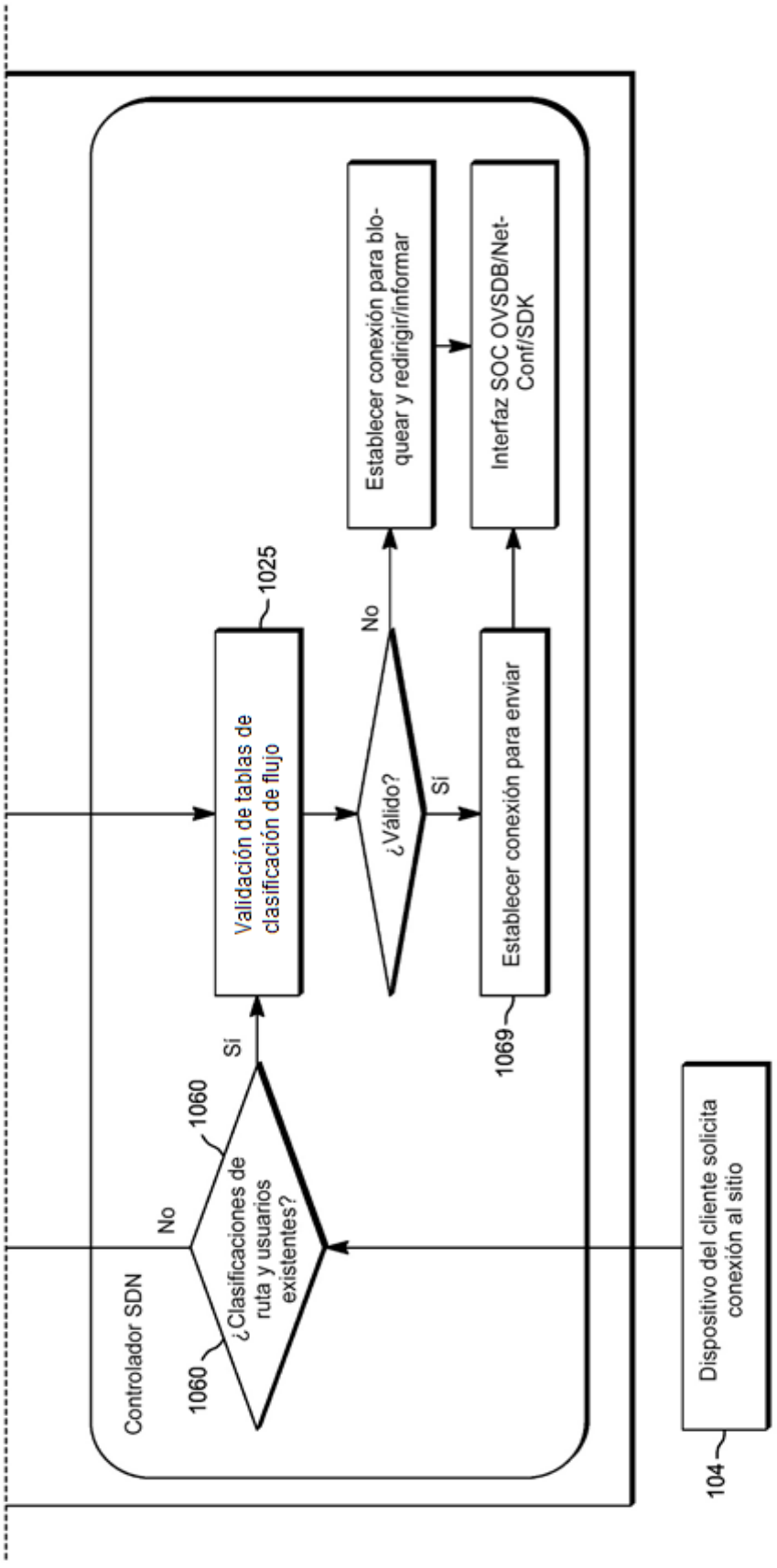
Controlador SDN
Dispositivo del cliente solicita conexión al sitio
104
¿Clasificaciones de ruta y usuarios existentes?
1060
1060
No
Sí
Validación de tablas de clasificación de flujo
1025
¿Válido?
No
Sí
Establecer conexión para bloquear y redirigir/informar
Interfaz SOC OVSDB/Net-Conf/SDK
Establecer conexión para enviar
1069

FIG. 20B

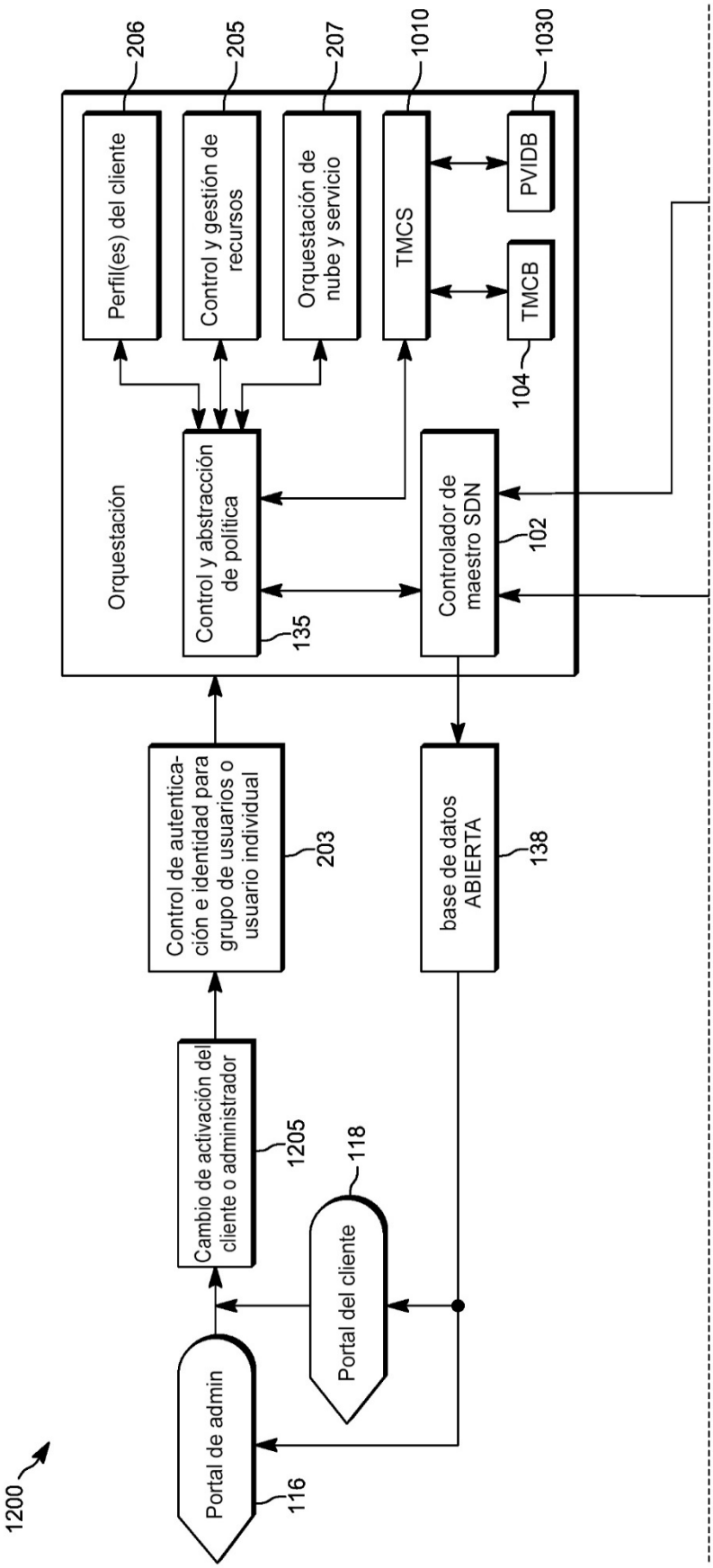
1200
Portal de admin
116
Portal del cliente
118
Cambio de activación del cliente o administrador
1205
Control de autentica-ción e identidad para grupo de usuarios o usuario individual
203
base de datos ABIERTA
138
Orquestación
Control y abstracción de política
135
Controlador de maestro SDN
102
Perfil(es) del cliente
206
Control y gestión de recursos
205
Orquestación de nube y servicio
207
TMCS
1010
PVIDB
TMCB
1030
104

FIG. 21A

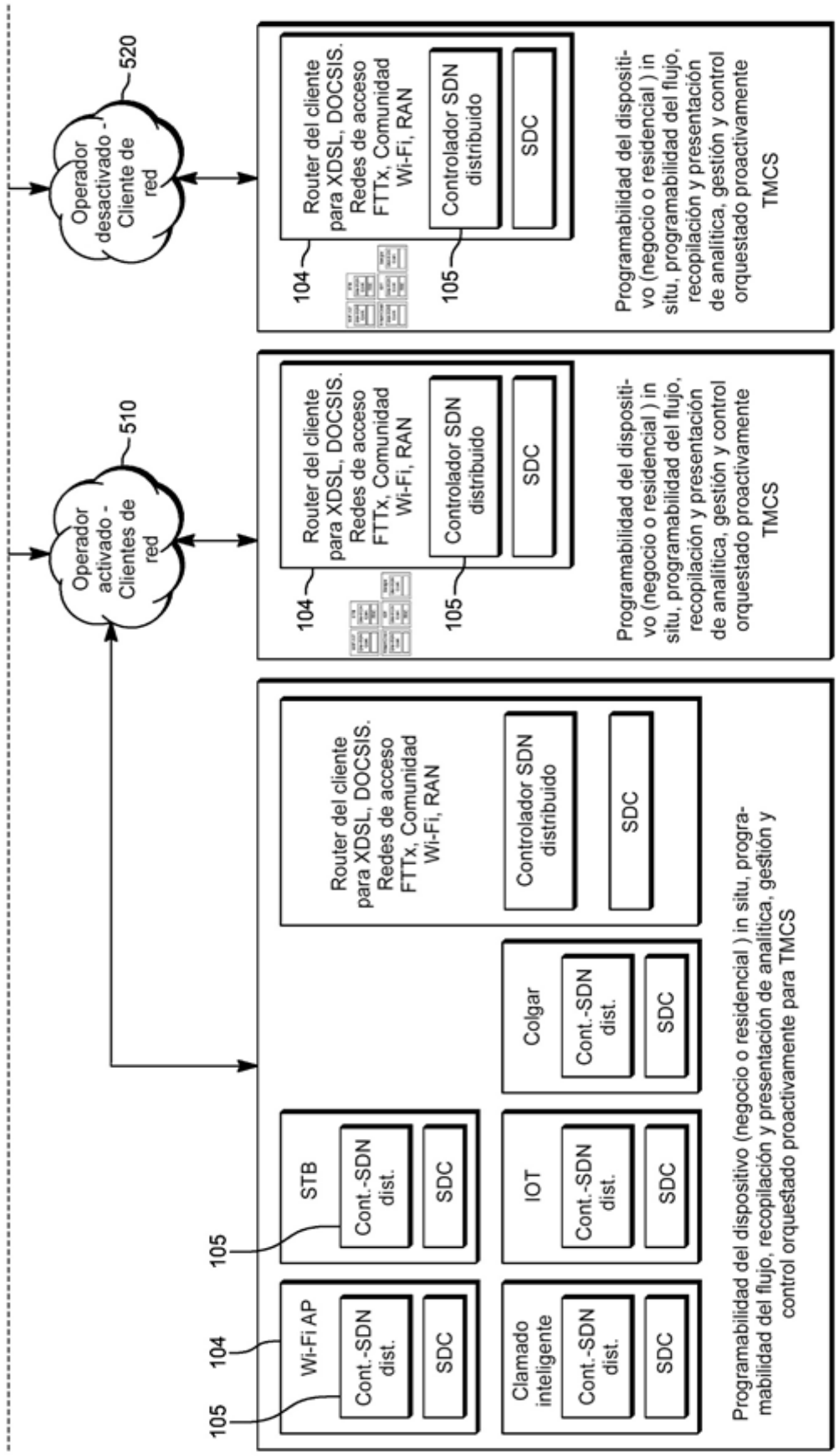
Operador desactivado - Cliente de red
520
Operador activado - Clientes de red
510
104
105
Router del cliente para XDSL, DOCSIS. Redes de acceso FTTx, Comunidad Wi-Fi, RAN
Controlador SDN distribuido
SDC
Programabilidad del dispositivo (negocio o residencial) in situ, programabilidad del flujo, recopilación y presentación de analítica, gestión y control orquestado proactivamente
TMCS
Wi-Fi AP
STB
IOT
Colgar
Clamado inteligente
Cont.-SDN dist.
Programabilidad del dispositivo (negocio o residencial) in situ, programabilidad del flujo, recopilación y presentación de analítica, gestión y control orquestado proactivamente para TMCS

FIG. 21B

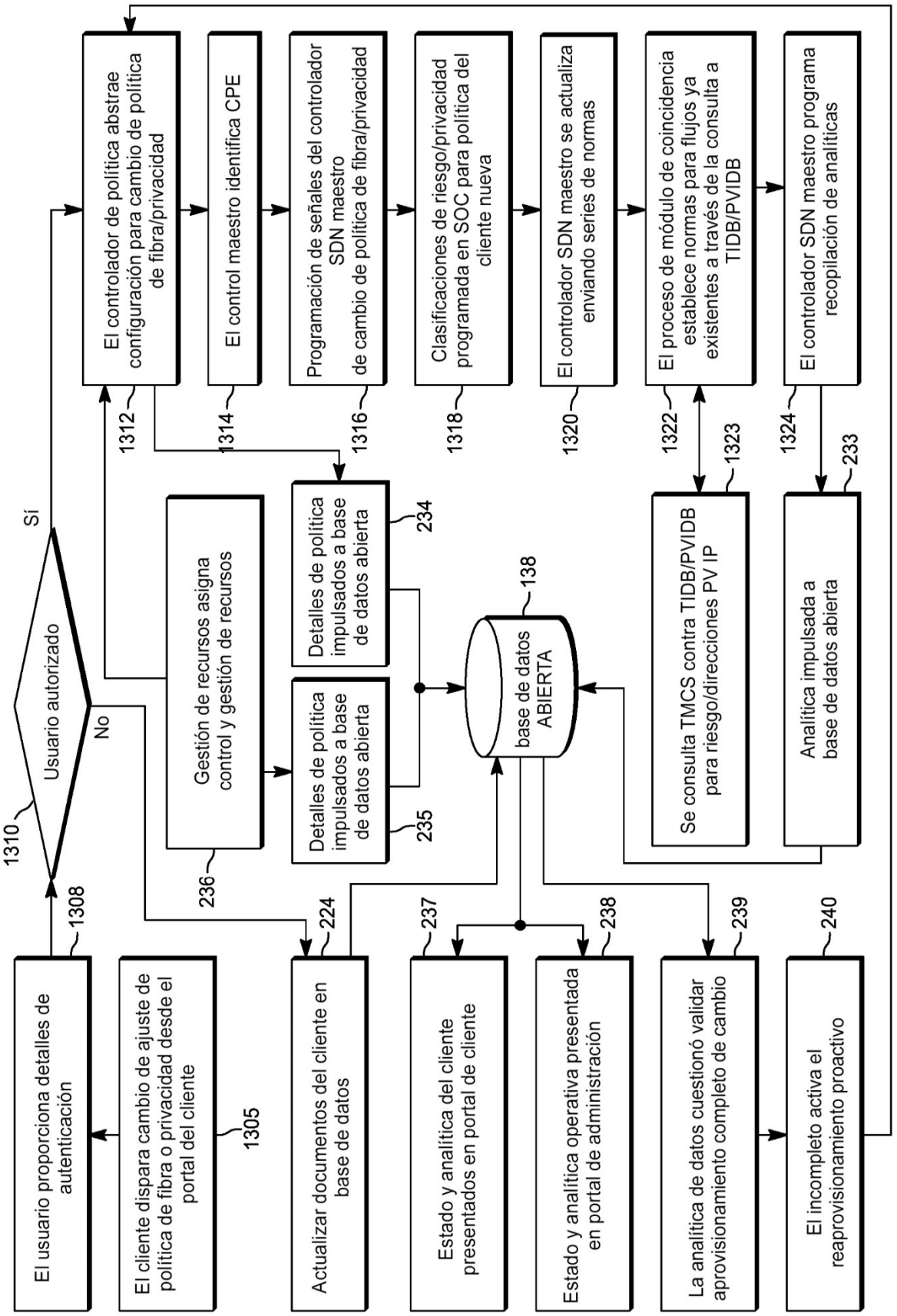
El usuario proporciona detalles de autenticación
1308
El cliente dispara cambio de ajuste de política de fibra o privacidad desde el portal del cliente
1305
Usuario autorizado
1310
Sí
No
Gestión de recursos asigna control y gestión de recursos
236
El controlador de política abstrae configuración para cambio de política de fibra/privacidad
1312
El control maestro identifica CPE
1314
Programación de señales del controlador SDN maestro de cambio de política de fibra/privacidad
1316
Clasificaciones de riesgo/privacidad programada en SOC para política del cliente nueva
1318
El controlador SDN maestro se actualiza enviando series de normas
1320
El proceso de módulo de coincidencia establece normas para flujos ya existentes a través de la consulta a TIDB/PVIDB
1322
El controlador SDN maestro programa recopilación de analíticas
1324
Detalles de política impulsados a base de datos abierta
234
Detalles de política impulsados a base de datos abierta
235
base de datos ABIERTA
138
Se consulta TMCS contra TIDB/PVIDB para riesgo/direcciones PV IP
1323
Analítica impulsada a base de datos abierta
233
Actualizar documentos del cliente en base de datos
224
Estado y analítica del cliente presentados en portal de cliente
237
Estado y analítica operativa presentada en portal de administración
238
La analítica de datos cuestionó validar aprovisionamiento completo de cambio
239
El incompleto activa el reaprovisionamiento proactivo
240

FIG. 22