APUNTES

SD-WAN: REDES DEFINIDAS POR SOFTWARE EN ENTORNOS WAN

Carlos M. Lentisco
e-mail: c.lentisco@upm.es
Departamento de Ingeniería de Sistemas Telemáticos
ETSIT-UPM

(Actualizado 2024)

CONTENIDO

1. Introducción a las redes WAN 3

1.1. Evolución de la arquitectura de la red WAN 4

1.2. Limitaciones de las redes WAN 6

2. SD-WAN: redes WAN definidas por software 6

2.1. Arquitectura de la red SD-WAN 7

2.1.1 Orquestación de servicios SD-WAN 12

2.2. Análisis de casos de uso 13

2.2.1 Servicios de red basados en NFV en centros de datos 15

3. Panorámica de soluciones SD-WAN existentes 18

3.1. Soluciones comerciales y académicas 18

3.1.1 Nuage 18

3.1.2 Viptela 19

3.1.3 Flexiwan 20

3.2. Otros trabajos de investigación 21

3.2.1 Ingeniería de tráfico (TE) basada en SDN 21

3.2.2 B4 24

3.2.3 SWAN 24

4. Conclusiones 25

5. Referencias 26

SD-WAN: REDES DEFINIDAS POR SOFTWARE EN ENTORNOS WAN

Este documento proporciona una visión sobre uno de los casos de éxito en lo que se refiere a la aplicación de soluciones basadas en redes definidas por software (*Software-Defined Networking* o SDN) [1] : las redes WAN definidas por software (*Software-Defined WAN* o SD-WAN). Los servicios SD-WAN son un mercado en expansión. Diferentes informes indican que la demanda de estos servicios ha aumentado significativamente. Es más, se espera que en el año 2023 los servicios SD-WAN generen hasta 5250 millones de dólares de beneficio [2] .

En primer lugar, el documento revisa conceptos fundamentales de las redes WAN tradicionales. Se proporciona una descripción sobre cómo estas redes han evolucionado con la migración de las aplicaciones a los entornos de computación en la nube. Además, se identifican las limitaciones que presentan estas redes y que motivan su transformación mediante la aplicación de soluciones de tipo SDN. A continuación, se presenta la arquitectura de las redes SD-WAN, revisando los estándares del Metro Ethernet Forum [3] . En la sección 2.2. Análisis de casos de uso se analizan los principales casos de uso de las redes SD-WAN, como, por ejemplo, escenarios donde se utilizan simultáneamente conexiones WAN públicas y privadas, o escenarios donde se aplican soluciones de ingeniería de tráfico basadas en SDN para el soporte de la calidad de servicio (*Quality of Service* o QoS). Finalmente, el documento ofrece una panorámica de soluciones SD-WAN existentes, tanto comerciales, como académicas. El documento finaliza proporcionando unas conclusiones.

1. INTRODUCCIÓN A LAS REDES WAN

Una red WAN (Wide Area Network) es una red de comunicaciones que opera más allá del ámbito geográfico de una red de área local (LAN). Las redes LAN interconectan computadoras y otros dispositivos periféricos, como por ejemplo impresoras, en un área geográfica pequeña. Las redes WAN interconectan redes LAN, permitiendo que dos dispositivos que están separados por una amplia distancia geográfica puedan comunicarse. Por ejemplo, las redes WAN permiten que dos equipos que pertenecen a la misma corporación, pero que están desplegados en ubicaciones remotas puedan comunicarse entre sí. La figura 1 muestra que la red WAN permite a los empleados de las oficinas A y B, situadas en diferentes ciudades del mismo país, acceder a servicios corporativos que se proporcionan desde un centro de procesamiento de datos (CPD) privado de la organización. Aunque la red de Internet es una red WAN, esta fue diseñada según el principio “Best Effort”, que se basa en tratar todos los paquetes IP que atraviesan la red por igual, sin tener en cuenta los requisitos de calidad de servicio de las aplicaciones. Es decir, la red de Internet trata por igual el tráfico de una aplicación de video conferencia, que tiene unos estrictos requisitos de retardo, que el tráfico generado por el servicio de correo electrónico, que presenta unos requisitos de retardo menos restrictivos. Por esta razón, las corporaciones contratan a los proveedores de servicios de Internet (*Internet Service Provider* o ISP) conexiones dedicadas que les garantizan un cierto nivel de QoS. De este modo, las prestaciones de las aplicaciones que son críticas para el negocio de la corporación no se ven afectadas por posibles variaciones de la QoS. Incluso así, las corporaciones mantienen una conexión hacia la red pública de Internet para poder establecer comunicación con dispositivos que no pertenecen a la red corporativa. De esta forma, coexisten múltiples conexiones WAN.

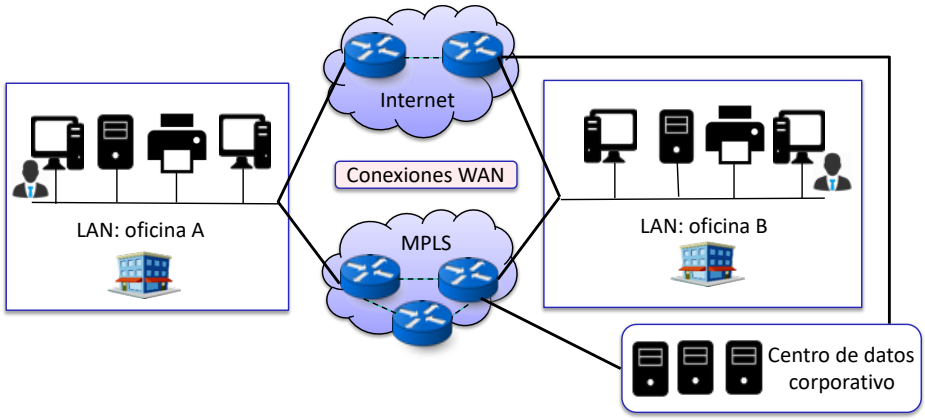

Figura 1 Redes WAN clásicas. La figura muestra que dos redes LAN desplegadas en dos oficinas de una corporación se interconectan a través de una red WAN

1.1. EVOLUCIÓN DE LA ARQUITECTURA DE LA RED WAN

Las redes corporativas han ido evolucionando para adaptarse al creciente uso de aplicaciones desplegadas en la "nube". La figura 2 muestra la arquitectura de las redes WAN antes de la irrupción de este paradigma de computación. Como puede observar, en la figura se representa un centro de datos privado que da soporte a las aplicaciones de negocio de la corporación y un conjunto de sedes centrales que se interconectan entre sí mediante una red MAN (*Metropolitan Area Network* o MAN). Las redes MAN también interconectan redes LAN en áreas extensas, pero normalmente su cobertura es más limitada que la de las redes WAN. La figura 2 muestra que las sedes y el CPD de la red MAN se comunican con oficinas ubicadas en otras ciudades a través de conexiones WAN. Como puede observar, los empleados de las oficinas remotas acceden a las aplicaciones de negocio desplegadas en el CPD privado a través de su conexión WAN. De ahí la importancia de que estas conexiones satisfagan los requisitos de QoS que imponen las aplicaciones. El objetivo es que las prestaciones de la red no afecten a las actividades de negocio de la corporación. Para ello, las corporaciones contratan las conexiones MAN y WAN a los operadores de red.

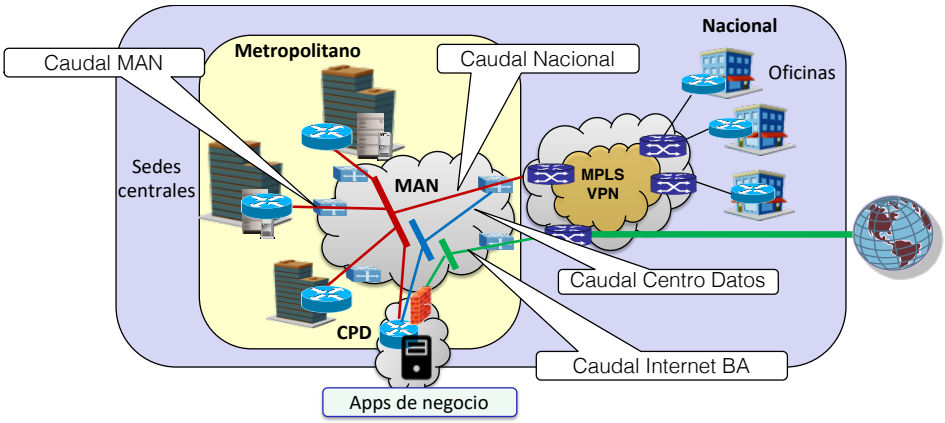

Figura 2 Evolución de las redes corporativas. Originalmente, las aplicaciones de negocio residían en centros de datos privados gestionados por la propia corporación. Las sedes centrales y el CPD se interconectan con las oficinas remotas mediante una conexión WAN basada en VPNs sobre MPLS.

Como se ha comentado anteriormente, existen diferentes tipos de conexiones WAN: la conexión WAN pública de Internet y las conexiones dedicadas basadas en MPLS (*MultiProtocol Label Switching*). MPLS surge

con la motivación inicial de acelerar el reenvío de paquetes en las redes IP. La idea consiste en que el reenvío se realiza en función de una etiqueta de longitud fija, y no mediante el uso de las direcciones IP que se incluyen en los paquetes. MPLS tiene diferentes aplicaciones, por ejemplo: permite implementar soluciones de ingeniería de tráfico (sección 3.2.1 Ingeniería de tráfico (TE) basada en SDN) o crear redes privadas virtuales (*Virtual Private Network* o VPN). Como puede observar en la figura 2, se ha considerado un escenario en el que las sedes centrales y oficinas remotas se comunican mediante una conexión WAN basada en VPNs creadas sobre redes MPLS. La idea es que el propio ISP defina las VPNs estableciendo rutas que separen el tráfico que circula por la VPN y el tráfico que atraviesa Internet. En el establecimiento de estas rutas, el ISP aplica soluciones que garantizan los requisitos de calidad servicio que se definen en los acuerdos de nivel de servicio (*Service Level Agreement* o SLA) que se establecen entre ambas partes (corporación e ISP). Aunque también se pueden establecer VPNs sobre la red de Internet, los requisitos de QoS no pueden garantizarse en este caso debido al principio "best effort" que rige la red. Aun así, es necesario proporcionar acceso a Internet a las sedes centrales y oficinas para que puedan comunicarse con el exterior. La figura muestra que, por motivos de seguridad de acceso, todo este tráfico se canaliza a través del CPD, que es el único punto de la red corporativa conectado a la red del ISP. En ocasiones, el tráfico dirigido hacia Internet debe cruzar buena parte las redes nacionales de la corporación. Piense que el tráfico que se origina en las "Oficinas", y que se dirige hacía Internet, antes debe atravesar antes la red MPLS y llegar al CPD.

Las aplicaciones telemáticas cada vez demandan más recursos de red, cómputo y almacenamiento para su correcto funcionamiento. Muchas de estas aplicaciones, que residían tradicionalmente en el CPD de la corporación, han pasado a desplegarse en la nube pública (por ejemplo, Azure, o AWS). Esto plantea nuevos desafíos para gestionar el tráfico de las redes corporativas. La figura 3 muestra que los usuarios de la red corporativa acceden a diferentes aplicaciones que se despliegan en la nube a través de su conexión a Internet. Algunas de estas aplicaciones se proporcionan como software bajo demanda siguiendo el modelo "software como servicio" (*Software as a Service* o SaaS). Este modelo se basa en que un proveedor externo aloja sus aplicaciones en la nube y las ofrece a los usuarios a través de Internet mediante un modelo de suscripción. La figura muestra algunas herramientas ofimáticas y aplicaciones de mensajería instantánea que siguen este modelo. Sin embargo, también es posible utilizar las plataformas de computación en la nube para hacer accesibles las aplicaciones propietarias de la corporación a través de Internet. La prestación de estos servicios sigue el modelo "infraestructura como servicio" (*Infrastructure as a Server* o IaaS). Siguiendo este modelo, las corporaciones contratan la utilización de recursos de cómputo, almacenamiento y red de la nube para desplegar sus propias aplicaciones.

La migración de las aplicaciones a la nube aumenta el caudal de tráfico que atraviesa la conexión a Internet, de forma que el acceso a Internet se convierte en el cuello de botella de la red corporativa. Una posible solución para evitar este problema es proporcionar acceso a Internet a cada sede y oficina de la corporación. La migración de aplicaciones a la nube ofrece diferentes ventajas: (1) *agilidad*. Una corporación puede realizar sus actividades de negocio sin tener que contratar una conexión WAN privada al ISP. (2) *Migración*. La corporación puede cambiar de proveedor de servicios en la nube según sus necesidades.

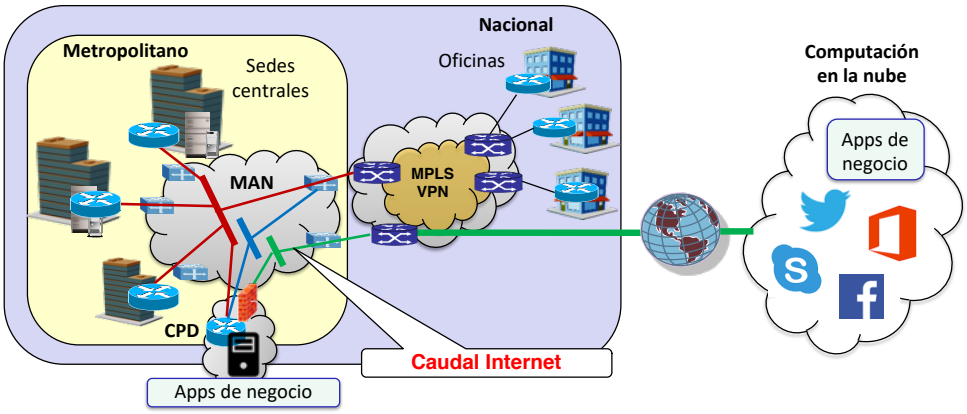

Figura 3 Evolución de las redes corporativas. El creciente uso de aplicaciones desplegadas en la nube plantea nuevos desafíos para garantizar la calidad de servicio que requieren las aplicaciones que utiliza la corporación

1.2. LIMITACIONES DE LAS REDES WAN

La migración de aplicaciones en la nube también tiene desventajas: (1) *seguridad*. Internet proporciona menos seguridad que las conexiones WAN privadas, por ejemplo, es posible realizar ataques de tipo "man in the middle" para capturar la información en tránsito. (2) *Calidad de servicio*. Internet no garantiza los requisitos de calidad de servicio que demandan las aplicaciones.

Por otro lado, la gestión de las arquitecturas de red WAN clásicas es compleja, en parte, por la ausencia de mecanismos que permitan configurar estas redes de una forma más flexible. Los administradores de las redes MPLS requieren tiempo para establecer y configurar las VPNs sobre MPLS. Por otro lado, y aunque las redes MPLS han sido diseñadas para dar soporte a calidad de servicio (modelo Diffserv [4]), si un cliente solicita más ancho de banda del que ha contratado, es necesario realizar modificaciones en las configuraciones de los equipos de red manualmente. Estas modificaciones no son inmediatas. Por esta razón, es bastante habitual que los clientes contraten con el ISP una conexión con más ancho de banda del que normalmente consumen, de forma que, si eventualmente se produce un mayor consumo, sea posible evitar la congestión de la conexión WAN. Como puede imaginar, además de la baja utilización de los enlaces, sobredimensionar el ancho de banda supone un mayor coste para las corporaciones. Los operadores de red también deben hacer frente a costes significativos de inversión en equipamiento y gestión de la red WAN. Estos costes de gestión se explican, en parte, por la necesidad de aplicar con frecuencia cambios en las configuraciones de los equipos de red, normalmente, mediante el uso de lenguajes específicos de cada fabricante.

2. SD-WAN: REDES WAN DEFINIDAS POR SOFTWARE

En las redes WAN tradicionales, los nodos de conmutación de paquetes integran funciones del plano de datos, del plano de control y del plano de gestión. El plano de datos se encarga del proceso de almacenamiento y reenvío de paquetes. El plano de control se encarga de determinar el contenido de la tabla de reenvío a partir de la información que intercambian los conmutadores de la red forma distribuida (figura 4a). El plano de gestión se ocupa de funciones relacionadas con la configuración, operación y mantenimiento del conmutador. En las redes SDN, el plano de control y el plano de datos se desacoplan. El plano de control se centraliza a nivel lógico en un nodo controlador que se encarga de programar la tabla de reenvío de los conmutadores SDN que componen la red (figura 4b).

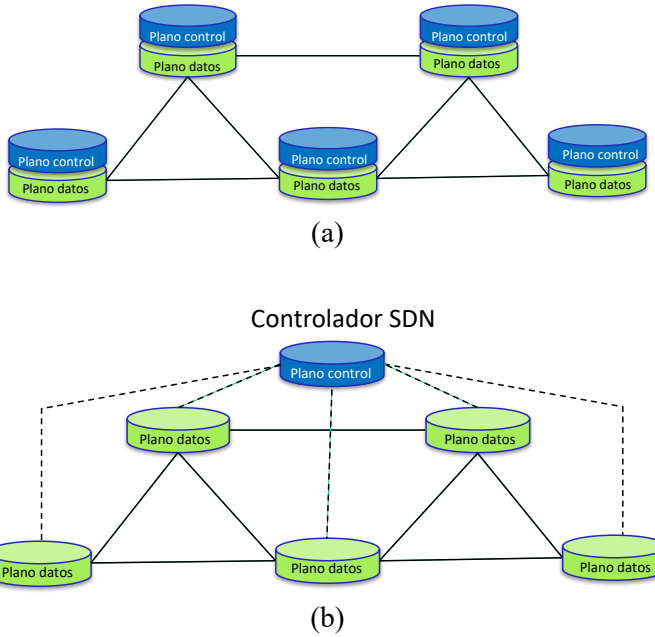

Figura 4 Arriba (a), la figura muestra una red de conmutación de paquetes tradicional. Los nodos integran las funciones del plano de datos y de control. Abajo (b), la figura muestra una red basada en SDN, donde existe un nodo controlador que centraliza la programación de la tabla de reenvío de los conmutadores.

Software-Defined Wide Area Network (SD-WAN) es el resultado de aplicar las tecnologías SDN a las conexiones WAN. La aplicación de soluciones basadas en SDN en este entorno proporciona diferentes ventajas:

- Facilita la implementación de mecanismos que mejoran la calidad que perciben los usuarios cuando hacen uso de las aplicaciones. Las redes SD-WAN reducen la complejidad que conlleva configurar el equipamiento de red para satisfacer los requisitos de QoS que imponen las aplicaciones. Desde el nodo controlador, es posible gestionar las políticas de QoS sin necesidad de configurar manualmente cada nodo de conmutación. Esto proporciona una gran flexibilidad, ya que, por ejemplo, es posible reprogramar la red dinámicamente si los requisitos de QoS varían en el tiempo.
- Agiliza la adaptación al negocio. Las redes SD-WAN reducen el tiempo de respuesta que se requiere para poner en marcha nuevos equipos, servicios, e incluso nuevas sedes u oficinas. Las redes SD-WAN automatizan el establecimiento de túneles VPN para conectar los diferentes puntos de la red corporativa.
- Permite realizar una gestión más eficiente de los recursos de red. En las redes corporativas clásicas es común sobredimensionar el ancho de banda de las conexiones WAN privadas para evitar que el rendimiento de las aplicaciones se degrade si el consumo de ancho de banda varía. Las redes SD-WAN permiten realizar una gestión más eficiente de los recursos de red, siendo posible asignar el ancho de banda bajo demanda.
- Reduce costes. El coste para gestionar y operar una red WAN también se reduce mediante la aplicación de soluciones de tipo SDN. Por ejemplo, es posible desplegar infraestructuras de red basadas en conmutadores de caja blanca, que son conmutadores basados en hardware de propósito general que operan con software de código abierto. El coste también se reduce por la capacidad de automatizar tareas de configuración y gestión de la red mediante software. Además, la disponibilidad de múltiples conexiones WAN (pública y privada) también puede reducir costes. El tráfico de las aplicaciones de negocio puede encaminarse sobre una conexión WAN privada para satisfacer sus requisitos de QoS. El tráfico de otras aplicaciones, sin estrictos requisitos de QoS, puede encaminarse sobre la red pública de Internet, que es más barata.

2.1. ARQUITECTURA DE LA RED SD-WAN

Según el estándar publicado por el MEF [5] , un servicio SD-WAN se define como una red virtual que conecta las redes del suscriptor garantizando unos requisitos de QoS determinados. Como se ha comentado anteriormente, el servicio SD-WAN puede operar sobre diferentes redes de transporte (*Underlay Connectivity Services* o UCS) como, por ejemplo, Internet o una VPN basada en MPLS. De aquí en adelante, se utilizará el término UCS para hacer referencia a estas conexiones WAN. Note que el proveedor de servicios SD-WAN y el proveedor de telecomunicaciones pueden ser diferentes actores del modelo de negocio. El estándar define que el proveedor de SD-WAN se encarga de gestionar el tráfico que se transporta sobre los UCS que ha contratado el suscriptor, pero estos UCSs pueden estar operados por un tercero; un proveedor de telecomunicaciones. En este caso, el suscriptor debe proporcionar información sobre sus UCSs al proveedor de SD-WAN. Aun así, esto no excluye la posibilidad de que el proveedor de SD-WAN también sea el operador de uno o varios de los UCSs del suscriptor. Durante la definición del servicio SD-WAN se especifican todas estas cuestiones. El suscriptor acuerda con el proveedor de SD-WAN cuáles son los UCSs que formarán parte del servicio. En ese acuerdo, el suscriptor puede indicar al proveedor cuál es el UCS principal y cuál es el UCS de respaldo.

Por otro lado, el suscriptor indica al proveedor de SD-WAN las localizaciones de las oficinas, sedes y centros de datos de la corporación, así como los requisitos de calidad de servicio que demandan las aplicaciones que va a utilizar. El proveedor, utilizando soluciones basadas en SDN, monitoriza el rendimiento del servicio SD-WAN y actúa en tiempo real para modificar la ruta que sigue el tráfico de las aplicaciones con el objetivo de satisfacer sus requisitos de QoS.

La figura 5 muestra los componentes del servicio SD-WAN, tal y como se definen en el estándar del MEF. Los nodos SD-WAN Edge implementan las funciones del plano de datos del servicio SD-WAN. Los nodos SD-WAN tienen interfaces hacía las redes del suscriptor (*SD-WAN User Network Interface* o SD-WAN UNI) e interfaces hacía los UCS. La unidad básica de transporte en los nodos SD-WAN Edge es el paquete IP. Cuando se recibe un paquete IP en la interfaz SD-WAN UNI, se determina su interfaz UCS de salida utilizando información de diversa índole: políticas de calidad de servicio, información de los UCSs y otros atributos del servicio SD-WAN. Para que un nodo SD-WAN Edge pueda tomar decisiones de encaminamiento sobre el tráfico de un suscriptor, es necesario que, previamente, este acuerde con el proveedor de servicios SD-WAN qué "flujos de aplicación" (*Application Flow*) pueden ser gestionados por el servicio SD-WAN. Un flujo de aplicación se describe como un conjunto de paquetes IP que comparten el valor de algunos campos de sus cabeceras (desde nivel 2 al nivel 7). Por ejemplo, se puede definir un flujo de aplicación como todos los paquetes que se transporten sobre RTP (*Real Time Protocol*), o como todos los paquetes que pertenezcan a una sesión de vídeoconferencia. Cuando se define un nuevo flujo de aplicación es necesario asignarle una política. Esta política proporciona los detalles sobre cuál va a ser el tratamiento que van a recibir los paquetes que ingresan en la interfaz SD-WAN UNI. Esto incluye reglas de encaminamiento, seguridad e información sobre el ancho de banda garantizado. Además, el estándar del MEF indica que un flujo de aplicación puede ser miembro de un "grupo de flujo de aplicación" (*Application Flow Group*). La agrupación de flujos hace posible, por ejemplo, asignar la misma política a todos los miembros del grupo.

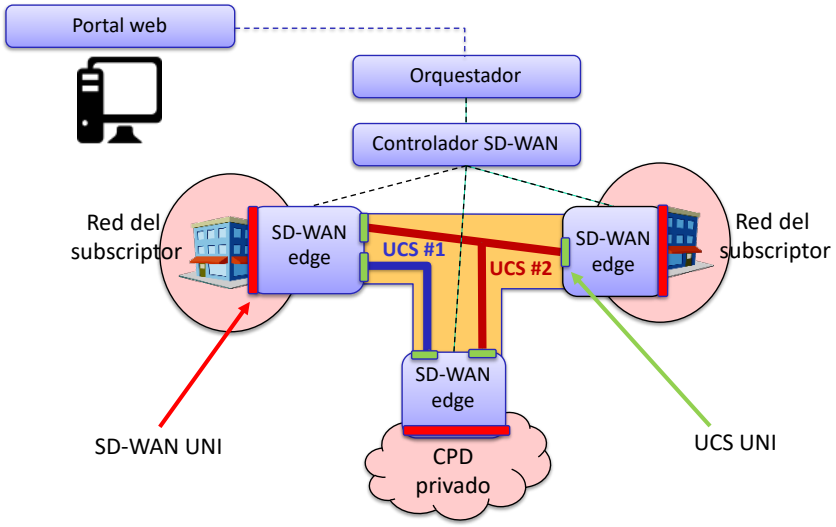

Figura 5 Arquitectura de la red SD-WAN. La figura muestra los elementos que definen los estándares de redes SD-WAN

La figura 6 muestra más detalles de la arquitectura de referencia. En este caso la figura muestra que el proveedor de servicios SD-WAN establece conexiones punto-a-punto sobre los UCS que tiene contratado el suscriptor. Estas conexiones son túneles virtuales (*Tunnel Virtual Connection*, TVC) como, por ejemplo, VPNs construidas sobre MPLS. Una de las principales funciones del nodo SD-WAN Edge es conmutar los paquetes que ingresan en la interfaz SD-WAN UNI a un TVC de salida que cumpla con las políticas que han sido definidas para el flujo de aplicación al que pertenece. Por otro lado, la figura 6 muestra que, cuando uno de los UCS contratados por la corporación es el servicio público de Internet, es posible enviar el tráfico de un flujo de aplicación directamente a Internet, en lugar de enviarlo a otra interfaz SD-WAN UNI. Para ello, el estándar define el campo "Internet-Breakout" que se incluye en las políticas que controlan los flujos de aplicación. Puede ocurrir que un flujo de aplicación tenga asignada una política donde se indica que el tráfico de la aplicación debe dirigirse a Internet, pero el nodo SD-WAN Edge que está procesando el paquete no tenga este acceso. En dicho caso, el SD-WAN Edge puede conmutar el tráfico a un TVC de salida cuyo destino sea un SD-WAN Edge que tenga acceso a Internet. Internet es un UCS que normalmente no está operado por el proveedor de SD-WAN. Es por ello, que el suscriptor debe facilitar al proveedor de SD-WAN información sobre: direccionamiento IP, ancho de banda de la conexión e información sobre la función NAT (*Network Address Translation*). El acceso a Internet, como se vio en la introducción, permite a los usuarios de la red corporativa acceder a aplicaciones que se proporcionan como SaaS en una nube pública.

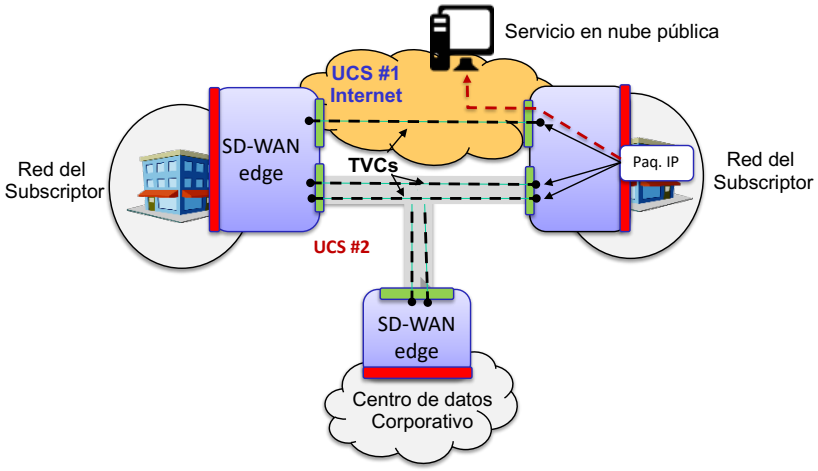

Figura 6 Arquitectura de la red SD-WAN. La figura muestra los túneles virtuales que se establecen sobre los UCS y como se realiza el acceso a Internet desde las redes del suscriptor

Finalmente, y a modo de resumen, la figura 7 ilustra el funcionamiento de los nodos SD-WAN Edge. Los paquetes IP de los flujos de aplicación entran en el nodo SD-WAN a través de la interfaz SD-WAN UNI. La primera función que realiza el SD-WAN Edge es comprobar si el paquete IP que ingresa en la interfaz pertenece a alguno de los flujos de aplicación que han sido definidos en el servicio SD-WAN. La clasificación se puede realizar considerando diferentes campos de las cabeceras del paquete (desde nivel 2 a nivel 7). Por ejemplo, los paquetes se pueden clasificar según el contenido de la cabecera 802.1q o en función de la dir. IP de origen y/o destino. Una vez se ha clasificado el paquete, el nodo SD-WAN edge debe aplicar la política asignada al flujo de aplicación. Las políticas se definen mediante la especificación de diversos campos. A continuación, se proporciona una descripción de estos campos:

- ENCRYPTION: si el valor de este campo es “yes” el nodo SD-WAN Edge que recibe el tráfico debe cifrarlo antes de encaminarlo al UCS de salida. Normalmente, esto se implementa estableciendo un túnel con cifrado.
- PUBLIC-PRIVATE: si el valor de este campo es “private-only” el tráfico del Application Flow solo puede transportarse sobre conexiones WAN privadas, es decir, sin atravesar Internet.
- INTERNET-BREAKOUT: si el valor de este campo es “yes” el tráfico del Application Flow debe encaminarse directamente a una conexión WAN pública con acceso a Internet.
- BILLING-METHOD: si el valor de este campo es “Flat-Rate-Only” el tráfico del Application Flow debe encaminarse a un UCS cuyo método de tarificación sea tarifa plana, no por uso.
- BACKUP: como se ha comentado anteriormente, el suscriptor puede indicar al proveedor de SD-WAN que puede utilizar un UCS de respaldo, por ejemplo, para evitar la caída de la comunicación ante fallos. Este UCS puede tener asociado un ancho disponible menor o un mayor coste, por lo que es recomendable controlar el acceso de las aplicaciones a este UCS. Si el valor de este campo es “yes”, el proveedor de SD-WAN considera el uso de este UCS de respaldo.
- BANDWITH: este campo es en realidad una tupla formada por dos elementos. El parámetro *commit* indica el ancho de banda promedio que requiere la aplicación. El parámetro *max*, el ancho de banda máximo.

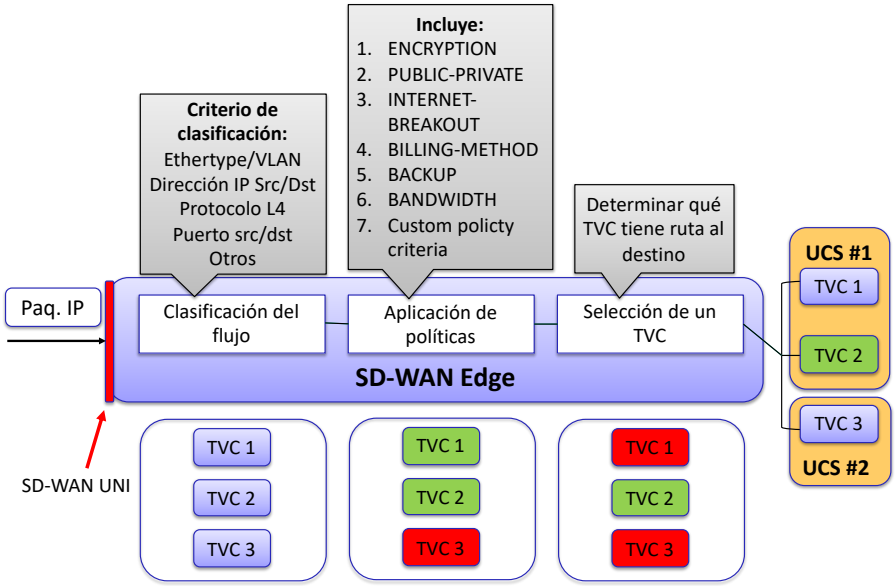

Figura 7 Ejemplo para ilustrar el funcionamiento del nodo SD-WAN Edge

La figura 7 muestra como ejemplo que el servicio SD-WAN se construye sobre tres TVCs diferentes. Sin embargo, solo dos de ellos cumplen con la política asignada al flujo de aplicación (TVC 1 y TVC 2). Imagine, por ejemplo, que el flujo de aplicación al que pertenece el paquete tiene asociada una política que indica que el tráfico debe cifrarse. El túnel TVC 3 no aplica mecanismos de cifrado por lo que no puede ser seleccionado para transportar el tráfico. Finalmente, el nodo SD-WAN edge toma una decisión para encaminar el paquete IP que ingresa en la interfaz SD-WAN UNI. Para ello, elige, de entre todos los TVCs que cumplen con la política del flujo de aplicación, aquel que tiene una ruta con el destino de la comunicación (TVC 2).

Existen diferentes estrategias para desplegar los nodos SD-WAN Edge en la red corporativa del suscriptor [6] . La primera, consiste en desplegar los nodos como equipos físicos en las oficinas, centros de datos y sedes de la corporación. La segunda, consiste en desplegar el nodo SD-WAN Edge como una función de red virtualizada (*Virtual Network Function* o VNF) que se instancia en un uCPE (*universal Custome Premise Equipment*) [7] . Un uCPE es una plataforma de computación que se despliega en las instalaciones de la corporación y que tiene capacidad para ejecutar VNFs. Las redes corporativas clásicas se basan en el uso de CPEs que integran software y hardware propietario en un mismo equipo. Este CPE incluye diversas funciones, como, por ejemplo, funciones de encaminamiento, firewall o balanceo de carga. Si la corporación está interesada en extender la funcionalidad de su red, por ejemplo, dando soporte a funciones avanzadas de firewall, se ve ante la necesidad de adquirir nuevo equipamiento. Las plataformas uCPEs ofrecen una gran flexibilidad a este respecto, puesto que es posible instanciar, en las instalaciones de la red corporativa, VNFs de diferentes tipos y fabricantes. Así, se considera que una posible estrategia para desplegar el SD-WAN es, instanciarlo como VNF en los uCPEs de la corporación. El ciclo de vida de esta VNF estaría gestionado por la plataforma de orquestación de VNFs (*NFV-Management and Orchestration*, NFV-MANO) del proveedor de servicios SD-WAN. Finalmente, la tercera estrategia de despliegue del nodo SD-WAN Edge es instanciar una VNF en la nube del proveedor de servicios SD-WAN, sin embargo, esta solución tiene la desventaja de que si se pierde la conexión de la red corporativa con la nube del proveedor de SD-WAN, el servicio se interrumpe.

Puede consultar más información acerca de la virtualización de funciones de red en la sección 2.2.1 Servicios de red basados en NFV en centros de datos de este documento.

2.1.1 Orquestación de servicios SD-WAN

SD-WAN simplifica la gestión y administración de las redes WAN. Crear una VPN para conectar dos puntos de presencia de una red corporativa es complejo desde el punto de vista de la configuración. Además, asignar ancho de banda bajo demanda a estas conexiones requiere frecuentes cambios en dicha configuración. La separación del plano de datos y control que proporcionan las redes SDN permite crear APIs abiertas que los administradores de red pueden utilizar para configurar las conexiones WAN, ya sea para configurar dinámicamente el ancho de banda asignado o para aplicar diferentes políticas de red. Por ejemplo, ante un ciberataque, el administrador podría definir una política de filtrado paquetes que el controlador SD-WAN se encargaría de implementar a través de la programación de los conmutadores SDN de la red. Esto evita modificar manualmente la configuración de los diversos equipos de red que componen la red WAN.

El diseño del API de la red SD-WAN debe considerar los siguientes aspectos:

1. El establecimiento de las conexiones WAN a través del API requiere tener una visión global de la red (que la SDN puede proporcionar). Sin embargo, y debido a cuestiones de seguridad, es recomendable no exponer demasiada información de la topología de la red. Por estos motivos, normalmente se considera que el orquestador del servicio trabaja con una versión resumida y lógica, es decir, con una abstracción de la red.
2. Detección de conflictos. Cuando un administrador utiliza un API para solicitar una conexión WAN debe definir las políticas que se aplican a los flujos de aplicación asociados al servicio (sección 2.1. Arquitectura de la red SD-WAN). Es necesario proporcionar consistencia entre las políticas definidas por el administrador para evitar comportamientos anómalos en el servicio. Imagine que se define una lista de control de acceso que indica que ciertos paquetes deben ser denegados (*deny*) y permitidos (*permit*) al mismo tiempo.
3. Asignación de ancho de banda. Cuando el administrador define una política para garantizar un requisito de QoS de un flujo de aplicación, el orquestador y controlador de la red SD-WAN gestionan esta petición, determinando, a través de soluciones de ingeniería de tráfico, cuál es la mejor ruta que debe seguir el tráfico. El objetivo es evitar que los clientes contraten más recursos de red de los que realmente consumen, y que la asignación de ancho de banda se realice bajo demanda.

Como ejemplo, se va a describir a continuación el diseño de una propuesta que ha sido publicada en una revista con alto impacto científico [15] . La figura 8 muestra los componentes de la arquitectura de Grace, el nombre con el que un grupo de investigadores ha bautizado su orquestador y controlador de la red SD-WAN. El núcleo de Grace está compuesto por varios módulos. Grace tiene un módulo de detección de conflictos (*conflict detection*) que comprueba todas las políticas que se han definido para cada suscriptor. Otro módulo es el compilador (*compiler*) que se encarga de convertir las solicitudes de conexiones WAN en reglas de encaminamiento que se programan en los conmutadores de la red. Para determinar estas rutas se ejecuta un algoritmo de asignación de ancho de banda (ingeniería de tráfico) que utiliza información de la topología de la red. Grace también cuenta con un planificador (*scheduler*), que es un módulo que se encarga de determinar cuándo se debe programar la red SDN para implementar la conexión WAN. Imagine que un suscriptor solicita una nueva conexión WAN, el planificador determina si es necesario implementar dicha conexión inmediatamente o si por el contrario es posible planificar su establecimiento más tarde.

Grace exporta un API que considera diferentes tipos de conexiones WAN: (1) conexiones que interconectan uno o más puntos de presencia de una red corporativa, como, por ejemplo, la conexión de la sede central con las oficinas remotas. (2) una conexión de una entidad que actúa como productor/consumidor de servicios gestionados por otra entidad que actúa como consumidor/productor. El escenario que se considera en este caso es el de una compañía B que accede a servicios alojados en los centros de datos privados de una compañía A. (3) la conexión hacía Internet.

Así, el API de Grace incluye los siguientes campos:

- *Connection name:* nombre de la conexión WAN solicitada
- *Connection type*: campo que especifica el tipo de conexión según lo comentado anteriormente.
- *Connection effective time*: tiempo de comienzo y final de la conexión WAN
- *Bandwidth/Transmission size*: ancho de banda requerido por el suscriptor para transmitir datos con un cierto volumen.
- *Customized network policies*: tupla formada por dos elementos: condición y acción. La condición es una lista de campos de cabeceras de paquetes que se utilizan para clasificar el tráfico. La acción son reglas de control de acceso (para permitir o denegar el tráfico) o reglas de conformación de tráfico (para garantizar una tasa de datos de servicio) que se aplican cuando la condición anterior se cumple.

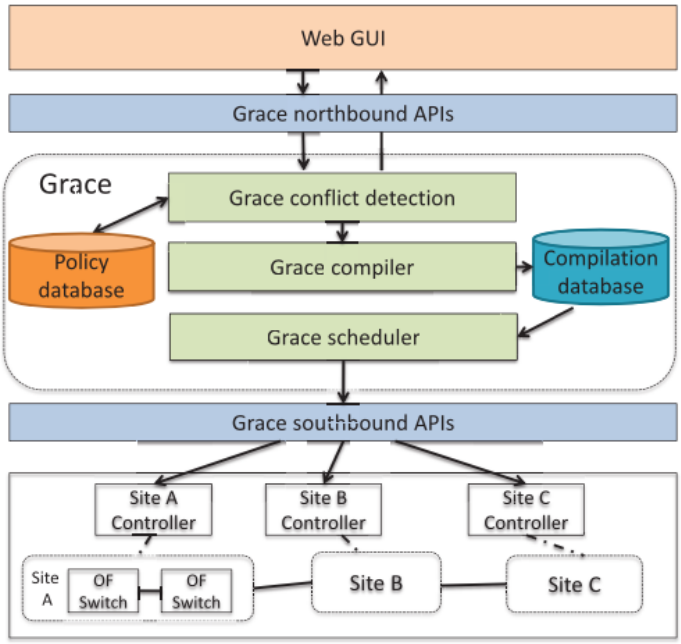

Figura 8 Arquitectura de Grace. La figura muestra los componentes del orquestador y controlador de la red SDWAN. Fuente: [15]

2.2. ANÁLISIS DE CASOS DE USO

En esta sección se analizan los principales casos de uso de las redes SD-WAN [6] . El primero de ellos (Figura 9a) es un servicio que se proporciona sobre dos VPNs basadas en MPLS. Un posible escenario es el de una corporación que ejecuta aplicaciones de misión crítica. Las aplicaciones de misión crítica tienen unos estrictos requisitos de seguridad debido a que contienen información sensible para la corporación. También deben proporcionar una gran tolerancia frente a fallos porque la disrupción del servicio afecta significativamente a los suscriptores del servicio y produce grandes pérdidas económicas en el proveedor WAN. En este contexto, los suscriptores suelen contratar dos VPNs basadas en MPLS para que una actúe como respaldo de la otra. El problema es que la conexión de respaldo permanece inactiva salvo que la conexión principal sufra una caída del servicio. El proveedor de servicios SD-WAN es capaz de utilizar ambas conexiones WAN ofreciendo un mayor nivel de disponibilidad de servicio.

El segundo caso de uso (Figura 9b) es muy semejante al anterior, solo que, en este caso, el servicio SD-WAN se proporciona sobre una VPN basada en MPLS y sobre un túnel cifrado sobre la red pública de Internet. Es por ello por lo que se considera este caso de uso como una red WAN híbrida, porque combina conexiones WAN

privadas y públicas. La idea es mejorar el servicio que proporciona la conexión WAN privada utilizando una conexión WAN pública de bajo coste. La conexión de Internet se puede utilizar como UCS de respaldo para dotar al servicio de una mayor tolerancia frente a fallos a un coste reducido. Pero, en general el servicio SD-WAN se encarga de encaminar el tráfico de las aplicaciones, o bien por la VPN, o bien a través de Internet, en función de los requisitos de QoS que demandan las aplicaciones. Es decir, el tráfico de las aplicaciones que no son críticas para el negocio de la corporación puede enviarse sobre Internet. Aun así, también es posible asignar el ancho de banda adicional que proporciona la conexión a Internet a las aplicaciones cuyo tráfico se transporta sobre la red VPN-MPLS.

El siguiente caso de uso (Figura 9c) es un servicio SD-WAN que se proporciona sobre redes de diferentes ISPs. En este caso, el proveedor de servicios SD-WAN puede crear redes WAN de muy largo alcance. A semejanza del anterior caso de uso, también existen diferentes rutas alternativas que permiten comunicar los diferentes puntos de presencia de la red corporativa, lo que puede ser utilizado para dotar al servicio de una mayor tolerancia a fallos. Por otro lado, es común en este tipo de escenario aplicar técnicas de optimización WAN. Las técnicas de optimización WAN permiten hacer un uso más eficiente del ancho de banda disponible, minimizar la pérdida de paquetes y reducir la latencia. Su aparición viene motivada por la necesidad de mejorar el rendimiento de las conexiones WAN privadas y con el objetivo de reducir costes. Existen diferentes técnicas de optimización WAN que se puede aplicar. Por ejemplo: (1) “data deduplication” es una técnica que consiste en evitar el envío de información que ha sido ya enviada previamente. Imagine que desde una oficina de la red corporativa se ha enviado al centro de datos un informe que posteriormente ha sufrido una modificación. En lugar de transmitir de nuevo el fichero, es posible enviar solo aquellas partes que han sido modificadas. (2) compresión de los datos antes de su transmisión sobre la red WAN. (3) aplicar técnicas de “Caching”, que consisten en almacenar localmente copias de los contenidos que solicitan los usuarios. Cuando se solicita un contenido, primero se comprueba si está almacenado en la memoria cache local. De esta forma, se evita su transmisión sobre la red WAN y se reduce el consumo de ancho de banda. (4) aceleración TCP. Existen diversas técnicas basadas en TCP que permiten maximizar el throughput y reducir la latencia de las aplicaciones. Por ejemplo, es posible maximizar el throughput aumentando el tamaño de la ventana de recepción. Para reducir la latencia también es posible asentir (ACK) los segmentos TCP localmente, evitando que estos asentimientos atraviesen toda la red WAN.

Otro caso de uso de servicios SD-WAN, que ha sido abordado en la sección 2.1. Arquitectura de la red SD-WAN (figura 6), es la posibilidad de enviar el tráfico de las aplicaciones directamente hacía Internet (Internet-breakout). Con la creciente demanda de servicios en la nube pública, era habitual que el tráfico de las aplicaciones se enviase primero al centro de datos privado de la organización, que actuaba como pasarela hacia Internet, para llegar a la nube donde se desplegaban las aplicaciones. El servicio SD-WAN gestiona el encaminamiento de este tipo de tráfico.

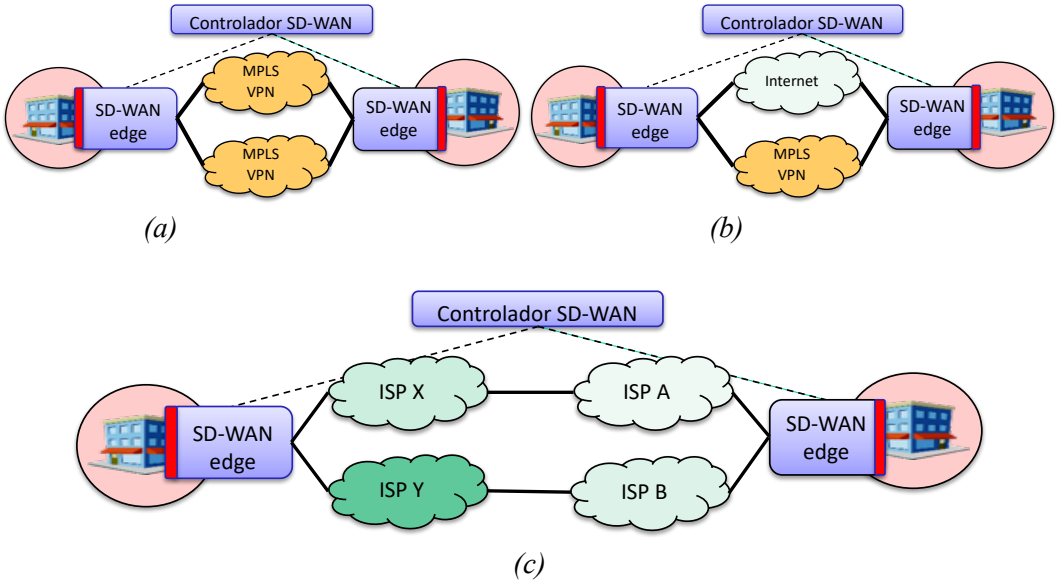

Figura 9 Casos de uso de servicios SD-WAN

Como se ha destacado anteriormente, es posible que el proveedor de servicios SD-WAN no sea el proveedor de servicios de Internet o el operador de la red MPLS que proporciona la conexión WAN privada. Es decir, puede ser otro actor independiente del modelo de negocio. Sin embargo, un caso de uso ampliamente estudiado en la literatura y los estándares es el que se representa en la figura 10, donde el proveedor del servicio SD-WAN también gestiona la red que une los diferentes puntos de presencia de la red corporativa.

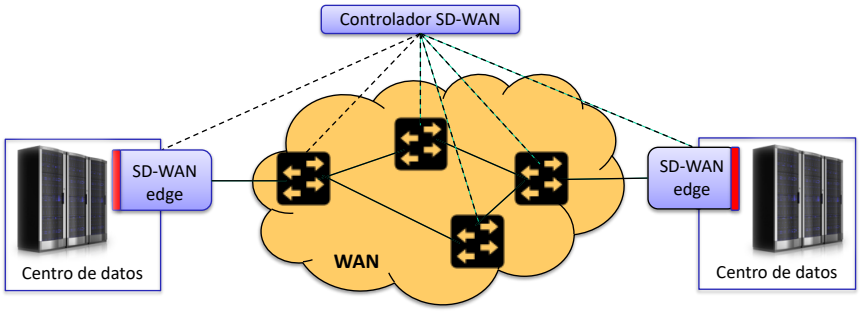

Figura 10 Servicio SD-WAN para conectar dos centros de datos

2.2.1 Servicios de red basados en NFV en centros de datos

La ETSI ha definido una arquitectura estándar (NFV-Management and Orchestration o NFV-MANO) [16] para la gestión y orquestación de servicios de red basados en NFV. NFV-MANO permite gestionar el ciclo de vida de las funciones de red virtualizadas o VNFs que componen los servicios de red basados en NFV. Además, la plataforma de orquestación también gestiona los recursos de cómputo, almacenamiento y red que se asignan a las VNFs. La Figura 11 muestra los componentes principales de NFV-MANO, descritos a continuación:

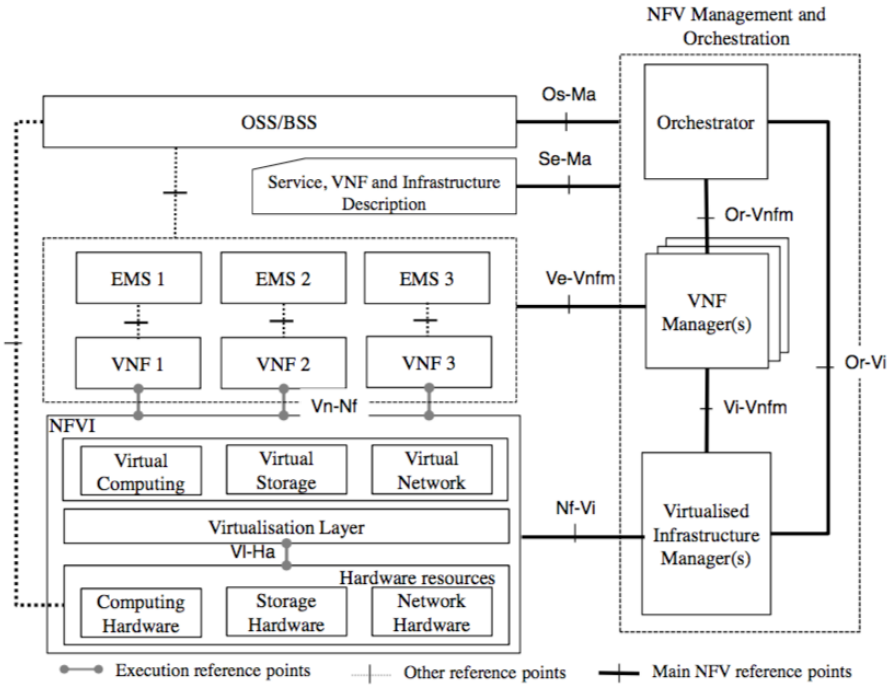

Figura 11: Arquitectura NFV detallada. Fuente:[16]

- *Network Functions Virtualization Infrastructure (NFVI)*. Está compuesto por los recursos hardware (servidores, almacenamiento y equipos de red) sobre los que se implementan las VNFs. Incluye la capa de virtualización que permite virtualizar esos recursos y ofrecerlos como recursos virtuales a los niveles superiores.
- *Virtualized Network Functions (VNF)*. Es el conjunto de VNFs que se implementan sobre la infraestructura NFVI.
- *NFV Management and Orchestration (MANO)*. Está formado por el software que interacciona con el NFVI y con el bloque de VNFs con el objeto de gestionar y coordinar todos los recursos físicos y virtualizados.
- *Virtualised Infrastructure Manager (VIM)* es el software que directamente controla y gestiona la infraestructura física, se ocupa de su virtualización y de ofrecer al nivel superior los recursos virtuales necesarios para implementar las VNFs. Como gestores VIM suelen utilizarse las plataformas de virtualización utilizadas en centros de datos para gestionar los servicios del tipo Infraestructure as a Service (IaaS), tales como el vSphere de VMware o la plataforma abierta Openstack.
- *VNF Manager (VNFM)* se ocupa de gestionar el ciclo de vida individual de las VNFs, así como el de los Elementos de Gestión (Element Management Systems o EMS) específicos de cada VNF.
- *NFV Orchestrator (NFVO)* se ocupa de gestionar el ciclo de vida de los servicios de red, formados por cadenas de VNFs. Hace las veces de orquestador de VNFs, interpretando las especificaciones de los servicios de red y traduciéndolas en solicitudes de creación e interconexión de las VNFs que componen un servicio de red. Se ocupa además de la gestión de los paquetes de VNFs disponibles (gestión del catálogo de VNFs disponible, instalación, etc.).

La ETSI ha definido un VIM para entornos WAN llamado WAN Infrastructure Manager (WIM) [16] que permite a una plataforma de gestión de VNFs (NFV-MANO) solicitar una conexión de red entre varios puntos de presencia de la red corporativa con el objetivo de conectar las funciones de red virtualizadas que allí se despliegan. Esta conexión debe cumplir con los requisitos de QoS que impone el servicio de red en términos de ancho de banda, latencia o jitter.

Aunque la figura muestra que cada punto de presencia (*NFVI-Point of Presence* o NFV-PoP) está gestionado por un VIM, es posible que en un único punto de presencia coexistan múltiples VIMs, cada uno responsable de un dominio administrativo. De la misma forma, también sería posible que un único VIM gestionara los recursos NFV desplegados a lo largo de la red corporativa. En el caso que se representa en la figura 12 (un VIM por cada NFVI-PoP) es necesario que estos VIM creen una red virtual dentro de su propio punto de presencia y exporten una interfaz que pueda utilizar el WIM para conectar ambos extremos.

La figura también representa el caso en el que los gestores VIM y WIM controlan los recursos de red la infraestructura NFV a través de un controlador de red SDN. Sin embargo, también es posible que el VIM/WIM programe el plano de datos de los nodos de conmutación directamente, integrando la funcionalidad del controlador.

El NFVO es la entidad encargada de orquestar el despliegue del servicio de red. Para ello, invoca a los gestores VIM y WIM, que establecen los enlaces virtuales que unen las VNFs que componen el servicio de red. El VIM, además, también asigna los recursos de cómputo y almacenamiento a las VNFs. El NFVO debe certificar que los requisitos de red que impone el servicio se cumplen, y para ello, monitoriza el ancho de banda, la latencia o la pérdida de paquetes que se produce en la ruta que une las VNFs.

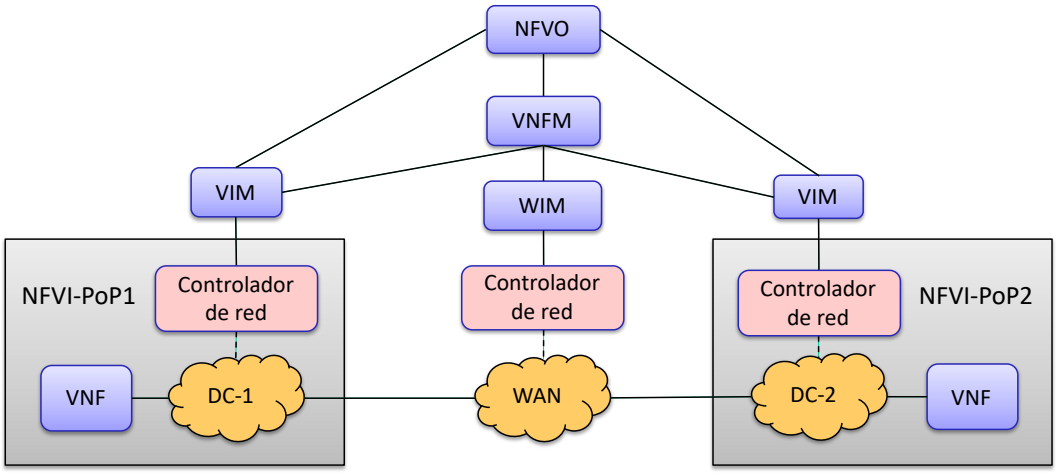

Figura 12 Arquitectura y orquestación y gestión de servicios de red sobre conexiones WAN

La ETSI ha analizado diferentes casos de usos que se basan en esta arquitectura de red [17] . El primero de ellos se trata de servicios que conectan el vCPE de la red corporativa con una VNF que se instancia en otro punto de presencia de la red. Para desplegar este servicio, el WIM debe crear un enlace virtual que una ambas VNFs. Otro posible escenario es el de conectar los nodos SD-WAN Edge (vCPE), cuando estos se despliegan como VNFs en los uCPE de la red corporativa.

La ETSI también define cómo es el API del WIM [18] . El API del WIM debe programarse para permitir la gestión de las conexiones extremo-a-extremo que se establecen para conectar las VNFs desplegadas en los puntos de presencia de la red corporativa. Es decir, debe permitir crear o terminar conexiones y solicitar o actualizar la información asociada a conexiones ya establecidas (por ejemplo, para modificar los requisitos de QoS de una conexión). El WIM también debe ofrecer información sobre la capacidad de la red subyacente,

indicando cuántos recursos se han consumido y cuantos recursos están disponibles. Por ejemplo, la ETSI define una operación que permite definir un umbral de capacidad que, si se supera, genera una notificación que informa al administrador de la red SD-WAN. En definitiva, el API debería poder utilizarse para extraer información sobre el rendimiento de las conexiones WAN. Por otro lado, el WIM también debe incluir operaciones para la gestión de fallos. La ETSI define operaciones para que el administrador pueda suscribirse a un servicio de notificación de alarmas generadas con este propósito.

3. PANORÁMICA DE SOLUCIONES SD-WAN EXISTENTES

3.1. SOLUCIONES COMERCIALES Y ACADÉMICAS

En esta sección se va a proporcionar una descripción sobre algunas de las soluciones de servicios SD-WAN que existen en el mercado. En concreto: Nuage (propuesta por Nokia). Viptela (propuesta por Cisco) y Flexiwan (una solución de código abierto)

3.1.1 Nuage

Nuage [19] es la solución SD-WAN desarrollada por Nokia. Automatiza la provisión, configuración y gestión de conexiones WAN para proporcionar calidad de servicio a bajo coste al tiempo que se satisfacen las políticas de negocio y seguridad de cada aplicación. Nuage implementa técnicas que se han detallado en secciones anteriores. Por ejemplo, permite utilizar la conexión pública de Internet, no solo como respaldo, sino también para encaminar el tráfico de aplicaciones que no tienen unos estrictos requisitos de calidad de servicio.

La Figura 13 muestra la arquitectura de Nuage. *Virtualized Services Directory* (VSD) es el sistema que permite al administrador de la red SD-WAN definir y aplicar las políticas de negocio a través de un portal web. VSD también proporciona informes sobre el tráfico de la red SD-WAN. Este servicio se puede configurar, por ejemplo, definiendo la periodicidad de la recolección de estadísticas o mediante la definición de alertas que indican si un determinado umbral de tráfico ha sido sobrepasado. Todas estadísticas se almacenan en una base de datos con el objetivo de que se puedan aplicar fácilmente soluciones de minería de datos.

El suscriptor del servicio SD-WAN puede contratar las funciones de red que desee a través de un catálogo de VNFs. Este catalogo incluye VNFs de firewalling, IPSec, NAT, blaanceo de carga, DHCP o DNS. VSD también permite registrar nuevas VNFs en la plataforma de gestión de VNFs (NFV-MANO), así como gestionar el ciclo de las VNFs que se despliegan en los puntos de presencia de la red corporativa. En estos puntos de presencia, se despliegan los equipos *Network Services Gateway* (NSG). Estos equipos pertenecen a la familia uCPE y soportan la instanciación de máquinas virtuales y contenedores que implementan las VNFs. La virtualización de las funciones de red simplifica estos dispositivos y reduce costes al proveedor de servicios de SD-WAN, ya que, en la mayoría de los casos, pueden adquirirlos y conectarlos sin ayuda del proveedor (son dispositivos *plug and play*).

Otro de los elementos de Nuage es el controlador SDN (*Virtualized Services Controller* o VCS), que se encarga de programar los NSGs utilizando el protocolo OpenFlow. A semejanza de otros controladores SDN, pueden desplegarse varias instancias que actúan como un clúster.

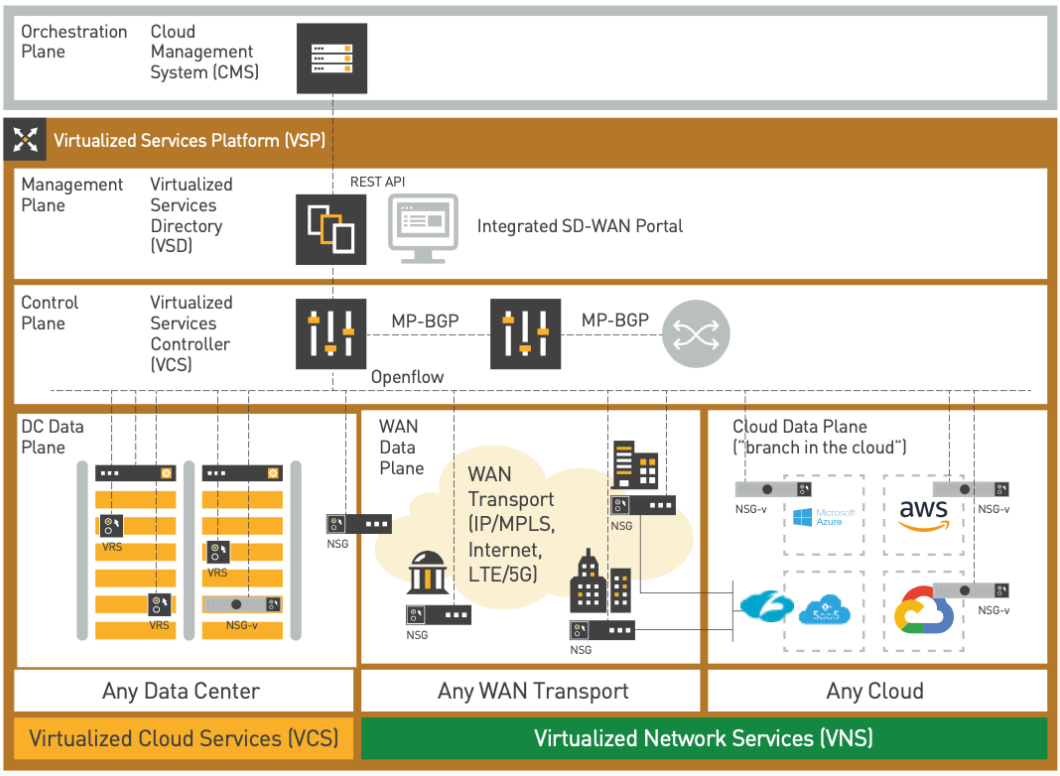

Figura 13 Arquitectura de Nuage [19]

3.1.2 Viptela

La Figura 14 muestra la arquitectura de Viptela, la solución SD-WAN propuesta por Cisco [21] . La arquitectura está compuesta por los siguientes elementos: vEdge, vSmart, vManage y vBond. El primero de ellos es vEdge, que es el dispositivo que se despliega en el punto de presencia de la red corporativa. Puede ser un dispositivo físico o estar virtualizado e instanciarse como una VNF en el uCPE de la corporación, al igual que el NSG de Nuage.

vSmart es el controlador de la red SD-WAN. Se encarga de programar el plano de datos de los nodos vEdge mediante el protocolo *Overlay Management Protocol* (OMP). OMP transporta prefijos, rutas o la información de las políticas que deben aplicarse al tráfico de las aplicaciones. La idea de OMP es distribuir información de control que permita establecer y mantener la red overlay. Esta información viaja dentro de una VPN que conecta los nodos vEdge con el controlador vSmart. Es por ello por lo que se propone utilizar OMP para poder establecer túneles IPSec sin la necesidad de utilizar el protocolo IKE. Con OMP, la información criptográfica también viaja en las VPNs que se establecen entre los nodos vEdge y los controladores vSmart.

Si piensa en las redes tradicionales, OMP es un protocolo muy similar a BGP. Se basa en el mismo concepto que el de un router reflector de BGP. Un router reflector se encarga de reenviar las rutas que ha recibido de un nodo iBGP al resto de nodos de la red. OMP permite centralizar la gestión del encaminamiento de la red overlay

sin la necesidad de utilizar protocolos de encaminamiento tradicionales como OSPF y BGP, que actúan de forma distribuida. La idea es distribuir a los nodos vEdge la información de control necesaria para que ellos mismos establezcan los túneles IPSec.

Otro elemento de Viptela es vManage cuya función es centralizar la gestión de la red. vManage proporciona una interfaz de usuario web desde donde se puede monitorizar la red y configurar todos los dispositivos. Soporta diferentes protocolos de gestión, como SNMP, NETCONF o Syslog, almacenando la configuración de todos los componentes de la red SD-WAN. Cuando un nodo vEdge se conecta a la red, este solicita un certificado y su configuración a la estación de gestión vManage.

El último nodo que compone Viptela es vBond, que orquesta la conectividad entre los planos de datos, control y gestión. vBond se encarga de registrar los nodos vEdge en la red SD-WAN, es decir, gestiona las comunicaciones entre los nodos vEdge y los controladores. Una vez que se establecen los túneles VPNs que conectan ambas entidades, los nodos vEdge activan el protocolo Bidirectional Forwarding Detection (BFD), que permite medir la latencia, jitter y detectar pérdidas de paquetes o fallos en la comunicación.

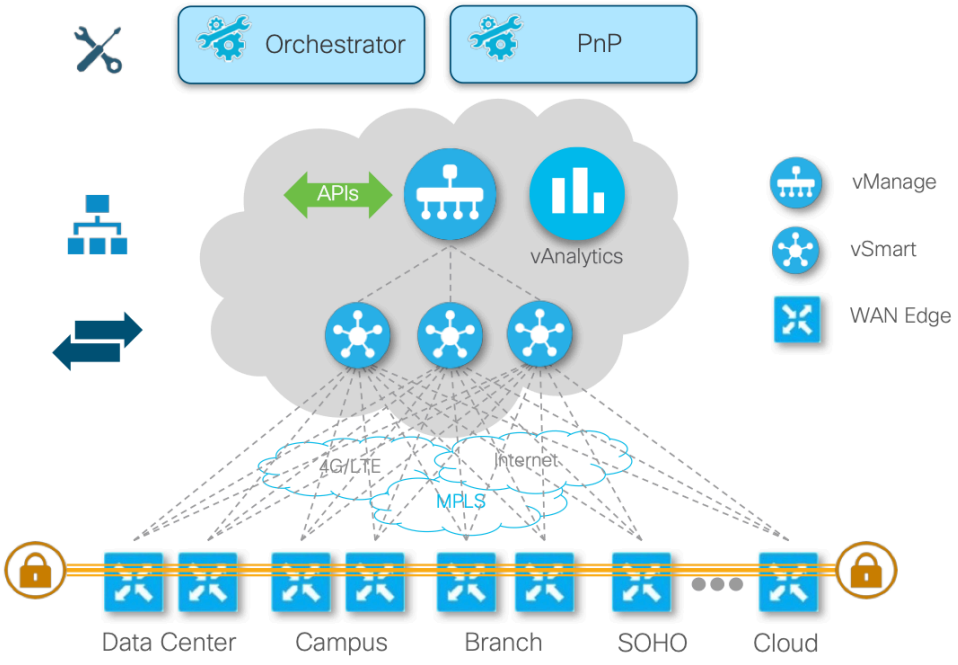

Figura 14 Arquitectura de Viptela, solución SD-WAN de Cisco. Fuente: [21]

3.1.3 Flexiwan

Flexiwan [20] es una solución SD-WAN de código abierto que se compone de dos elementos fundamentales. El primero de ellos es *flexiEdge*, un dispositivo basado en software que se instancia en el punto de presencia de la red corporativa. El sistema de gestión de la red SD-WAN es *flexiManage*, que es la entidad encargada de programar los nodos *flexiEdge,* así como de recolectar medidas de rendimiento de la red. Por el momento, flexiwan soporta, entre otras funciones, la creación túneles IPSec sobre VxLAN, la configuración estática de rutas y cambios dinámicos en la configuración de los nodos *flexiEdge*. Actualmente, su equipo de desarrollo

está trabajando para proporcionar servicios de red que utilicen simultáneamente múltiples conexiones WAN, así como soluciones para el soporte de la calidad de servicio.

El nodo flexiwan se trata de una máquina virtual con un Ubuntu 18.04 que tiene instalado un agente de flexiwan. Este agente conecta el nodo *flexiEdge* con *flexiManage*. Además, el nodo *flexiEdge* tiene instalado VPP (*Vector Packet Processor*) y FRR (*Free Range Routing*). FRR es una suite basada en Quagga que implementa diferentes protocolos de encaminamiento, como, por ejemplo, OSPF o BGP. VPP es un módulo software que permite acelerar el procesamiento de paquetes al tratar con vectores. Los paquetes no se procesan secuencialmente, uno a uno, sino que se procesan varios de forma simultánea, los que pertenecen al vector.

3.2. OTROS TRABAJOS DE INVESTIGACIÓN

Proveedores de servicios como Google y Microsoft han desarrollado sus propias soluciones de red SD-WAN para gestionar el tráfico cursado entre sus centros de datos. Dado que, en estos casos, los proveedores de servicios operan su propia infraestructura de red, estas soluciones suelen estar orientadas a optimizar los algoritmos de encaminamiento que se ejecutan en la red de transporte. Es decir, se centran en aplicar soluciones de ingeniería de tráfico en las conexiones SD-WAN. Además, estas redes de centros de datos tienen unos requisitos de QoS muy específicos, lo que se debe a que se realizan grandes transferencias de ficheros para sincronizar la información de los centros de datos. Para entender mejor las soluciones propuestas por estos proveedores de servicios, primero se proporciona una visión de ingeniería de tráfico en SDN.

3.2.1 Ingeniería de tráfico (TE) basada en SDN

En general, la ingeniería de tráfico consiste en adecuar el tráfico a las condiciones de la red para utilizar de forma equilibrada los recursos disponibles y proporcionar calidad de servicio. A continuación, se describen los objetivos que, en particular, persiguen las soluciones de ingeniería de tráfico:

- *Minimizar la congestión de los recursos de red*: es posible aplicar técnicas que permiten denegar el acceso a los recursos congestionados, redistribuir los flujos de tráfico en la red o establecer rutas de encaminamiento multicamino.
- *Minimizar el retardo extremo-a-extremo*: una de las técnicas más utilizadas para cumplir con este objetivo se basa en el uso del algoritmo de encaminamiento *Constrained Shortest Path First* (CSPF). CSPF es un algoritmo que determina el camino más corto que cumple con ciertas restricciones de QoS (por ejemplo, ancho de banda o retardo).
- *Minimizar la pérdida de paquetes*: la pérdida de paquetes puede ocasionarse, no solo por congestión, sino también por fallos en los enlaces y nodos de conmutación. Este objetivo puede cumplirse sobredimensionando la red desplegando enlaces y nodos de respaldo.
- *Maximización de la calidad de la experiencia*: la calidad de la experiencia se define como la aceptabilidad de una aplicación o servicio, tal y como ser percibe subjetivamente por los usuarios finales. Esto incluye cualquier efecto del sistema extremo a extremo (cliente, terminal, red, infraestructura del servicio).
- *Optimización de la utilización de los recursos de red*: una correcta utilización de los recursos de red puede permitir a los operadores de red transportar un mayor volumen de tráfico. Para cumplir con este

objetivo se proponen técnicas para planificar las transferencias de datos. Por ejemplo, es posible programar transferencias para replicar datos (copiar datos como respaldo) en horas no cargadas, por ejemplo, por la noche.

El encaminamiento basado en etiquetas (MPLS) permite implementar muchas de estas soluciones de ingeniería de tráfico mediante la creación explicita de rutas (*Label Switched Path* o LSP). Sin embargo, MPLS-TE presenta diversas limitaciones que pueden superarse aplicando soluciones de tipo SDN. Una de las limitaciones de MPLS-TE es que, minimizar la congestión mediante el encaminamiento multicamino, puede implicar una reordenación de paquetes excesiva, sobre todo, en aplicaciones que se ejecutan sobre TCP. Además, que los segmentos TCP lleguen desordenados puede activar innecesariamente el mecanismo de prevención de la congestión (*congestion avoidance*) de TCP, lo que produce una degradación del throughput de las aplicaciones.

Otra de las limitaciones de MPLS-TE es su dependencia con el protocolo RSVP (*Resource Reservation Protocol* o RSVP), que permite reservar recursos de red en una ruta ya establecida por otros protocolos de encaminamiento. El establecimiento y configuración de los LSPs aumenta el retardo, algo que las redes SDN pueden evitar.

Aunque se han propuesto soluciones de ingeniería de tráfico basadas en SDN para distintos protocolos de la interfaz sur, a continuación, se proporciona una breve descripción de propuestas que consideran OpenFlow [8] , el protocolo del interfaz sur más extendido en la literatura. OpenFlow incluye diversos mecanismos que facilitan la implementación de soluciones de ingeniería de tráfico. Por ejemplo, incluye dos mecanismos para el soporte de la calidad de servicio: colas y medidores. Un conmutador OpenFlow puede tener una o varias colas asociadas a un puerto de salida. Estas colas permiten proporcionar garantías de ancho de banda, configurables. La garantía se consigue aplicando algoritmos de planificación ("scheduling") a la transmisión de paquetes por el puerto. Con respecto a los medidores, estos se utilizan para monitorizar la tasa de paquetes de un flujo. La idea consiste en definir “bandas” asociadas a umbrales de tasa, para procesar el paquete en cada banda (modificar campos, descartarlo, etcétera). Una banda que descarta el paquete se comporta como un limitador de tasa.

Las soluciones existentes de ingeniería de tráfico basadas en SDN [9] se pueden clasificar según los objetivos definidos anteriormente. Con respecto a la optimización de la utilización de los recursos de red, Google y Microsoft han diseñado soluciones SD-WAN llamadas B4 [10] y SWAN [11] que serán descritas con más detalle a continuación. B4 define una aplicación SDN para ingeniería de tráfico que se basa en el principio de reparto equitativo (max-min fair). El principio de reparto equitativo consiste en dividir los recursos de red disponibles (la capacidad de los enlaces de comunicaciones) entre las diferentes aplicaciones en orden creciente de demanda. Aquellas aplicaciones que no pueden satisfacer su demanda, se reparten los recursos que quedan disponibles una vez que se ha asignado el ancho de banda a las aplicaciones con menor demanda.

Como ejemplo, suponga que un enlace con 15 Mbps de capacidad transporta tráfico de cuatro aplicaciones. La primera aplicación (app1) demanda 2 Mbps, la segunda (app2) demanda 3 Mbps, la tercera (app3) 5 Mbps y la última (app4) 7 Mbps. Si dividimos los 15 Mbps entre las cuatro aplicaciones por igual, cada aplicación tendría asignado 3.75 Mbps. Sin embargo, la app1 solo demanda 2 Mbps, por lo que se le asignan 2 Mbps y el resto (3,75 – 2 = 1,75 Mbps) se reparte entre las aplicaciones app2, app3 y app4. Es decir, si dividimos 1,75 Mbps entre las tres aplicaciones, a cada una le correspondería un ancho de banda adicional de 0,58 Mbps, y, por tanto, un total de 4,33 Mbps (3,75 + 0,58).

A continuación, repetimos el mismo procedimiento. La app2 solo demanda 3 Mbps, por lo que se puede satisfacer su demanda y repartir el remanente (es decir 4,33 – 3 = 1,33 Mbps) entre las aplicaciones app3 y app4. Si dividimos 1,33 Mbps entre estas dos aplicaciones, a cada una le correspondería un ancho de banda adicional de 0,66 Mbps, y, por tanto, un total de 5 Mbps (4,33+0,66).

La app3 demanda 5 Mbps que es justo el ancho de banda que tiene asignado. Es decir, en este caso, la app3 no puede "cederle" ancho de banda a la app4. La app4 demanda 7 Mbps, pero dado que la capacidad restante ya ha sido consumida, se le asignan los 5 Mbps que le corresponden. Así, las asignaciones quedarían como sigue: app1 ➔ 2 Mbps, app2 ➔ 3 Mbps, app3 ➔ 5 Mbps, app4 ➔ 5 Mbps.

SWAN es una solución algo semejante a B4, solo que, en este caso, se definen clases de tráfico, de forma que la asignación de ancho de banda se realiza en función de las prioridades establecidas. Otras soluciones para optimizar la utilización de los recursos de red se centran en técnicas de balanceo de carga. Por ejemplo, en [12] proponen utilizar Multi-path TCP (MPTCP) para transmitir datos a través de múltiples caminos (también llamados subflujos TCP) de forma simultánea. La Figura 15 muestra como ejemplo un flujo MPTCP que se compone de dos subflujos TCP que se establecen sobre dos redes de acceso diferentes: una red móvil LTE y una red de fibra óptica Gigabit Passive Optical Network (GPON). MPTCP tiene la capacidad de balancear el tráfico de acuerdo con la carga de los flujos de tráfico que atraviesan una determinada ruta. La solución propuesta en [12] se basa en una aplicación SDN que determina los caminos óptimos que deben seguir los distintos subflujos TCP que componen el flujo MPTCP.

Con respecto a minimizar la congestión, también se han propuesto soluciones basadas en técnicas de balanceo de carga. Por ejemplo, en [13] proponen asignar a cada flujo de tráfico dos rutas: una primaria y otra de respaldo. Con el encaminamiento multicamino es posible evitar situaciones de congestión, por ejemplo, encaminando el tráfico excedente sobre la ruta de respaldo. Otra solución para minimizar la congestión es implementar el algoritmo de encaminamiento CSPF, que, además, también permite reducir el tráfico extremo-a-extremo. La centralización a nivel lógico del plano de control de la red también permite tomar decisiones de encaminamiento más precisas utilizando medidas extraídas en tiempo real de la utilización de los enlaces de la red.

Con respecto a minimizar la tasa de pérdidas de paquetes, las redes SDN también permiten reaccionar con una mayor rapidez ante fallos en enlaces y nodos de conmutación. El controlador puede monitorear el ancho de banda consumido en cada enlace para redistribuir los flujos en rutas menos cargadas y para detectar fallos en los enlaces [14] .

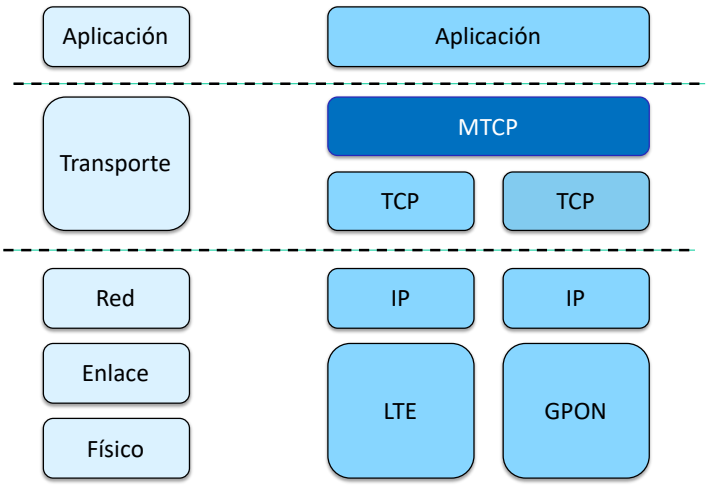

Figura 15 MPTCP con dos subflujos TCP sobre redes de acceso LTE y GPON

3.2.2 B4

B4 [10] es la solución SD-WAN desarrollada por Google para conectar sus centros de datos. Se considera que los centros de datos se conectan mediante redes de conmutación basadas en SDN, es decir, se basan en la utilización de conmutadores OpenFlow. Inicialmente, el desarrollo de B4 se centró en diseñar aplicaciones SDN de encaminamiento e ingeniería de tráfico, considerando los requisitos de QoS de las aplicaciones de la organización. Por ejemplo, Google tiene necesidad de gestionar eficientemente el tráfico de aplicaciones que consumen un gran ancho de banda, por ejemplo, aplicaciones para realizar copias masivas de ficheros entre centros de datos. El objetivo de las aplicaciones SDN es, por tanto: implementar algoritmos de encaminamiento multicamino para aprovechar los recursos de red disponibles. Segundo, adaptar la asignación del ancho de banda a las demandas variables de las aplicaciones y posibles caídas de los enlaces y conmutadores SDN. A través de estas aplicaciones, Google asegura que ha mejorado la utilización de sus enlaces.

La aplicación de ingeniería de tráfico utiliza una abstracción de la red SDN que se basa en un grafo donde los vértices representan los diferentes centros de datos. Los controladores SDN proporcionan esta abstracción a la aplicación TE para que la utilice en su algoritmo de optimización. Este algoritmo, básicamente, determina los túneles virtuales que se tienen que programar en la red de conmutación para que se satisfagan los requisitos de las aplicaciones. El ancho de banda asignado se determina en función de la prioridad de las aplicaciones. B4 categoriza el tráfico de las aplicaciones en diferentes clases. Por ejemplo, una clase de tráfico es el que generan las copias de datos de los usuarios en los centros de datos (e-mail, informes y ficheros multimedia). Otra categoría es el tráfico generado por la sincronización de los centros de datos (copias masivas de ficheros). La prioridad se establece en función del volumen y la sensibilidad frente a retardos de la aplicación. Por ejemplo, el tráfico de las copias de los datos de los usuarios tiene más prioridad que el tráfico de sincronización, puesto que tiene menor volumen y mayor sensibilidad frente a retardos. En definitiva, la aplicación TE trabaja con agrupaciones de flujos de aplicación (Application Flow Group). En OpenFlow, esto se consigue agregando flujos mediante la opción Flow Groups.

3.2.3 SWAN

SWAN (Software-Drive WAN) [11] es la solución SD-WAN desarrollada por Microsoft para conectar sus centros de datos. Uno de los desafíos que aborda SWAN es cómo superar las limitaciones que presentan las soluciones tradicionales de ingeniería de tráfico en las redes MPLS. Las redes MPLS no proporcionan la flexibilidad que se requiere para eliminar, en tiempo real, un flujo de un camino de forma que otro con más prioridad pueda ocuparlo. SWAN, al igual que B4, establece diferentes clases de servicio y asigna los recursos de red disponibles a los servicios en función de su prioridad. Dentro de cada clase de servicio se aplica una política de reparto justo (max-min fair) que consiste en dividir los recursos disponibles entre las diferentes aplicaciones en orden creciente de demanda. Así, las aplicaciones que demandan pocos recursos satisfacen su demanda, mientras que las aplicaciones cuya demanda no se puede satisfacer se reparten los recursos restantes. Al igual que B4, consideran que la red que interconecta los centros de datos está basada en conmutadores OpenFlow. Por otro lado, desarrollan una aplicación de ingeniería de tráfico que determina la ruta que debe seguir el tráfico de las aplicaciones teniendo en cuenta la prioridad de la clase de servicio y el reparto justo. Uno de los aspectos que diferencia SWAN de B4 se ilustra en la figura 16. El controlador SD-WAN, además de controlar el encaminamiento del tráfico en la red (a partir de información de la topología de la red), también controla la tasa de datos de servicio, es decir, controla la velocidad a la que pueden transmitir los emisores de tráfico. Para ello, los clientes deben reportar al controlador el ancho de banda que demandan.

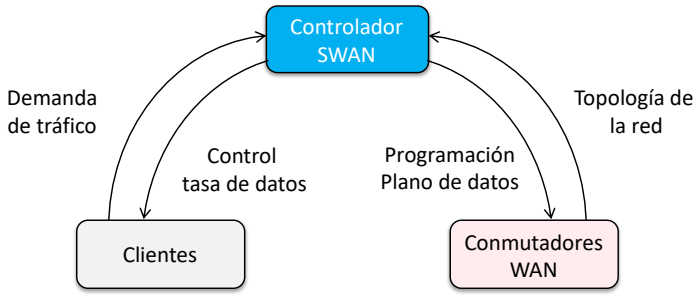

Figura 16 Flujo del sistema para maximizar la utilización de los enlaces

4. CONCLUSIONES

1. SD-WAN surge de la necesidad de actualizar las redes corporativas para integrarlas en los "servicios en la nube".
2. Es una tecnología y servicio que aplica los conceptos fundamentales de SDN (separación de los planos de control y datos, control centralizado) al establecimiento de túneles entre nodos SD-WAN Edge conectados a través de múltiples accesos (Internet, VPN, …).
3. En el modelo SD-WAN son cruciales la automatización de la gestión de los túneles, las reglas de encaminamiento de tráfico en los nodos SD-WAN Edge y la monitorización continua de los parámetros de QoS.
4. Los servicios SD-WAN reducen costes de inversión inicial en equipamiento y costes de operación.

5. REFERENCIAS

[1] William Stallings, “Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud”, Pearson, 2016.

[2] IDC, “SD-WAN Infrastructure Market Poised to Reach $5.25 Billion in 2023, According to New IDC Forecast”. [Online]. Disponible: https://www.idc.com/getdoc.jsp?containerId=prUS45380319

[3] Metro Ethernet Forum. [Online]. Disponible: https://www.mef.net

[4] Servicios Diferenciados. [Online]. Disponible: https://es.wikipedia.org/wiki/Servicios_Diferenciados

[5] *SD-WAN Service Attributes and Services,* MEF 70, Jul. 2019

[6] “MEF 3.0 SD-WAN Services”, MEF, White Paper, Último acceso: Mar. 2020. [Online]. Disponible: https://www.mef.net/mef-white-paper-request/

[7] John Donovan and Krish Prabhu. 2017. Building the Network of the Future: Getting Smarter, Faster, and More Flexible with a Software Centric Approach (100 Cases) (1st. ed.). Chapman & Hall/CRC.

[8] OpenFlow Switch Specification v1.5.1 (TS-025). Open Networking Foundation, 2015.

[9] A. Mendiola, J. Astorga, E. Jacob and M. Higuero, "A Survey on the Contributions of Software-Defined Networking to Traffic Engineering," in IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 918-953, Secondquarter 2017.

[10] Sushant Jain, Alok Kumar, Subhasree Mandal, Joon Ong, Leon Poutievski, Arjun Singh, Subbaiah Venkata, Jim Wanderer, Junlan Zhou, Min Zhu, Jon Zolla, Urs Hölzle, Stephen Stuart, and Amin Vahdat. 2013. B4: experience with a globally-deployed software defined wan. In Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM (SIGCOMM ’13). Association for Computing Machinery, New York, NY, USA, 3–14. DOI:https://doi.org/10.1145/2486001.2486019

[11] Chi-Yao Hong, Srikanth Kandula, Ratul Mahajan, Ming Zhang, Vijay Gill, Mohan Nanduri, and Roger Wattenhofer. 2013. Achieving high utilization with software-driven WAN. In Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM (SIGCOMM ’13). Association for Computing Machinery, New York, NY, USA, 15–26. DOI:https://doi.org/10.1145/2486001.2486012

[12] Ronald van der Pol, Sander Boele, Freek Dijkstra, Artur Barczyk, Gerben van Malenstein, Jim Hao Chen, and Joe Mambretti. 2012. Multipathing with MPTCP and OpenFlow. In Proceedings of the 2012 SC Companion: High Performance Computing, Networking Storage and Analysis (SCC ’12). IEEE Computer Society, USA, 1617–1624. DOI:https://doi.org/10.1109/SC.Companion.2012.339

[13] W. Braun and M. Menth, "Load-dependent flow splitting for traffic engineering in resilient OpenFlow networks," 2015 International Conference and Workshops on Networked Systems (NetSys), Cottbus, 2015, pp. 1-5.

[14] K. Phemius and M. Bouet, "Implementing OpenFlow-based resilient network services," 2012 IEEE 1st International Conference on Cloud Networking (CLOUDNET), Paris, 2012, pp. 212-214.

[15] H. Yan, Y. Li, W. Dong and D. Jin, "Software-Defined WAN via Open APIs," in IEEE Access, vol. 6, pp. 33752-33765, 2018.

[16] *“Network Function Virtualisation (NFV); Management and Orchestration”*, ETSI GS NFV-MAN 001 v1.1.1, 2014.

[17] *“Network Function Virtualisation (NFV) Release 3; Management and Orchestration; Report on Management and Connectivity for Multi-Site Services”*, ETSI GS NFV-IFA 022 v3.1.1, 2018.

[18] *“Network Function Virtualisation (NFV) Release 3; Management and Orchestration; Interface and Information Model Specification for Multi-Site Conenectivity Services”*, ETSI GS NFV-IFA 032 v3.2.1, 2019.

[19] Nokia, “Virtualized Network Services”. [Online]. Disponible: https://resources.nokia.com/asset/183178
[20] Flexiwan’s documentation. [Online]. Disponible: https://docs.flexiwan.com
[21] Cisco, “Cisco Extended Enterprise SD-WAN Design Guide”. [Online]. Disponible: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/EE/DG/ee-WAN-dg.pdf