

DISEÑO Y SIMULACIÓN DE SOLUCIÓN  
SD-WAN PARA CLIENTE RETAIL CON  
CONSUMO DE SERVICIOS EN LA NUBE

T E S I S

QUE PARA OPTAR POR EL GRADO DE:  
**Especialista en Diseño de Redes Telemáticas**

PRESENTA:

**JOAN SEBASTIÁN QUINTERO CEBALLOS**  
**JOSÉ ARMANDO SON ROJAS**

DIRECTOR:  
Jesús Cantillo



Bogotá DC, Colombia, 2019

# Justificación

---

La administración centralizada de la red mediante una solución SD-WAN permitiría realizar cambios de políticas de red de forma mucho más ágil, evitando que la red se vuelva un cuello de botella para la ejecución de proyectos de TI.

La solución propuesta mejoraría el comportamiento de la red en varios aspectos, principalmente en disponibilidad y calidad de servicio pero también en otras áreas críticas para la organización como la seguridad, es un rediseño completo que permitiría a la empresa ser más competitiva con unos mayores tiempos de disponibilidad de sus servicios tanto para las regionales como para las tiendas y con una menor carga de trabajo sobre la gestión de la red al asegurarse de que la conmutación de los servicios se realice de forma automática y al garantizar una utilización más eficiente de los recursos de la red al realizar el balanceo de carga.

El esquema de balanceo de carga asegura que los recursos de la red se utilicen de forma más eficiente y que de esta manera cuando el cliente tenga picos de tráfico no se vea afectado todo el tráfico por un enlace mientras que el otro enlace se encuentra disponible y podría utilizarse, además de esto el balanceo reduce costos ya que aumenta la capacidad real de la conexión WAN y por tanto no se requerirían ampliaciones de ancho de banda por el momento.

La disponibilidad también mejoraría notablemente al eliminar la dependencia de la conexión de las tiendas con el canal de Internet de una sola regional, esta dependencia se eliminaría bajo un esquema de túneles dinámicos que cambian el actual comportamiento de topología estrella a una topología en malla, dichos túneles dinámicos contarían además con los niveles de encriptación adecuados para mitigar los problemas de seguridad que se han presentado.

Un cambio de esta magnitud tomaría mucho tiempo bajo el modelo de gestión actual, si en cambio se utiliza una red SD-WAN con gestión centralizada de los recursos de red el cambio se haría de forma mucho más ágil, lo que al final representa menores costos para la compañía.

# Objetivos

---

## Objetivo General

Diseñar y simular solución SD-WAN para cliente retail con consumo de servicios en la nube.

## Objetivos Específicos

- Diseñar solución de conectividad que permita balanceo de carga y redundancia a través de un enlace de internet y un canal MPLS.
- Diseñar las soluciones de cifrado y decontrol y priorización de tráfico (calidad de servicio) en la red para sus enlaces más críticos.
- Diseñar solución SD-WAN que permita configurar las sedes remotas de forma centralizada.
- Simular el diseño propuesto con el fin de garantizar que la solución sea funcional.

# Índice general

---

<b>Justificación</b>	<b>I</b>
<b>Objetivos</b>	<b>II</b>
<b>Índice de figuras</b>	<b>V</b>
<b>Índice de tablas</b>	<b>VI</b>
<b>1. Introducción</b>	<b>1</b>
1.1. Título . . . . .	1
1.2. Presentación . . . . .	1
1.3. Descripción del Proyecto . . . . .	2
1.4. Definición del Problema . . . . .	2
1.5. Aspectos a Solucionar . . . . .	4
1.6. Solución de la Propuesta . . . . .	5
1.7. Metodología . . . . .	6
1.8. Contribuciones . . . . .	7
1.9. Estructura de la tesis . . . . .	7
<b>2. Estado del Arte</b>	<b>8</b>
2.1. Marco de Referencia Teórico . . . . .	8
2.1.1. Conceptos generales de SD-WAN . . . . .	8
2.1.2. Modelos de Programabilidad de Red . . . . .	8
2.1.3. NFV . . . . .	9
2.1.4. OpenFlow . . . . .	10
2.1.5. NETCONF . . . . .	10
2.1.6. Modelos de Datos . . . . .	12
2.1.6.1. YANG . . . . .	12
2.1.7. RESTful APIs . . . . .	13
2.1.8. RESTCONF . . . . .	13
2.1.9. Marco de Referencia Tecnológico . . . . .	13
2.1.10. Open Daylight . . . . .	14
2.1.11. IWAN . . . . .	15

2.1.12. Cisco VIPTELA . . . . .	21
2.1.13. NSX SD-WAN . . . . .	21
2.2. WAN definida por software (SD-WAN) . . . . .	22
2.3. Controladores de negocio SD-WAN (SDWAN) . . . . .	23
2.3.1. Enfoque al cliente: costo, confiabilidad, seguridad . . . . .	25
2.3.2. Solo en premisa . . . . .	26
2.3.2.1. Mejor ajuste: . . . . .	26
2.3.2.2. Beneficios: . . . . .	27
2.3.3. Cloud . . . . .	27
2.3.3.1. Mejor ajuste: . . . . .	27
2.3.3.2. Beneficios: . . . . .	28
2.3.4. Cloud backbone . . . . .	28
2.3.4.1. Mejor ajuste: . . . . .	28
2.3.4.2. Beneficios: . . . . .	29
<b>3. Requerimientos</b>	<b>30</b>
3.1. Requerimientos funcionales . . . . .	30
3.2. Requerimientos no Funcionales . . . . .	30
<b>4. Metodología de Desarrollo</b>	<b>32</b>
<b>5. Diseño de la solución SD-WAN</b>	<b>34</b>
5.1. Selección de proveedor y tecnología . . . . .	34
5.2. Consideraciones iniciales del diseño . . . . .	36
<b>6. Resultados</b>	<b>37</b>
<b>7. Discusión</b>	<b>38</b>
<b>8. Conclusiones</b>	<b>39</b>
<b>9. Bibliografía</b>	<b>40</b>
<b>A. Código/Manuales/Publicaciones</b>	<b>41</b>
A.1. Apéndice . . . . .	41

# Índice de figuras

---

1.1. Descripción de una SD-WAN . . . . .	4
2.1. Apis Programable . . . . .	9
2.2. Network Function Virtualization . . . . .	10
2.3. Openflow áreas de especificaciones open Datapath . . . . .	11
2.4. NetConf . . . . .	12
2.5. RestConf . . . . .	13
2.6. Open Daylight . . . . .	15
2.7. Flujo que ocurre entre estos elementos dentro del funcionamiento de la controladora. . . . .	16
2.8. Iwan. . . . .	16
2.9. Api-EMC Controller . . . . .	17
2.10. DMVPN . . . . .	18
2.11. Túneles se forman agregando un encabezado IP externo al paquete con la información IP . . . . .	19
2.12. Funcionamiento de NHRP . . . . .	20
2.13. Arquitectura de esta propuesta VIPTELA . . . . .	21
2.14. Distribución de los componentes . . . . .	22
2.15. WAN definida por software (SD-WAN) . . . . .	23
2.16. WAN definida por software (SD-WAN) . . . . .	24
2.17. WAN definida por software (SD-WAN) . . . . .	24
5.1. OpenDayLight como controlador SD-WAN . . . . .	35
5.2. Soluciones SDN . . . . .	35

# Índice de tablas

---

---

## Capítulo 1

# Introducción

---

### 1.1. Título

**DISEÑO Y SIMULACIÓN PARA CLIENTE SD-WAN PARA CLIENTE RETAIL CON CONSUMO DE SERVICIOS EN LA NUBE.**

### 1.2. Presentación

El presente proyecto corresponde al tema a SD-WAN (**“Software Defined Networking in Wide Area Networks”**) significa en español solución de conectividad definida por software para redes de área extensa. Es una herramienta que se usa exclusivamente en el campo de las telecomunicaciones dispuesto en una red o sistema para ser un dispositivo de hardware de virtualización que ejecuta su propio procedimiento sobre circuitos, realizando funciones de enrutado, con el que los administradores pueden desplegarse en un costo reducido en gran cantidad de nodos de la red.

La característica principal de esta tecnología de la información se ocupa en la protección de datos, simula servicios, programas, aplicaciones redes, posibilidad de personalizar cada dispositivo de forma local y controlar una arquitectura de telecomunicaciones de forma centralizada.

Para analizar los SD-WAN es necesario mencionar sus causas, conectividad en el entorno de negocio empresarial, debido a que un administrador de red no puede cubrir dichas necesidades solo con servicios de MPLS WAN para interconectar Datacenter y oficinas remotas.

La investigación de esta tecnología se realizó por el interés de conocer la creación de redes híbridas que adicionan múltiples tecnologías de acceso, incluyendo servicios de Internet, enrutamiento de tráfico dinámico disponiendo en tiempo real la conectividad.



Esto permite obtener una ventaja adicional frente a equipos convencionales ya que el sistema sabe qué tipo de contenido se está transmitiendo y la mejor forma de procesarlo.

### 1.3. Descripción del Proyecto

El proyecto pretende utilizar la topología real de un cliente retail con una infraestructura de VPN manuales que presenta inconvenientes de disponibilidad, seguridad y confiabilidad y sin definiciones claras de calidad de servicio, esto genera actualmente pérdida de productividad para la compañía ya que de la infraestructura de red dependen entre otros los procesos de facturación e inventario.

La solución planteada por el proyecto es realizar un diseño de SD-WAN que aproveche al máximo los componentes existentes en la red y que permita simplificar la gestión de la red, automatizar las operaciones de cambios de políticas dentro de la red y mejorar la disponibilidad, seguridad y rendimiento de la red permitiendo al mismo tiempo un incremento del ancho de banda disponible mediante balanceo de carga que permita soportar el incremento de tráfico en las redes WAN que implica migrar algunas de las aplicaciones críticas hacia la nube.

### 1.4. Definición del Problema

Un cliente del sector retail como parte de su proyecto de renovación tecnológica se encuentra migrando sus servicios y aplicaciones internas a la nube, el cliente es consciente de que esta migración generaría mucha mayor carga sobre sus enlaces WAN, y se consideran inviables las ampliaciones de todos sus canales principal y Backup para el tráfico estimado ya que esto aumentaría los costos de tal forma que se haría inviable. Además de la migración a la nube este es un cliente que se encuentra creciendo a un ritmo muy acelerado y cuenta en el momento con alrededor de 700 sedes remotas, por lo cual con la infraestructura actual a veces no es capaz de darle manejo a todo el tráfico que tiene cuando se presentan picos.

La gestión de la red se realiza de forma manual en cada equipo, y al contar con tantas sedes los cambios y la implementación de las políticas de red se ejecutan de forma muy lenta y por tanto realizar cambios a nivel de IT se vuelve muy complicado dado el cuello de botella en la gestión de la red, lo cual aumenta los tiempos de ejecución de los cambios de red para el cliente.

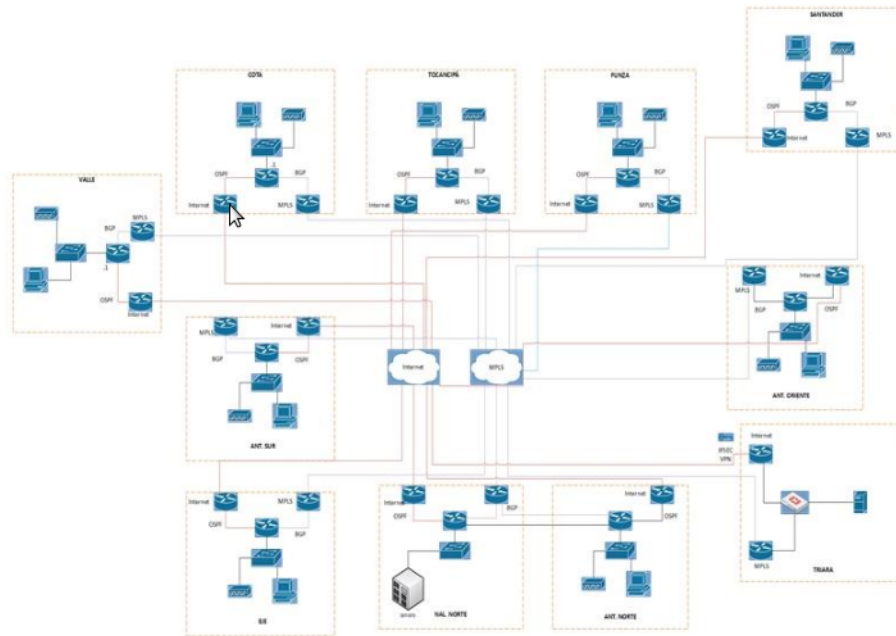
El cliente presenta un aumento de tráfico que supera la capacidad de sus enlaces WAN

actuales al migrar sus servicios a la nube, dicho aumento afecta la calidad de los servicios en tiempo real como la telefonía y los servicios de videoconferencia. Al validar los costos de las ampliaciones necesarias para soportar la cantidad de tráfico se identifica que el costo recurrente mensual es excesivo para el presupuesto de la compañía por lo que se debe encontrar una alternativa que se ajuste tanto a las necesidades como al presupuesto del cliente. Adicionalmente cuando se presentan fallas en la MPLS el cliente debe conmutar su tráfico al datacenter de forma manual, lo cual aumenta los tiempos de gestión de las fallas y por tanto la indisponibilidad del servicio. Adicional a estos problemas de disponibilidad y de saturación se han presentado ataques de seguridad sobre la infraestructura del cliente y robo de información utilizando los canales de Internet que tiene el cliente y los datos que por allí transporta.

El cliente es una de las compañías líderes del sector retail en Colombia, con alrededor de 700 sucursales a nivel nacional y con 11 oficinas regionales que se encargan de la administración de estas sucursales, cada una de las sucursales se encuentra conectada por túneles L2TP hacia su respectiva regional, estos túneles son formados a través de enlaces de internet banda ancha y mediante ellos se accede a los servicios de red, algunos de estos servicios como telefonía IP, servidor de archivos y directorio activo se encuentran ubicados en el centro de datos privado del cliente, mientras que otros servicios como SAP y la interconexión con instituciones financieras y con sus aliados estratégicos se encuentran como servicios virtualizados en grandes centros de datos. Adicional a esto el cliente se encuentra utilizando servicios en la nube como skype para colaboración, Gsuite y algunos servicios de Amazon.

La comunicación con cada uno de estos servicios se establece desde Internet para el caso de las sucursales, para el caso de sus regionales y el centro de datos en donde se encuentran sus servicios virtualizados esta comunicación se establece mediante los canales MPLS presentes en cada una de las regionales y el backup de esta comunicación son túneles EoIP mediante el canal de internet de cada regional. A continuación se muestra la topología de la compañía que muestra la forma como se interconectan las sedes regionales entre sí y con el centro de datos desde el cual se accede a los servicios críticos de la compañía (figura 1.1 SD-WAN):

Se identifican como causas de los inconvenientes anteriormente mencionados la utilización de servicios en la nube y el hecho de que cada una de las sucursales debe enviarle el tráfico a las regionales para consumir cualquier recurso de red, inclusive si es una llamada a otra sucursal esto ha ocasionado los altos picos de tráfico sobre los canales de intranet de las sucursales. Adicional a esto las sucursales cuentan con túneles EoIP configurados entre las sedes en caso de falla de su canal MPLS, pero los túneles son utilizados únicamente como backup, por lo que el ancho de banda de los canales de internet no es utilizado aún cuando se presentan picos de saturación sobre la intranet. Por otro lado la causa de la lentitud en la configuración de nuevas políticas o servicios de red es el hecho de que los cambios se realizan manualmente, es por este motivo que



**Figura 1.1:** Descripción de una SD-WAN

dentro de la solución se propondrá el hecho de que haya gestión centralizada desde la controladora SD-WAN. En cuanto a los problemas de seguridad presentados se incluye dentro de la solución el cifrado de los túneles que interconectan tanto las sucursales como las oficinas regionales, de manera que el tráfico deje de cursar en texto claro por la red pública.

Por otro lado una de las causas más importantes de los problemas de disponibilidad de servicio que ha presentado el cliente ha sido que bajo el modelo actual la conmutación de sus servicios de Datacenter se realiza a través de unas VPN IPSEC que se suben manualmente en los equipos, lo que incrementa el tiempo de indisponibilidad de los servicios y los tiempos de gestión de fallas.

## 1.5. Aspectos a Solucionar

La gestión de la infraestructura de red debe realizarse de forma manual en cada una de las tiendas.

La comunicación por internet entre las diferentes regionales se realiza sin cifrar y la de las tiendas se cifra bajo un protocolo que ya no es considerado seguro.

La conexión hacia el centro de datos no cuenta con un respaldo automático sino que en este momento debe realizarse de forma manual lo cual aumenta el tiempo de gestión de una falla y por lo tanto disminuye el tiempo de disponibilidad.

En momentos de congestión de la red el tráfico cursa únicamente por el canal principal de la MPLS y el ancho de banda disponible por el canal de internet no es aprovechado.

La conexión de las tiendas hacia todos los servicios que consume depende del canal de internet de la regional, si este se cae todas las tiendas que están asociadas a él quedan sin conexión.

## 1.6. Solución de la Propuesta

Se propone realizar un diseño para el cambio de esquema de conectividad WAN del cliente de una solución tradicional a una solución SD-WAN que permita realizar los cambios de forma centralizada y más ágil, esta automatización debe realizarse en conjunto con políticas de conectividad que le garanticen al cliente el balanceo de carga del tráfico WAN de manera eficiente e inteligente utilizando los enlaces dependiendo de las necesidades del tráfico de cada aplicación.

La solución debe incluir además un esquema de transporte que de independencia del medio o servicio que se utilice (Internet o Intranet) y que permita tanta flexibilidad de cambiar el tipo de servicio de manera transparente cómo reducir los costos mensuales del cliente en cuanto a enlaces WAN, esto debe realizarse con el protocolo de enrutamiento que más se ajuste al esquema y con las políticas de QoS necesarias para garantizar que el tráfico de cada servicio funcione de forma adecuada.

La solución debe diseñarse además de forma que todos los aspectos mencionados anteriormente apliquen tanto para el tráfico que el cliente utilice para aplicaciones en la nube como para el tráfico de aplicaciones que aún se encuentren en Datacenter administrado por ellos o en el centro de datos del ISP (Proveedor de Servicio de Internet).

El cliente requiere por tanto una solución de SD-WAN que disminuya los costos de la operación y al mismo tiempo incremente la disponibilidad de ancho de banda y eficiencia de sus conexiones WAN mediante un balanceo de carga entre sus enlaces principal y de respaldo. El cliente requiere un diseño de red que cumpla con los siguientes criterios:

- Balanceo de tráfico inteligente: el cliente requiere que sea utilizado el ancho de banda de los dos canales que tiene en cada sede para soportar la cantidad de tráfico que implica su migración de servicios a la nube, este balanceo debe ser

inteligente de manera que se cumpla con los requisitos de retardo, jitter y pérdida de paquetes que requiere cada aplicación de la compañía, si estos criterios no se cumplen bajo uno de los canales el tráfico debe ser enviado por el otro de forma automática.

- **Seguridad:** al tratarse de tráfico transaccional el cliente requiere que el transporte de datos cumpla con todos los requisitos de seguridad en la compañía en cuanto a la integridad, privacidad y disponibilidad.
- **Disponibilidad:** se requiere que el servicio tenga una alta disponibilidad y que esta se priorice para las aplicaciones críticas del cliente, el esquema de alta disponibilidad debe ser automático.
- **Aprovisionamiento ágil:** se requiere que en caso de requerir cambios generales a nivel de red WAN estos no tengan que ser configurados de forma manual en cada una de las sedes, sino que por el contrario puedan configurarse políticas de forma centralizada y enviarse las configuraciones de forma masiva para agilizar la implementación de cambios.
- **Independencia del transporte:** se requiere una solución que no dependa de la forma de transporte, que pueda establecerse por Internet o por MPLS sin inconvenientes y que si se decide cambiar de tecnología esto sea transparente para el servicio.
- **Adecuado para nube híbrida:** la solución propuesta debe cumplir los requerimientos tanto para las aplicaciones que se encuentran en la nube como para aquellas que aún están en el Datacenter del cliente, y debe realizar balanceo y dar prioridad a las aplicaciones.
- **Calidad de servicio:** el diseño debe tener unas políticas de QoS que garanticen el correcto funcionamiento de todas las aplicaciones que cursan por la red, que incluyen tráfico de voz y video.
- **Conexiones dinámicas:** El diseño propuesto debe utilizar tecnologías que eliminan la necesidad de configurar túneles estáticos cada vez que se agregue una sede o regional, sino que estos se configuren dinámicamente en una tecnología en malla.

## 1.7. Metodología

Se tiene un objetivo principal, y para llegar a él Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem

ipsum dolor sit amet, consectetur adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

## 1.8. Contribuciones

La principal contribución de este trabajo es Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

## 1.9. Estructura de la tesis

Este trabajo está dividido en XX capítulos. Al principio se encuentra

Finalmente se encuentra la parte de

## Estado del Arte

---

### 2.1. Marco de Referencia Teórico

#### 2.1.1. Conceptos generales de SD-WAN

SD-WAN es una aplicación específica de la tecnología de redes SDN aplicada a las conexiones WAN utilizadas para conectar redes empresariales sobre grandes distancias geográficas suministrando una arquitectura overlay moviendo el plano de control a la nube, sea esta pública o privada. Según SDN central, SDN puede definirse como un enfoque de software centrado a las tecnologías de networking que reducen los costos operacionales y de capital (Capex y Opex) mediante un control programático de la infraestructura de red, facilitando la customización optimización e innovación.

#### 2.1.2. Modelos de Programabilidad de Red

Existen actualmente 4 modelos de programabilidad de red, considerados como arquitecturas SDN, la diferenciación fundamental entre los 4 modelos consiste en la forma como el plano de control se comunica con el plano de datos de los dispositivos. Estos modelos pueden resumirse como sigue:

- **APIs programables:** la primera aproximación a SDN es la inclusión de API (Interfaz de Programación de Aplicaciones) dentro de los dispositivos de red, en este modelo sin embargo no hay un desacoplamiento de los planos de datos y control y estos siguen estando dentro del dispositivo de red, los equipos de red se comunican directamente con las aplicaciones a través de APIs u otro mecanismo como NETCONF (Protocolo de Configuración de Red) ver figura 2.1.A.
- **SDN Clásico:** en este modelo el plano de control y el plano de datos si se encuentran desacoplados completamente, el plano de control se comunica con las aplicaciones mediante APIs y con el plano de datos mediante “Openflow” u otro protocolo propietario, ver figura 2.1.B.

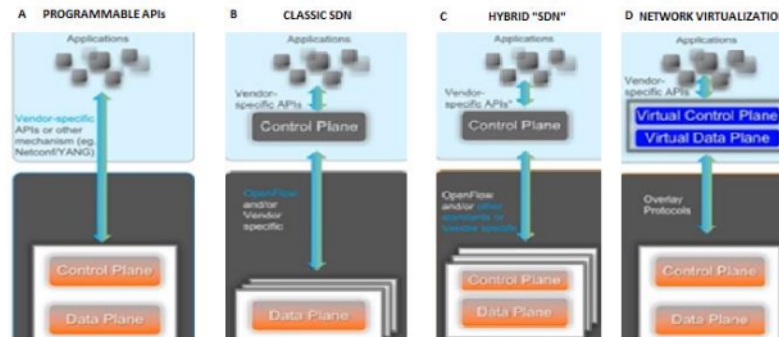


Figura 2.1: Apis Programable

- **SDN híbrido:** funciona bajo el mismo concepto que la arquitectura clásica de SDN, con la diferencia de que en este caso los dispositivos mantienen su propio plano de control, pero siguen comunicándose con las aplicaciones a través de Openflow mediante una controladora que mantiene el plano de control de todos los equipos, figura 2.1.C.
- **Virtualización de red:** la tendencia de la virtualización ha dividido las redes en un dominio físico y uno virtual, la tendencia es que las decisiones de enrutamiento y seguridad se hagan por software en el plano de virtualización, la comunicación entre este plano virtual y el físico se realiza mediante tecnologías desarrolladas por los fabricantes de software de virtualización, uno de los ejemplos más conocidos es NFX, ver figura 2.1.D.

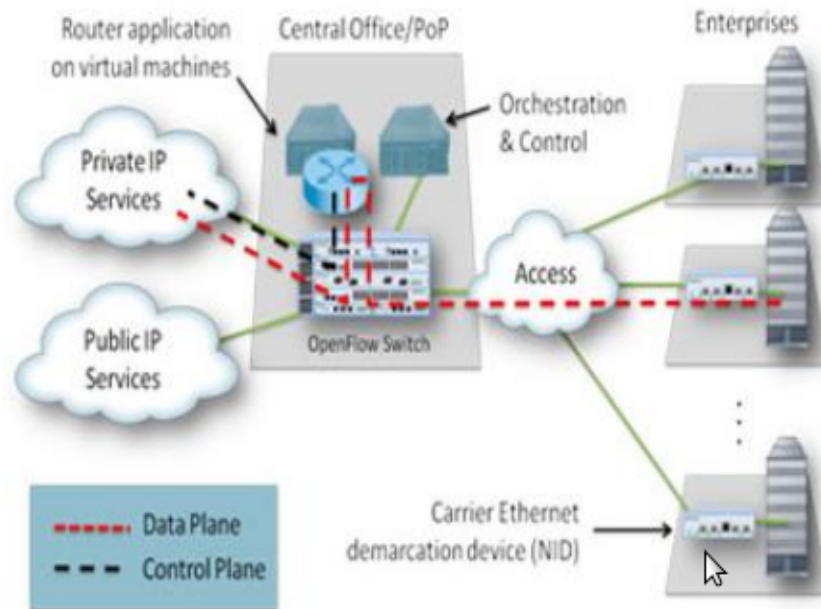
### 2.1.3. NFV

*“Network Function Virtualization o NFV ofrece una nueva forma de diseñar, aprovisionar y administrar los servicios de red, desacoplando las funciones de red de los hardware propietarios y realizando funciones en software como NAT (“Network Address Translation”), firewall y DNS (Sistema de Nombres de Dominio) por nombrar algunos ejemplos. Esta tecnología se encuentra diseñada para consolidar los componentes de red requeridos para lograr una infraestructura completamente virtualizada.”*

Bajo este concepto toda la orquestación y control de los dispositivos físicos se realizaría desde un punto central desde donde se administran las funciones de red, desacoplando así las funciones de red de los dispositivos físicos. La siguiente imagen (figura 2.2) muestra un ejemplo de cómo funcionaría una red bajo este esquema.

NFV se diferencia de SDN tradicional en cuanto a que en lugar de desacoplar como tal el plano de control se enfoca en las funciones de red como tal, pero cumple el mismo objetivo de obtener una infraestructura de red que sea más ágil y escalable.





**Figura 2.2:** Network Function Virtualization

#### 2.1.4. OpenFlow

*“Es un protocolo utilizado para suministrar una interfaz abierta para controlar la conectividad y los flujos de dicha conectividad dentro de una red SDN, es un protocolo extensible por lo que permite a los programadores definir elementos adicionales que permitan al protocolo adaptarse a diferentes redes y a nuevas tecnologías.”<sup>2</sup>*

Openflow funciona principalmente a través de programas Datapath en donde se define el comportamiento esperado para cada tipo de paquete y el camino que debe tomar dentro de la red, para esto Openflow utiliza diversos componentes durante su ejecución que pueden verse en la figura 2.3.(OFN SDN evolution ver 1.0,Open Networking Foundation, 2016.

#### 2.1.5. NETCONF

*“El protocolo se encuentra definido por el estándar RFC6241 de la IETF y suministra mecanismos para instalar, manipular y eliminar configuración en dispositivos de red utilizando el formato XML. NETCONF define un mecanismo simple mediante el cual un dispositivo obtiene una API, esto con el objetivo de que las aplicaciones utilicen dicha API para enviar y recibir configuraciones desde y hacia los dispositivos de red, esto utilizando el paradigma RPC de forma que el cliente codifique un RPC en formato XML y lo envíe a un servidor, quien responderá con otro XML codificado.”<sup>4</sup>*

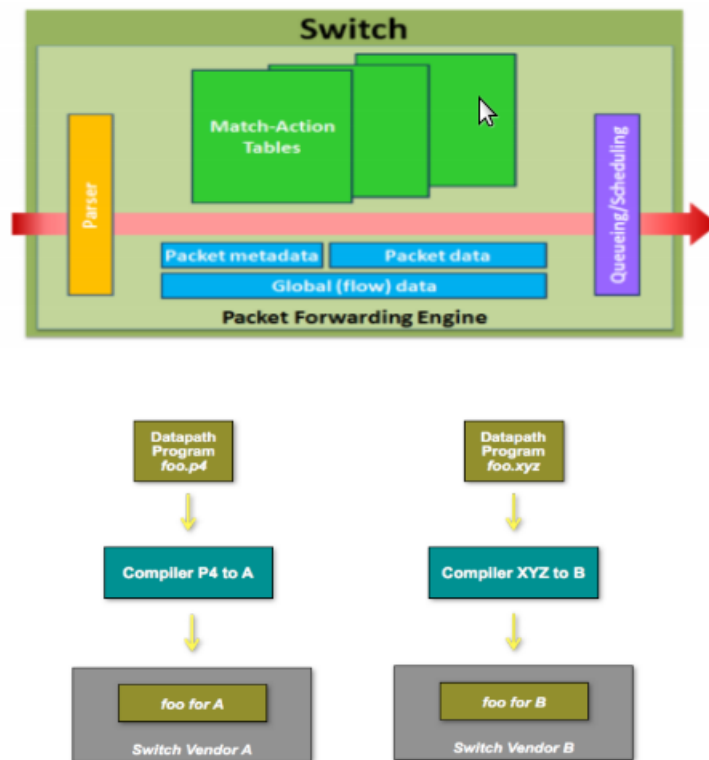


Figura 2.3: Openflow áreas de especificaciones open Datapath

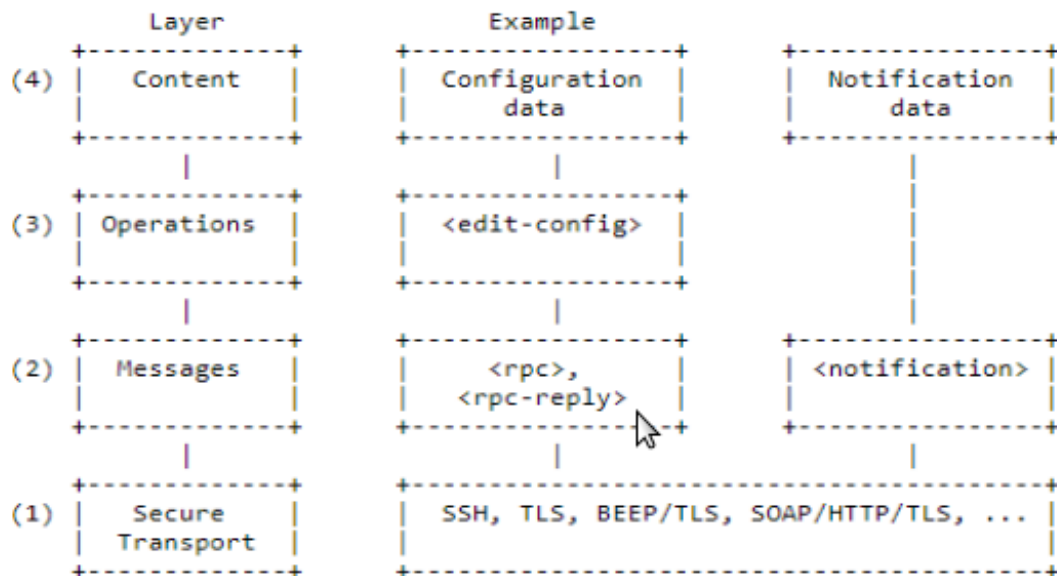


Figura 2.4: NetConf

Conceptualmente el protocolo NETCONF se divide en 4 capas como lo muestra la siguiente figura 2.4:

## 2.1.6. Modelos de Datos

### 2.1.6.1. YANG

Es un lenguaje de modelado de datos que se utiliza para modelar datos de estado y configuración del protocolo NETCONF y se encuentra definido bajo el RFC6020 de la IETF, YANG modela la organización jerárquica de los datos como un árbol y provee una descripción clara de cada nodo, así como su relación con otros nodos.<sup>5</sup> YANG define cuatro tipos de nodo para el modelado de datos. 6:

- **Nodo leaf:** Contiene datos simples como enteros o strings, contiene un tipo de valor particular y no tiene nodos hijos.
- **Nodo leaf-list:** es una secuencia de nodos leaf, en donde cada uno tiene su valor particular.
- **Nodo contenedor:** Es utilizado para agrupar nodos relacionados en un sub árbol, este tipo de nodos no tiene valor y sólo tiene nodos hijos. Un contenedor

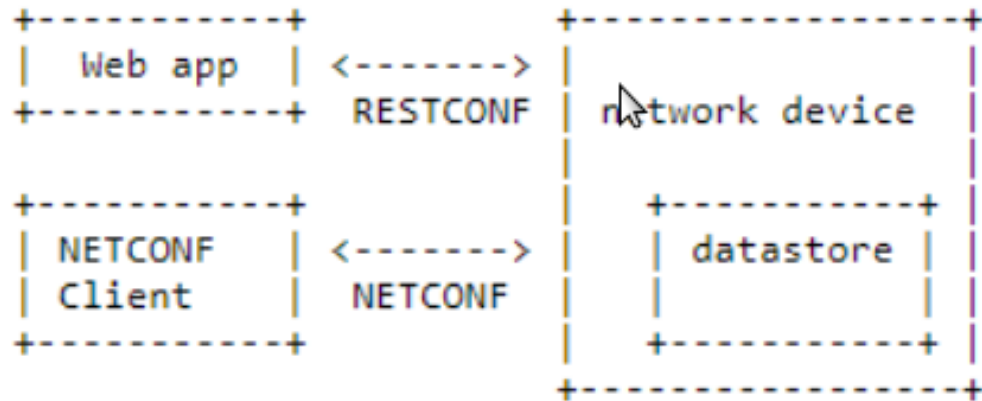


Figura 2.5: RestConf

puede contener nodos de cualquier tipo, incluyendo leaf, list, leaf-list o incluso otros contenedores.

- **Nodo listo:** Define una secuencia de entradas de lista identificados por el valor de su leaf “key” una lista puede contener varias de estas llaves y contener cualquier número de nodos de cualquier tipo.

### 2.1.7. RESTful APIs

Arquitectura de software para sistemas distribuidos, diseñado para realizar aplicaciones en red. Ajustándose a ciertas condiciones.

### 2.1.8. RESTCONF

RestConf es un protocolo basado en HTTP que suministra una interfaz programática para acceder a datos definidos en YANG.<sup>7</sup> Netconf y RestConf suelen trabajar en conjunto permitiendo la ejecución de operaciones CRUD, hay dispositivos que soportan los dos protocolos en conjunto de la siguiente manera (figura 2.5):

Al estar basado en “HTTP” las operaciones “CRUD” de “RESTCONF” se realizan mediante los métodos tradicionales, como los son los siguientes: “get, post, push, patch, delete”.

### 2.1.9. Marco de Referencia Tecnológico

Sobre este proyecto se tratará con algunas de las tecnologías SD-WAN más conocidas y utilizadas en el mercado, las tecnologías aquí tratadas son las que se consideran viables

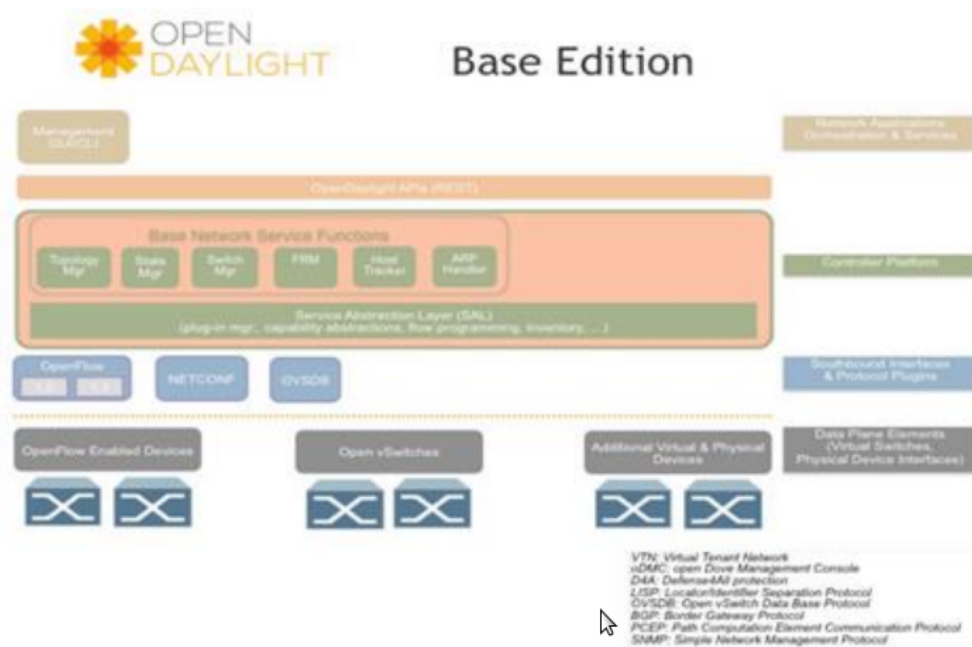
para el proyecto en alguna medida, esto teniendo en cuenta que a día de hoy existen soluciones de este tipo tanto propietarias como abiertas y por tanto en este documento únicamente se refieren las soluciones abiertas y las propietarias que coincidan con la infraestructura actual del cliente (Cisco).

#### 2.1.10. Open Daylight

El proyecto OpenDaylight es una plataforma de código abierto para SDN que hace uso de protocolos abiertos para suministrar control centralizado y programático de los dispositivos de red, así como monitoreo de estos. La plataforma se basa en una arquitectura de “Microservicios” en la que cada microservicio es un protocolo o servicio particular requerido por el usuario durante la instalación de la controladora. La controladora soporta un amplio rango de protocolos de red para su funcionamiento como lo son: Openflow, p4 BGP, PCEP, LISP, Netconf, Ovsdb y Snmp. La capa de abstracción del servicio se encuentra basada en YANG, el cual se utiliza para crear esquemas de bancos de datos, generar REST API (RESTCONF) y generación automática de código.

OpenDaylight suministra un gran conjunto de servicios de red para diferentes servicios, uno de los más interesantes para este proyecto es el servicio de NRO(Network Resource Optimization), en donde los algoritmos en la controladora explotan el hecho de la naturaleza centralizada de una SD-WAN, sus analíticas y su mecanismo de políticas para lograr implementar ingeniería de tráfico a través de una infraestructura heterogénea. La controladora divide la operación de la red en 4 planos diferentes:

- **Elementos del plano de datos:** Son los dispositivos físicos que se encargan de dar conectividad a la red, esta es la red tradicional que se conoce normalmente, la diferencia es que los equipos deben soportar Openflow u otro protocolo a través del cual la controladora pueda configurar los equipos.
- **Interfaces Southbound:** Es la forma de comunicación de la controladora con el resto de la red, esto a través de tecnologías como Openflow o NETCONF.
- **Controladora:** consta de la capa de abstracción de servicio - SAL, que se encarga de la abstracción del plano de control de la red de los dispositivos físicos a la controladora y de las funciones de servicios de red, que vienen a ser aplicaciones predefinidas que vienen por defecto sobre la controladora.
- **Aplicaciones de red orquestación y servicios:** Esta es la capa de la controladora que se encarga de a través de RESTful API permitir la programabilidad de la red y por tanto la automatización de procesos sobre la red. Las funciones de cada una de las capas y la relación entre ellas pueden verse de forma más clara en la siguiente figura 2.6:



**Figura 2.6:** Open Daylight

Uno de los aspectos clave de la controladora OpenDaylight es MD-SAL (Model Driven Service Abstraction Layer), el cual autogenera APIs RESTCONF para los objetos en los modelos de los que aprende, la solución se basa por tanto en RESTCONF y MD-SAL en conjunción con modelos YANG de datos para la configuración de red, colección de estadísticas y orquestación de servicios. La siguiente figura 2.7 muestra el flujo que ocurre entre estos elementos dentro del funcionamiento de la controladora.

### 2.1.11. IWAN

IWAN es una solución SD-WAN propietaria de Cisco cuyo objetivo es la reducción de costos para el transporte de la información del cliente al hacer viable mediante una serie de tecnologías la utilización de enlaces menos costosos como internet, en esta solución el tráfico se enruta de manera dinámica según las condiciones de la aplicación, la solución está diseñada para empresas cuyas sucursales tengan un aumento en su tráfico WAN por el uso de aplicaciones en la nube, Cisco dice ofrecer las siguientes ventajas con su aplicación de IWAN:

IWAN se compone de varias tecnologías que hacen de la solución una alternativa efectiva para las sucursales que utilizan tanto consumo de aplicaciones centralizadas como aplicaciones en la nube figura 2.8:

- **Independencia de transporte:** La solución utiliza DMVPN para la creación de

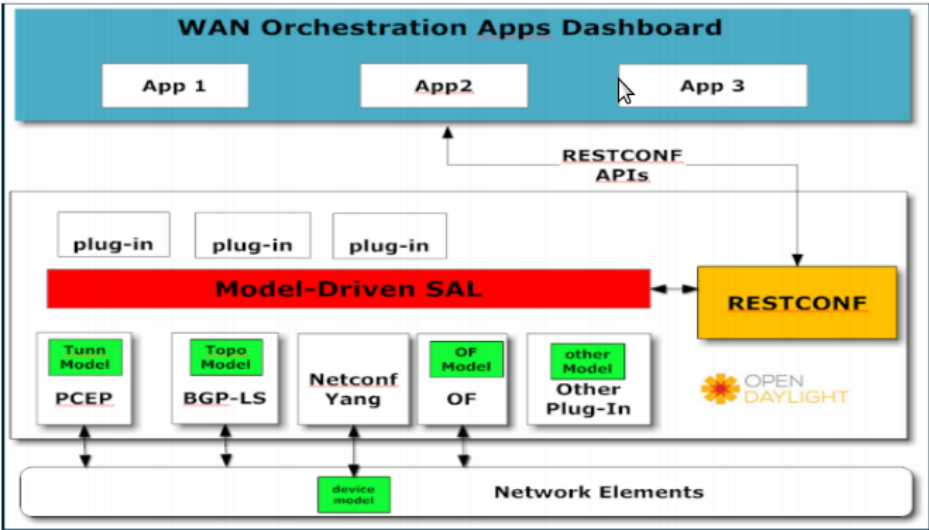
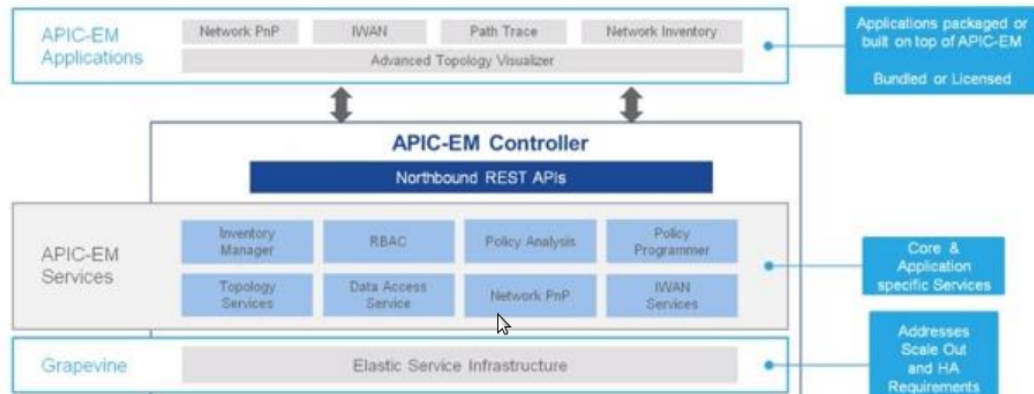


Figura 2.7: Flujo que ocurre entre estos elementos dentro del funcionamiento de la controladora.

Usuarios temporales Wi Fi	SaaS MS 365 Google Docs Salesforce.com	Aplicaciones de alto consumo de ancho de banda Video, VDI	Ahorros de gastos operativos
<ul style="list-style-type: none"><li>Más ancho de banda</li><li>Visibilidad y control</li><li>Defensa contra amenazas</li><li>DIA: sin backhaul</li></ul>	<ul style="list-style-type: none"><li>DIA: baja latencia</li><li>Activación de enlace rápida</li><li>Visibilidad y control</li></ul>	<ul style="list-style-type: none"><li>Más ancho de banda</li><li>Activación de enlace rápida</li><li>DIA para el tráfico correcto, enlace correcto</li></ul>	<ul style="list-style-type: none"><li>Uso de enlaces de Internet de bajo costo</li><li>Uso de flexibilidad para servicios nuevos</li></ul>
Flexibilidad del proveedor • Mayor productividad • Costos más bajos			

Figura 2.8: Iwan.



**Figura 2.9:** Api-EMC Controller

túneles dinámicos entre todas las sedes, estos túneles se encuentran encriptados para garantizar un componente de seguridad sobre el transporte, aunque vaya por la red pública, esto permite obtener una topología “full-mesh” de manera automática y al mismo tiempo obtener una configuración independiente del tipo de transporte y del proveedor de servicios que sea contratado.

- **Enrutamiento basado en aplicación:** La solución utiliza además de EIGRP como protocolo de enrutamiento, una solución propietaria de Cisco llamada performance routing, que permite tomar decisiones de enrutamiento basándose en el estado actual de los enlaces y en las necesidades de calidad de servicio de cada aplicación.
- **Gestión centralizada:** mediante la controladora SDN APIC-EM es posible gestionar los equipos remotos desde un punto centralizado y realizar cambios a una gran cantidad de dispositivos al mismo tiempo, agilizando y automatizando los cambios de red.
- **Optimización de recursos WAN:** la solución incluye una tecnología de compresión de tráfico llamada WAAS que permite ahorrar costos en los enlaces WAN haciendo más efectivo el uso del ancho de banda.

La controladora SDN que utiliza esta tecnología se denomina APIC-EM, esta controladora no solamente cumple la función de plano de control, sino que también contiene aplicaciones de red embebidas que aprovechan la naturaleza centralizada, entre esas aplicaciones se encuentra IWAN, que es la solución SD-WAN puntual que se presenta en este documento, la SDN sin embargo es el puente entre la aplicación y la red física, esto puede apreciarse con mayor detalle en la siguiente figura 2.9:

Una de las mayores ventajas de esta controladora es que no necesita de equipos de



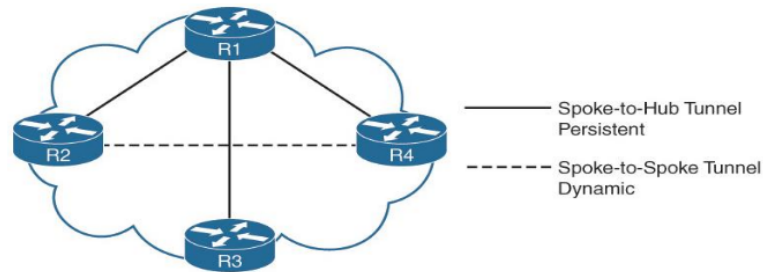


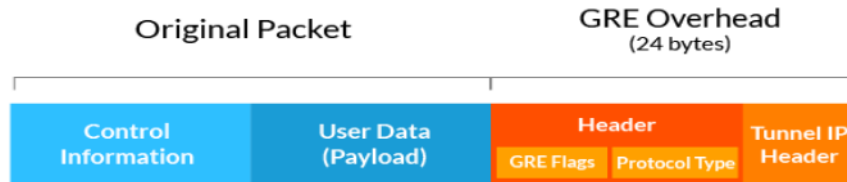
Figura 2.10: DMVPN

red especiales que soporten los protocolos de SDN, aunque esto último es lo recomendado el APIC-EM trae las ventajas de SDN sin requerir de una gran inversión en cambio de equipos de red, lo que lo hace una opción bastante atractiva para una compañía que quiera empezar a adentrarse en la programabilidad de la red sin requerir una inversión inicial tan fuerte.

DMVPN(Dynamic Multipoint VPN) es la solución de transporte propietaria de Cisco que hace parte de la solución de IWAN, es una solución de overlay en donde las ubicaciones remotas establecen un túnel estático hacia una ubicación central(centro de operaciones) y establece túneles de manera dinámica entre diferentes ubicaciones remotas(spokes). Esto permite tener conectividad full-mesh sin tener que realizar las configuraciones de todos los túneles de forma manual, los túneles entre spokes son removidos después de un periodo de inactividad, liberando así recursos de memoria y CPU y por tanto eliminando la necesidad de routers tan robustos en las sedes remotas, los equipos de enrutamiento de mayor capacidad deben ser por tanto utilizados en el sitio central (centro de operaciones). La siguiente figura 2.10 muestra el comportamiento dinámico de DMVPN. DMVPN utiliza diversas tecnologías para lograr este objetivo, las más relevantes se enuncian a continuación.

**Túneles mGRE:** es un protocolo de entunelamiento capaz de transportar múltiples protocolos como IPv4, IPv6 y otros, estos túneles son asignados a una interfaz física y requieren direccionamiento propio en la interfaz del túnel, la diferencia entre esta tecnología y los túneles GRE tradicionales es que mGRE puede conectar más de 2

dispositivos utilizando el mismo túnel. los túneles se forman agregando un encabezado IP externo al paquete con la información IP fuente y destino correspondiente a las interfaces fuente y destino del túnel como lo muestra la figura 2.11. **NHRP:** Este protocolo se encuentra definido bajo el RFC 2332, y es utilizado para que un equipo fuente determine el siguiente salto hacia un destino en una red NBMA, es decir realiza una resolución de direccionamiento, similar a lo que ocurre con ARP en la resolución de dirección IP a dirección MAC. El protocolo funciona utilizando un NHS que se encarga de la resolución de direccionamiento dentro de la nube de NHRP, por su parte los equi-

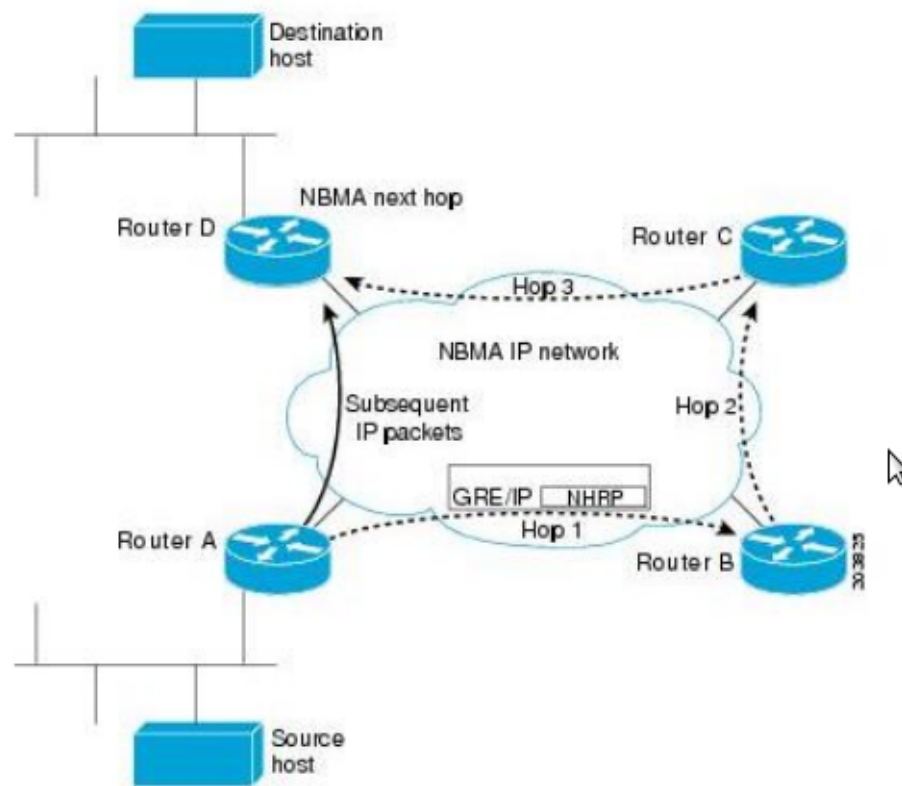


**Figura 2.11:** Túneles se forman agregando un encabezado IP externo al paquete con la información IP

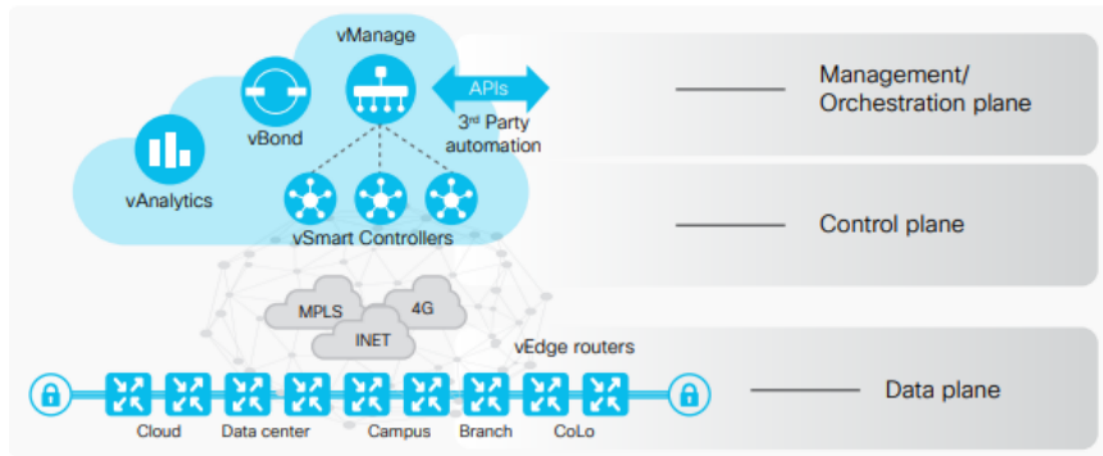
pos NHC son aquellos que realizan las peticiones de NHRP hacia el NHS. La siguiente figura 2.12 representa el funcionamiento de NHRP en términos generales: Adicional al registro de los NHC con los NHS, NHRP tiene la capacidad de que los NHC encuentren un camino más corto sobre la infraestructura o formar uno mediante una conexión virtual directamente hacia otro NHC, esta habilidad es utilizada en DMVPN para establecer una topología full mesh sin todo el trabajo administrativo que esto conlleva. Por su parte WAAS es una tecnología propietaria de Cisco que se encarga de optimizar el tráfico TCP en la red con el principal objetivo de disminuir la utilización de ancho de banda utilizando algoritmos de compresión para este fin. Son varias las tecnologías que reúne WAAS para la optimización del ancho de banda a nivel WAN, de ellas vale la pena resaltar las 3 más relevantes.

- **TFO Optimization:** utiliza varias tecnologías de optimización de flujo para optimizar el tráfico TCP, realizando funciones como escalamiento de ventanas TCP, maximización del tamaño de ventana inicial, Buffering incrementado, BIC TCP.
- **Compresión:** utiliza algoritmos de eliminación de datos redundantes (DRE) y compresión LZ para optimizar el tráfico WAN.
- **Aceleración específica de aplicaciones:** analiza y predice el tráfico de una aplicación para transformar una secuencia de comandos en una más pequeña, generando así ahorro en la utilización del ancho de banda.

Todas las tecnologías mencionadas con anterioridad junto con el protocolo de enrutamiento especificado (el recomendado es EIGRP) conforman la solución de IWAN, que más que una solución de SD-WAN es un conjunto de tecnologías y un diseño que optimiza el tráfico WAN de la red, sin embargo, al utilizar este conjunto de tecnologías con la controladora SDN de Cisco se logra una solución SD-WAN que vale la pena considerar 8.



**Figura 2.12:** Funcionamiento de NHRP



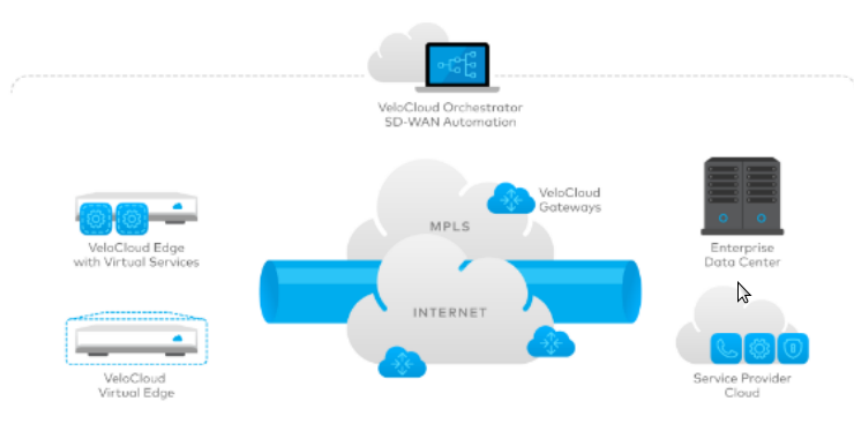
**Figura 2.13:** Arquitectura de esta propuesta VIPTELA

#### 2.1.12. Cisco VIPTELA

La nueva solución SD-WAN de Cisco divide la topología de red en 3 planos diferentes, un plano de datos, uno de control y uno de gestión y orquestación, integrado con su nueva arquitectura DNA, la solución pretende automatizar las configuraciones de red creando una red overlay que permite agilizar las configuraciones y en donde los equipos físicos pasan a un segundo plano en cuanto a gestión de la red, la siguiente figura 2.13 muestra la arquitectura de esta propuesta de Cisco. Es importante notar que los protocolos que corren en el “underlay” sobre la infraestructura siguen siendo los mismos que en el caso de IWAN, es decir Pfr, DMVPN y EIGRP y WAAS como protocolos principales, sin embargo en esta solución lo que cambia es la administración y la gestión, ya que en lugar de la plataforma APIC-EM se tiene un ecosistema más rico por la inteligencia de la red, compuesto por el vManage como componente principal encargado de crear nuevos servicios de red en demanda y garantizar la automatización end-to-end de toda la infraestructura. Cabe mencionar que IWAN sigue siendo una de las aplicaciones más utilizadas dentro del nuevo esquema de SD-WAN de Cisco, la diferencia radica en la controladora y el funcionamiento general de la arquitectura.

#### 2.1.13. NSX SD-WAN

Esta solución de VMware se encuentra desarrollada en base a un appliance que actúa como CPE especialmente diseñado para la función de SD-WAN de NSX, aunque también es posible utilizar una VNF de CPE para este propósito. Este dispositivo utiliza Dynamic Multipath Optimization (DMO) y deep application recognition agregan múltiples enlaces y dirige el tráfico sobre los enlaces óptimos. La solución se divide en 3 componentes diferentes listados a continuación:



**Figura 2.14:** Distribución de los componentes

- **NSX-SDWAN Gateway:** proporciona rutas de datos optimizadas para las aplicaciones, las sucursales y los centros de datos, al mismo tiempo que da la capacidad de brindar servicios de redes en la nube.
- **NSX-SDWAN Edge:** Ofrecen conectividad a aplicaciones, híbridas, privadas y públicas, este componente puede encontrarse en forma de dispositivo físico o en forma de instancia virtual.
- **NSX-SDWAN Orchestrator:** Es el componente de la solución que contiene la inteligencia y la automatización, su objetivo es habilitar el aprovisionamiento de servicios virtuales de forma ágil y automatizada.

La distribución de estos componentes dentro de la solución puede apreciarse en la siguiente figura 2.14:

## 2.2. WAN definida por software (SD-WAN)

La red de área amplia definida por software (SD-WAN o SDWAN) es una aplicación específica de la tecnología de red definida por software (SDN) aplicada a conexiones WAN como Internet de banda ancha, 4G, LTE o MPLS.

Conecta redes empresariales, incluidas sucursales y centros de datos, en grandes distancias geográficas. Se puede usar una WAN, por ejemplo, para conectar sucursales a una red central corporativa o para conectar centros de datos separados por distancia. En el pasado, las conexiones WAN a menudo usaban tecnología que requería hardware propietario especial.

SD-WAN, por otro lado, utiliza Internet o una red privada nativa de la nube. SD-WAN desacopla la red del plano de gestión y separa las funciones de gestión y supervisión del tráfico del hardware. Se basa en cuatro componentes centrales:

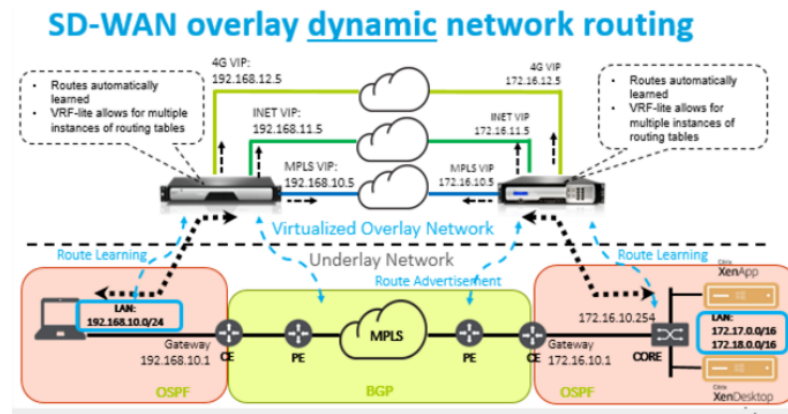


Figura 2.15: WAN definida por software (SD-WAN)

- Abstracción de conectividad de borde
- Virtualización WAN
- Gestión centralizada y dirigida por políticas

Gestión elástica del tráfico.

## 2.3. Controladores de negocio SD-WAN (SDWAN)

Los clientes empresariales exigen tecnologías WAN más flexibles, abiertas y basadas en la nube, en lugar de instalar tecnología WAN patentada o especializada que a menudo involucra costosos circuitos fijos o hardware propietario.

Muchas de las nuevas ofertas de WAN definidas por software, por ejemplo, se pueden usar para mejorar y asegurar la conectividad a internet, lo que la hace más competitiva con tecnologías WAN heredadas más caras como T-1 o MPLS.

Sin embargo, según un estudio de Nemertes, el 78 % de las organizaciones que implementan SD-WAN no tienen planes de eliminar completamente el MPLS de su WAN”.

En algunos casos, la tecnología WAN definida por software utiliza conexiones de banda ancha de Internet para reemplazar soluciones más caras. La tecnología de virtualización puede aplicar la seguridad y la tecnología de red privada virtual (VPN) a las conexiones de Internet de banda ancha, lo que las hace más seguras.

Una tendencia notable en el ámbito de las redes es la creciente adopción de la multi-nube en las redes empresariales. La multi-nube es una mezcla de nubes privadas y públicas. Las combinaciones comunes son varias nubes públicas o una nube pública y una nube privada, y cada nube sirve una aplicación empresarial específica.

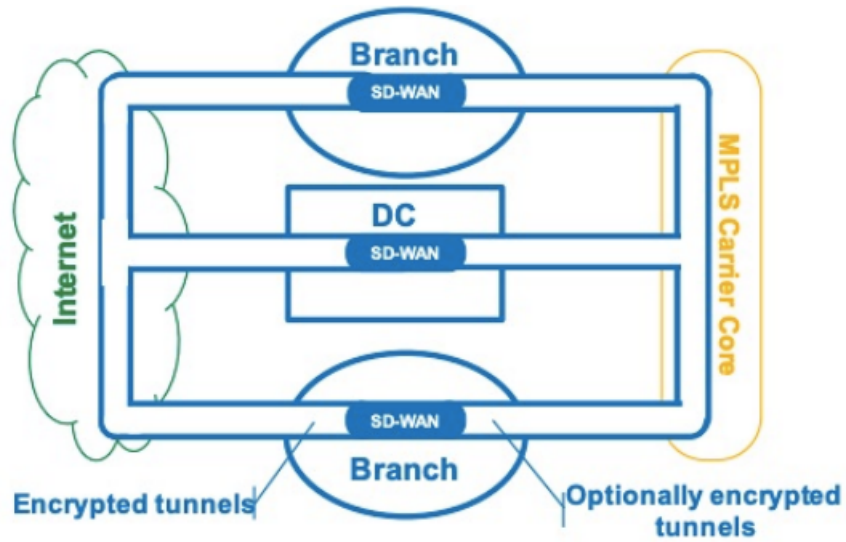


Figura 2.16: WAN definida por software (SD-WAN)

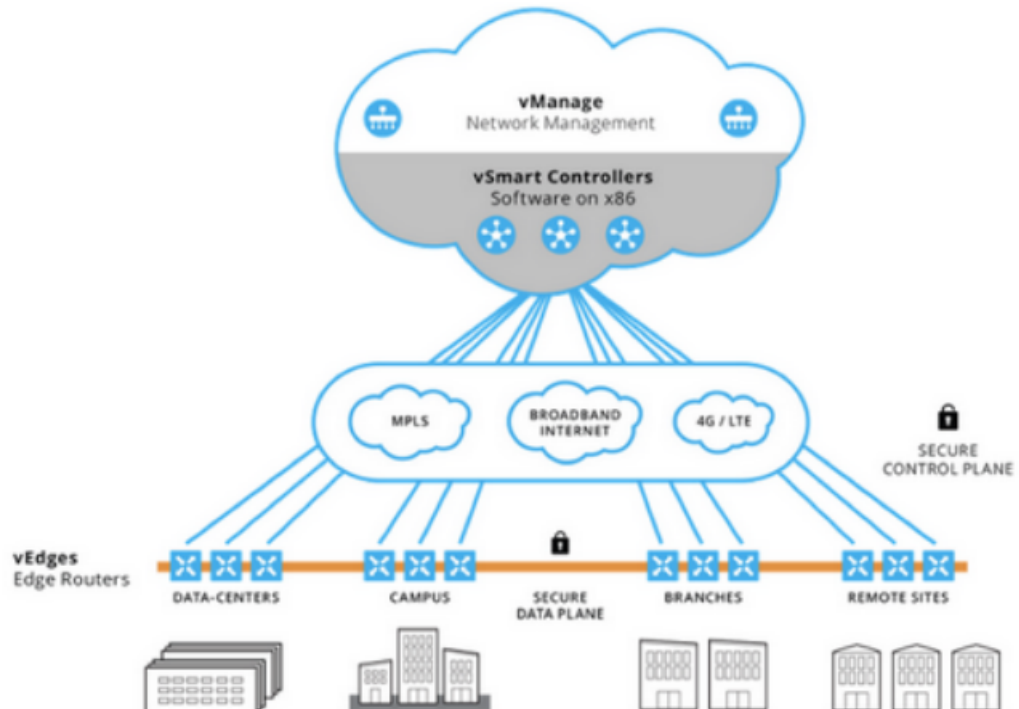


Figura 2.17: WAN definida por software (SD-WAN)

SD-WAN a menudo se integra en una estrategia de nube múltiple ya que mejora la conectividad y aumenta la seguridad en la nube múltiple.

Su escalabilidad en numerosas ubicaciones y su administración centralizada para la nube pública y privada facilitan la administración de la nube múltiple. Varios productos SD-WAN cifran los datos en los puntos de conectividad y proporcionan firewalls y seguridad basada en aplicaciones.

### 2.3.1. Enfoque al cliente: costo, confiabilidad, seguridad

Un resumen de investigación de SDxCentral, SD-WAN seguro: Buscando el Santo Grial, enfatiza que ".en encuesta tras encuesta (incluidas las de SDxCentral), la seguridad generalmente se ubica entre las tres principales en cuanto a capacidades clave de SD-WAN".

El objetivo principal de SD-WAN La tecnología WAN consiste en ofrecer una conexión WAN en la nube, segura y simple, de clase empresarial, con la mayor cantidad de tecnología abierta y basada en software que sea posible.

Esto se puede usar para brindar conectividad WAN básica, o se puede usar para servicios empresariales de primera calidad como VPN, optimización de WAN y control de entrega de aplicaciones (ADC).

Muchas nuevas empresas buscan el potencial en el mercado de WAN definido por software, y las empresas establecidas también están persiguiendo el mercado. Según el IDC, el mercado SD-WAN crecerá a una tasa de crecimiento anual compuesta de 40.4 % de 2017 a 2022 para llegar a \$ 4.5 mil millones".

Gartner identifica a los jugadores clave en la tecnología SD-WAN en su Cuadrante Mágico de 2018 para el Informe de Infraestructura de Borde WAN. Nombró a tres líderes: Silver Peak, Cisco y VMware. La firma también reconoció que Riverbed, Citrix, Fortinet, Aryaka y Huawei también son fuertes competidores en el mercado.

Muchos de estos proveedores tienen enfoques del mercado ligeramente diferentes. Por ejemplo, Silver Peak se enfoca en acelerar las aplicaciones de Software-as-a-Service (SaaS) en la nube. VMware integró el producto VeloCloud en su propia línea de productos, el VMware NSX SD-WAN de VeloCloud, después de que adquirió VeloCloud en diciembre de 2017.

El producto contiene aplicaciones de vanguardia, orquestación y puertas de enlace residentes en la nube. Aryaka construyó una red global para que las empresas puedan usar WAN como una red como servicio (NaaS) en cualquier lugar, incluso fuera del área de



uno de los puntos de presencia (POP) de Aryaka.

Los proveedores incumbentes de tecnología WAN, como Cisco y Riverbed, que fabrican dispositivos especializados para la conectividad WAN, ahora se centran más en la optimización de WAN y en las ofertas WAN de vanguardia.

Espere que la tendencia se acelere en los próximos años. Lo que comenzó como una solución para conectividad WAN de sucursales y centros de datos que requieren menos equipos patentados parece expandirse a una amplia gama de ofertas y tecnologías SD-WAN (SDWAN) que incluyen VPN, seguridad, ventaja, optimización de WAN, NaaS y Control de políticas de aplicación.

Los 3 tipos de arquitectura SD-WAN.

Si está considerando si SD-WAN mejorará la red de área amplia de su empresa, he aprendido que es importante conocer primero las diferentes arquitecturas de SD-WAN.

Como un proveedor de servicios de Internet (ISP) y agente de la nube desde hace mucho tiempo, he tenido el mejor asiento en la casa para ver cómo la locura de SD-WAN toma vuelo. A medida que aparecen docenas de ofertas de productos SD-WAN, tengo el envidiable trabajo de darle sentido a todo. [suspiro]

En mi observación, hay 3 grupos principales de arquitectura SD-WAN, cada uno de los cuales beneficia a ciertos tipos de empresas. La arquitectura que sea "mejor" depende de las aplicaciones a las que acceda su empresa a través de su WAN.

### 2.3.2. Solo en premisa

Una arquitectura SD-WAN "solo para uso local.<sup>es</sup> exactamente como suena. Su empresa tiene una caja SD-WAN (esencialmente un enrutador plug-and-play), que realiza la configuración del tráfico en tiempo real en cada sitio ... y eso es todo.

Nota al margen: tenga en cuenta que estoy utilizando astutamente la terminología "prem.<sup>a</sup>cortada para eludir el argumento gramatical de "premisa frente a premisa" notoriamente acalorado [¡decir ah!]

A diferencia de algunas de las otras arquitecturas, el cuadro SD-WAN en el sitio no se conecta a una puerta de enlace en la nube (se explica más adelante). Solo se conecta a los otros sitios de su empresa.

#### 2.3.2.1. Mejor ajuste:

Empresas que alojan todas sus aplicaciones en la empresa (sin ninguna aplicación en la nube). Si su empresa no utiliza aplicaciones en la nube, no es necesario utilizar una solución SD-WAN habilitada para la nube.

Agregar la habilitación de la nube aumentará los costos, innecesariamente. Una configuración común es mantener una red MPLS (mucho más pequeña) para aplicaciones en tiempo real (es decir, voz, video o escritorio virtual), y utilizar la Internet pública (controlada por SD-WAN) para todo lo demás.

### **2.3.2.2. Beneficios:**

Costes de ancho de banda de habilitación de nube SD-WAN mensuales más bajos o más bajos. Equilibrio de carga multi-circuito / ISP. Conformación del tráfico en tiempo real, que mejora el rendimiento de todas las aplicaciones WAN. Mejor recuperación de desastres (DR), al tener una mejor copia de seguridad de conectividad.

### **2.3.3. Cloud**

En una arquitectura SD-WAN habilitada para la nube, la solución ofrece una caja SD-WAN en el sitio que se conecta a una puerta de enlace (virtual) en la nube. Con esta arquitectura, su empresa obtiene los beneficios de una arquitectura solo en la premisa (es decir, configuración de tráfico en tiempo real y balanceo de carga de múltiples circuitos), además de un mayor rendimiento y confiabilidad de sus aplicaciones en la nube.

La puerta de enlace de la nube está conectada en red directamente a los principales proveedores de la nube (es decir, Office 365, AWS, Salesforce, etc.), lo que se traduce en una mejora general del rendimiento de sus aplicaciones en la nube. Además, si el circuito de Internet de su empresa falla al usar una aplicación en la nube, la puerta de enlace puede mantener una sesión en la nube activa (mientras que el circuito falla).

Si su empresa tiene un circuito de Internet alternativo, la SD-WAN puede redirigir su aplicación en la nube de forma instantánea al circuito de Internet alternativo de su empresa, evitando la interrupción de una sola sesión.

#### **2.3.3.1. Mejor ajuste:**

Compañías que ejecutan aplicaciones en la nube de renombre, como Office 365, AWS, Drop Box, Azure, Salesforce, etc. Una configuración común es tener aplicaciones internas en tiempo real que se ejecutan en una pequeña red MPLS y tener aplicaciones en la nube (y todo else), corriendo sobre la Internet pública, controlada por una SD-WAN.

#### **2.3.3.2. Beneficios:**

- Cloud gateways, mejorando el rendimiento de las aplicaciones en la nube.
- Cloud gateways, mejorando la fiabilidad de las aplicaciones en la nube.
- Equilibrio de carga multi-circuito / ISP.
- Conformación del tráfico en tiempo real, que mejora el rendimiento de todas las aplicaciones WAN.
- DR mejorado por tener una mejor copia de seguridad de conectividad.

#### **2.3.4. Cloud backbone**

Siempre es bueno tener una columna vertebral, ¿verdad? La arquitectura SD-WAN habilitada para la nube se puede llevar a otro nivel cuando obtiene una red troncal. La arquitectura SD-WAN "habilitada para la nube más la red troncal." ofrece una caja SD-WAN en el sitio que conecta su sitio con el punto de presencia de red (POP) más cercano del proveedor de SD-WAN, donde su tráfico salta en la parte privada del proveedor de SD-WAN. Fibra óptica, red troncal.

Mientras el tráfico de su WAN atraviesa la red troncal privada del proveedor de SD-WAN, se garantiza que mantendrá bajos niveles de latencia, pérdida de paquetes y fluctuaciones.

Esto mejora el rendimiento de todo el tráfico de red, particularmente el tráfico en tiempo real como voz, video y escritorio virtual. La red troncal también está conectada directamente con los principales proveedores de aplicaciones en la nube (es decir, Office 365, AWS, etc.), que, al igual que la arquitectura anterior, aumenta el rendimiento y la confiabilidad de esas aplicaciones.

##### **2.3.4.1. Mejor ajuste:**

Una empresa que ejecuta una gran cantidad de aplicaciones de red en tiempo real, que desea eliminar completamente su red MPLS (para reducir los costos), pero no quiere que su tráfico en tiempo real se desplace al 100 % a través de la Internet pública (por temor a una alta latencia, paquetes pérdida y jitter).

#### **2.3.4.2. Beneficios:**

El tráfico de WAN se basa principalmente en una red troncal privada, lo que mejora el rendimiento de todas las aplicaciones de red, especialmente las aplicaciones en tiempo real.

- **Cloud gateways, mejorando el rendimiento de las aplicaciones en la nube.**
- **Cloud gateways, mejorando la fiabilidad de las aplicaciones en la nube.**
- **Equilibrio de carga multi-circuito / ISP.**
- **Conformación del tráfico en tiempo real, que mejora el rendimiento de todas las aplicaciones WAN.**
- **DR mejorado por tener una mejor copia de seguridad de conectividad.**

Actualmente no hay muchos proveedores que ofrezcan esta arquitectura.

Sin embargo, como muchos ISP han agregado el servicio SD-WAN a su cartera de productos (ya que los ISP ya tienen la infraestructura de red troncal), solo tiene sentido que varios ISP finalmente agreguen esta opción a su oferta de SD-WAN.

Suena bastante simple, ¿verdad? Así un poco. Por supuesto, dentro de cada una de estas 3 arquitecturas hay varias variables más, pero creo que esto le brinda un comienzo sólido para evaluar y diseñar con precisión una solución SD-WAN para su empresa.

---

## Capítulo 3

# Requerimientos

---

El presente trabajo de investigación se consideró con los siguientes requerimientos, un estudio descriptivo debido a la comprensión de aspectos cualitativos y cuánticos, su propósito es el planteamiento y descripción de un problema y propone estrategias en el diseño de red SD - WAN.

### 3.1. Requerimientos funcionales

La aplicación de estrategias en diseño de red SD-WAN contribuye con calidad de servicio en la protección de datos, fácil administración. La investigación sugiere preguntas que a continuación se relacionó con los requerimientos funcionales de partida.

- **Posibilidades:** etapa de conceptualización del proceso de diseño
- **Efectividad:** modelamiento del sistema puede ser evaluado por novedad y viabilidad.
- **Estructura:** ordenador o herramientas necesarias para el diseño e implementación.
- **Método:** solución del problema.

El avance de la tecnología ha creado nuevos sistemas y herramientas para los sistemas de telecomunicaciones.

### 3.2. Requerimientos no Funcionales

La implementación de políticas del diseño de una red SD-WAN empresa reduce los riesgos, protección de datos, mantenimiento, fácil administración, entre otros.

Contribución a la calidad de servicio (QOS) y navegación segura.

Personal calificado para capacitación, crea conciencia de seguridad en los empleados de la organización.

---

## Capítulo 4

# Metodología de Desarrollo

---

*Para el desarrollo del presente proyecto de grado se tomó en cuenta: “El método de investigación cualitativa es la recogida de información basada en la observación de comportamientos naturales, discursos, respuestas abiertas para la posterior interpretación de significados. Investigadores cualitativos estudian la realidad en su contexto natural.”*

Utilización de la Metodología del Project Management Institute (PMI)

Método PMI *“Ofrece una serie de directrices que orientan la gestión y dirección de proyectos, válidas para la gran mayoría de proyectos. Sin embargo, este método no debe concebirse como algo cerrado.”*

Tomando en cuenta los siguientes procesos de desarrollo del presente trabajo de grado.

*“Un proceso está compuesto por todas aquellas actividades interrelacionadas que se deben ejecutar para poder obtener el producto o prestar el servicio. Existen dos tipos de procesos que se superponen e interactúan entre sí.*

Procesos de la dirección de proyectos. Compuesto por cinco procesos o categorías diferentes, estos procesos, aseguran el progreso adecuado del proyecto a lo largo de todo su ciclo de vida.

- Proceso de iniciación
- Proceso de planificación
- Proceso de ejecución
- Proceso de supervisión y control
- Proceso de cierre del proyecto.
- Procesos orientados al producto. Este tipo de procesos especifican y crean el producto. Varían en función del área de conocimiento.”

---

Con las siguientes áreas de conocimiento:

- Gestión de la Integración
- Gestión del Alcance
- Gestión del Tiempo
- Gestión de Costes
- Gestión de la Calidad
- Gestión de los Recursos Humanos



## Diseño de la solución SD-WAN

---

### 5.1. Selección de proveedor y tecnología

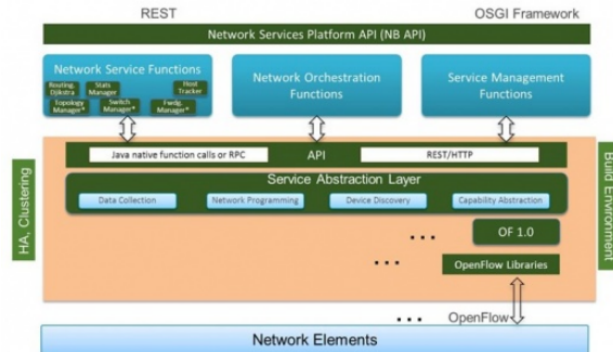
Para la selección de la solución específica que se diseña tenemos en cuenta los costos de cada una de ella y por supuesto las ventajas en términos de servicio que obtendría el cliente, el principal criterio de selección es utilizar la solución que cumpla con los objetivos del proyecto sin implicar costos demasiado grandes para el cliente. Teniendo esto en cuenta debemos considerar la solución actual del cliente.

Hace poco tiempo el cliente migró su infraestructura de unos equipos Mikrotik a dispositivos Cisco, por lo que de ser posible el proyecto debe conservar dichos equipos para no perder la inversión realizada por el cliente. La migración realizada fue de equipos Mikrotik a equipos Cisco 891 en las diferentes tiendas y equipos Cisco 4331 en las regionales y la sede nacional.

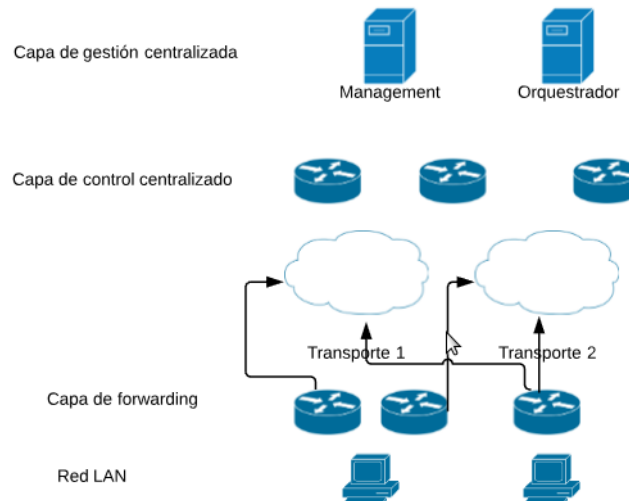
Dados los criterios definidos anteriormente se procede a analizar cada una de las soluciones que se plantearon para el desarrollo del proyecto.

La primera opción que se consideró fue utilizar OpenDayLight como controlador SD-WAN ya que este utiliza totalmente software abierto para su funcionamiento, esta plataforma utiliza protocolos abiertos como Openflow y Netconf, la figura 5.1 muestra la arquitectura de esta solución: Esta arquitectura aunque al utilizar protocolos estándar permite que se conecte cualquier elemento de red que hable Openflow tiene la limitante de que los equipos de red tradicionales, incluyendo los que tiene el cliente no soportan OpenFlow por defecto, y por tanto los enrutadores que utiliza el cliente hoy en día no se integran con esta arquitectura de SDN, lo que significa que implementar esta solución requeriría cambiar todos los enrutadores por unos que soporten OpenFlow.

Se tuvieron en cuenta también soluciones de varios fabricantes para el proyecto, más precisamente las soluciones SD-WAN de Nokia(Nuage), Cisco(Viptela), vmware(Velo



**Figura 5.1:** OpenDayLight como controlador SD-WAN



**Figura 5.2:** Soluciones SDN

cloud) y Silverpeak, estas son las soluciones que dominan el mercado a la fecha de elaboración de este documento. Todas estas son soluciones SDN que desagregan completamente los planos de control y gestión de los enrutadores en las sedes Branch y los centralizan en controladoras y servidores de gestión, aunque todas las soluciones mencionadas utilizan protocolos diferentes su arquitectura y funcionamiento es muy similar figura 5.2.

Dentro de cada una de estas opciones se desagregan las capas de control y de gestión en un sitio centralizado, normalmente un centro de datos, y en los branch solamente se tiene la capa de envío de datos o forwarding, estas sedes remotas se comunican entre ellas en todos los casos mediante túneles que se forman automáticamente gracias al

plano de control centralizado, sin embargo la tecnología con la que se forman dichos túneles y con la que se envía la información de enrutamiento del plano de control al plano de forwarding cambia considerablemente entre todas las soluciones, y por tanto son incompatibles entre ellos. Las siguientes son las tecnologías que cada una de las soluciones mencionadas utiliza para la comunicación contra los routers de borde:

- **Nokia (nuage): Openflow**
- **Cisco (Viptela): Netconf, OMP**
- **Vmware (VeloCloud): Dynamic multipath Optimization**
- **Silverpeak: Dynamic path control**

Podemos ver entonces que los enrutadores tradicionales no soportan ninguno de los protocolos de los diferentes fabricantes, por tanto cada fabricante desarrolla sus propios routers de borde para su solución SD-WAN, y por esta razón la implementación de cualquiera de estas soluciones implicaría un reemplazo total de los equipos.

Existe una solución SD-WAN de Cisco basada en los enrutadores tradicionales llamada IWAN, esta solución combina diferentes protocolos ya activos en los enrutadores tradicionales: EIGRP, DMVPN, PfR, WAAS y NBAR para generar una solución basada en aplicaciones que balancee y enrute el tráfico de forma inteligente en la red, todo automatizado a través de su controlador SDN: APIC-EM. Los enrutadores con los que cuenta el cliente soportan cada una de las aplicaciones aquí mencionadas y por tanto esta sería la única solución que no requiere un reemplazo total de los equipos del cliente.

Por esta razón IWAN fue la solución seleccionada para el desarrollo de este proyecto, ya que de otra forma la inversión que se requeriría al reemplazar todos los enrutadores del cliente con cualquiera de las demás soluciones aquí consideradas sería tan alta que impediría el desarrollo del proyecto, ya que el capital con el que se cuenta para el desarrollo del mismo es limitado.

## 5.2. Consideraciones iniciales del diseño

---

Capítulo 6

# Resultados

---

---

Capítulo 7

## Discusión

---

---

Capítulo 8

# Conclusiones

---

---

Capítulo 9

## Bibliografía

---

---

Apéndice A

## Código/Manuales/Publicaciones

---

### **A.1. Apéndice**

Apéndice