Universidad El Bosque

Trabajo de Grado

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

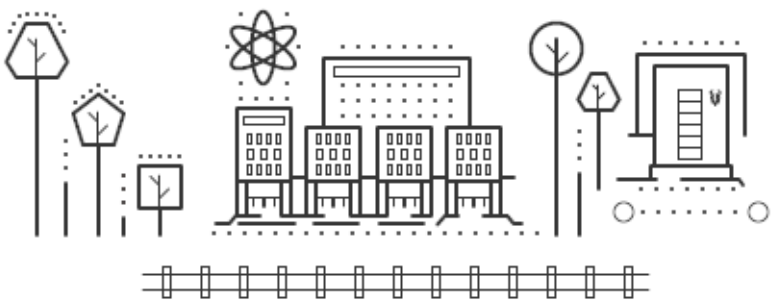
Tesis que para Optar por el Grado de: Especialista en

Diseño de Redes Telemáticas

Presentado por: **Joan Sebastian Quintero Ceballos**,
José Armando Son Rojas,
Ingeniero en Telecomunicaciones
Ingeniero Electrónico

Ingeniero:

Director: Jesús Rafael Cantillo Alzamora



Facultad de Ingeniería
Universidad El Bosque
Bogotá D.C. Colombia

Junio, 2019

Diseño y Simulación de Solución SD-WAN para un Cliente Retail con Consumo de Servicios en la Nube

Este documento fue generado por el procesador (pdf)LaTeX, com base de template “novathesis” [1] y editado por José Armando Son Rojas [2]. [1] https://github.com/jsonArmando/thesis [2] https://www.uelbosque.edu.co

Agradecimentos

A nuestra querida Universidad y a todas las autoridades por permitirnos concluir con una etapa de nuestras vidas, gracias a la paciencia, orientación y guía en el desarrollo de este proyecto de grado.

A cada uno de los profesores quienés impartieron sus conocimientos con mucho esfuerzo por hacer posible este trabajo de grado.

Al director **Jesús Rafael Cantillo Alzamora** por ser guía y aporte.

Al ingeniero **Oscar Arias** con la enseñanza de sus valiosos conocimientos durante todo el proceso, colaboración y dirección permitió este trabajo.

Al ingeniero **Jairo Hernán García Triana** por ayudarnos en esta formación académica.

A cada uno de nuestros compañeros cada momento vivido son simplemente únicos.

Muchas Gracias a Todos Ustedes

A la Facultad de Ingeniería y a la Universidad, por la formación que nos han dado. Es gracias a ustedes que es posible el presente trabajo. En verdad, gracias.

Resumen

Varias empresas de diferentes campos laborales hoy en día estan implementado SD-WAN **("Software Defined Networking in Wide Area Networks")**, para contrarestar el alto costo de equipos de telecomunicaciones y mejor administración de sus infraestructuras. Para financiar sus proyectos han buscado alternativas como la nube o cloud, virtualización entre otros. Sin embargo actualmente las empresas no han buscado la migración o adaptación de sus redes a esta nueva tecnología, creando una brecha en subdesarrollo en este campo de "Networking".

El objetivo de estudio es determinar cómo la virtualización de nuevas redes puede aumentarse y mejorar en las empresas que lo necesitan, con este fin la pregunta de investigación es la siguiente, ¿Es necesario la implementación de SD-WAN **("Software Defined Networking in Wide Area Networks")**? En este contexto es una tecnología que hoy en día es muy necesario.

Los estudios realizados sugiere que se debe llevar a cabo una implementación y diseño para un Cliente Retail una SD-WAN **("Software Defined Networking in Wide Area Networks")**, para mejorar su funcionalidad en las redes, obtener mejor administración y riesgo a vulnerabilidades describiendo varias estrategias cualitativas y cuantitativas para dar una solución que converja a mejorar la infraestructura de la empresa

Palabras-clave: SD-WAN, MPLS, Virtualización, Cloud, Capex, Opex, Redes...

Abstract

Several companies in different fields of work today are implementing SD-WAN **("Software Defined Networking in Wide Area Networks")**, to counteract the high cost of telecommunications equipment and better management of their infrastructures. To finance their projects have searched for alternatives such as cloud or cloud, virtualization among others. However, companies have not sought migration or adaptation of their networks to this new technology, creating a gap in underdevelopment in this field of "Networking".

The objective of the study is to determine how the virtualization of new networks can be increased and improve in the companies that need it. To this end, the research question is as follows: Is it necessary to implement SD-WAN **("Software Defined Networking in Wide Area Networks")**? In this context, it is a technology that is very necessary today.

The studies carried out suggest that an SD-WAN **("Software Defined Networking in Wide Area Networks")** must be implemented and designed for a Retail Client, in order to improve its functionality in the networks, obtain better administration and risk to vulnerabilities describing several qualitative and quantitative strategies to give a solution that converges to improve the infrastructure of the company.

Keywords: SD-WAN, MPLS, Virtualization, Cloud, Capex, Opex, Networks ...

Índice

1 Título **1**

2 Introducción **3**

3 Descripción General del Proyecto **5**
3.1 Definición del Problema 5
3.2 Aspectos a Solucionar 8
3.3 Solución Propuesta 8

4 Estado del Arte **11**
4.1 Marco de Referencia Teórico 11
4.1.1 Conceptos Generales de una SD-WAN 11
4.1.2 Modelos de Programabilidad de Red 11
4.1.3 Network Function Virtualization (NFV) 12
4.1.4 OpenFlow 13
4.1.5 NETCONF 15
4.1.6 Modelos de datos 16
4.1.7 RESTful APIs 18
4.1.8 RESTCONF 18
4.2 Marco de Referencia Tecnológico 19
4.2.1 IWAN 19
4.2.2 DMVPN 21
4.2.3 WAAS 23
4.2.4 EIGRP 24
4.2.5 PFR 25
4.3 Open Daylight 27
4.4 Cisco VIPTELA 29
4.5 NSX SD-WAN 29
4.6 WAN definida por software (SD-WAN) 30

5 Glosario de Términos **33**

6 Justificación **35**

7 Objetivos **37**
7.1 Objetivo General . . . 37
7.2 Objetivos Específicos . . . 37

8 Requerimientos **39**
8.1 Requerimientos Funcionales . . . 39
8.2 Requerimientos no Funcionales . . . 39

9 Metodología de Desarrollo **41**
9.1 Utilización de la Metodología del Project Management Institute (PMI) . . . 41

10 Diseño de una Red SD-WAN **43**
10.1 Inversión para una SD-WAN . . . 43
10.2 Precios en una Red SD-WAN . . . 43
10.3 Costos para Implementación en Infraestructura Cloud . . . 44
10.3.1 Amazon . . . 44
10.3.2 Microsoft Azure . . . 45
10.3.3 Google Cloud . . . 47
10.3.4 Oracle Cloud . . . 47
10.4 Análisis de Inversión para Cloud . . . 48
10.4.1 Enfoque al Cliente: Costo, Confiabilidad, Seguridad . . . 48
10.5 Controladores de Negocio SD-WAN . . . 49
10.6 Introducción a SD-WAN . . . 49
10.7 Tipos de Arquitectura SD-WAN . . . 50
10.7.1 Enfoque de una SD-WAN . . . 50
10.7.2 Cloud . . . 51
10.7.3 Cloud Backbone . . . 52
10.8 Selección de Proveedor y Tecnología . . . 53
10.9 Ventajas y Desventajas de la Solución Propuesta . . . 56
10.10 Requerimientos de Aplicaciones . . . 56
10.11 Requerimientos de Ancho de Banda . . . 58
10.11.1 Sede Nacional Tocancipá: . . . 59
10.11.2 Sede Nacional Medellín: . . . 59
10.11.3 Sede Nacional Antioquia Norte: . . . 62
10.11.4 Sede Nacional Antioquia Norte: . . . 62
10.12 Diseño del DataCenter . . . 64
10.13 Diseño de Sedes Remotas . . . 67
10.14 Diseño de Tiendas . . . 67
10.15 Diseño de Regionales . . . 67
10.16 Diseño de Sedes Nacionales . . . 69
10.17 Diseño de Enrutamiento . . . 69
10.18 Simulación . . . 71

10.18.1Infraestructura Utilizada para la Simulación 71
10.18.2Topologías y Configuraciones Realizadas 72

11 Resultados **77**

12 Discusión **81**

13 Conclusiones **83**

Bibliografia **85**

Anexos **87**

I Anexo **87**

II Anexo 2 **91**

III Anexo 3 **95**

Lista de Figuras

3.1 Caracteríticas de un red SD-WAN 7

4.1 Modelos Programables de Red 12
4.2 Network Function Virtualization (NFV) 13
4.3 OpenFlow 14
4.4 DataPath OpenFlow 14
4.5 Capas del Protocolo NETCONF 15
4.6 RestFull API 18
4.7 Estructura RESTCONF 19
4.8 Ventajas de una IWAN 20
4.9 Estructura de APIC-EM 21
4.10 DMVPN 22
4.11 Túneles mGRE: 22
4.12 Protocol NHRP: 23
4.13 PfR 26
4.14 Branch PFR 26
4.15 Red Orquestación Open Daylight 28
4.16 Funcionamiento de una Controladora 28
4.17 Arquitectura Cisco VIPTELA. 29
4.18 Distribución de los Componentes 30
4.19 WAN definida por software (SD-WAN) 31

10.1 Precio en Máquinas Virtuales en Azure 45
10.2 Precio en Redes Virtuales en Azure 46
10.3 Diferentes características en Azure para Telecomunicaciones 46
10.4 Plataform Pricing Calculator Google 47
10.5 WAN definida por software (SD-WAN) 50
10.6 Arquitectura de una SD-WAN 51
10.7 Solución de la Arquitectura 54
10.8 Solución y Funcionamiento de una red SD-WAN 55
10.9 Telefonía 58
10.10 Sede Nacional Tocancipá 60
10.11 Sede Nacional Medellín 61

10.12Sede Nacional Antioquia Norte 62
10.13Sede Nacional Valle 63
10.14Diseño de DataCenter 65
10.15Topología de DataCenter 65
10.16Configuración de Túneles para el DataCenter 66
10.17Topología de Tiendas 68
10.18Topología Regionales 68
10.19Topología Sedes Nacionales 69
10.20Infraestructura Utilizada para la Simulación 71
10.21La topología configurada en GNS3 72
10.22Branch1 73
10.23Branch2 73
10.24Configuración EIGRP 73
10.25Configuración EIGRP 73
10.26Registros de los Routers 74
10.27Registros de los Routers 74
10.28Topología Router Branch 75
10.29Registro desde el Router 75
10.30Adyacencias EIGRP por los Túneles GRE 75
10.31Protocolo PfR 76

11.1 Conectividad 77
11.2 Ruta 77
11.3 Enrutado a través de la MPLS 78
11.4 Disponibilidad Deseada en la Red 78
11.5 Reconocimiento del cambio en PfR 78
11.6 Topología de las Sedes Regionales 78
11.7 Conectividad exitosa a través de la MPLS 79
11.8 Decisión de PfR 79
11.9 Falla de Fibra 79
11.10Enlace de INET 79

III.1 Algoritmo para el Diseño de la SD-WAN 95

Listagens

4.1 RPC Estructura en YANG 16
4.2 Interface YANG 17
I.1 HBR1 Configuration 87
II.1 HBR2 Configuration 91

Capítulo 1

Título

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

Capítulo 2

Introducción

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 **("Software Defined Networking in Wide Area Networks")** es necesario mencionar sus acciones, conectividad en el entorno de negocio empresarial, debido un administrador de red no puede cubrir dichas necesidades solo con servicios de MPLS **("del inglés Multiprotocol Label Switching")** WAN **("Wide Area Network en inglés")** 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.

Ante los retos de las redes modernas, en donde el reto consiste en aumentar la disponibilidad, confiabilidad y seguridad de una red mientras se reducen los costos de CAPEX

y OPEX y para un cliente que se enfrenta a una transformación digital en donde sus aplicaciones se encontrarán ahora con un esquema de red híbrida en lugar de datacenter tradicional, al migrar muchas de sus aplicaciones claves de negocio a la nube. Se requiere una solución que simplifique la gestión y la administración de una red compleja con cientos de sitios branch y permita aprovechar los beneficios de la nube sin suponer esto un aumento demasiado grande en los costos de OPEX. Ante estos retos SD-WAN **("Software Defined Networking in Wide Area Networks")** se plante hoy día como una de las mejores soluciones para gozar de una red inteligente y simple que esté enfocada al uso de las aplicaciones.

El proyecto como tal plantea el diseño y simulación para un cliente retail en este caso, que cuenta con cientos de redes *"branch"* alrededor de todo el país y requiere mejorar la disponibilidad y confiabilidad de su red al mismo tiempo que la adapta a las tecnologías cloud que ya se encuentran adaptando a su negocio.

Capítulo 3

Descripción General del Proyecto

El proyecto pretende utilizar la topología real de un cliente retail con una infraestructura de VPN **(en inglés Virtual Private Network)** 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, 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 **("Software Defined Networking in Wide Area Networks")** 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 **("Wide Area Network en inglés")** que implica migrar algunas de las aplicaciones críticas hacia la nube.

3.1 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 **("Wide Area Network en inglés")**, 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 **(Tecnología de la Información)** 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. Presenta un aumento de tráfico que supera la capacidad de sus enlaces WAN **("Wide Area Network en inglés")** 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 MPLS **("del inglés Multiprotocol Label Switching")** 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 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 **(("Layer 2 Tunneling Protocol"))** 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 **("(Internet Protocol)")**, servidor de archivos y directorio activo se encuentran ubicados en el centro de datos privado del cliente, mientras que otros servicios como SAP **(Soluciones de Software Empresarial)** 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 sucursales, las regionales y el centro de datos en donde se encuentran sus servicios virtualizados esta comunicación se establece mediante los canales MPLS **("del inglés Multiprotocol Label Switching")** presentes en cada una y el *"backup"* de esta comunicación son túneles EoIP **("en inglés Ethernet over IP")** mediante el canal de internet regional. A continuación se muestra la topología que interconectan las sedes regionales entre sí y con el

centro de datos desde el cual se accede a los servicios críticos de la compañía a **(figura 3.1 SD-WAN):**

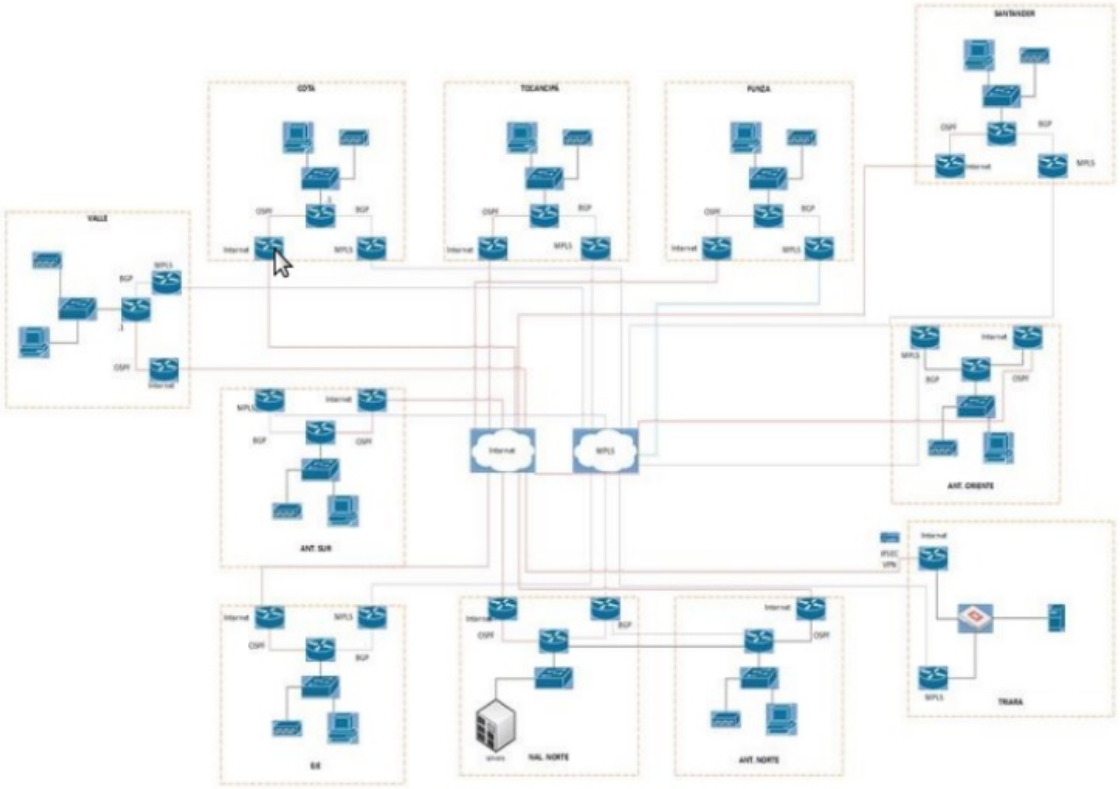


Figura 3.1: Caracteríticas de un red SD-WAN

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.

Adicional a esto las sucursales cuentan con túneles EoIP **("en inglés Ethernet over IP")** configurados entre las sedes en caso de falla de su canal MPLS **("del inglés Multiprotocol Label Switching")**, 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 dentro de la solución se propondrá el hecho de que haya gestión centralizada desde la controladora SD-WAN **(“Software Defined Networking in Wide Area Networks”)**. 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 **(en inglés Virtual Private Network)** IPSEC **("abreviatura de Internet Protocol security")** que se suben manualmente en los equipos, lo que incrementa el tiempo de indisponibilidad de los servicios y los tiempos de gestión de fallas.

3.2 Aspectos a Solucionar

La gestión de la infraestructura de red debe realizar 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 **("del inglés Multiprotocol Label Switching")** 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.

3.3 Solución Propuesta

Se propone realizar un diseño para el cambio de esquema de conectividad WAN **("Wide Area Network en inglés")** del cliente de una solución tradicional a una solución SD-WAN **("Software Defined Networking in Wide Area Networks")** 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 **("Wide Area Network en inglés")** 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 **("Wide Area Network en inglés")**, esto debe realizarse con el protocolo de enrutamiento que más se ajuste al esquema y con las políticas de QoS **Calidad de Servicio** 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 que se encuentren en DataCenter administrado por ellos o en el centro de datos del ISP **("en inglés de Internet service provider")**.

El cliente requiere por tanto una solución de SD-WAN **("Software Defined Networking in Wide Area Networks")** que disminuya los costos de la operación y al mismo tiempo incremente la disponibilidad de ancho de banda y eficiencia de sus conexiones WAN **("Wide Area Network en inglés")** mediante un balanceo de carga entre sus enlaces principal y de respaldo. El cliente requiere 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 **("Wide Area Network en inglés")** 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 **("del inglés Multiprotocol Label Switching")**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 **(Calidad de Servicio)** 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 eliminen la necesidad de configurar túneles estáticos cada vez que se agregue una sede o regional sino que estos se configuran dinámicamente en una tecnología en malla.

Capítulo 4

Estado del Arte

4.1 Marco de Referencia Teórico

4.1.1 Conceptos Generales de una SD-WAN

SD-WAN **(“Software Defined Networking in Wide Area Networks”)** es una aplicación específica de la tecnología de redes SDN **("en inglés Software Defined Networking, SDN")** aplicada a las conexiones WAN **("Wide Area Network en inglés")** 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 **("en inglés Software Defined Networking, SDN")** central, puede definirse como un enfoque de software centrico 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 optimización e innovación.

4.1.2 Modelos de Programabilidad de Red

Existen actualmente 4 modelos de programabilidad de red, considerados como arquitecturas SDN **("en inglés Software Defined Networking, 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:

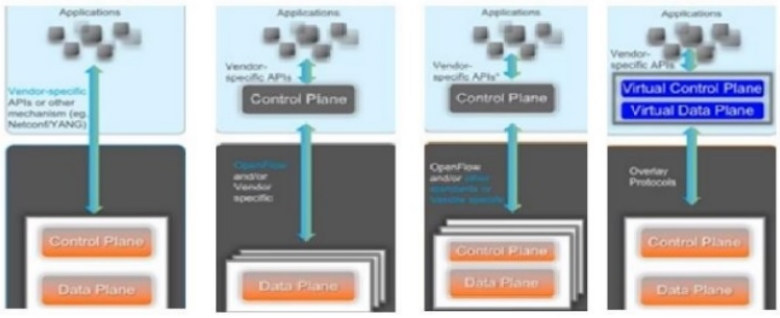
- **APIs programables:** la primera aproximación a SDN **("en inglés Software Defined Networking, SDN")** es la inclusión de API **(del inglés API: Application Programming Interface)** dentro de los dispositivos de red, en este modelo sin embargo no hay un desacoplamiento de los planos de datos y control y estos siguen estando dentro, los equipos de red se comunican directamente con las aplicaciones a través

de APIs **(del inglés API: Application Programming Interface)** u otro mecanismo como NETCONF **El Protocolo de Configuración de Red**. **Ver figura 4.1(a) Apis Programables**.

- **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 **(del inglés API: Application Programming Interface)** y con el plano de datos mediante *"Openflow"* u otro protocolo propietario. **Ver figura 5.1(b) SDN Clásico**.

- **SDN Híbrido:** funciona bajo el mismo concepto que la arquitectura clásica de SDN **("en inglés Software Defined Networking, 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. **Ver figura 5.1(c) SDN Híbrido**.

- **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 **"(en inglés: Neutral czFree eXchange)"**. **Ver figura 5.1(d) Virtualización de Red**.



(a) Apis Programables (b) SDN Clásica (c) SDN Híbrida (d) Virtualización de Red

Figura 4.1: Modelos Programables de Red

4.1.3 Network Function Virtualization (NFV)

Network Function Virtualization o NFV ofrece una nueva forma de diseñar, aprovisionar y administrar los servicios de red, desacoplando las funciones de los hardware propietarios y realizando funciones en software como NAT ***(del inglés "Network Address Translation")****, firewall y DNS* ***Domain Name System o 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}` [1]

Bajo este concepto toda la orquestración y control de los dispositivos físicos se realizaría desde un punto central donde se administrarán las funciones de red, desacoplando así las funciones de red de los dospositivos físicos. La siguiente imagen muestra **Ver figura 4.2 NFV** un ejemplo de cómo funcionaría una red bajo este esquema.

NFV **"Network Function Virtualization"** se diferencia de SDN **"en inglés Software Defined Networking, 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.

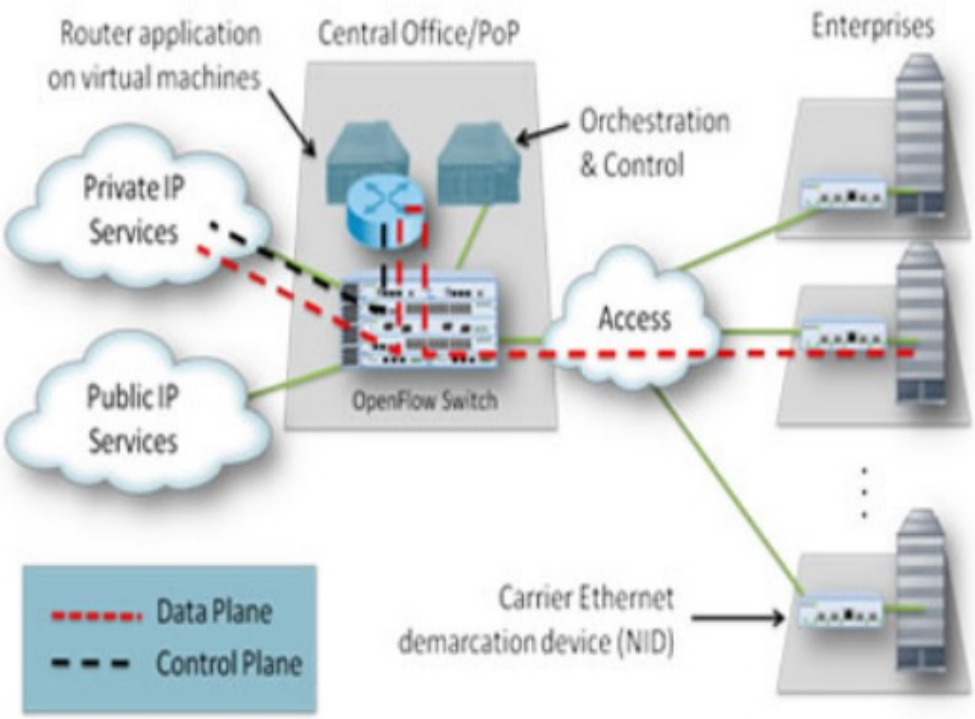


Figura 4.2: Network Function Virtualization (NFV)

4.1.4 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 **"en inglés Software Defined Networking, 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.

[1] http://www.5gamericas.org/es/newsroom/press-releases/nfv-controlando-las-redes-virtuales/

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 `esto{0penF1ow}` [2] de **OFN SDN evolution ver 1.0, Open Networking Foundation, 2016.** utiliza diversos componentes durante su ejecución puede **Ver figura 4.3 OpenFlow**.

Cada uno de estos programas de datapath **Ver figura 4.4 Datapath OpenFlow** es posteri-

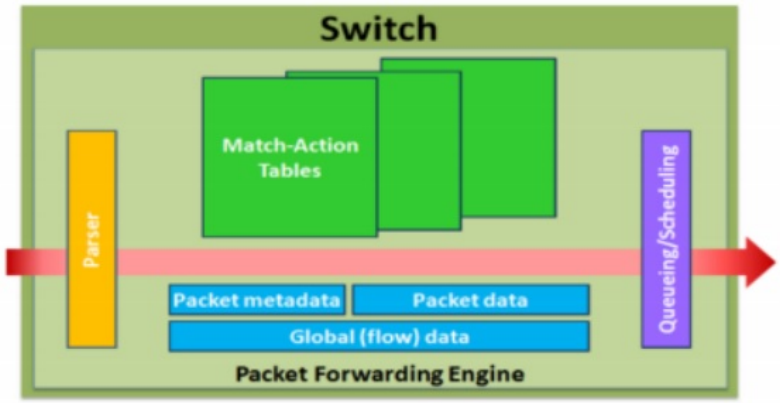


Figura 4.3: OpenFlow

ormente compilado para ser ejecutado en el código nativo de cada uno de los vendedores de los dispositivos de hardware, de esta manera el programa de datapath puede ser utilizado independientemente del vendedor del hardware.

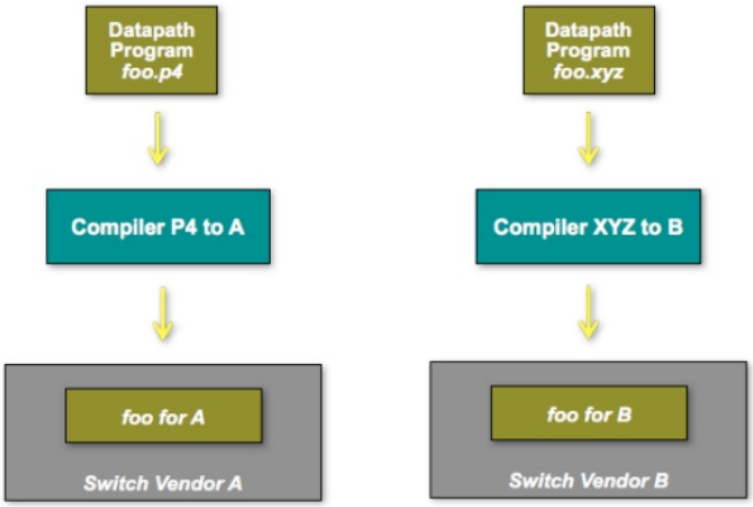


Figura 4.4: DataPath OpenFlow

[2] https://www.opennetworking.org/technical-communities/areas/specification/open-datapath/

4.1.5 NETCONF

El protocolo se encuentra definido por el estándar {RFC6241} [3] ***de la** IETF **"Internet Engineering Task Force"** y suministra mecanismos para instalar, manipular y eliminar configuración en dispositivos de red utilizando el formato XML **(Lenguaje de Marcado Extensible)**.*

*NETCONF define un mecanismo simple mediante el cual un dispositivo obtiene una API **(del inglés API: Application Programming Interface)**, esto con el objetivo de que las aplicaciones utilicen dicha API **(del inglés API: Application Programming Interface)** para enviar y recibir configuraciones desde y hacia los dispositivos de red, esto utilizando el paradigma RPC **Remote Procedure Call - Llamada a Procedimiento Remoto** de forma que el cliente codifique en formato XML **(Lenguaje de Marcado Extensible)** y lo envíe a un servidor, quien responderá con otro XML **(Lenguaje de Marcado Extensible)** codificado.*

Conceptualmente el protocolo NETCONF se divide en 4 capas **Ver figura 4.5 Capas NETCONF**

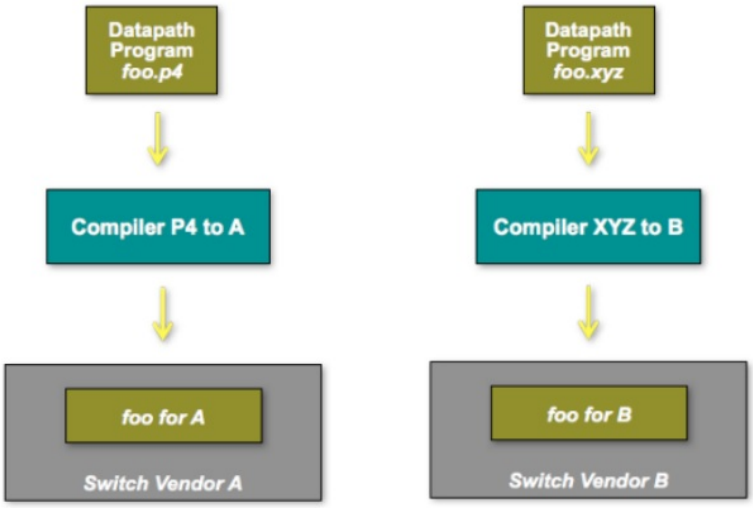


Figura 4.5: Capas del Protocolo NETCONF

- **Capa de transporte seguro suministra un camino de comunicación entre cliente y servidor, en general NETCONF puede ser utilizado sobre cualquier protocolo de transporte que cumpla con ciertas características.**

- **La capa de mensajes provee un mecanismo de entramado independiente del transporte para la codificación de RPC Remote Procedure Call - Llamada a Procedimiento Remoto y notificaciones.**

[3] https://tools.ietf.org/html/rfc6241

- **La capa de operaciones define un set de funciones básicas de protocolos invocados como métodos RPC con parámetros en codificación XML. (Lenguaje de Marcado Extensible)**

4.1.6 Modelos de datos

4.1.6.1 YANG

Es un lenguaje de modelado de datos que se utiliza para realizar operaciones de datos es estado y configuración del protocolo NETCONF y se encuentra definido bajo el {RFC 6020} [4] **de la** IETF **"Internet Engineering Task Force"**, YANG modela en forma jerárquica los datos como un árbol y provee una descripción clara de cada nodo así como su relación con otros nodos. YANG define cuatro tipos de nodo para el modelado de datos:

- **Nodo Leaf:** contiene datos simples como enteros o cadenas.
- **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 puede contener nodos de cualquier tipo, incluyendo "leaf", "list", "leaf-list"o incluso otros contenedores.
- **Nodo Lista:** 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.

YANG permite la definición de RPC de NETCONF, los nombres y parámetros de entrada y salida de las operaciones se encuentran modelados utilizando YANG así como las notificaciones. El siguiente ejemplo muestra como se encuentra estructurado un RPC **(en inglés, Remote Procedure Call)** en YANG **ver Script 5.1. Formato JSON (JavaScript Object Notation)**.

Listagem 4.1: RPC Estructura en YANG

```
1 /**
2  * JSON es un formato de texto sencillo para el intercambio de datos.
3  */
4 rpc activate-software-image {
5       input {
6          leaf image-name {
7             type string;
8          }
```

[4] https://tools.ietf.org/html/rfc6020

```
9       }
10      output {
11          leaf status {
12              type string;
13          }
14      }
15  }
```

En el caso de las interfaces, existe un estándar bajo el {RFC 7223} [5] **de la** IETF **"Internet Engineering Task Force"** en el que se define una estructura común en YANG para las interfaces de red, como tal la IETF definió la siguiente estructura de datos **ver Script 5.1. Interfaces:**

Listagem 4.2: Interface YANG

```
/**
 * Interfaces
 */
+--rw interfaces
    | +--rw interface* [name]
    | +--rw name string
    | +--rw description? string
    | +--rw type identityref
    | +--rw enabled? boolean
    | +--rw link-up-down-trap-enable? enumeration
    +--ro interfaces-state
       +--ro interface* [name]
          +--ro name string
          +--ro type identityref
          +--ro admin-status enumeration
          +--ro oper-status enumeration
          +--ro last-change? yang:date-and-time
          +--ro if-index int32
          +--ro phys-address? yang:phys-address
          +--ro higher-layer-if* interface-state-ref
          +--ro lower-layer-if* interface-state-ref
          +--ro speed? yang:gauge64
          +--ro statistics
             +--ro discontinuity-time yang:date-and-time
             +--ro in-octets? yang:counter64
             +--ro in-unicast-pkts? yang:counter64
             +--ro in-broadcast-pkts? yang:counter64
             +--ro in-multicast-pkts? yang:counter64
             +--ro in-discards? yang:counter32
             +--ro in-errors? yang:counter32
             +--ro in-unknown-protos? yang:counter32
             +--ro out-octets? yang:counter64
             +--ro out-unicast-pkts? yang:counter64
```

[5] https://tools.ietf.org/html/rfc7223

```
34              +--ro out-broadcast-pkts? yang:counter64
35              +--ro out-multicast-pkts? yang:counter64
36              +--ro out-discards? yang:counter32
37              +--ro out-errors? yang:counter32
```

4.1.7 RESTful APIs

Una API RESTful, también conocida como servicio web RESTful, se basa en la tecnología de transferencia de estado representacional (REST), un estilo arquitectónico y un enfoque de las comunicaciones a menudo utilizadas en el desarrollo de servicios web.

REST utilizado por los navegadores puede considerarse como el idioma de Internet. Con el uso de la nube en aumento, las API **(del inglés API: Application Programming Interface)** están emergiendo para exponer los servicios web. REST **(en inglés "representational state transfer")**es una opción lógica para crear API **(del inglés API: Application Programming Interface)** que permiten a los usuarios conectarse e interactuar con servicios en la nube. Las API RESTful son utilizadas por sitios como Amazon, Google, LinkedIn y Twitter **Ver figura 4.6 Rest Web Services**.

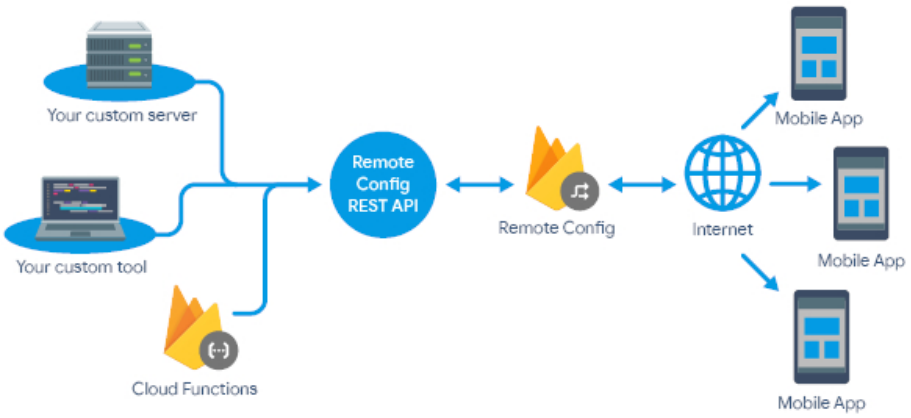


Figura 4.6: RestFull API

4.1.8 RESTCONF

Restconf es un protocolo basado en HTTP **(en inglés: Hypertext Transfer Protocol o HTTP)** que suministra una interfaz programática para acceder a datos definidos en YANG utilizando los conceptos de datastore definidos en el protocolo NETCONF.

NETCONF y RESTCONF suelen trabajar en conjunto permitiendo la ejecución de operaciones CRUD **(del original en inglés: Create, Read, Update and Delete) Ver figura 4.7 Estructura RESTCONF**. Al estar basado en HTTP **(en inglés: Hypertext Transfer Protocol o HTTP)** las operaciones CRUD de RESTCONF se realizan mediante los métodos tradicionales, como los son los siguientes:

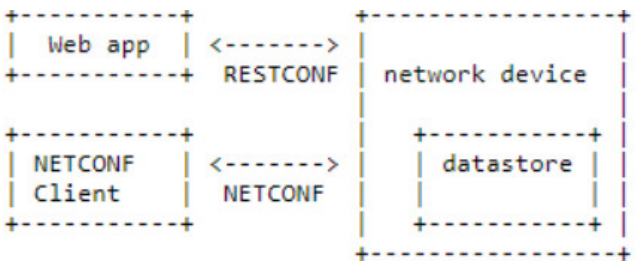


Figura 4.7: Estructura RESTCONF

- **Get:** "read or retrieve data".
- **Post:** "add new data".
- **Put:** "update data that already exists".
- **Delete:** "remove data".

RESTCONF requiere de HTTP **(en inglés: Hypertext Transfer Protocol o HTTP)** para su transporte y requiere soporte de TLS **(Transport Layer Security, seguridad de la capa de transporte)** para su transporte, aunque no se especifica que versión, para RESTCONF si se recomienda por lo menos HTTP1.1, dado que los servidores RESTCONF deben soportar HTTPS **(en inglés: Hypertext Transfer Protocol Secure o HTTPS)**, dichos servidores tienen que presentar un certificado dígital X509v3.

4.2 Marco de Referencia Tecnológico

La solución definida en este proyecto es una red IWAN de Cisco, en el capitulo "selección de la solución" en este mismo documento se plantean las razones por las cuales se escogió IWAN **WAN inteligente de Cisco®** como la mejor solución para el caso de este cliente. Por tanto este apartado estará dedicado a las tecnologías que componen la solución.

4.2.1 IWAN

IWAN **WAN inteligente de Cisco®** es una solución SD-WAN **("Software Defined Networking in Wide Area Networks")** 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 **(Wide Area Network en inglés)** por el uso de aplicaciones en la nube, Cisco dice ofrecer las siguientes ventajas con su aplicación de IWAN **Ver figura 4.8 Ventajas de una IWAN**.:

IWAN **WAN inteligente de Cisco®** 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 4.8: Ventajas de una IWAN

- **Independencia de transporte:** la solución utiliza DMVPN **("Dynamic Multipoint VPN")** para la creación de 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 **(Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado en español)** 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 **(en inglés Software Defined Networking)** APIC-EM **"Cisco Application Policy Infrastructure Controller"** 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 **(Wide Area Augmentation System)** que permite ahorrar costos en los enlaces WAN **(Wide Area Network en inglés)** haciendo más efectivo el uso del ancho de banda.

La controladora SDN **(en inglés Software Defined Networking)** 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 de la controladora, entre esas aplicaciones se encuentra IWAN **"Cisco Application Policy Infrastructure Controller"**, que es la solución SD-WAN **(“Software Defined Networking in Wide Area Networks”)**puntual que se presenta en este documento, la controladora SDN **(en inglés Software Defined Networking)** sin embargo es el puente entre la aplicación y la red física, esto puede apreciarse con mayor detalle en la siguiente **Ver figura 4.9 Estructura de APIC-EM**.

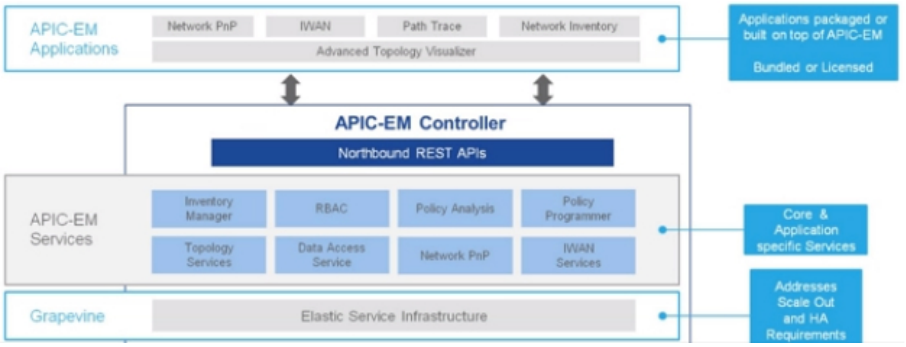


Figura 4.9: Estructura de APIC-EM

Una de las mayores ventajas de esta controladora es que no necesita de equipos de red especiales que soporten los protocolos de SDN **(“Software Defined Networking in Wide Area Networks”)**, aunque esto último es lo recomendado el APIC-EM **"Cisco Application Policy Infrastructure Controller"** 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.

4.2.2 DMVPN

DMVPN **(Dynamic Multipoint VPN)** es la solución de transporte propietaria de Cisco que hace parte de la solución de IWAN **WAN inteligente de Cisco®**, es una solución de *"Overlay"* en donde las ubicaciones remotas establecen un túnel estático hacia una ubicación central(hub) 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"**(del inglés: central processing unit)** 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 (hub). La siguiente **Ver figura 4.10 DMVPN** muestra el comportamiento dinámico de DMVPN **(Dynamic Multipoint VPN)**.

DMVPN **(Dynamic Multipoint VPN)** 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 **Internet Protocol version 4**, IPv6 **Internet Protocol version 6** y otros, estos túneles son asignados a una interface física y requieren direccionamiento propio en la interfaz del túnel, la diferencia entre esta tecnología y los túneles

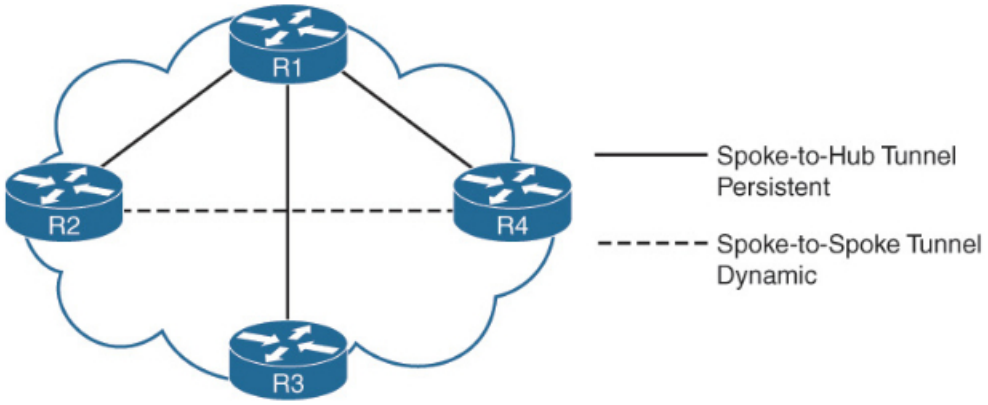


Figura 4.10: DMVPN

GRE **(Generic Routing Encapsulation)** tradicionales es que mGRE **Multipoint Generic Routing Encapsulation** puede conectar más de 2 dispositivos utilizando el mismo túnel **Ver figura 4.11 Túneles mGRE**.

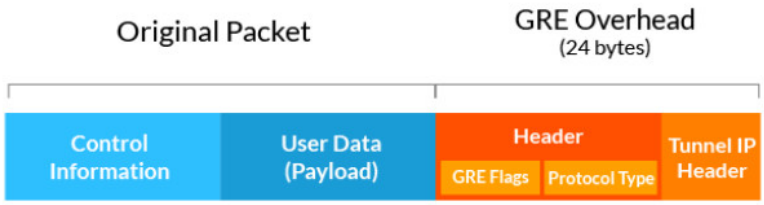


Figura 4.11: Túneles mGRE:

- **NHRP:** este protocolo se encuentra definido bajo el {RFC 2332} [6], y es utilizado para que un equipo fuente determine el siguiente salto hacia un destino en una red NBMA **("non-broadcast multiple access")**, es decir realiza una resolución de direccionamiento, similar a lo que ocurre con ARP **el inglés Address Resolution Protocol** en la resolución de dirección IP **(Internet Protocol)** a direccion MAC **del inglés Medium Access Control**. El protocolo funciona utilizando un NHS que se encarga de la resolución de direccionamiento dentro de la nube de NHRP, por su parte los equipos NHC **"New Horizon Communications"** son aquellos que realizan las peticiones de NHRP **"Next Hop Resolution Protocol"** hacia el NHS. La siguiente **Ver figura 4.12 Protocolo NHRP:** representa el funcionamiento de NHRP en terminos generales:

  Adicional al registro de los NHC **"New Horizon Communications"** con los NHS, NHRP **"Next Hop Resolution Protocol"** tiene la capacidad de que los NHC **"New Horizon Communications"** encuentren un camino más corto sobre la infraestructura o formar uno mediante una conexión virtual directamente hacia otro NHC

[6] https://tools.ietf.org/html/rfc2332

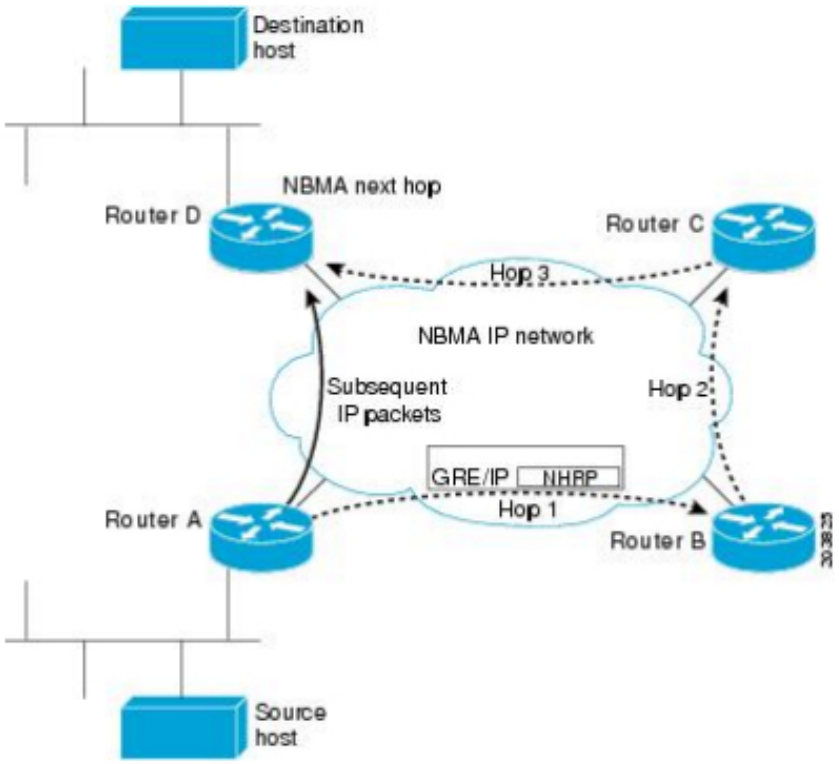


Figura 4.12: Protocol NHRP:

"New Horizon Communications", esta habilidad es utilizada en DMVPN **Dynamic Multipoint VPN** para establecer una topología "Full Mesh"sin todo el trabajo administrativo que esto conlleva.

4.2.3 WAAS

Por su parte WAAS **Wide Area Application Services** es una tecnología propietaria de Cisco que se encarga de optimizar el tráfico TCP **Transmission Control Protocol** 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 **Wide Area Application Services** para la optimización del ancho de banda a nivel WAN **Wide Area Network en inglés**, 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 **Transmission Control Protocol**, maximización del tamaño de ventana inicial, "Buffering"incrementado, BIC TCP **Transmission Control Protocol**.

- **Compresión:** utiliza algoritmos de eliminación de datos redundantes (DRE) y compresión LZ para optimizar el tráfico WAN **Wide Area Network en inglés**.

- **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 (BW).

4.2.4 EIGRP

EIGRP **(Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado en español)** es el protocolo seleccionado por Cisco para hacerse cargo del plano de enrutamiento en la solución **SD-WAN**, este protocolo aunque Cisco lo considera como un protocolo híbrido con características de protocolos vector distancia y de protocolos estado de enlace, es realmente un protocolo vector distancia ya que no mantiene la topología general del sistema autónomo. Sin embargo este ha demostrado ser un protocolo escalable y de convergencia rápida por lo que se integra adecuadamente en el diseño de IWAN **WAN inteligente de Cisco®** .

EIGRP **(Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado en español)** logra una convergencia rápida mediante la construcción de una tabla topológica utilizando la información enseñada por sus vecinos, la diferencia entre esta tabla topológica y la construida por un protocolo de estado de enlace es que EIGRP **(Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado en español)** al ser un protocolo vector distancia solo le enseña a sus vecinos las mejores rutas y no todas las rutas que conoce como sería el caso en un protocolo estado de enlace.

Aún así la convergencia es extremadamente rápida ya que basado en su métrica el protocolo selecciona la mejor ruta (succesor) y la segunda mejor ruta *("Feasable Succesor")*, de esta forma cuando una red deja de aprenderse por la mejor ruta el protocolo utiliza inmediatamente la segunda mejor ruta, por tanto obteniendo unos tiempos de milisegundos para la convergencia.

Para distribuir las rutas a través de la red EIGRP **(Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado en español)** utiliza actualizaciones de enrutamiento incrementales y no periódicas, esto quiere decir que solo se envía un update cada vez que hay un cambio en la red. EIGRP **(Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado en español)** depende por lo tanto de sus relaciones de vecinos para propagar de manera confiable los cambios en la tabla de enrutamiento a través de la red. Esta relación de vecindad se forma cuando dos routers corriendo EIGRP **(Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado en español)** ven los paquetes del otro equipo, estos paquetes son enviados cada 5 segundos. EIGRP **(Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado en español)**utiliza una métrica compuesta por los siguientes parámetros para calcular la ruta más corta:

- **Ancho de banda:** el menor ancho de banda de la ruta hacia el destino, sin embargo

el número utilizado para el cálculo de la métrica.

- **Delay:** el retardo total reportado por la interface, sin embargo este valor también es modificado para el calculo de la métrica.

- **Load:**el porcentaje de carga(utilización) que tiene el enlace.

- **Reliability:** valor configurable administrativamente

4.2.5 PFR

PFR es parte integral de la solución de IWAN **WAN inteligente de Cisco®**, y es la mayor responsable de la inteligencia de la solución, su objetivo es mejorar el rendimiento y disponibilidad de las aplicaciones realizando una optimización del control de enrutamiento basándose en los requerimientos de cada aplicación.

PfR monitorea el rendimiento de red y selecciona el mejor camino basándose en criterios de alcanzabilidad, *"delay"*, *"jitter"* y pérdida de paquetes mientras balancea el tráfico entre los enlaces disponibles. **PfR** define varios roles para los dispositivos que componen la solución, dichos roles son *"Master Controler (MC)"y "Border Router (BR)"*, el **MC** actúa como plano de control para el **PfR** y el **BR** sería el plano de datos al seleccionar el camino basándose en las decisiones tomadas por el **MC**.

En **PfR** las políticas de tráfico son definidos basados en DSCP o en la aplicación por sí misma, que se identifica mediante "AVC"**(Application visibility and Control)**. dichas políticas contienen la información de requerimientos en cuanto a parámetros de retardo, *"jitter"* y pérdida de paquetes para cada aplicación así como la preferencia de camino de cada una de ellas. Una vez definida la política **PfR detecta** el tráfico y comienza a realizar mediciones de ancho de banda y rendimiento, posteriormente el **MC** toma la decisión mediante la comparación de métricas en tiempo real y le da la instrucción al **BR** de utilizar el camino apropiado. **Ver figura 4.13 PfR** muestra el flujo de la operación de **PfR**:

Dentro de los roles de **MC y BR** existen dos variantes, los equipos Hub y los *"Branch"*, equipos Hub son los responsables del plano de control en el caso del MC y del plano de datos en el caso del BR para toda la topología de red, el HUB MC se encarga mediante **SAF** de propagar las políticas, especificaciones de los monitores para medir rendimiento de los canales y prefijos de los sitios a los MC en cada Branch y a los HUB BR, los **"BRANCH MC"** a su vez propagan las políticas a los *"BRANCH BR"*. La siguiente **Ver figura 4.14 Branch** detalla este flujo de información entre los elementos de IWAN **WAN inteligente de Cisco®** .

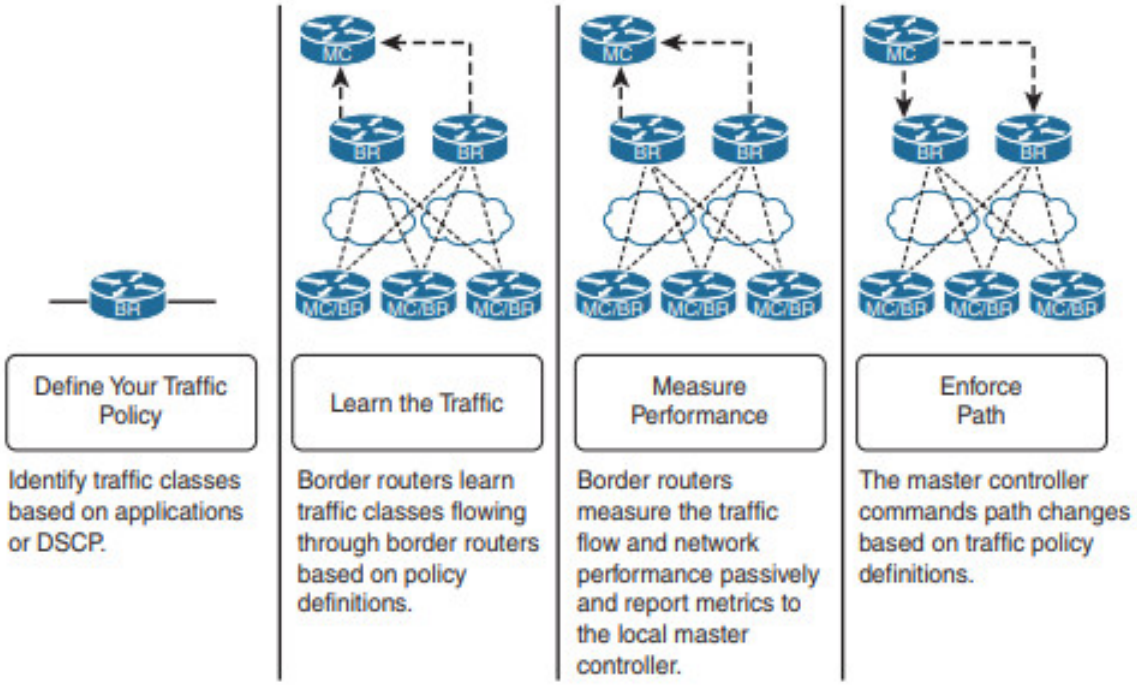


Figura 4.13: PfR

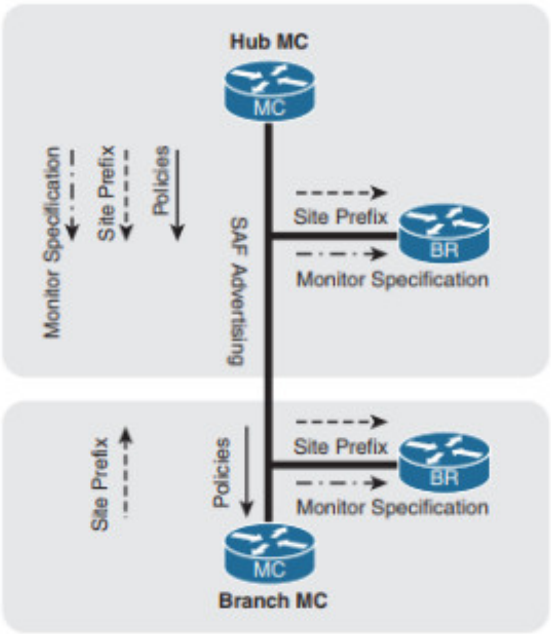


Figura 4.14: Branch PFR

4.3 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 ingenieríade 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 **Ver figura 4.15 Red Orquestación**

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.**Ver figura 4.16 Flujo que ocurre entre estos**

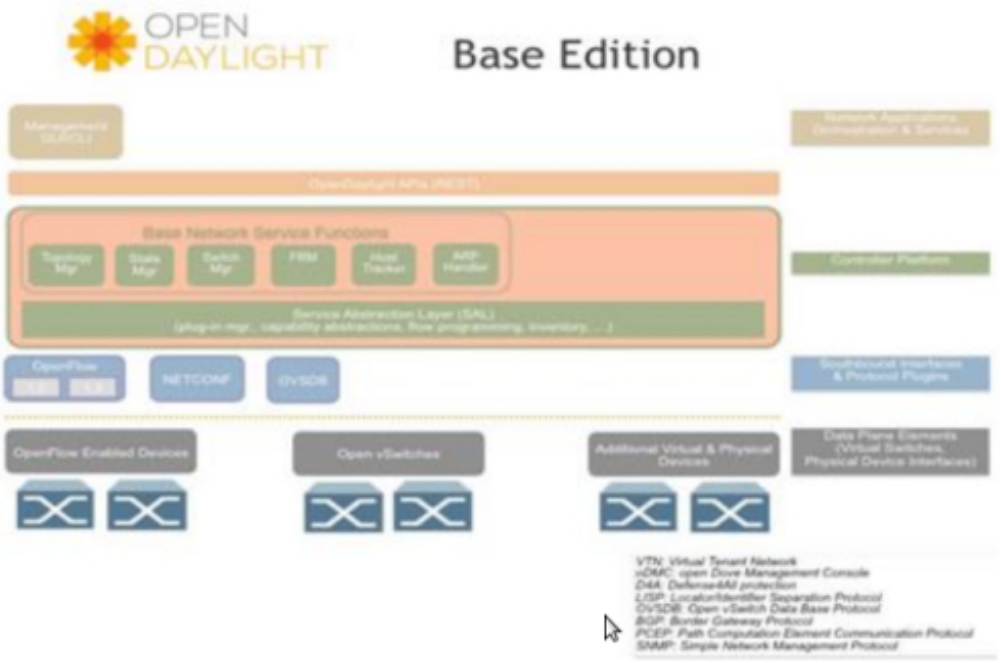


Figura 4.15: Red Orquestación Open Daylight

elementos dentro del funcionamiento de la controladora. muestra el flujo que ocurre entre estos elementos dentro del funcionamiento de la controladora.

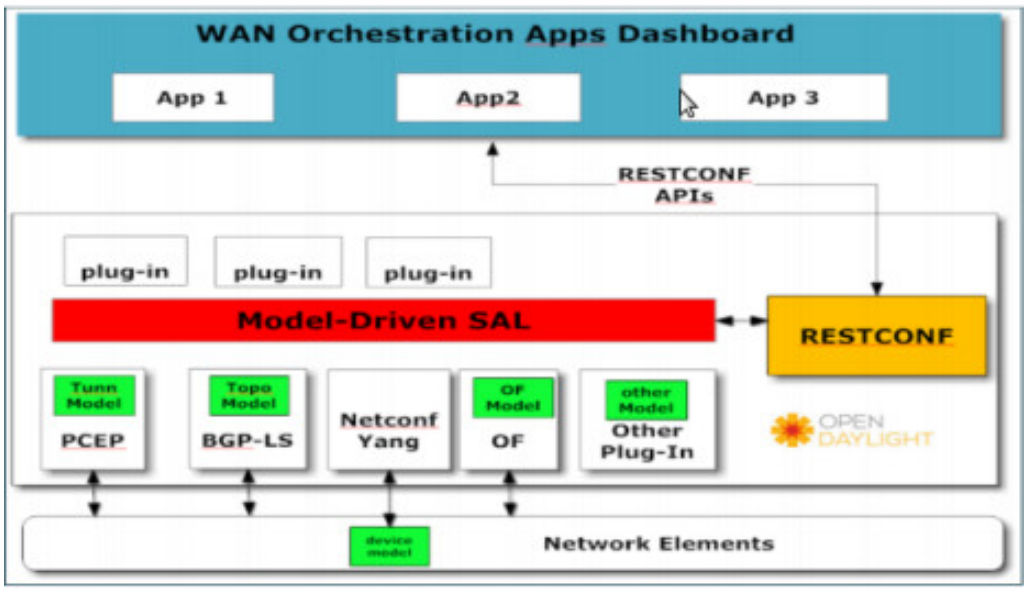


Figura 4.16: Funcionamiento de una Controladora

4.4 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 **Ver figura 4.17 Arquitectura Cisco VIPTELA.** muestra la arquitectura propuesta por 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 **WAN inteligente de Cisco®** , es decir PfR, DMVPN y EIGRP **(Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado en español)** 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 en 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 **WAN inteligente de Cisco®** 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.

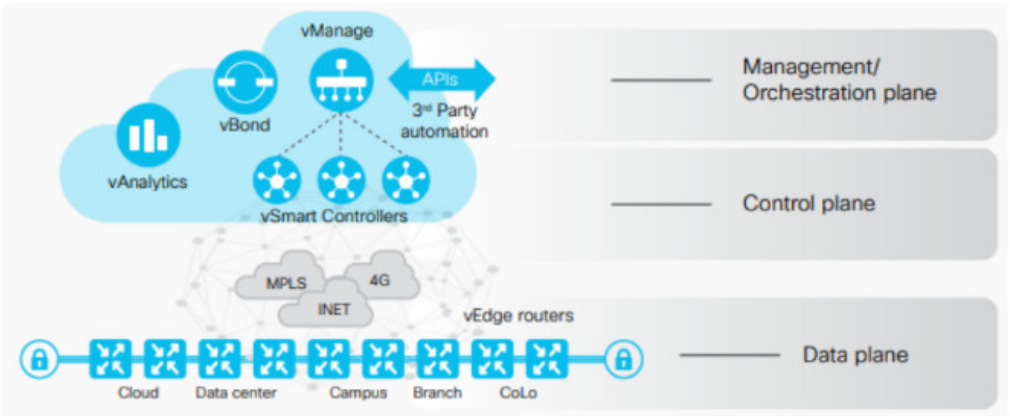


Figura 4.17: Arquitectura Cisco VIPTELA.

4.5 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:

- **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 apliaciones, 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. **Ver figura 4.18 Distribución de los Componentes.**

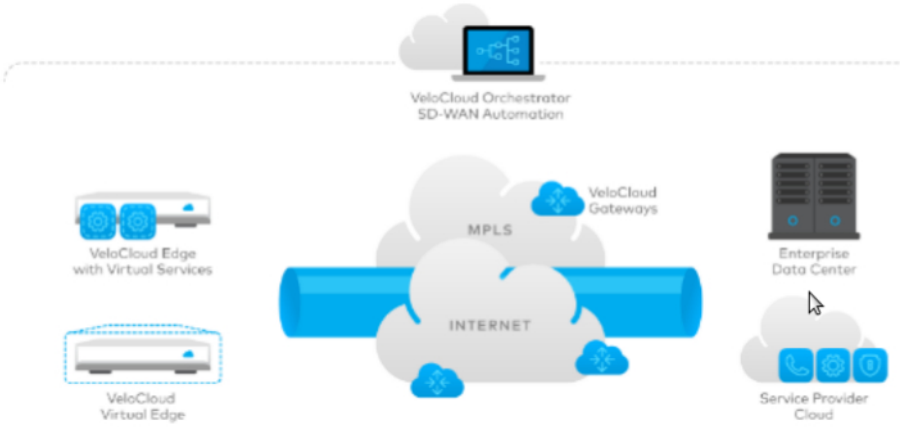


Figura 4.18: Distribución de los Componentes

4.6 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 **Ver figura 4.19 WAN definida por software (SD-WAN)** 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:

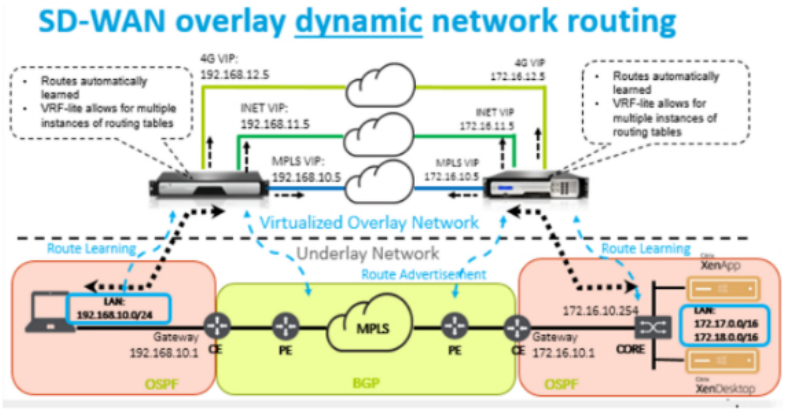


Figura 4.19: WAN definida por software (SD-WAN)

- **Abstracción de conectividad de borde**
- **Virtualización WAN**
- **Gestión centralizada y dirigida por políticas**
- **Gestión elástica del tráfico**

Capítulo 5

Glosario de Términos

L2TP: Layer 2 Tunneling protocol. es un protocolo utilizado por redes privadas virtuales que fue diseñado por un grupo de trabajo de IETF como el heredero aparente de los protocolos PPTP y L2F, creado para corregir las deficiencias de estos protocolos y establecerse como un estándar aprobado por el IETF (RFC 2661).

EOIP: Túnel Ethernet over IP.

ISP: Proveedor de servicios de internet. El proveedor de servicios de Internet, (ISP, por la sigla en inglés de Internet Service provider) es la empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, cablemódem, GSM, dial-up, etcétera.

SD-WAN: Software Defined - Wide Area Network.

QoS: Quality of Service.

WAN: Wide Area Network.

TI: Tecnologías de la información.

RETAIL: Sector economico que engloba a las empresas especializadas en la venta masiva de productos.

DATACENTER: Centro de datos.

EGRP: (Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado en español) es un protocolo de encaminamiento vector distancia avanzado, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancias y del estado de enlace.

DMVPN: La red privada virtual dinámica multipunto es una forma dinámica de túnel de una red privada virtual compatible con enrutadores basados en Cisco IOS, enrutadores Huawei AR G3 y firewalls USG, y en sistemas operativos tipo Unix.

APIC-EM: Controlador de infraestructura de políticas de aplicaciones (APIC) de Cisco es el punto unificador de automatización y administración para la estructura de Infraestructura centrada en aplicaciones (ACI).

MD-SAL: Model-Driven SAL (MD-SAL) es un conjunto de servicios de infraestructura destinados a brindar soporte común y genérico a los desarrolladores de aplicaciones y complementos.

BGP: En telecomunicaciones, el protocolo de puerta de enlace de frontera o BGP (del inglés Border Gateway Protocol) es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos.

LISP: (Históricamente LISP) es una familia de lenguajes de programación de computadora de tipo multiparadigma con larga historia y una inconfundible y útil sintaxis basada en la notación polaca.

SNMP: El Protocolo simple de administración de red oSNMP (del inglés Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

NBMA: Una red de acceso múltiple no de difusión es una red informática a la que se conectan múltiples hosts, pero los datos se transmiten solo directamente desde una computadora a otro único host a través de un circuito virtual o a través de un tejido conmutado.

Capítulo 6

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 encripción 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.

Capítulo 7

Objetivos

7.1 Objetivo General

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

7.2 Objetivos Específicos

7.2.1 Diseñar solución de conectividad que permita balanceo de carga y redundancia a través de un enlace de internet y un canal MPLS.

7.2.2 Diseñar las soluciones de cifrado y decontrol y priorización de tráfico (calidad de servicio) en la red para sus enlaces más críticos.

7.2.3 Diseñar solución SD-WAN que permita configurar las sedes remotas de forma centralizada.

7.2.4 Simular el diseño propuesto con el fin de garantizar que la solución sea funcional.

Capítulo 8

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.

8.1 Requerimientos Funcionales

La aplicación de estratégias 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.

8.2 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 9

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."

9.1 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.

- **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.**

Capítulo 10

Diseño de una Red SD-WAN

10.1 Inversión para una SD-WAN

10.2 Precios en una Red SD-WAN

Una de las mayores motivaciones para el desarrollo de este proyecto es reducir el costo en OPEX que costarían los enlaces de los proveedores de servicio al trasladar los servicios de la empresa a la nube, ya que los costos de ancho de banda se reducirían notablemente al realizar esta migración con SD-WAN **la tabla 10.1** muestra una comparación aproximada de los costos de los enlaces WAN requeridos con y sin SD-WAN.

Dichos costos son calculados tomando en cuenta los valores publicados por google para su aplicación de Gsuite, ya que el cliente entre otras cosas realizará reuniones a través de Google Meet, esto requiere 3.2MB de ancho de banda por participante.

Tabela 10.1: Tabla de Precios para la Implementación de una SW-WAN.

Tipo de Oficina	Tienda	Regional	Oficina Regional
[**Usuarios**] Promedio	3	25	60
[**Sesiones**] de Video Simultáneas	1	8	20
[**Trafico**] de Datos	5MB	10MB	20MB
[**BW**] Servicio Actual	10	7	14
[**BW**] Requerido	9MB	25MB	84MB
[**Costo**] Actual	221741	1260741	1803563
[**Costo**] Mensual Red Legacy	221741	3607126	6782000
[**Costo**] Mensual SD-WAN	221741	1842102	3972361
Total	–	–	–

Adicional al costo de los enlaces, el OPEX también se vería reducido al requerir menor tiempo de los recursos de IT en la administración de la red, ya que al automatizar las configuraciones y cambios la velocidad de aprovisionamiento se vería ampliamente mejorada y por tanto su costo sería menor.

10.3 Costos para Implementación en Infraestructura Cloud

10.3.1 Amazon

Amazon: multinacional de comercio electrónico y servicios de computación en la nube, contiene cuatro modelos para compra de instancias en Cloud conocido como Amazon EC2.

- **Baja Demanda:** *"Con las instancias bajo demanda, paga por la capacidad informática por hora o por segundo, según las instancias que use. Ya no serán necesarios los contratos a largo plazo ni los pagos iniciales. Puede aumentar o reducir la capacidad informática en función de las exigencias de su aplicación y pagar únicamente la tarifa por hora específica de la instancia que use."En la* ***tabla 10.2*** *se observa algunos costos de baja demanda.*

Tabela 10.2: Amazon EC2 Pricing.

vCPU	ECU	Memory (GiB)	Instance Storage (GB)	Linux/UNIX Usage
[**a1.medium**] 1	N/A	2GiB	EBS Only	$0.0255 per Hour
[**a1.large**] 2	N/A	4GiB	EBS Only	$0.051 per Hour
[**a1.xlarge**] 4	N/A	4GiB	EBS Only	$0.051 per Hour
[**a1.2xlarge**] 8	N/A	16GiB	EBS Only	$0.204 per Hour
[**a1.4xlarge**] 16	N/A	32GiB	EBS Only	$0.408 per Hour
[**t3.nano**] 2	N/A	0.5GiB	EBS Only	$0.0052 per Hour
[**t3.micro**] 2	N/A	1GiB	EBS Only	$0.0104 per Hour
Total	–	–	–	

- **Instancias Reservadas:***Las instancias reservadas ofrecen un descuento importante (de hasta el 75 %) en comparación con los precios de las instancias bajo demanda. Además, cuando se asignan instancias reservadas a una zona de disponibilidad específica, se proporciona una reserva de capacidad, lo que le aporta más tranquilidad en relación con la posibilidad de lanzar instancias cuando las necesite.*

  Para las aplicaciones con estado constante o uso previsible, las instancias reservadas pueden suponer un ahorro considerable en comparación con las instancias bajo demanda. Consulte Cómo adquirir instancias reservadas para obtener más información.

- **Instancias de Spot:** *Las instancias de spot de Amazon EC2 le permiten solicitar capacidad informática sobrante de Amazon EC2 con descuentos de hasta el 90% en comparación con el precio de las instancias bajo demanda.*

- **Host Dedicados:***Un host dedicado es un servidor físico de EC2 exclusivo para su uso. Los hosts dedicados pueden ayudarle a reducir costos porque le permiten usar sus licencias existentes de software enlazado al servidor, incluidos Windows Server, SQL Server y SUSE Linux Enterprise Server (en función de los términos de su licencia). También pueden ayudarle a cumplir requisitos de conformidad.* ***tabla 10.3***

Tabela 10.3: On-Demand Pricing.

General purpose	Price Per Hour
[**a1**]	$0.449
[**m5**]	$5.069
[**m5d**]	$5.966
[**m4**]	$2.42
Total	–

Donde se puede implementar infraestructura de telecomuicaciones a un bajo costo, contando con todos los servicios necesarios de una red.

10.3.2 Microsoft Azure

Azure: es en constante expansión de servicios en la nube para ayudar a su organización a sastifacer sus necesidades comerciales. Le otorga la libertad de crear, administrar e implementar aplicaciones en una red mundial.

Para máquinas virtuales tenemos la siguiente **figura 10.1 Costo con Azure**

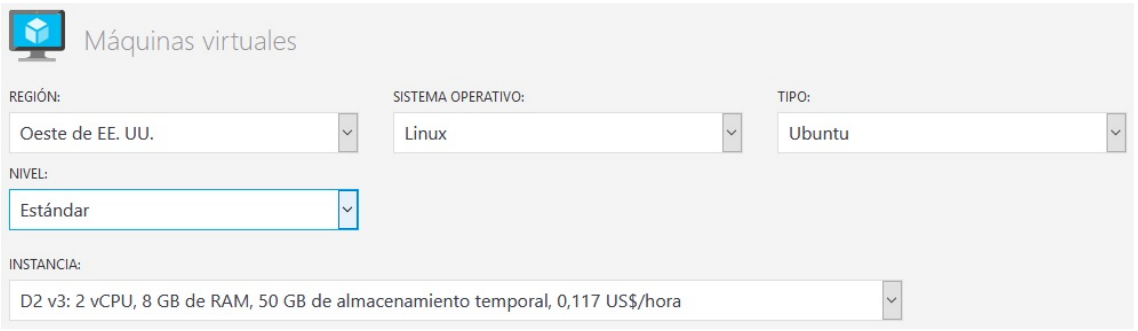


Figura 10.1: Precio en Máquinas Virtuales en Azure

Para redes virtuales tenemos la **figura 10.2 Redes Virtuales en Azure**
Podemos encontrar diferentes características, que se requiere en una infraestructura de telecomunicaciones Inicie sesión para ver cotizaciones **figura 10.3 Infraestructura en Azure**.

*El costo estimado total se basa en los precios aplicables en el día en que se creó la estimación. El costo estimado total real puede variar. Vuelva a abrir el costo estimado para ver el importe total con los precios más recientes

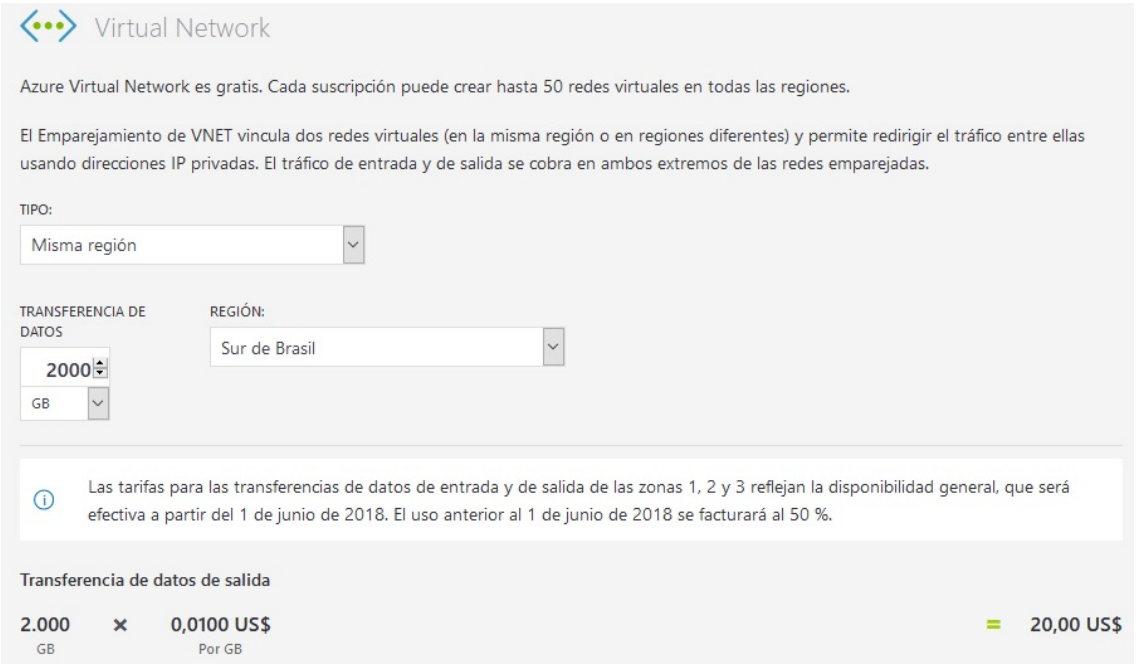


Figura 10.2: Precio en Redes Virtuales en Azure

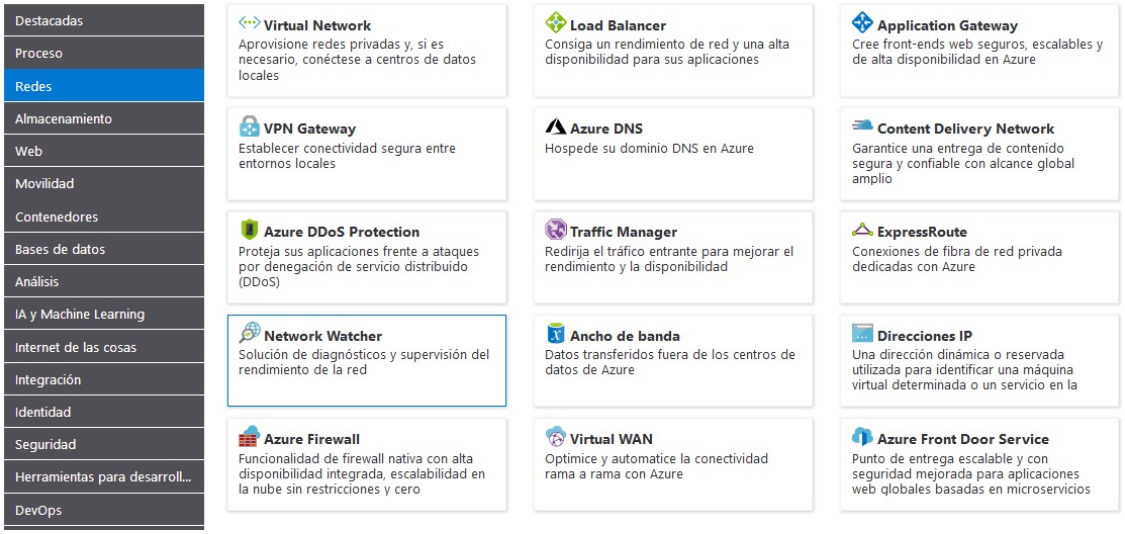


Figura 10.3: Diferentes características en Azure para Telecomunicaciones

10.3.3 Google Cloud

Google Cloud: es una plataforma que ha asociado todas las aplicaciones de desarrollo web que Google estaba ofreciendo por separado.
Al adjuntar más servicios en un solo contenedor se desarrolla un fácil administración de los diferentes elementos como almacenamiento, redes, entre otros.

Con Google Cloud se implemento distintos Router para el área diseño de la presente tésis. Los Router que se pudo llegar a implementar fue de la propiedad Cisco el Router CSR 1000v.
Para Google Cloud se puede realizar una estimación de precios en diferentes áreas del mundo ejemplo observamos la **figura 10.4 Plataform Pricing Calculator**.

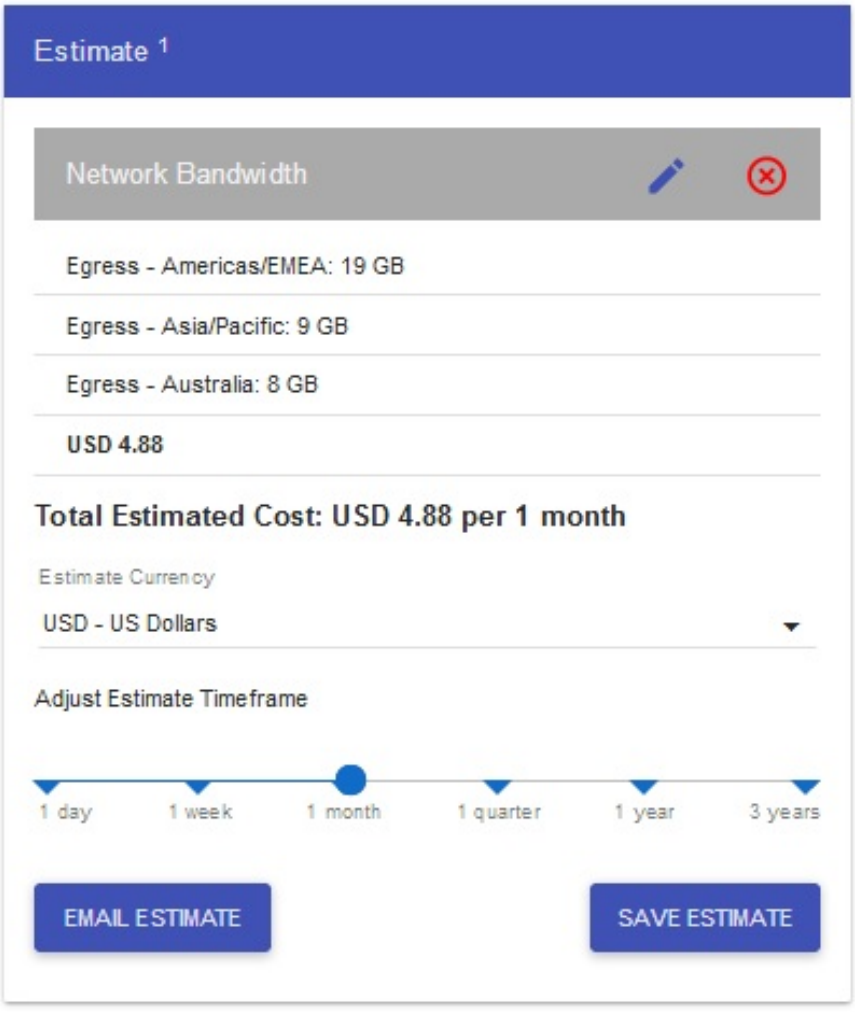


Figura 10.4: Plataform Pricing Calculator Google

10.3.4 Oracle Cloud

Oracle: uno de los más grandes en Base de Datos que enfreta una competencia con IBM desde hace algunos años tiene en sus filas la implementación de Cloud fortaleciendo

con grandes herramientas de sistemas opertativos como Linux, también presenta una infratestructura robusta, para instanciar las diferentes máquinas virtuales para nuestro diseño. En la siguiente **tabla 10.4 Precios Oracle** se detalla la implementación de un Computador con caracteríticas para una empresa entre 100 a 200 empleados.

Tabela 10.4: Dedicated Compute Classic.

Product	Price	Metric
[**Compute Classic - Model 500**]	USD $50,000.00	500 OCPUs Month
[**Compute Classic - Model 1000**]	USD $81,000.00	1000 OCPUs Month
[**Compute Classic - Model 1500**]	USD $114,000.00	1500 OCPUs Month
[**Compute Classic - Model 2000**]	USD $148,000.00	2000 OCPUs Month

10.4 Análisis de Inversión para Cloud

10.4.1 Enfoque al Cliente: Costo, Confiabilidad, Seguridad

Un resumen de investigación de SDxCentral, SD-WAN seguro se ubica entre las tres principales en cuanto a capacidades clave de una red. 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. Esto se puede usarse para brindar conectividad WAN básica, opara 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.

Si está considerando si SD-WAN mejorará la red de área amplia de su empresa, se ha aprendido que es importante conocer primero las diferentes arquitecturas de SD-WAN. Como un proveedor de servicios de Internet (ISP) y profesional en este campo 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.

10.5 Controladores de Negocio SD-WAN

10.6 Introducción a SD-WAN

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. **Ver figura 10.5 WAN definida por software (SD-WAN)**.

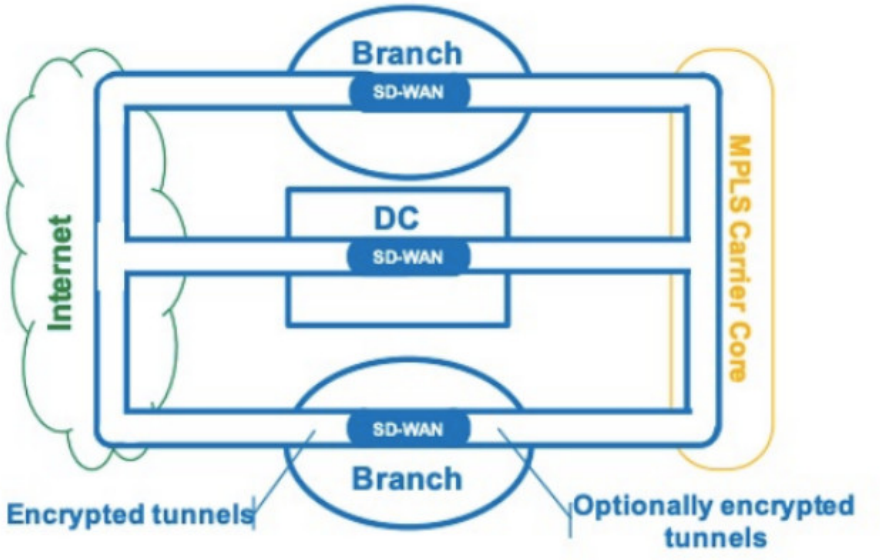


Figura 10.5: WAN definida por software (SD-WAN)

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. **Ver figura 10.6 Arquitectura de una SD-WAN**.

10.7 Tipos de Arquitectura SD-WAN

10.7.1 Enfoque de una SD-WAN

Una arquitectura SD-WAN (esencialmente es un enrutador "plug-and-play"), que realiza la configuración del tráfico en tiempo real en cada sitio. A diferencia de otras arquitecturas, el cuadro SD-WAN en el sitio no se conecta a una puerta de enlace en la nube, solo se conecta a los otros sitios de su empresa.

10.7.1.1 Mejor Ajuste

Empresas que alojan todas sus aplicaciones en la empresa (sin ninguna aplicación en la nube), 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.

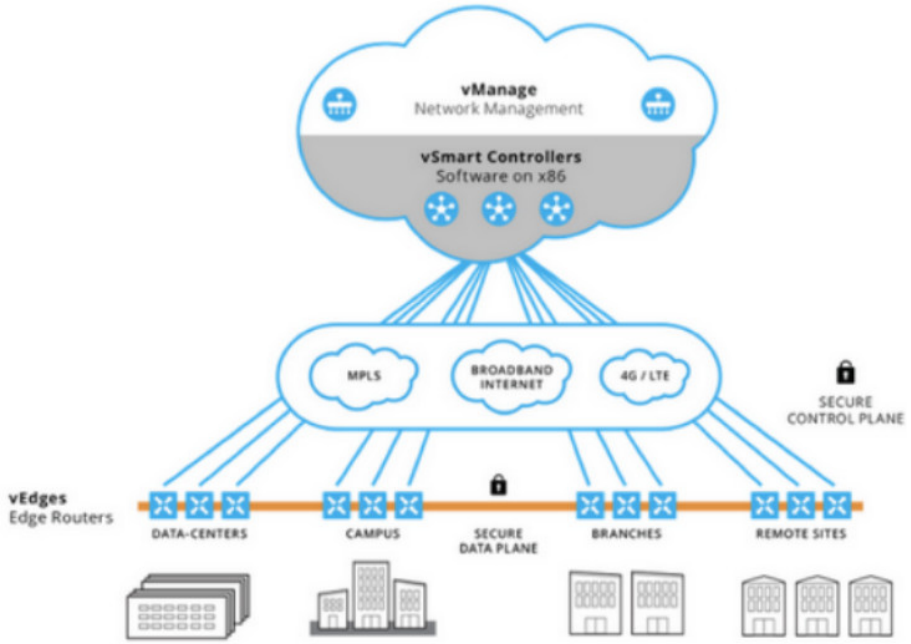


Figura 10.6: Arquitectura de una SD-WAN

10.7.1.2 Beneficios

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.

10.7.2 Cloud

En una arquitectura SD-WAN habilitada para la nube, la solución de una 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 (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 un mejor 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

10.7.2.1 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, corriendo sobre la Internet pública, controlada por una SD-WAN.

10.7.2.2 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.**

10.7.3 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 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.

10.7.3.1 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).

10.7.3.2 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.

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.

10.8 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, **Ver figura 10.7 Solución de la Arquitectura**.

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.

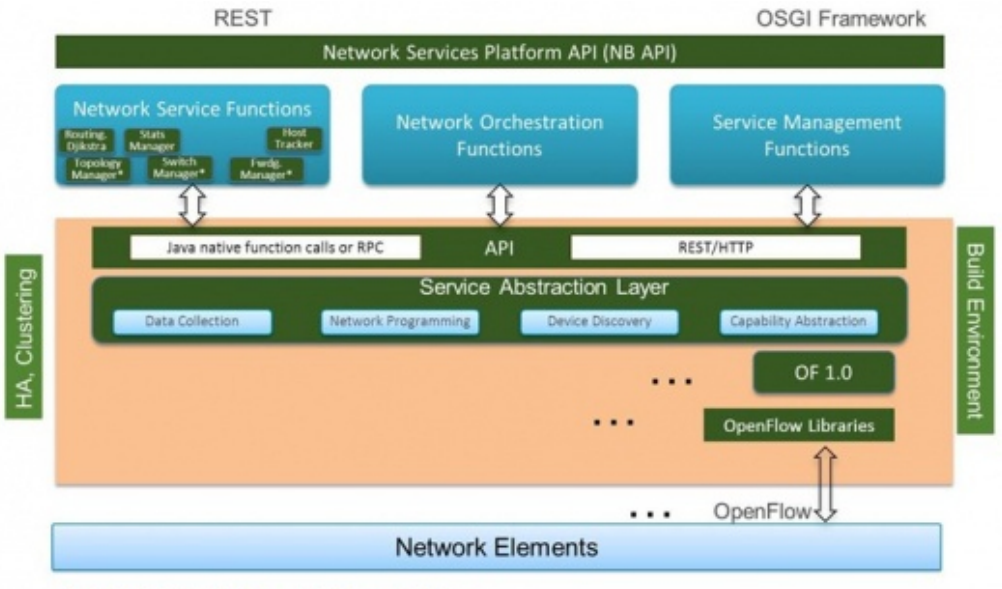


Figura 10.7: Solución de la Arquitectura

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 cloud) y Silverpeak, estas son las soluciones que dominan el mercado a la fecha de elaboración de este documento. Todas estas son soluciones SDN **Ver figura 10.8 Solución y Funcionamiento de una red SD-WAN**. 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. 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**

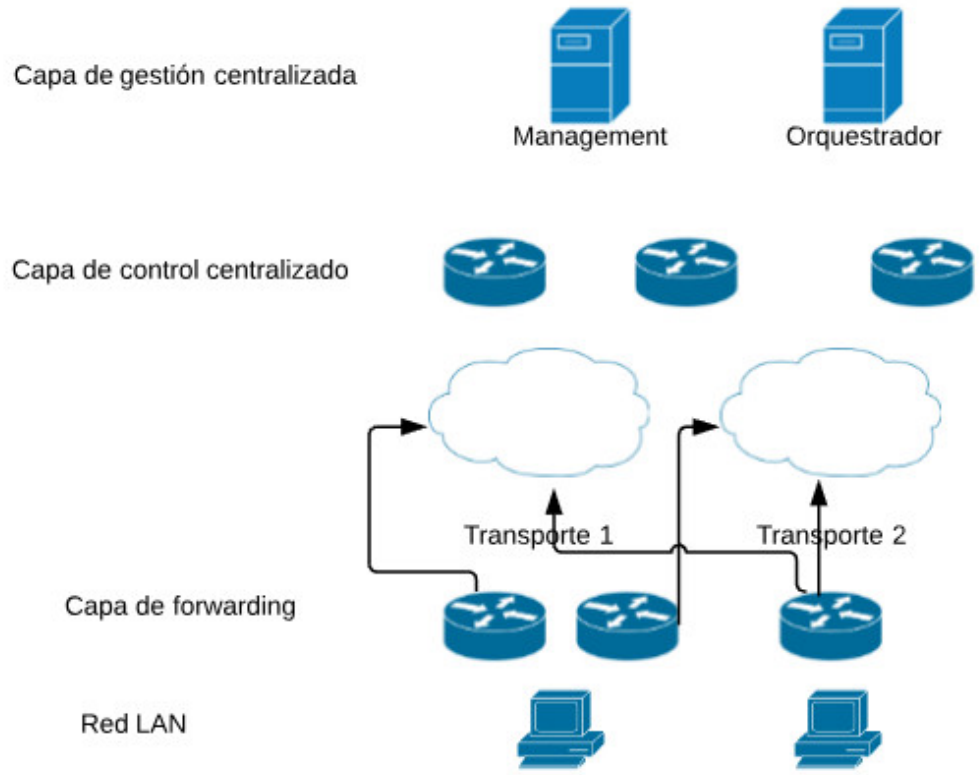


Figura 10.8: Solución y Funcionamiento de una red SD-WAN

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.

10.9 Ventajas y Desventajas de la Solución Propuesta

Esta sección permite establecer las ventajas y desventajas del uso de la tecnología SD-WAN seleccionada en comparación con la solución actual que tiene el cliente en sus equipos.

Una de las ventajas más notorias es el tiempo que se ahorra en los procesos tanto de implementación como de cambios, a continuación hay un comparativo de los tiempos para la nueva solución y para la solución anterior **tabla 10.5 Implementación y Ahorro de Precios en SD-WAN**.

Tabela 10.5: Implementación y Ahorro de Precios en SD-WAN

Proceso	IWAN	Tiempo	Solución Actual	Tiempo
Aprovisionamiento tienda nueva	Se ingresan datos básicos sobre el APIC-EM	30min	Se configura túnel en la tienda y en la regional y enrutamiento hacia internet y hacia las tiendas.	3h
Aprovisionamiento regional nueva	Se ingresan datos básicos sobre el APIC-EM	30min	Se deben configurar túneles IPSEC contra todas las demás regionales, además de configurar protocolos de enrutamiento dinámico contra el proveedor y contra las demás regionales por medio del canal de internet.	2d
Cambio general de políticas	Se configura script y se agenda para ser aplicado en todos los equipos	1h	Se ingresa equipo por equipo a realizar los cambios manualmente.	4meses

Adicional a los tiempos, las dos soluciones tienen diferencias importantes a nivel de servicio por lo que la siguiente tabla muestra en detalle dichas diferencias para establecer qué solución conviene más para las necesidades del negocio **tabla 10.6 Necesidades de Negocio SD-WAN**.

Como puede verse en ambas tablas, la solución de IWAN genera ventajas tanto en tiempos como en costos y en redundancia y servicio, por lo que en general está más alineada con las necesidades del negocio.

10.10 Requerimientos de Aplicaciones

Este diseño se encuentra enfocado a las aplicaciones del cliente, por lo que este capítulo está enfocado a determinar los requerimientos de ancho de banda, latencia y jitter para

Tabela 10.6: Necesidades de Negocio SD-WAN

Caracterítica	IWAN	Solución Legacy
Redundancia	4 puntos concentradores de la solución, principal y backup de intranet y principal y backup de internet.	único punto de falla, si el internet de la regional cae, cae la conexión de todas las tiendas asociadas a dicha regional.
Calidad de Servicio	Por aplicación, utilizando NBAR para la identificación y priorización de aplicaciones.	Por redes o por puerto, la clasificación se realiza en capa 4 del modelo OSI.
Balanceo de Carga	Nativo, se utiliza PfR para validar según las necesidades de la aplicación, cuál es el mejor camino para enviar el tráfico.	Es posible el balanceo pero este sería estático, si algún enlace está degradado igualmente se enviará tráfico a través de él.

las aplicaciones críticas del cliente, esto con el fin de establecer un diseño de QoS y para definir el ancho de banda necesario en los enlaces, cabe aclarar que el uso de estas aplicaciones cambia en los 3 tipos de sedes definidos en el proyecto. Las aplicaciones definidas por el cliente son las siguientes:

- **Telefonía:** telefonía IP en todas las sedes, un telefóno IP por tienda y un segmento de red para telefonía en cada una de las regionales y en la sede nacional, este servicio de telefonía utiliza SIP como protocolo de señalización y túneles IAX entre las plantas telefónicas, hay una planta telefónica en cada regional a donde se registran los teléfonos de cada tienda, a continuación se muestra el diagrama general del servicio de telefonía actualmente. **Ver figura 10.9 Telefonía**.

- **FTP:**Cada una de las tiendas realiza un proceso de inventariado semanalmente, estos archivos de inventario son subidos a un servidor FTP en la sede nacional de Medellín, por lo tanto el servicio de FTP es considerado como crítico para el negocio.

- **Videoconferencia:** el cliente utiliza un servicio de videoconferencia en la nube, más específicamente google Hangouts, que para una calidad óptima de video utiliza 3.2Mbps por videoconferencia, por lo que es una de las aplicaciones que más consumo de ancho de banda genera, es además una de las aplicaciones más críticas para la compañía, ya que es utilizada por los altos directivos.

- **CCTV:** el cliente monitorea mediante el enlace de internet de las tiendas, todas la plataforma de CCTV, por lo que se debe garantizar el acceso desde internet a esta aplicación.

- **Servicios Web privados:** el cliente cuenta con una Intranet en la que las tiendas y las regionales realizan procesos corporativos vitales para la empresa, de igual forma al hacer parte de un grupo empresarial, consumen en forma de servicios Web aplicaciones en datacenter de otros miembros del grupo empresarial.

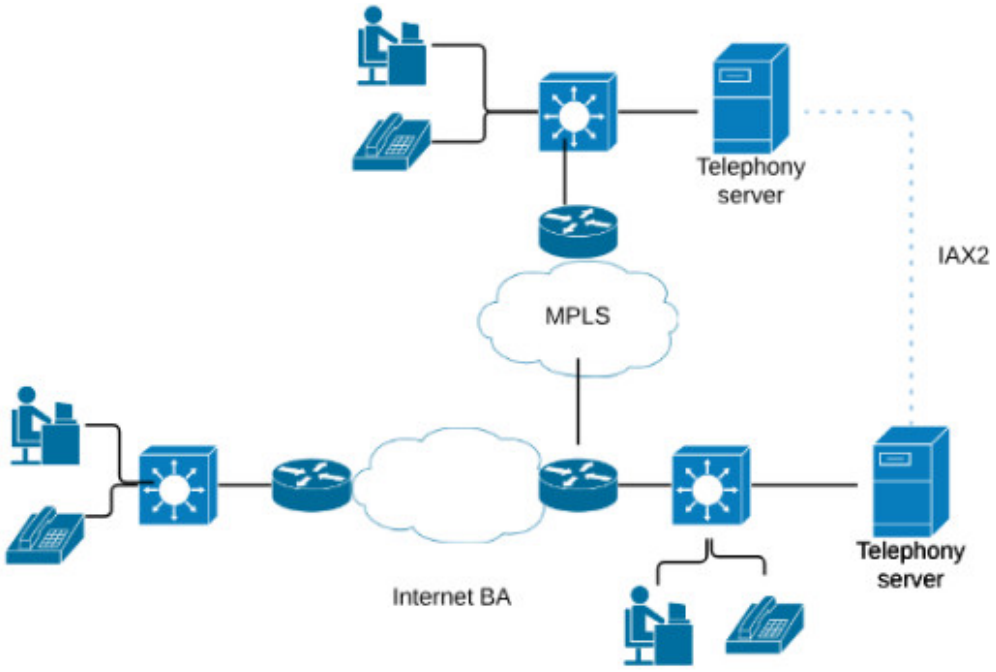


Figura 10.9: Telefonía

- **Internet:** desde cada una de las tiendas y las regionales se tiene acceso a internet para navegación, sin embargo este no es un servicio crítico para el cliente.
- **Escritorio Remoto:** el grupo de soporte de TI requiere conectividad por escritorio remoto a regionales y tiendas de manera que se pueda realizar un soporte remoto de aplicaciones y equipos de computo.
- **Correo:** el cliente cuenta con buzones de correo de google que acceden mediante sus enlaces a internet.

Los requerimientos de ancho de banda, jitter y delay así como la criticidad de cada servicio se resumen en la siguiente **tabla 10.7 Características de Calidad de Servicio en un SD-WAN**:

10.11 Requerimientos de Ancho de Banda

Con cada una de las aplicaciones descritas se procede a calcular por tanto el ancho de banda requerido en cada una de las sedes, y se genera una estadística del consumo actual en cada una de esas sedes para establecer tanto de manera teórica como práctica el ancho de banda requerido en cada uno de los tipos de sedes remotas y en el centro de datos. **Algoritmo para Diseño de SD-WAN Anexo III**

Se realiza un análisis del consumo actual de ancho de banda del cliente utilizando las herramientas de monitoreo disponibles y se obtienen los siguientes datos de consumo

Tabela 10.7: Características de Calidad de Servicio en un SD-WAN

Aplicación	BW	Delay	Jitter	Packet Loss	Description
[**Telefonia**]	80kbps call	150ms max	30ms max	1% max	Mission-critical
[**Videoconferencia**]	3.2Mbps	150ms max	30ms max	1% max	Mission-critical
[**FTP**]	3Mbps	tolerant	tolerant	5% max	Mission-critical
[**CCTV**]	2Mbps	1s max	tolerant	2% max	Business-class
[**Web Privada**]	1Mbps	tolerant	tolerant	5% max	Business-class
[**Internet**]	1Mbps	tolerant	tolerant	5% max	Best effort
[**Escritorio remoto**]	2Mbps	200ms max	30ms max	1% max	Business-class
[**Correo**]	1Mbps	tolerant	tolerant	5% max	Best effort
Total	–	–	–		

para cada una de las 11 sedes regionales y nacionales **tabla 10.8 Análisis de consumo en las Sedes**:

Tabela 10.8: Análisis de consumo en las Sedes

Sede	Consumo Promedio	BW Contratado
[**Nacional Medellin**]	14Mbps	14Mbps
[**Antioquia Norte**]	20Mbps	15Mbps
[**Nacional Tocancipa**]	20Mbps	20Mbps
[**Soacha**]	7Mbps	7Mbps
[**Antioquia Sur**]	7Mbps	7Mbps
[**Antioquia Oriente**]	7Mbps	7Mbps
[**Eje Cafetero**]	14Mbps	7Mbps
[**Valle**]	13Mbps	7Mbps
[**Cota**]	7Mbps	7Mbps
[**Bucaramanga**]	7Mbps	7Mbps
[**Funza**]	8Mbps	7Mbps
Total	–	–

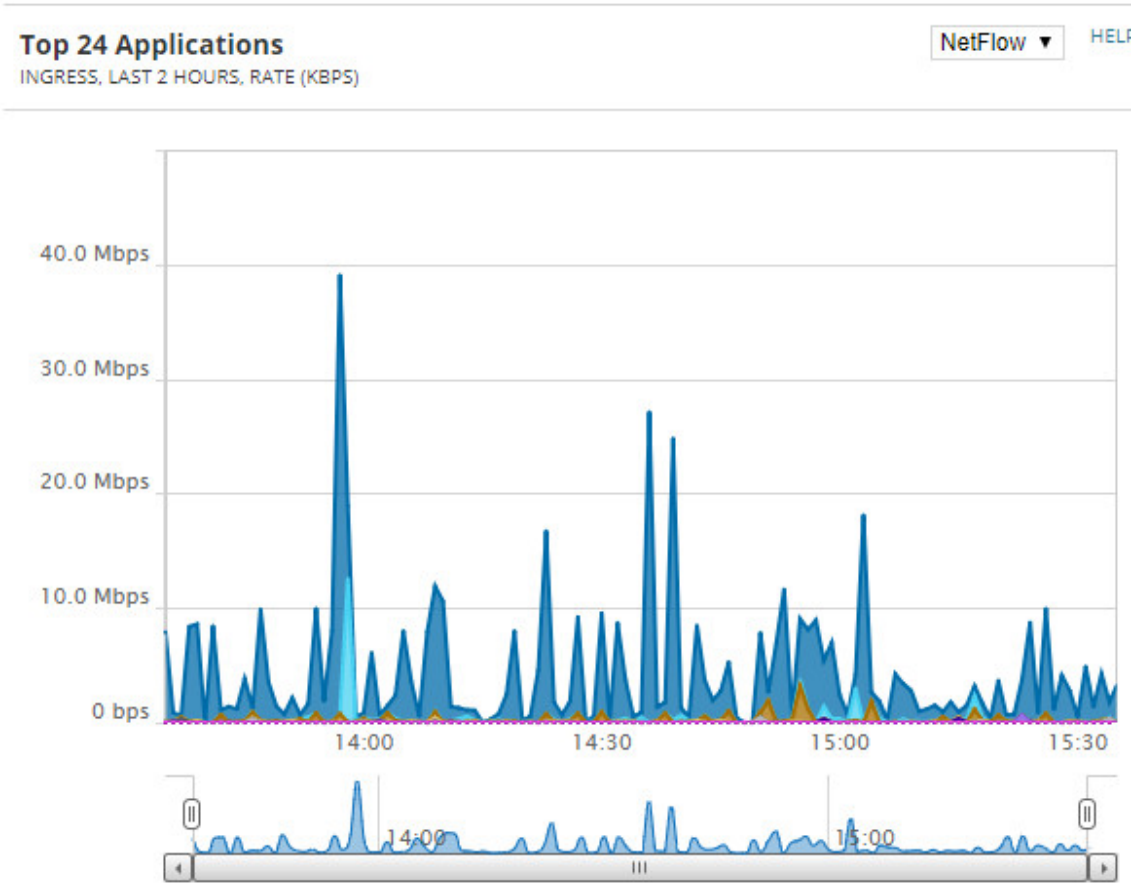
Con estos datos se puede concluir que ya hay saturación en las sedes, y que por tanto la solución actual está presentando retardos y pérdidas de paquetes en la comunicación. Se toman muestras de tráfico utilizando el protocolo Netflow con el fin de caracterizar el tráfico de cada una de las aplicaciones obteniendo los siguientes resultados:

10.11.1 Sede Nacional Tocancipá:

Ver figura 10.10 Sede Nacional Tocancipá.

10.11.2 Sede Nacional Medellín:

Ver figura 10.11 Sede Nacional Medellín.

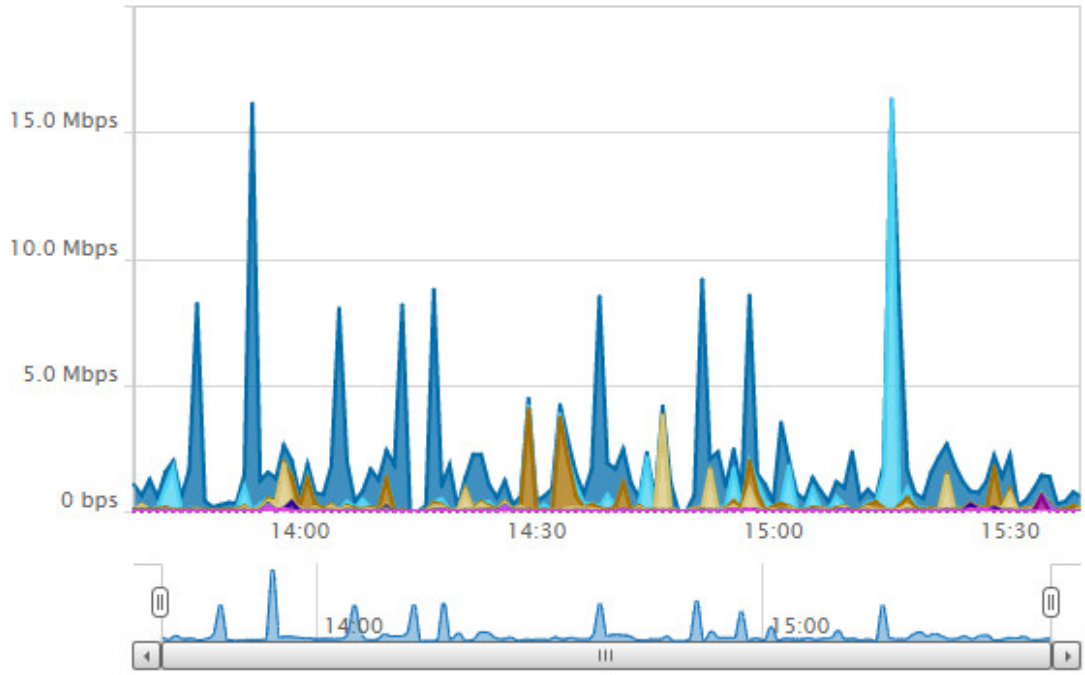


APPLICATION	INGRESS BYTES	INGRESS PACKETS	PERCENT
http protocol over TLS/SSL (443)	3,5 Gbytes	2,62 M	89,23%
Unmonitored traffic	191,0 Mbytes	629,19 k	4,84%
World Wide Web HTTP (80)	169,8 Mbytes	120,3 k	4,3%
Microsoft-DS (445)	26,4 Mbytes	79,9 k	0,67%
Lightweight Directory Access Protocol (389)	8,6 Mbytes	10,88 k	0,22%
RTP (UDP)	7,6 Mbytes	37,99 k	0,19%
MS WBT Server (3389)	6,6 Mbytes	70,41 k	0,17%
ARCP (7070)	4,4 Mbytes	16,07 k	0,11%
Zabbix Agent (10050)	2,2 Mbytes	35,72 k	0,06%
SNMP (161)	1,9 Mbytes	9,1 k	0,05%

Figura 10.10: Sede Nacional Tocancipá

Top 24 Applications
INGRESS, LAST 2 HOURS, RATE (KBPS)

NetFlow ▾ HELP

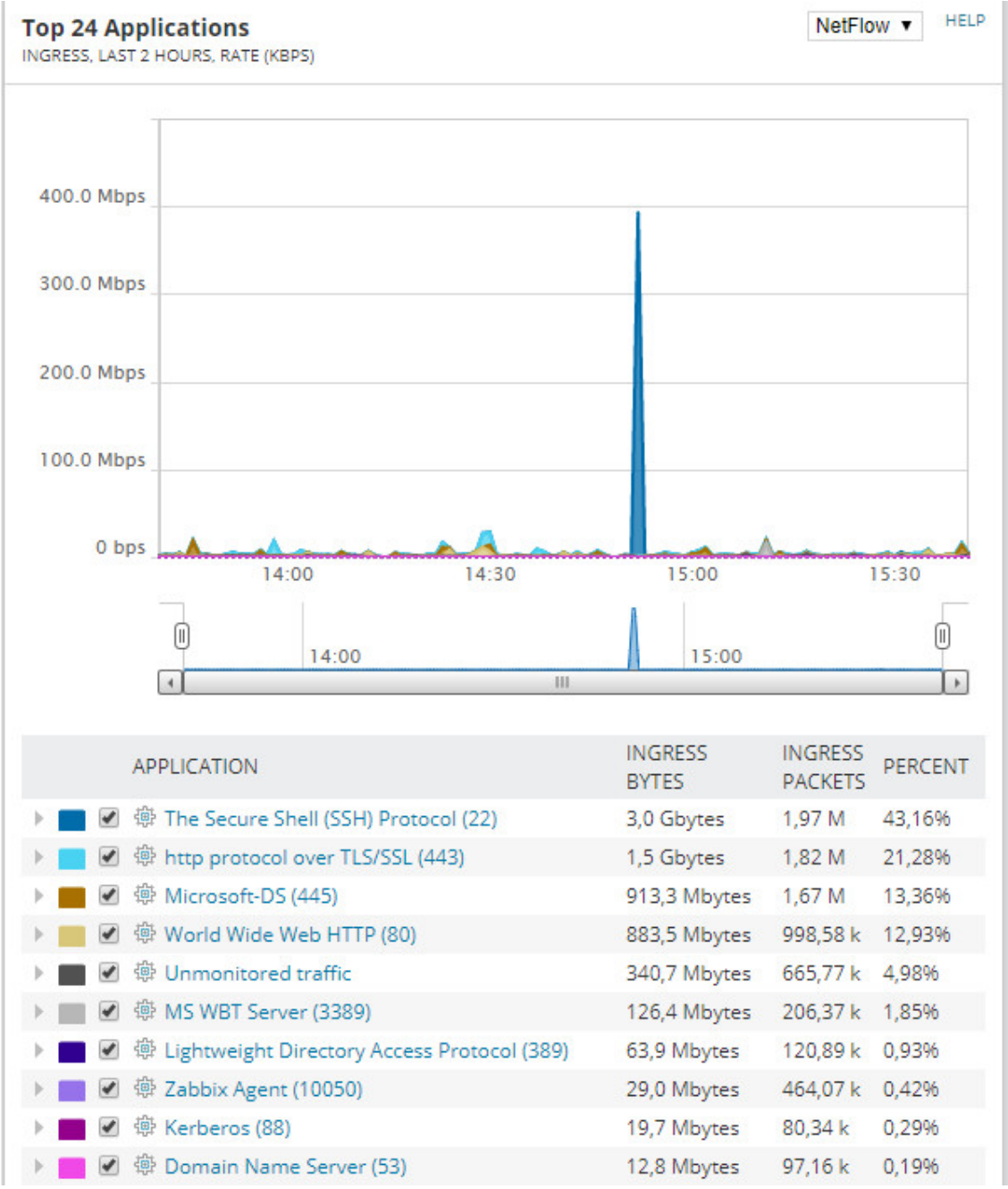


	APPLICATION	INGRESS BYTES	INGRESS PACKETS	PERCENT
▸	http protocol over TLS/SSL (443)	1,2 Gbytes	1,54 M	66,54%
▸	Unmonitored traffic	250,7 Mbytes	642,07 k	13,92%
▸	World Wide Web HTTP (80)	176,9 Mbytes	200,18 k	9,82%
▸	Microsoft-DS (445)	125,6 Mbytes	374,15 k	6,97%
▸	Lightweight Directory Access Protocol (389)	9,6 Mbytes	21,95 k	0,53%
▸	Domain Name Server (53)	7,9 Mbytes	63,55 k	0,44%
▸	Simple Mail Transfer (25)	5,3 Mbytes	5,15 k	0,29%
▸	MS WBT Server (3389)	4,7 Mbytes	36,68 k	0,26%
▸	RTP (UDP)	4,4 Mbytes	22,22 k	0,25%
▸	NewsEDGE server TCP (TCP 1) (8888)	4,3 Mbytes	46,33 k	0,24%

Figura 10.11: Sede Nacional Medellín

10.11.3 Sede Nacional Antioquia Norte:

Ver figura 10.12 Sede Nacional Antioquia Norte.



APPLICATION	INGRESS BYTES	INGRESS PACKETS	PERCENT
The Secure Shell (SSH) Protocol (22)	3,0 Gbytes	1,97 M	43,16%
http protocol over TLS/SSL (443)	1,5 Gbytes	1,82 M	21,28%
Microsoft-DS (445)	913,3 Mbytes	1,67 M	13,36%
World Wide Web HTTP (80)	883,5 Mbytes	998,58 k	12,93%
Unmonitored traffic	340,7 Mbytes	665,77 k	4,98%
MS WBT Server (3389)	126,4 Mbytes	206,37 k	1,85%
Lightweight Directory Access Protocol (389)	63,9 Mbytes	120,89 k	0,93%
Zabbix Agent (10050)	29,0 Mbytes	464,07 k	0,42%
Kerberos (88)	19,7 Mbytes	80,34 k	0,29%
Domain Name Server (53)	12,8 Mbytes	97,16 k	0,19%

Figura 10.12: Sede Nacional Antioquia Norte

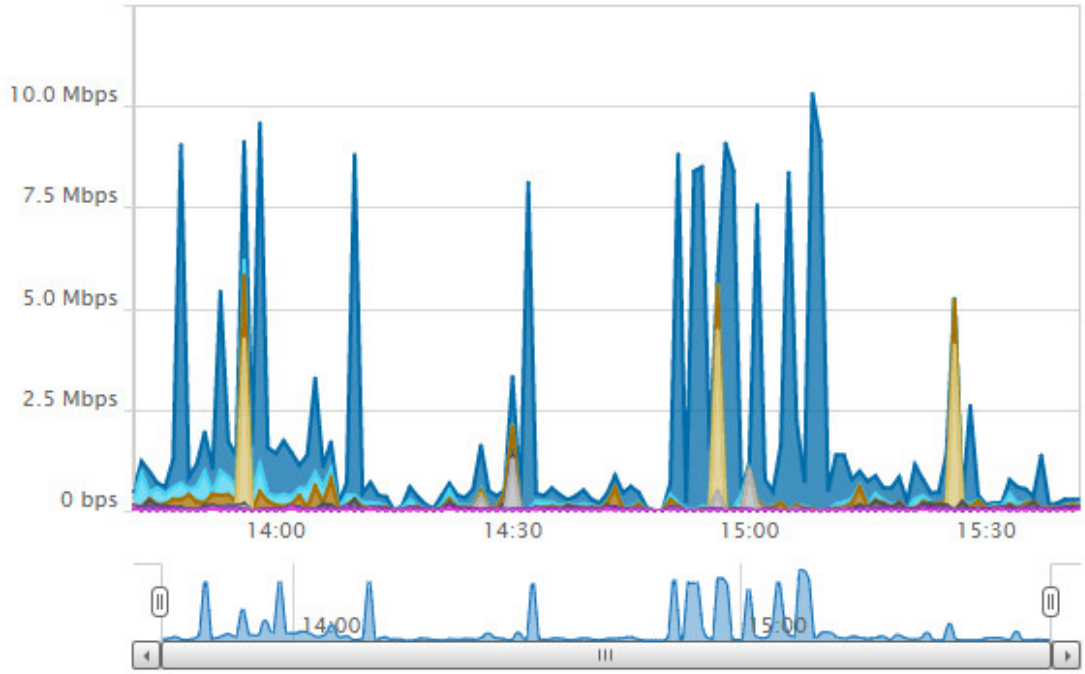
10.11.4 Sede Nacional Antioquia Norte:

Ver figura 10.13 Sede Nacional Valle.

De estos resultados se concluye que para todos los casos el Tráfico Web representa la gran mayoría del tráfico que se genera tanto en las regionales como en las sedes nacionales

Top 24 Applications
INGRESS, LAST 2 HOURS, RATE (KBPS)

NetFlow ▾ HELP



APPLICATION	INGRESS BYTES	INGRESS PACKETS	PERCENT
http protocol over TLS/SSL (443)	1,3 Gbytes	1,41 M	76,16%
Unmonitored traffic	109,7 Mbytes	222,45 k	6,63%
World Wide Web HTTP (80)	97,1 Mbytes	124,96 k	5,87%
iRDMI (8000)	92,5 Mbytes	113,28 k	5,59%
Microsoft-DS (445)	28,3 Mbytes	107,86 k	1,71%
MS WBT Server (3389)	24,0 Mbytes	117,74 k	1,45%
Sun Web Server Admin Service (8800)	13,1 Mbytes	61,07 k	0,8%
Lightweight Directory Access Protocol (389)	11,1 Mbytes	27,67 k	0,67%
Domain Name Server (53)	7,7 Mbytes	51,03 k	0,47%
SNMP (161)	5,6 Mbytes	20,18 k	0,34%

Figura 10.13: Sede Nacional Valle

El tráfico en todos los casos se encuentra al límite de la capacidad, las herramientas de monitoreo no muestran pérdidas de paquetes pero si latencias y jitter que puede afectar la calidad del tráfico de voz y las videoconferencias, adicionalmente en la actualidad no habría posibilidad de crecimiento, teniendo en cuenta el nivel de consumo actual se definen los siguientes anchos de banda para el proyecto **tabla 10.9 Ancho de Banda para los Proyectos**:

Tabela 10.9: Ancho de Banda para los Proyectos

Sede	Consumo Promedio	BW MPLS	BW
[**Nacional Medellin**]	14Mbps	15Mbps	20Mbps
[**Antioquia Norte**]	20Mbps	20Mbps	50Mbps
[**Nacional Tocancipa**]	20Mbps	20Mbps	20Mbps
[**Soacha**]	7Mbps	10Mbps	20Mbps
[**Antioquia Sur**]	7Mbps	10Mbps	20Mbps
[**Antioquia Oriente**]	7Mbps	10Mbps	20Mbps
[**Eje Cafetero**]	14Mbps	15Mbps	20Mbps
[**Valle**]	13Mbps	15Mbps	20Mbps
[**Cota**]	7Mbps	10Mbps	20Mbps
[**Bucaramanga**]	7Mbps	10Mbps	20Mbps
[**Funza**]	8Mbps	10Mbps	20Mbps
Total	–	–	

10.12 Diseño del DataCenter

El diseño del centro del centro de datos se realiza de acuerdo a las mejores prácticas dadas por Cisco en su guía de diseño, para esta solución la topología utilizada es la que Cisco llama diseño híbrido de IWAN, ya que se requieren dos medios de transporte independientes, MPLS e internet banda ancha. **Ver figura 10.1 Diseño de DataCenter**.

En este diseño se requiere acceso a los dos transportes desde el centro de datos, en el datacenter se encuentran los Hub Border routers que son quienes lo interconectan con las dos tecnologías de transporte y el Master controller, estos equipos estarán conectados mediante una infraestructura de switches(existente) que soporta PIM y otras tecnologías de multicast para el correcto funcionamiento del plano de control.

Se sugiere al cliente por redundancia tener dos centros de datos con esta topología para garantizar la alta disponibilidad de la solución, sin embargo por costos el cliente indica que no es posible contar con una topología de ese estilo, por ende se garantiza disponibilidad de equipos en un solo centro de datos para que la falla de algún equipo de borde no genere afectación en el plano de datos del cliente, la topología adoptada para esta solución es la siguiente **Ver figura 10.14 Topología de DataCenter**.

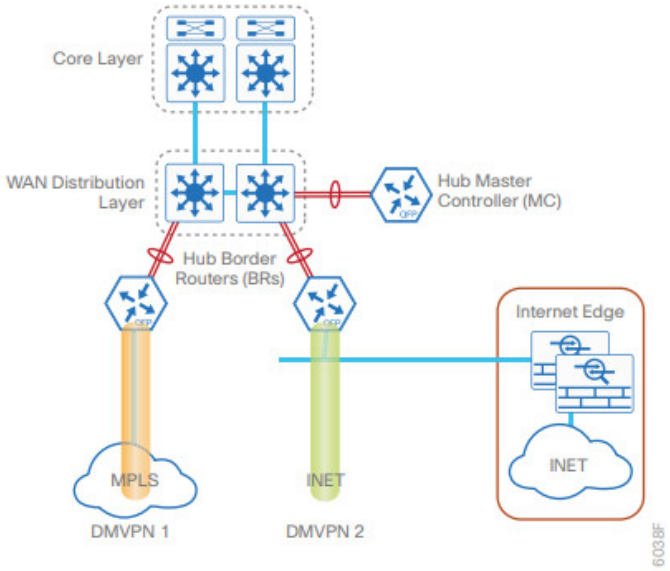


Figura 10.14: Diseño de DataCenter

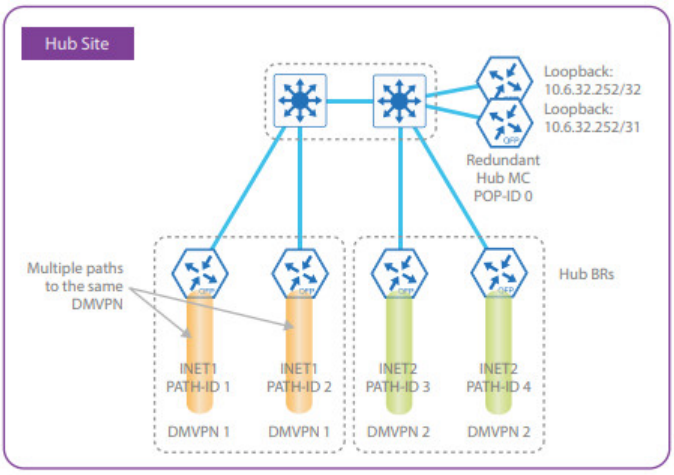


Figura 10.15: Topología de DataCenter

De esta manera, para cada tecnología de transporte se tendrán dos Hub Border Router para garantizar la redundancia en la terminación de túneles DMVPN contra el datacenter, de igual forma la redundancia del plano de control se da mediante la utilización de dos Master controller en el centro de datos.

Sin embargo con el fin de disminuir la cantidad de equipos que deben ser adquiridos por el cliente para la implementación de la solución se utiliza la tecnología MTT (Multiple Tunnel Termination), esto permite utilizar únicamente dos HBR(Hub Border Router) en el centro de datos y establecer la redundancia configurando múltiples túneles en cada equipo, la siguiente imagen muestra la idea general de esta tecnología **Ver figura 10.15 Configuración de Túneles para el DataCenter**.

Por lo que al final el diseño utilizaría dos equipos para realizar la función de HBR,

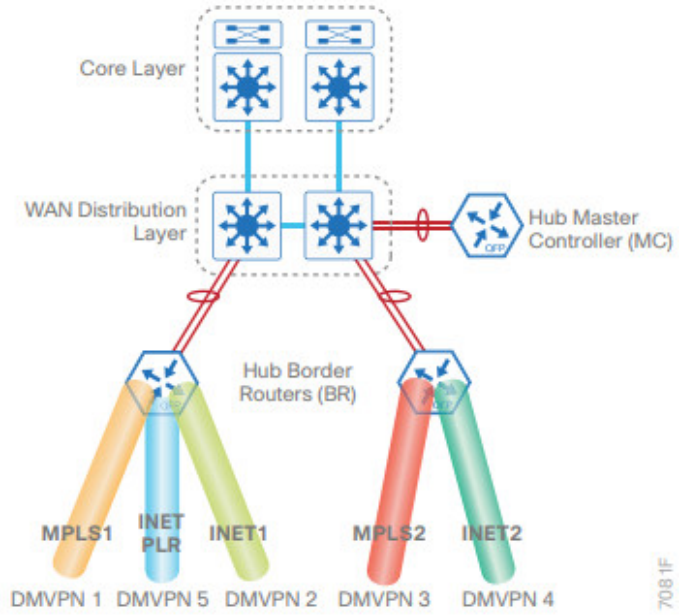


Figura 10.16: Configuración de Túneles para el DataCenter

cada uno terminando túneles hacia los dos transportes (internet banda ancha y MPLS) y dos equipos para hacer la función de MC.

La función del MC es definir las políticas de PfR que se utilizarán para el balanceo de carga y los requerimientos de cada una de las aplicaciones que componen la solución, para este cliente se definen agruparon las aplicaciones en ciertos grupos y se definieron los requerimientos de cada uno de ellos. En capítulos posteriores se definieron cada una de las aplicaciones, sus requerimientos y su grupo, sin embargo en el caso de PfR la agrupación debe realizarse por requerimientos de la aplicación. la siguiente tabla define el grupo para cada una de las aplicaciones y sus requerimientos a nivel de parámetros de red. **tabla 10.10 Requerimientos de la Aplicación**:

Tabela 10.10: Requerimientos de la Aplicación

Aplicación	BW	Delay	Jitter	Packet Loss	Description
[**Telefonia**]	80kbps call	150ms max	30ms max	1% max	Real Time
[**Videoconferencia**]	3.2Mbps	150ms max	30ms max	1% max	Real Time
[**FTP**]	3Mbps	tolerant	tolerant	5% max	Business
[**CCTV**]	2Mbps	1s max	tolerant	2% max	Business
[**Web Privada**]	1Mbps	tolerant	tolerant	5% max	Business
[**Internet**]	1Mbps	tolerant	tolerant	5% max	Business
[**Escritorio remoto**]	2Mbps	200ms max	30ms max	1% max	Best effort
[**Correo**]	1Mbps	tolerant	tolerant	5% max	Best effort
Total	–	–	–		

Por tanto se crearán 4 clases de tráfico en PfR y sus parámetros corresponden a los

requerimientos de las aplicaciones que componen el grupo, la siguiente **tabla 10.11 Requerimientos Configurados PfR**resume los requerimientos de cada uno de los grupos que corresponden a los parámetros configurados en PfR .

Tabela 10.11: Requerimientos Configurados PfR

Grupo	Delay	Jitter	Perdidas Paquetes
[**Real-Time**]	150ms	20ms	1%
[**Business-class**]	250ms	30ms	2%
[**Best Effort**]	500ms	N/A	5%
[**Scavenger**]	500ms	N/A	10%
Total	–	–	–

Dentro de la topología de datacenter es importante mencionar que los HBR deben compartir rutas internamente a través del protocolo de enrutamiento EIGRP, y estas rutas deben compartirse entre los transportes de internet y de intranet.

10.13 Diseño de Sedes Remotas

Para el caso de las sedes remotas no se tiene un solo diseño, sino que este cambia dependiendo de si la sede es una tienda, una regional o una oficina nacional, ya que la criticidad de cada una de las sedes cambia y por tanto requieren diseños de red diferentes.

10.14 Diseño de Tiendas

Por costos las tiendas contarán como transporte únicamente con un enlace de internet banda ancha y no estarán conectadas a la MPLS, contarán con un único equipo en la sede que genere los túneles DMVPN contra las demás sedes.

Este equipo contará con un puerto troncal hacia la LAN del cliente que incluirá los diferentes segmentos de red cada uno con una VLAN independiente.La siguiente imagen muestra de forma general la topología de red para estas tiendas **Ver figura 10.17 Topología de Tiendas**.

La topología WAN de las tiendas es por tanto bastante sencilla, el router en la tienda actuará como un spoke de los dos equipos HBR ubicados en el centro de datos, garantizando de esta manera la integración entre la infraestructura de IWAN y las tiendas.

10.15 Diseño de Regionales

Las regionales al requerir de mayor ancho de banda, mayor disponibilidad y mayor performance de la red, contarán con dos transportes en el router de borde, de esta forma la tecnología de IWAN realizará el balanceo de carga entre el enlace de internet banda

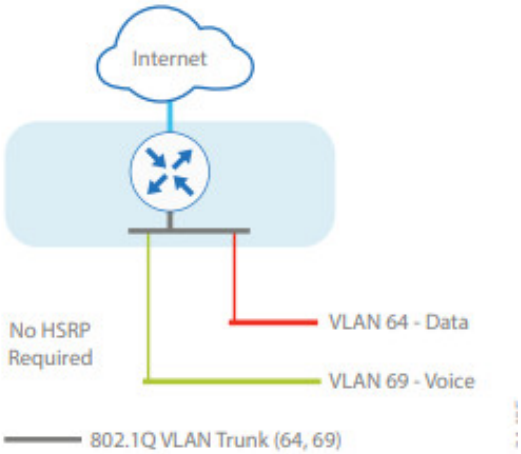


Figura 10.17: Topología de Tiendas

ancha y el enlace MPLS, y contará con redundancia en caso de que alguno de estos enlaces falle.La siguiente imagen muestra de forma general la topología para las regionales.**Ver figura 10.18 Topología Regionales**.

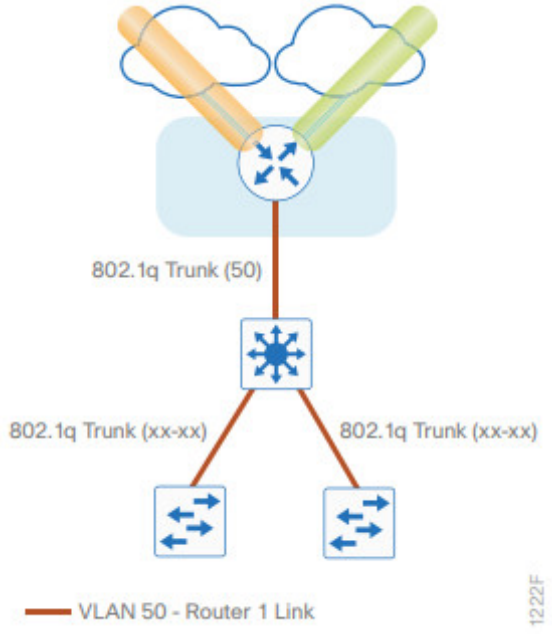


Figura 10.18: Topología Regionales

El router formará túneles tanto por internet como por la MPLS hacia el centro de datos y desde allí hacia las demás sedes, en este caso se tendrá una interconexión entre el router de borde y el switch core de la sede, se utilizarán rutas estáticas para alcanzar los diferentes segmentos internos, y estas rutas serán enseñadas al resto de la red mediante el protocolo EIGRP.

En este caso hay redundancia de enlaces ya que el router de borde cuenta con conexión hacia internet y hacia la MPLS por lo que el protocolo PfR se encargará de realizar el balanceo entre los dos enlaces y asegurar la calidad de la voz, video y demás servicios.

10.16 Diseño de Sedes Nacionales

Para el caso de las sedes nacionales debido a su criticidad se requiere no solamente redundancia de enlaces y de fibra sino también de equipos de borde, por lo que la topología cambia para garantizar una mayor disponibilidad en estas sedes. La topología que se tendría en estas sedes es la siguiente: **Ver figura 10.19 Topología Sedes Nacionales**.

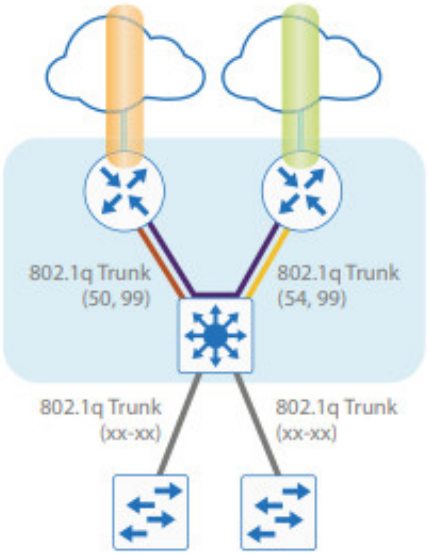


Figura 10.19: Topología Sedes Nacionales

En este caso las LAN de los router de borde utilizarían el protocolo HSRP para garantizar la redundancia en caso de presentarse falla sobre alguno de los dos equipos, sin embargo con el fin de asegurar que siga habiendo balanceo de carga entre el enlace de internet y el de MPLS se configura el protocolo EIGRP entre los dos equipos, y se configura uno de los dos routers como branch hub y el otro como spoke con el fin de que PfR siga siendo el responsable de tomar la decisión de por cual de las dos últimas millas se envía el tráfico.

10.17 Diseño de Enrutamiento

Como se ha mencionado con anterioridad la conectividad entre las sedes se da por medio de túneles GRE multipunto, tecnología también llamada DMVPN, esta es una consideración importante dentro de el diseño de enrutamiento, ya que influye en la decisión de cuál de los protocolos de enrutamiento disponibles son viables para obtener una conectividad

escalable y resiliente.
Los protocolos de enrutamiento dinámico considerados para la realización del proyecto fueron los siguientes:

- **OSPF**
- **EIGRP**
- **BGP**

El protocolo OSPF es la primera opción en la mayoría de los casos para la conectividad interna del cliente, sin embargo este protocolo de enrutamiento no es recomendado para su utilización con DMVPN debido a su estructura jerárquica. DMVPN tiene una topología Hub and Spoke pero soportando tráfico directamente entre los spokes, aún así esta topología quiere decir que a nivel de enrutamiento todas las sedes deben establecer sus adyacencias a nivel de enrutamiento contra el Hub, con el fin de hacer de DMVPN una topología más escalable se recomienda establecer una sumarización en el Hub de los prefijos de los Spokes, disminuyendo de esta forma la cantidad de espacio de la tabla de enrutamiento y haciendo el enrutamiento más eficiente y más escalable.

Implementar OSPF en una sola área no sería escalable ya que se requerirían enrutadores con muy altas capacidades en cada sede para soportar la tabla topológica completa incluyendo todas las rutas hacia las más de 700 sedes. En inconveniente puntual con OSPF es que dada su naturaleza jerárquica, la sumarización de las rutas puede hacerse únicamente en los ABR, lo cuál implicaría para la topología de DMVPN que cada sede estuviera en un área diferente, lo cuál tampoco escalaría ya que se perderían las ventajas de protocolo de estado de enlace que posee OSPF.

BGP por otro lado es posiblemente el protocolo de enrutamiento existente con la mayor escalabilidad, sin embargo no es muy utilizado como IGP ya que su tiempo de convergencia no es muy alto, con la configuración por defecto de sus temporizadores BGP puede tardar hasta 180 segundos para converger. Por tanto para garantizar un tiempo de convergencia más rápido se excluye este protocolo de enrutamiento de las posibles opciones.

EIGRP por su parte es un protocolo escalable y de rápida convergencia, y en dónde la sumarización puede realizarse en cualquier equipo de la red, por lo que es el protocolo de enrutamiento seleccionado para la solución del cliente. Las adyacencias se realizarían a través de los túneles mGRE y estas se establecerán desde cada una de las sedes remotas contra el router Hub. A continuación se presenta un resumen de cómo se realizan estas adyacencias en EIGRP y la sumarización realizada.

10.18 Simulación

Con el fin de definir el comportamiento del diseño planteado se realizaron simulaciones de los dos escenarios, tanto de sedes remotas como de sedes nacionales, para asegurar que la red se comporta tal como se predijo y que se están cumpliendo los requisitos de la disponibilidad y calidad de servicio.

10.18.1 Infraestructura Utilizada para la Simulación

La simulación se realizó utilizando el software GNS3, sin embargo dados los requerimientos de protocolos y dado que se requería de equipos que soporten IWAN no se utilizó GNS3 en su modo tradicional emulando routers directamente en su plataforma, por el contrario se creó una máquina virtual Ubuntu cuyo objetivo es realizar la virtualización de equipos de red, por lo que la simulación fue realizada con VNF creando una máquina virtual para cada uno de los routers simulados, se utiliza por tanto el concepto de virtualización anidada de forma que cada router virtual se crea como una máquina virtual dentro de otra máquina virtual, el esquema de esta virtualización **Ver figura 10.20 Infraestructura Utilizada para la Simulación**. Esta virtualización Anidada se realizó utilizando

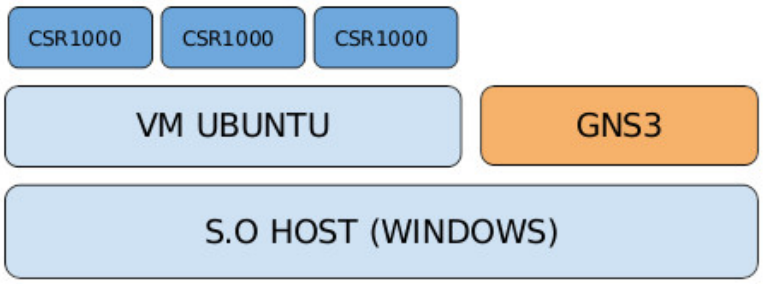


Figura 10.20: Infraestructura Utilizada para la Simulación

VMware workstation pro, mediante esta herramienta se virtualizó la VM de Ubuntu dentro del sistema operativo Windows, a su vez dentro de esta máquina virtual de Ubuntu se utilizó virtualización KVM para montar cada uno de los enrutadores virtuales.

Esta configuración permite por un lado mantener contenidos dentro de la máquina virtual Ubuntu los recursos que utilizan los enrutadores virtuales de manera que la utilización de estas máquinas no colapse el sistema operativo host al dejar sin recursos el sistema operativo y permite por otro lado integrar GNS3 con routers VNF reales, en este caso los CSR1000v de Cisco que están diseñados específicamente para servicios en la nube y soportan todas las características requeridas por la solución de IWAN. Estos enrutadores virtuales requieren 1 core y 3GB de RAM, por tanto la simulación se realizó en un equipo con las siguientes carácteristicas técnicas **tabla 10.12 Caracteríticas Técnicas**:

De estos recursos tuvieron que asignarse 12MB de memoria RAM para la máquina

Tabela 10.12: Caracteríticas Técnicas

Dipositivo	Recursos
[**Memoria RAM**]	16 GB
[**CPU**]	intel core i7 7700HQ - 4 cores
[**Disco Duro**]	1T HD + 128GB SSD
Total	–

virtual ya que cada uno de los routers requiere 3MB de Memoria para funcionar correctamente y 4 threads de procesamiento de los 8 disponibles para el procesamiento requerido por los enrutadores, por otra lado solamente 8GB de disco duro fueron suficientes para esta máquina virtual.

10.18.2 Topologías y Configuraciones Realizadas

Dado el diseño planteado se realizaron pruebas con dos topologías diferentes, la primera siendo la topología de las sedes nacionales, es decir dos CPE en la sede cada uno recibiendo un hilo de fibra por un transporte diferente. Para esta topología se incluyeron un total de 5 enrutadores, dos realizando la función de HBR (Hub Border Router) que actúan como Hubs para los túneles en la topología DMVPN y un MC(Master Controller) encargado de establecer las políticas de PfR de cada una de las aplicaciones y propagar las políticas por el resto de la red.**Ver figura 10.21 La topología configurada en GNS3**.

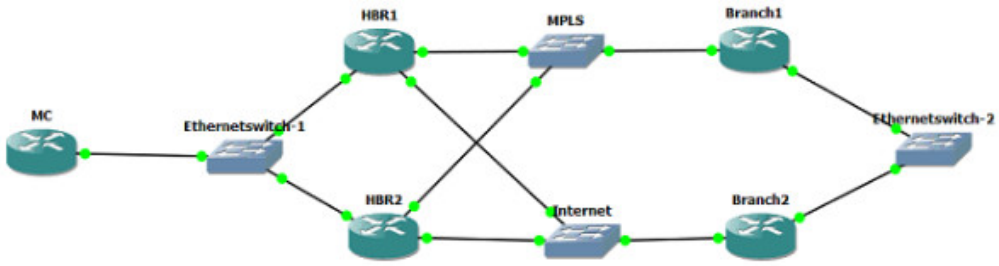


Figura 10.21: La topología configurada en GNS3

En la topología se simulan los diferentes transportes con switches, uno para la MPLS y otro para el transporte de internet, esto es una simplificación de las redes de transporte reales ya que estas son mucho más complejas, pero en este caso la simulación mantiene su validez ya que para establecer los túneles que funcionan acá como la red "underlay" únicamente se requiere conectividad IP entre los routers Branch y los HBR sin importar la forma como esta se de.

Como se mencionó anteriormente los HBR actúan como Hubs para la topología DMVPN y en esta topología los dos equipos Branch se registran contra dichos equipos como lo muestra **Ver figura 10.22 Branch1** para el Branch1 y **Ver figura 10.24 Branch2** para el Branch2

```
Branch-1#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
----------------------------------------------------------------------

Interface: Tunnel10, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 10.168.73.222         10.60.0.1    UP 00:44:19     S
     1 10.168.73.223        10.60.0.56    UP 00:44:19     S
```

Figura 10.22: Branch1

```
Branch-2#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
----------------------------------------------------------------------

Interface: Tunnel11, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 200.0.0.1           10.60.2.1    UP 00:24:35     S
     1 200.0.0.2          10.60.2.56    UP 00:24:35     S
```

Figura 10.23: Branch2

Además de estas adyacencias de DMVPN se configuró EIGRP como protocolo de enrutamiento utilizado tanto hacia los túneles como entre los routers Branch y en data-center entre los HBR y el MC, las **Ver figura 10.25 Configuración EIGRP** y **Ver figura 10.26 Configuración EIGRP** muestran los establecimientos de dichas adyacencias en el Branch.

```
Branch-1#sh ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
2   10.10.10.3              Gi1               12 00:28:51   13   100  0  15
1   10.60.0.1               Tu10              11 00:46:10   13   100  0  29
0   10.60.0.56              Tu10              10 00:46:52   71   426  0  27
```

Figura 10.24: Configuración EIGRP

```
Branch-2#sh ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
2   10.10.10.2              Gi1               10 00:29:23    7   100  0  18
1   10.60.2.1               Tu11              13 00:36:42   27   162  0  30
0   10.60.2.56              Tu11              14 00:36:42   10   100  0  29
```

Figura 10.25: Configuración EIGRP

Finalmente el otro componente que hace parte de la solución de IWAN es PfR, en este caso uno de los routers (El activo en la configuración de HSRP) toma el rol de master en

PFR encargándose de distribuir las políticas a los border router del Branch, las imagenes **Ver figura 10.27 Registros de los Routersy Ver figura 10.28 Registros de los Routers** muestran el registro de los dos routers con PfR.

```
Branch-1#sh domain ONE master status

 *** Domain MC Status ***

Master VRF: Global

 Instance Type:    Branch
 Instance id:      0
 Operational status:  Up
 Configured status:  Up
 Loopback IP Address: 10.60.4.29
 Operational Mode: With Hub
 Load Balancing:
  Operational Status: Up
  Max Calculated Utilization Variance: 0%
  Last load balance attempt: never
  Last Reason:  Variance less than 20%
  Total unbalanced bandwidth:
        External links: 0 Kbps  Internet links: 0 Kbps
 Route Control: Enabled
 Transit Site Affinity: Enabled
 95% Bandwidth Check: Enabled
 Load Sharing: Enabled
 Connection Keepalive: 10 seconds
 Mitigation mode Aggressive: Disabled
 Policy threshold variance: 20
 Minimum Mask Length Internet: 24
 Minimum Mask Length Enterprise: 24
 Syslog TCA suppress timer: 180 seconds
 Traffic-Class Ageout Timer: 5 minutes
 Global Fallback Timer: 3 minutes
 Minimum Packet Loss Calculation Threshold: 15 packets
 Minimum Bytes Loss Calculation Threshold: 10240 bytes
 Branch to Branch Traffic Control: Enabled
 Direct Cloud Access : Disabled
 Maximum Traffic Classes Supported: 4000
 Minimum Requirement: Met
```

Figura 10.26: Registros de los Routers

```
Branch-2#sh domain ONE border status

Wed May 29 01:54:34.640
------------------------------------------------------------------------
  **** Border Status ****

Instance Status: UP
Present status last updated: 00:26:57 ago
Loopback: Configured Loopback789 UP (10.60.4.30)
Master: 10.60.4.29
Master version: 2
Connection Status with Master: UP
MC connection info: CONNECTION SUCCESSFUL
Connected for: 00:26:56
Route-Control: Enabled
Asymmetric Routing: Disabled
Minimum Mask Length Internet: 24
Minimum Mask Length Enterprise: 24
Connection Keepalive: 10 seconds
Sampling: off
Channel Unreachable Threshold Timer: 4 seconds
Minimum Packet Loss Calculation Threshold: 15 packets
Minimum Byte Loss Calculation Threshold: 10240 bytes
Monitor cache usage: 4000 (20%) Auto allocated
Minimum Requirement: Met
Smart Probe Profile:
  General Monitor:
    Current Provision Level: Master Hub
        Master Hub:
            Packets per burst: 1
            Interval(secs): 1
  Quick Monitor:
    Current Provision Level: Master Hub
        Master Hub:
            Packets per burst: 20
            Interval(secs): 1
  Notification to PD:
    add: 1, upd: 0, del: 0
```

Figura 10.27: Registros de los Routers

El diseño para las sedes regionales difiere de las sedes nacionales en cuanto a que por costos no se utilizan dos routers sino uno sólo con dos métodos de transporte independientes, en este sentido la distribución y configuración de la topología en datacenter se mantiene exactamente igual, el único cambio de configuración se realiza sobre el router

Branch, la topología simulada para este caso es ilustrada en la figura **Ver figura 10.29 Topología Router Branch**

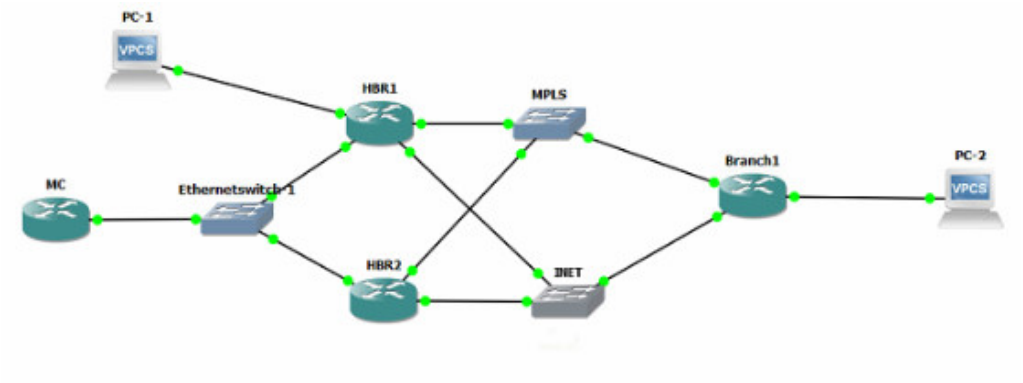


Figura 10.28: Topología Router Branch

En este caso el único router branch contará con 4 adyacencias de DMVPN, dos por cada HBR, correspondientes a los diferentes tipos de transporte. Esto asegura que hay redundancia en caso de que alguno de los HBR falle o en caso de ruptura de fibra óptica para alguno de los canales de transporte. la imagen **Ver figura 10.30 Registro desde el Router** ilustra la forma como se ve este registro desde el router.

```
Branch-1#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel10, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 10.168.73.222         10.60.0.1    UP 01:20:49     S
     1 10.168.73.223        10.60.0.56    UP 01:25:57     S

Interface: Tunnel11, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 200.0.0.1             10.60.2.1    UP 00:00:51     S
     1 200.0.0.2            10.60.2.56    UP 00:00:38     S
```

Figura 10.29: Registro desde el Router

De igual forma a pesar de que se forman adyacencias EIGRP por los túneles GRE multipunto únicamente contra los 2 HBR se establecen 4 vecindades de HSRP diferentes, dos por cada HBR, este comportamiento puede verse más claramente en el router como lo muestra la figura **Ver figura 10.31 Adyacencias EIGRP por los Túneles GRE**

```
Branch-1#sh ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
3   10.60.2.1               Tu11              11 00:09:50   17   102  0  12
2   10.60.2.56              Tu11              13 00:09:50   14   100  0  27
1   10.60.0.1               Tu10              10 01:33:53   19   114  0  10
0   10.60.0.56              Tu10              13 01:38:44  150   900  0  25
Branch-1#
```

Figura 10.30: Adyacencias EIGRP por los Túneles GRE

En cuanto al protocolo PfR el mismo router cumple las funciones de master y de borde para el branch, registrándose y descargando las políticas desde el MC en el datacenter. La imagen **Ver figura 10.32 Protocolo PfR** muestra dicho registro.

Figura 10.31: Protocolo PfR

Capítulo 11

Resultados

En la topología de dos routers, correspondiente al diseño de las sedes nacionales se observó que el diseño realizado garantiza la conectividad hacia el centro de datos, y dependiendo de la aplicación que se utilice el tráfico será enrutado por una última milla o por la otra, las imágenes **Ver figura 11.1 Conectividad** y **Ver figura 11.2 Ruta** muestran esta conectividad y la ruta que se está tomando para dicho tráfico.

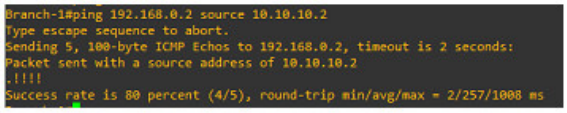


Figura 11.1: Conectividad

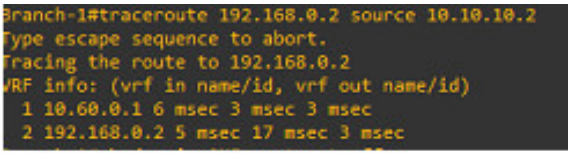


Figura 11.2: Ruta

El router reconoce mediante Nbar las aplicaciones que cursan por la red y dependiendo de esto y de los parámetros de retardo, jitter y pérdida de paquetes decide por cuál de las interfaces disponibles enviar el tráfico, en este caso el tráfico de ping fue enrutado a través de la MPLS como lo indica la figura **Ver figura 11.3 Enrutado a través de la MPLS**

Posterior a realizar las pruebas de conectividad se quisieron medir los mecanismos de redundancia implementados y para ello se simuló la caída del enlace MPLS con el fin de verificar que se cumpla la alta disponibilidad deseada en la red.

Al simular una ruptura de fibra sobre la MPLS el tráfico conmutó al enlace de internet y ya que PfR mide pérdidas de paquetes en los túneles toda la solución de IWAN conmutó

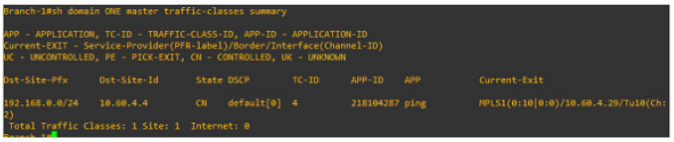


Figura 11.3: Enrutado a través de la MPLS

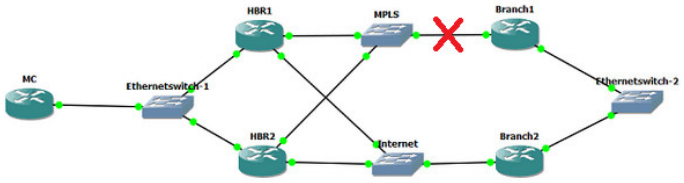


Figura 11.4: Disponibilidad Deseada en la Red

hacia el único enlace disponible. La figura **Ver figura 11.4 Disponibilidad Deseada en la Red** muestra como el tráfico ahora tomo otro camino para llegar al mismo destino y la figura **Ver figura 11.5 Reconocimiento del cambio en PfR** ilustra el reconocimiento del cambio en PfR y por tanto el cambio en las políticas de enrutamiento.

Figura 11.5: Reconocimiento del cambio en PfR

El mismo tipo de pruebas fueron realizadas sobre la topología de las sedes regionales, que cuentan con conexión a dos tipos de transporte diferentes pero un solo CPE en la sede, las pruebas de conectividad arrojaron exactamente los mismos resultados que en el escenario anterior, es decir conectividad exitosa a través de la MPLS como puede verse en la figura **Ver figura 11.6 Topología de las Sedes Regionales** y **Ver figura 11.7 Conectividad exitosa a través de la MPLS**

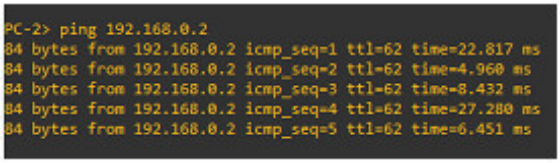


Figura 11.6: Topología de las Sedes Regionales

Al igual que en el escenario de dos router la aplicación es reconocida y enrutada a través de la MPLS según las políticas de PfR, por lo que se comprueba que tanto el reconocimiento de aplicaciones como el enrutamiento basado en aplicación se encuentra funcionando apropiadamente. La figura **Ver figura 11.8 Decisión de PfR** muestra la decisión de PfR de enrutar el tráfico ping a través de la MPLS.

Al igual que como se realizó con el escenario de dos routers, se generaron pruebas de

```
PC-2> trace 192.168.0.2
trace to 192.168.0.2, 8 hops max, press Ctrl+C to stop
 1   10.10.10.2   5.456 ms  1.985 ms  1.986 ms
 2   10.60.0.1   9.415 ms  14.876 ms  10.918 ms
 3   *192.168.0.2   17.854 ms (ICMP type:3, code:3, Destination port unreachable)
```

Figura 11.7: Conectividad exitosa a través de la MPLS

```
Branch-1#sh domain ONE master traffic-classes summary

APP - APPLICATION, TC-ID - TRAFFIC-CLASS-ID, APP-ID - APPLICATION-ID
Current-EXIT - Service-Provider(PFR-label)/Border/Interface(Channel-ID)
UC - UNCONTROLLED, PE - PICK-EXIT, CN - CONTROLLED, UK - UNKNOWN

Dst-Site-Pfx      Dst-Site-Id       State DSCP        TC-ID      APP-ID    APP          Current-Exit

192.168.0.0/24    10.60.4.4         CN    default[0]  2          218104287 ping         MPLS1(0:10[0:0)/10.60.4.29/Tu10(Ch:
3)
 Total Traffic Classes: 1 Site: 1  Internet: 0
```

Figura 11.8: Decisión de PfR

simulación de falla de fibra con el fin de comprobar que la redundancia de la operación funcione correctamente. La figura **Ver figura 11.9 Falla de Fibra** se ilustra la prueba realizada para este escenario.

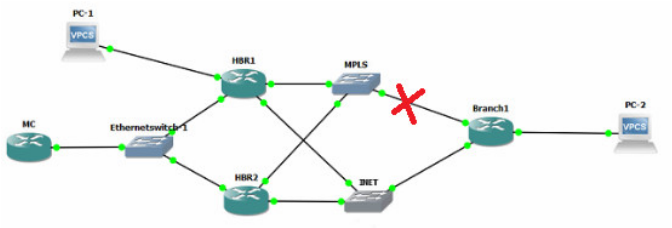


Figura 11.9: Falla de Fibra

Después de simular esta falla se realizaron pruebas de conectividad exitosa **Ver figura 11.10 Enlace de INET** y tal como lo indica la traza tomada,el tráfico conmutó correctamente a través del enlace de INET.

```
PC-2> trace 192.168.0.2
trace to 192.168.0.2, 8 hops max, press Ctrl+C to stop
 1   10.10.10.2   1.983 ms  6.449 ms  3.967 ms
 2   10.60.2.1   10.418 ms  3.469 ms  9.427 ms
 3     *  *  *
 4   *192.168.0.2   27.280 ms (ICMP type:3, code:3, Destination port unreachable)
```

Figura 11.10: Enlace de INET

Los resultados de la simulación muestran por tanto que el esquema de redundancia funciona apropiadamente ante una falla de un equipo o en el caso de ruptura de fibra, lo mismo aplica para casos de degradación de los servicios por pérdidas de paquetes o retardos excesivos en alguno de los transportes.

Capítulo 12

Discusión

Al realizar una investigación sobre los diferentes diseños de redes obteniendo como resultado SD-WAN procede a realizar discusiones que sirven para consolidar lo obtenido.

El objetivo planteado en la investigación diseño de una SD-WAN para un cliente Retail, se incluye un desarrollo sobre donde se aplica este campo en las telecomunicaciones, comparando que existe mayor confiabilidad en el uso de IWAN que implementando infraestructura mejorando una calidad de servicio.

Vamos a centrar la discusión en aquellos aspectos más revelantes que se ha extraído de la investigación, diseño resultados y resultados obtenidos disponiendo de elementos especifícos y comparación de aportes con nuestra experiencia adquirida.

Se tiene en cuenta como hoy en día como las redes ha ido avanzando, tal el caso que las infraestructuras están siendo migradas al **"Cloud"** o conocido naturalmente como la nube, esto ha ocacionado mayor ventajas debido a que se presenta mayor confiabilidad en la redes, mejor administración, control del tráfico y evitando fallas en menor riesgo.

El análisis de resultados llevó a una tendencia del diseño presente en la SD-WAN, la utilización de OpenDayLight como controladora, utilización de software libre, permite el uso de protocolos como **OpenFlow** y **NetConf**.

Esta arquitectura permite conectar cualquier elemento de red, haciendo facilmente para la realización de conexiones y permitiendo fácil configuración de equipos como **CSV 1000v** de Cisco, mientras se utiliza otra tecnología se puede tener dificultad por licencias, permisos, etc.

A continuación se describe las puntuaciones utilizadas en el diseño que actuan como controladoras de red.

Redundancia: dictribución de las funciones de la red, como es distribución de equipos de una forma que no permita generar redundancia.
Calidad de Servicio: siempre se llevo manejo de buenas prácticas para obtener una calidad de servicio al 100%.
Balanceo de Carga: se distribuyó el tráfico de internet de acuerdo a las sedes, para evitar congestiones, caídas, retardos, etc.

El objetivo del diseño pretende conseguir un nivel óptimo de tráfico en la red para un cliente retail, enfocado hacia el **Cloud** y la utilización de una SD-WAN, que permitió un diseño estable para las sedes.

SD-WAN global con calidad MPLS pero sin costo: Las SD-WAN reducen los costos, aumentan la agilidad de la red y mejoran la confiabilidad en gran parte al aprovechar los servicios de Internet asequibles. Pero junto con sus beneficios, las redes troncales de Internet también introducen problemas de coherencia ausentes en las WAN globales estructuradas en torno a MPLS. Las nuevas arquitecturas principales definidas por software ofrecen una solución, que proporciona a las empresas alternativas de backbone asequibles y de alta calidad a los servicios MPLS tradicionales.

Pruebas recientes realizadas por expertos SD-WAN destacaron los problemas del núcleo de Internet. Medimos y comparamos la demora de extremo a extremo en varios servicios de última milla, varias redes troncales de Internet y una red troncal privada (la red de AWS). Nuestras pruebas demostraron que si bien como porcentaje, las conexiones de la última milla podrían ser las más erráticas, la gran longitud a través del núcleo de Internet en una conexión global hace que el rendimiento de la milla media sea un determinante mucho mayor de la latencia general. Por ejemplo, la variación de la última milla en cuatro caminos a Bangalore desde San José, Londres, Tokio y Sydney fue de 5.88 ms (la mediana era 3 ms). En contraste, las millas medias variaron de 36% a 85%, 92 ms a 125 ms, un impacto 20 veces mayor en la conexión.

Para llevar los desafíos de una SD-WAN se tuvo en cuenta: Insistir en la protección nativa de firewall de próxima generación. La integración es fundamental. El tráfico encriptado debe ser inspeccionado.

Una SD-WAN, como la transformación de la red.

Capítulo 13

Conclusiones

La solución cumple con los requerimientos del proyecto según la simulación realizada, ya que se está realizando el balanceo de carga sobre los diferentes enlaces utilizando PfR y la redundancia utilizando EIGRP como protocolo de enrutamiento y HSRP en el caso de la topología de dos routers.

Se establece el diseño para los diferentes escenarios que maneja el cliente, un diseño para el centro de datos, uno para las sedes nacionales, para las sedes principales y finalmente el diseño de las tiendas. Esto permite adaptar la solución a los diferentes escenarios del cliente.

El diseño de calidad de servicio permite establecer la prioridad necesaria para tráfico sensible al retardo, jitter y pérdida de paquetes y por lo tanto mejorar la experiencia del usuario final.

Al realizar el enrutamiento basado en aplicación y establecer umbrales según sus necesidades de cada una de ellas se garantiza una mejora en la experiencia de los usuarios finales en el uso de todas las aplicaciones.

El diseño utilizando una controladora centralizada permite realizar cambios y aprovisionar servicios de forma mucho más rápida y eficiente, generando una disminución en las tareas repetitivas que debe realizar el departamento de IT.

Con MPLS, los proveedores tenían un interés comercial en minimizar la latencia, en parte optimizando su enrutamiento. De lo contrario, los clientes se sentirían molestos, lo que aumentaría su insatisfacción. En última instancia, los proveedores verían una mayor

rotación de clientes y pérdidas de ingresos. Pero los proveedores de la red troncal de Internet buscan maximizar el valor de sus redes, no el rendimiento de ninguna aplicación.

A menudo, puede tener más sentido descargar el tráfico en la red troncal de otro proveedor que trasladarlo por una ruta más rápida a lo largo de su propia red. Así es como terminas con el "enrutamiento"demasiado familiar para los ingenieros de Internet.

Gran parte de los problemas con el enrutamiento de Internet ocurren en el núcleo de la red. Cuando el tráfico se mantiene dentro de la región, el impacto del núcleo de Internet a menudo se minimiza. Una diferencia del 20% en una ruta de 20 ms es insignificante para la mayoría de las aplicaciones. Pero la misma variación en una ruta de 200 ms puede significar la diferencia entre una llamada de voz clara y una ininteligible.

Bibliografia

[1] Párraga Granados, Martin Ángel, *Gestión Eficaz de Proyectos de Telecomunicaciones e Infraestructuras Críticas* 1ª ed. Español: ISBN 9788490522141, 2019, Páginas 264

[2] Molina García Pardo, José María, Pascual García,Martines Inglés,Maria Teresa, *Problemas Resueltos en los sistemas de Comunicación* 2ª ed. Español: ISBN 9788416325320, 2017

[3] CVU – Cisco Virtual Update, *Cisco SD-WAN* 1ª ed. Español: 2018, Páginas 55

[4] Cisco Validated Design, *Cisco SD-WAN Design Guide* 1ª ed. Inglés: 2018, Páginas 31

[5] Cisco Validated Design, *Cisco Services for SD-WAN* 1ª ed. Inglés:Seamlessly transition to SD-WAN with Cisco's expert guidance, 2018, Páginas 4

[6] Cisco Validated Design, *Cisco SD-WAN Deployment Guide* 1ª ed. Inglés: 2018, Páginas 253

[7] Tom CofService provider product sales specialist , *Cisco SD-WAN* 1ª ed. Inglés: ISBN 9788447218189, 2018, Páginas 9

[8] Papán Somet, F. Javier, *Problemas de Comunicaciones Digitales* 4ª ed. Español: ISBN 9788447218189, 2016, Páginas 408

[9] Herrera, E, *Introducción a las telecomunicaciones modernas.* 3ª ed. Sevilla: Limusa, 2006

[10] Mc Graw Hill, *Fundamentos de redes* 1ª ed. Madrid: Hallberg, B., 2006

[11] Barcia, N., *Redes de computadoras y arquitectura de comunicaciones* 4ª ed. Valencia: Pearson, 2005

[12] Derfler, F., *Como funcionan las redes* 2ª ed. Valencia: Anaya Multimedia, 2006

ANEXO I

ANEXO

Listagem I.1: HBR1 Configuration

```
1
2  Current configuration : 7360 bytes
3  ! Last configuration change at 17:23:54 UTC Sun Jun 2 2019
4  version 16.10
5  service timestamps debug datetime msec
6  service timestamps log datetime msec
7  service call-home
8  platform qfp utilization monitor load 80
9  no platform punt-keepalive disable-kernel-core
10 platform console serial
11 hostname HBR-1
12 boot-start-marker
13 boot-end-marker
14 no aaa new-model
15 call-home
16  ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
17  ! the email address configured in Cisco Smart License Portal will be used as contact
       ↪ email address to send SCH notifications.
18  contact-email-addr sch-smart-licensing@cisco.com
19  profile "CiscoTAC-1"
20   active
21   destination transport-method http
22   no destination transport-method email
23 ip vrf IWAN-TRANSPORT-2
24 ip vrf WAN-TRANSPORT-1
25  rd 100:1
26 ip vrf WAN-TRANSPORT-2
27  rd 100:2
28 ip dhcp pool DC
```

```
 network 192.168.0.0 255.255.255.0
 default-router 192.168.0.1
login on-success log
subscriber templating
multilink bundle-name authenticated
domain ONE
 vrf default
  border
   source-interface Loopback789
   master 10.60.4.4
crypto pki trustpoint TP-self-signed-1840273319
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1840273319
 revocation-check none
 rsakeypair TP-self-signed-1840273319
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
crypto pki certificate chain TP-self-signed-1840273319
 certificate self-signed 01
  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  ...

  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
       quit
license udi pid CSR1000V sn 9VG6JUVEGXV
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
interface Loopback789
 ip address 10.60.4.2 255.255.255.255
 ip pim sparse-mode
interface Tunnel10
 bandwidth 300000
 ip address 10.60.0.1 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication cisco123
 ip nhrp network-id 101
 ip nhrp redirect
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source GigabitEthernet2
 tunnel mode gre multipoint
 tunnel key 101
 tunnel vrf WAN-TRANSPORT-1
 domain ONE path MPLS1 path-id 10
```

```
interface Tunnel11
 bandwidth 150000
 ip address 10.60.2.1 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication cisco123
 ip nhrp network-id 102
 ip nhrp redirect
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source GigabitEthernet3
 tunnel mode gre multipoint
 tunnel key 102
 tunnel vrf WAN-TRANSPORT-2
 domain ONE path INET1 path-id 11
interface GigabitEthernet1
 ip address 10.230.6.3 255.255.255.0
 negotiation auto
 no mop enabled
 no mop sysid
interface GigabitEthernet2
 ip vrf forwarding WAN-TRANSPORT-1
 ip address 10.168.73.222 255.255.255.192
 negotiation auto
 no mop enabled
 no mop sysid
interface GigabitEthernet3
 ip vrf forwarding WAN-TRANSPORT-2
 ip address 200.0.0.1 255.255.255.248
 negotiation auto
 no mop enabled
 no mop sysid
interface GigabitEthernet4
 ip address 192.168.0.1 255.255.255.0
 negotiation auto
 no mop enabled
 no mop sysid
router eigrp 100
 network 10.60.0.0 0.0.1.255
 network 10.60.2.0 0.0.1.255
 network 10.60.4.2 0.0.0.0
 network 10.230.6.0 0.0.0.255
 network 192.168.0.0
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
no service-routing capabilities-manager
```

```
control-plane
line con 0
 stopbits 1
line vty 0 4
 login
end
```

ANEXO II

ANEXO 2

Listagem II.1: HBR2 Configuration

```
Current configuration : 7226 bytes
! Last configuration change at 17:24:26 UTC Sun Jun 2 2019
version 16.10
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
platform console serial
hostname HBR-2
boot-start-marker
boot-end-marker
no aaa new-model
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact
     ↪ email address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
  active
  destination transport-method http
  no destination transport-method email
ip vrf IWAN-TRANSPORT-1
 rd 100:1
ip vrf IWAN-TRANSPORT-2
 rd 100:3
login on-success log
subscriber templating
multilink bundle-name authenticated
```

```
domain ONE
 vrf default
  border
   source-interface Loopback789
   master 10.60.4.4
crypto pki trustpoint TP-self-signed-4033344212
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4033344212
 revocation-check none
 rsakeypair TP-self-signed-4033344212
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
crypto pki certificate chain TP-self-signed-4033344212
 certificate self-signed 01
  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 050
  ...
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
       quit
license udi pid CSR1000V sn 9V1OHJMYH13
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
interface Loopback789
 ip address 10.60.4.3 255.255.255.255
 ip pim sparse-mode
interface Tunnel10
 bandwidth 300000
 ip address 10.60.0.56 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication cisco123
 ip nhrp network-id 101
 ip nhrp redirect
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source GigabitEthernet2
 tunnel mode gre multipoint
 tunnel key 101
 tunnel vrf IWAN-TRANSPORT-1
 domain ONE path MPLS1 path-id 20
interface Tunnel11
 bandwidth 150000
 ip address 10.60.2.56 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim nbma-mode
```

```
 ip pim sparse-mode
 ip nhrp authentication cisco123
 ip nhrp network-id 102
 ip nhrp redirect
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source GigabitEthernet3
 tunnel mode gre multipoint
 tunnel key 102
 tunnel vrf IWAN-TRANSPORT-2
 domain ONE path INET1 path-id 21
interface GigabitEthernet1
 ip address 10.230.6.2 255.255.255.0
 negotiation auto
 no mop enabled
 no mop sysid
interface GigabitEthernet2
 ip vrf forwarding IWAN-TRANSPORT-1
 ip address 10.168.73.223 255.255.255.192
 negotiation auto
 no mop enabled
 no mop sysid
interface GigabitEthernet3
 ip vrf forwarding IWAN-TRANSPORT-2
 ip address 200.0.0.2 255.255.255.248
 negotiation auto
 no mop enabled
 no mop sysid
interface GigabitEthernet4
 no ip address
 shutdown
 negotiation auto
 no mop enabled
 no mop sysid
router eigrp 100
 network 10.60.0.0 0.0.1.255
 network 10.60.2.0 0.0.1.255
 network 10.60.4.3 0.0.0.0
 network 10.230.6.0 0.0.0.255
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
no service-routing capabilities-manager
control-plane
line con 0
 stopbits 1
line vty 0 4
 login
end
```

ANEXO III

ANEXO 3

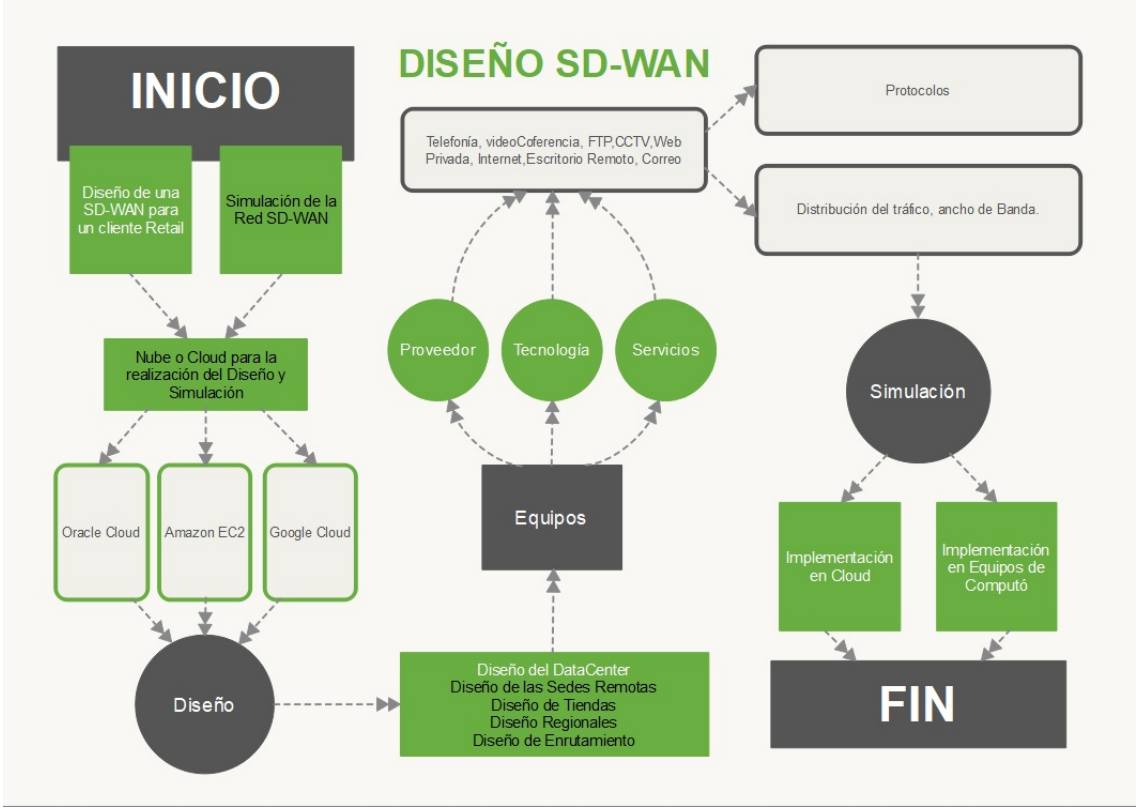


Figura III.1: Algoritmo para el Diseño de la SD-WAN