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

PRESENTADO POR:

JOAN SEBASTIAN QUINTERO CEBALLOS

JOSE ARMANDO SON

ASESOR TÉCNICO DE PROYECTO:

ING. JESUS CANTILLO

UNIVERSIDAD EL BOSQUE

FACULTAD DE INGENIERÍA ELECTRÓNICA

ESPECIALIZACIÓN EN DISEÑO DE REDES TELEMATICAS

BOGOTÁ, COLOMBIA

[Fecha de última actualización del documento]

# RESUMEN

Escribir el resumen del documento

# PALABRAS CLAVE

Basandose en el thesaurus IEEE definir el conjunto de palabras separadas por comas que un buscador identificará para encontrar su documento.

# ABSTRACT

Traducción del resumen al idioma Inglés.

# KEYWORDS

Traducción de las palabras clave al idioma Inglés

Tabla de contenido

[**1.**](#_30j0zll) **Título 3**

[**2.**](#_1fob9te) **Introducción 3**

[**3.**](#_3znysh7) **Descripción general del proyecto 3**

[**3.1**](#_2et92p0) **Definición del problema 3**

[**3.2**](#_tyjcwt) **Aspectos a solucionar 3**

[**3.3**](#_3dy6vkm) **Solución propuesta 3**

[**4.**](#_1t3h5sf) **Estado del arte 3**

[**5.**](#_4d34og8) **Glosario de términos 3**

[**6.**](#_2s8eyo1) **Justificación 3**

[**7.**](#_17dp8vu) **Objetivos 3**

[**7.1.**](#_3rdcrjn) **General. 3**

[**7.2.**](#_26in1rg) **Específicos 3**

[**8.**](#_lnxbz9) **Requerimientos 3**

[**8.1**](#_35nkun2) **Requerimientos funcionales 4**

[**8.2**](#_1ksv4uv) **Requerimientos no funcionales 4**

[**9.**](#_44sinio) **Metodología 4**

[**10.**](#_2jxsxqh) **Capítulos de desarrollo 4**

[**11.**](#_z337ya) **Resultados 4**

[**12.**](#_3j2qqm3) **Discusión 4**

[**13.**](#_1y810tw) **Conclusiones 4**

[**14.**](#_4i7ojhp) **Documentación de Referencia 4**

[**15.**](#_2xcytpi) **Anexos 4**

Incluir Índice de Figuras y de Tablas si se utilizan dentro del documento

# 1. Título

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

# 2. Introducción

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 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.

# 3. Descripción general del proyecto

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

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

# 3.1 Definición del problema

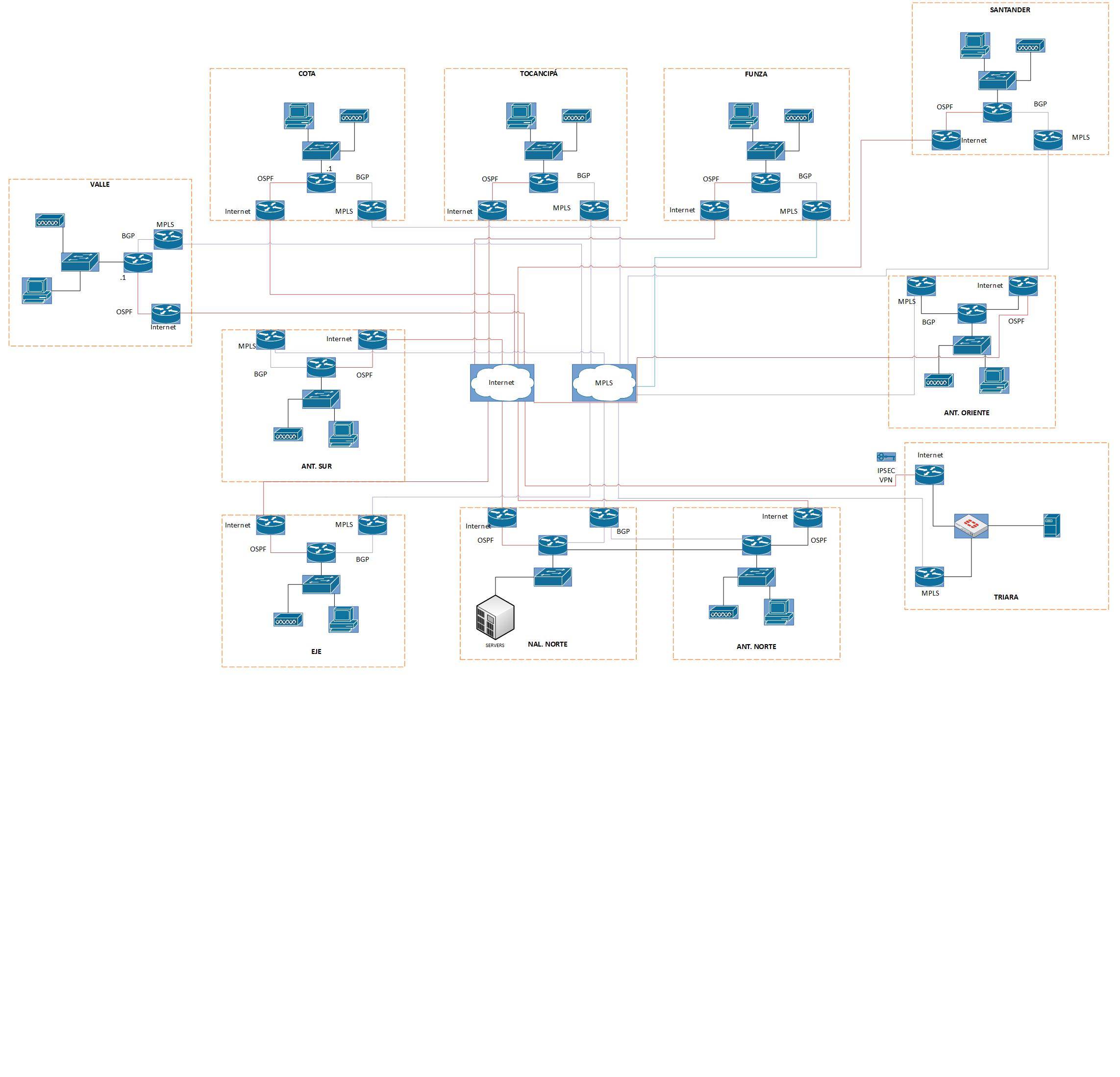
Un cliente del sector *retail* como parte de su proyecto de renovación tecnológica se encuentra migrando sus servicios y aplicaciones internas a la nube, el cliente es consciente de que esta migración generaría mucha mayor carga sobre sus enlaces WAN, y se consideran inviables las ampliaciones de todos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

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

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

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

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



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

Por otro lado la causa de la lentitud en la configuración de nuevas políticas o servicios de red es el hecho de que los cambios se realizan manualmente, es por este motivo que dentro de la solución se propondrá el hecho de que haya gestión centralizada desde la controladora SD-WAN. En cuanto a los problemas de seguridad presentados se incluye dentro de la solución el cifrado de los túneles que interconectan tanto las sucursales como las oficinas regionales, de manera que el tráfico deje de cursar en texto claro por la red pública.

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

# 3.2 Aspectos a solucionar

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

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

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

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

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

# 3.3 Solución propuesta

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

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

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

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

* **Balanceo de tráfico inteligente**: el cliente requiere que sea utilizado el ancho de banda de los dos canales que tiene en cada sede para soportar la cantidad de tráfico que implica su migración de servicios a la nube, este balanceo debe ser inteligente de manera que se cumpla con los requisitos de retardo, jitter y pérdida de paquetes que requiere cada aplicación de la compañía, si estos criterios no se cumplen bajo uno de los canales el tráfico debe ser enviado por el otro de forma automática.
* **Seguridad:** Al tratarse de tráfico transaccional el cliente requiere que el transporte de datos cumpla con todos los requisitos de seguridad en la compañía en cuanto a la Integridad, privacidad y disponibilidad.
* **Disponibilidad:** Se requiere que el servicio tenga una alta disponibilidad y que esta se priorice para las aplicaciones críticas del cliente, el esquema de alta disponibilidad debe ser automático.
* **Aprovisionamiento ágil:** Se requiere que en caso de requerir cambios generales a nivel de red WAN estos no tengan que ser configurados de forma manual en cada una de las sedes, sino que por el contrario puedan configurarse políticas de forma centralizada y enviarse las configuraciones de forma masiva para agilizar la implementación de cambios.
* **Independencia del transporte:** Se requiere una solución que no dependa de la forma de transporte, que pueda establecerse por Internet o por MPLS sin inconvenientes y que si se decide cambiar de tecnología esto sea transparente para el servicio.
* **Adecuado para nube híbrida:** La solución propuesta debe cumplir los requerimientos tanto para las aplicaciones que se encuentran en la nube como para aquellas que aún están en el datacenter del cliente, y debe realizar balanceo y dar prioridad a las aplicaciones.
* **Calidad de servicio:** El diseño debe tener unas políticas de QoS que garanticen el correcto funcionamiento de todas las aplicaciones que cursan por la red, que incluyen tráfico de voz y video.
* **Conexiones dinámicas:** El diseño propuesto debe utilizar tecnologías que 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.

# 4. **Estado del arte**

**4.1 Marco de referencia teórico**

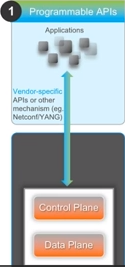
**4.1.1 Conceptos generales de SD-WAN**

SD-WAN es una aplicación específica de la tecnología de redes SDN aplicada a las conexiones WAN utilizadas para conectar redes empresariales sobre grandes distancias geográficas suministrando una arquitectura *overlay* moviendo el plano de control a la nube, sea esta pública o privada. Según SDN central, SDN puede definirse como un enfoque de software 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 customización optimización e innovación.

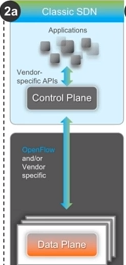
**4.1.2 Modelos de programabilidad de red**

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

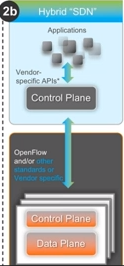
* APIs programables: la primera aproximación a SDN es la inclusión de API dentro de los dispositivos de red, en este modelo sin embargo no hay un desacoplamiento de los planos de datos y control y estos siguen estando dentro del dispositivo de red, los equipos de red se comunican directamente con las aplicaciones a través de APIs u otro mecanismo como NETCONF.



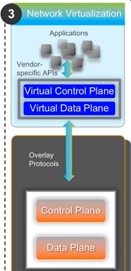
* SDN Clásico: En este modelo el plano de control y el plano de datos si se encuentran desacoplados completamente, el plano de control se comunica con las aplicaciones mediante APIs y con el plano de datos mediante Openflow u otro protocolo propietario.



* SDN híbrido: Funciona bajo el mismo concepto que la arquitectura clásica de SDN, con la diferencia de que en este caso los dispositivos mantienen su propio plano de control pero siguen comunicándose con las aplicaciones a través de Openflow mediante una controladora que mantiene el plano de control de todos los equipos.



* 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.

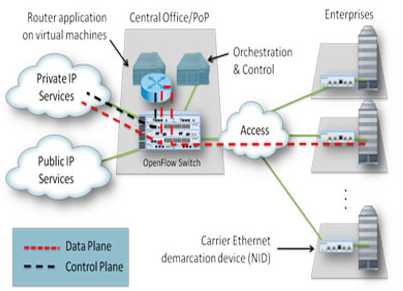
****

**4.1.3 NFV**

**<https://www.sdxcentral.com/nfv/definitions/whats-network-functions-virtualization-nfv/>**

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

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

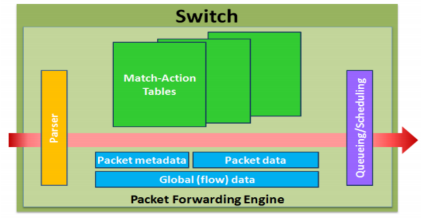


NFV se diferencia de SDN tradicional en cuanto a que en lugar de desacoplar como tal el plano de control se enfoca en las funciones de red como tal, pero cumple el mismo objetivo de obtener una infraestructura de red que sea más ágil y escalable.

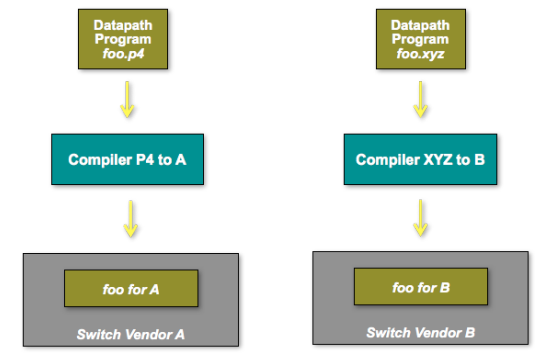
**4.1.4 Openflow**

Es un protocolo utilizado para suministrar una interfaz abierta para controlar la conectividad y los flujos de dicha conectividad dentro de una red SDN, 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. https://www.opennetworking.org/technical-communities/areas/specification/open-datapath/

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



Cada uno de estos programas de datapath es posteriormente 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.

****

**<https://www.opennetworking.org/technical-communities/areas/specification/open-datapath/>**

**4.1.5 NETCONF**

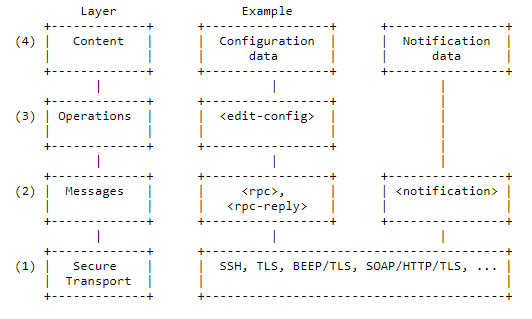
https://tools.ietf.org/html/rfc6241

https://tools.ietf.org/html/rfc6242

El protocolo se encuentra definido por el estándar RFC6241 de la IETF y suministra mecanismos para instalar, manipular y eliminar configuración en dispositivos de red utilizando el formato XML.

NETCONF define un mecanismo simple mediante el cual un dispositivo obtiene una API, esto con el objetivo de que las aplicaciones utilicen dicha API para enviar y recibir configuraciones desde y hacia los dispositivos de red, esto utilizando el paradigma RPC de forma que el cliente codifique un RPC en formato XML y lo envíe a un servidor, quien responderá con otro XML codificado.

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



1. La 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.
2. La capa de mensajes provee un mecanismo de entramado independiente del transporte para la codificación de RPC y notificaciones.
3. La capa de operaciones define un set de operaciones básicas de protocolos invocados como métodos RPC con parámetros en codificación XML.

**4.1.6 Modelos de datos**

**YANG**

<https://www.ietf.org/rfc/rfc7223.txt>

https://tools.ietf.org/html/rfc6020

Es un lenguaje de modelado de datos que se utiliza para modelar datos de estado y configuración del protocolo NETCONF y se encuentra definido bajo el RFC 6020 de la IETF, YANG modela la organización jerárquica de los datos como un árbol y provee una descripción clara de cada nodo así como su relación con otros nodos.

YANG define cuatro tipos de nodo para el modelado de datos:

Nodo leaf: Contiene datos simples como enteros o strings, contiene un tipo de valor particular y no tiene nodos hijos.

Nodo leaf-list: es una secuencia de nodos leaf, en donde cada uno tiene su valor particular.

Nodo contenedor: Es utilizado para agrupar nodos relacionados en un sub arbol, 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 YANG.

rpc activate-software-image {

input {

leaf image-name {

type string;

}

}

output {

leaf status {

type string;

}

}

}

Un módulo YANG puede ser traducido a una sintaxis alternativa basada en XML conocida como YIN, YIN y YANG contienen información equivalente utilizando una sintaxis diferente. Utilizando la notación de YIN los desarrolladores pueden representar modelos YANG en XML, y por tanto utilizar cualquiera de las múltiples herramientas basadas en XML para realizar filtrado y validación de datos, generación de código automático y documentación.

En el caso de las interfaces, existe un estándar bajo el RFC 7223 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:

+--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

+--ro out-broadcast-pkts? yang:counter64

+--ro out-multicast-pkts? yang:counter64

+--ro out-discards? yang:counter32

+--ro out-errors? yang:counter32

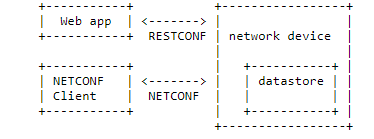
**4.1.x RESTful APIs**

**4.1.x RESTCONF**

**<https://tools.ietf.org/html/rfc8040>**

Restconf es un protocolo basado en 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, hay dispositivos que soportan los dos protocolos en conjunto de la siguiente manera:



Al estar basado en HTTP las operaciones CRUD de RESTCONF se realizan mediante los métodos tradicionales, como los son los siguientes:

GET:

POST:

PUSH:

PATCH:

DELETE:

RESTCONF requiere de HTTP para su transporte y requiere soporte de TLS para su transporte, aunque no se especifica que versión específica se requiere para RESTCONF si se recomienda por lo menos HTTP1.1, dado que los servidores RESTCONF deben soportar HTTPS, dichos servidores tienen que presentar un certificado dígital X509v3.

**4.2 Marco de referencia tecnológico**

La solución definida en este proyecto es el IWAN de Cisco, en el capitulo “selección de la solución” en este mismo documento se plantean las razones por las cuales se seleccionó IWAN como la mejor solución para el caso de este cliente. Por tanto este apartado estará dedicado a las tecnologías que componen la solución de IWAN.

**4.2.1 IWAN**

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

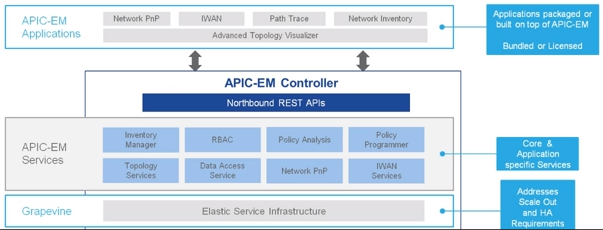


Tomado de<https://www.cisco.com/c/dam/global/es_mx/assets/iwan/pdfs/aag_iwan_spa.pdf>

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

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

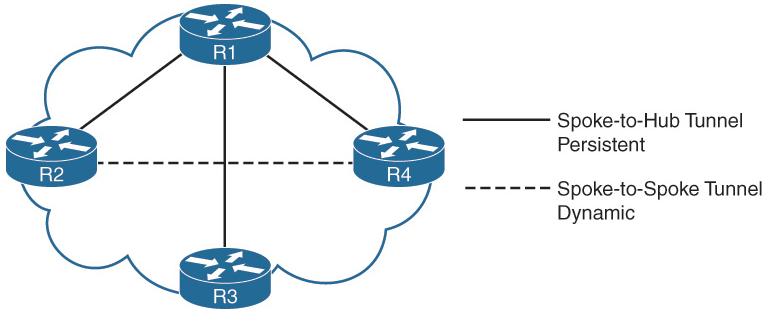
La controladora SDN que utiliza esta tecnología se denomina APIC-EM, esta controladora no solamente cumple la función de plano de control sino que también contiene aplicaciones de red embebidas que aprovechan la naturaleza centralizada de la controladora, entre esas aplicaciones se encuentra IWAN, que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



Una de las mayores ventajas de esta controladora es que no necesita de equipos de red especiales que soporten los protocolos de SDN, aunque esto último es lo recomendado el APIC-EM trae las ventajas de SDN sin requerir de una gran inversión en cambio de equipos de red, lo que lo hace una opción bastante atractiva para una compañía que quiera empezar a adentrarse en la programabilidad de la red sin requerir una inversión inicial tan fuerte.

**4.2.2 DMVPN**

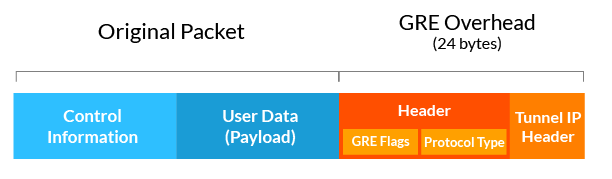
DMVPN(Dynamic Multipoint VPN) es la solución de transporte propietaria de Cisco que hace parte de la solución de IWAN, es una solución de overlay en donde las ubicaciones remotas establecen un túnel estático hacia una ubicación central(hub) y establece túneles de manera dinámica entre diferentes ubicaciones 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 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 imagen muestra el comportamiento dinámico de DMVPN.



DMVPN utiliza diversas tecnologías para lograr este objetivo, las más relevantes se enuncian a continuación.

* túneles mGRE: mGRE es un protocolo de entunelamiento capaz de transportar múltiples protocolos como IPv4, IPv6 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 GRE tradicionales es que mGRE puede conectar más de 2 dispositivos utilizando el mismo túnel.

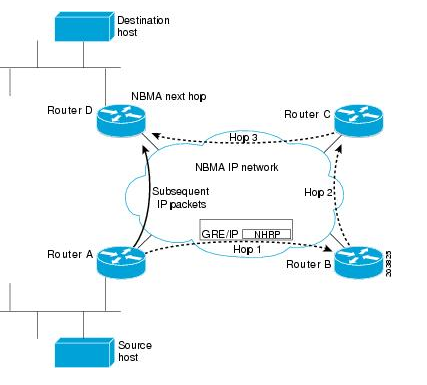
los túneles se forman agregando un encabezado IP externo al paquete con la información IP fuente y destino correspondiente a las interfaces fuente y destino del túnel como lo muestra la figura x.



tomado de imperva incapsula

* NHRP: Este protocolo se encuentra definido bajo el RFC 2332, y es utilizado para que un equipo fuente determine el siguiente salto hacia un destino en una red NBMA, es decir realiza una resolución de direccionamiento, similar a lo que ocurre con ARP en la resolución de dirección IP a direccion MAC. El protocolo funciona utilizando un NHS que se encarga de la resolución de direccionamiento dentro de la nube de NHRP, por su parte los equipos NHC son aquellos que realizan las peticiones de NHRP hacia el NHS.

La siguiente imagen representa el funcionamiento de NHRP en terminos generales:



<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nhrp/configuration/xe-16/nhrp-xe-16-book/config-nhrp.html>

Adicional al registro de los NHC con los NHS, NHRP tiene la capacidad de que los NHC encuentren un camino más corto sobre la infraestructura o formar uno mediante una conexión virtual directamente hacia otro NHC, esta habilidad es utilizada en DMVPN para establecer una topología full mesh sin todo el trabajo administrativo que esto conlleva.

**4.2.3 WAAS**

Por su parte WAAS es una tecnología propietaria de Cisco que se encarga de optimizar el tráfico TCP en la red con el principal objetivo de disminuir la utilización de ancho de banda utilizando algoritmos de compresión para este fin. Son varias las tecnologías que reúne WAAS para la optimización del ancho de banda a nivel WAN, de ellas vale la pena resaltar las 3 más relevantes.

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

**4.2.4 EIGRP**

EIGRP 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.

EIGRP 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 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.

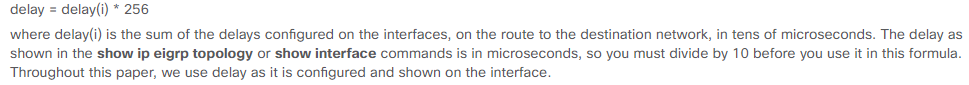
Para distribuir las rutas a través de la red EIGRP utiliza actualizaciones de enrutamiento incrementales y no periódicas, esto quiere decir que solo se envía un *update* cada vez que hay un cambio en la red. EIGRP depende por lo tanto de sus relaciones de vecinos para propagar de manera confiable los cambios en la tabla de enrutamiento a través de la red. Esta relación de vecindad se forma cuando dos routers corriendo EIGRP ven los paquetes Hello del otro equipo, estos paquetes son enviados cada 5 segundos.

EIGRP 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 no es puramente el ancho de banda sino que está caracterizado bajo la ecuación 1:



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



* Load: el porcentaje de carga(utilización) que tiene el enlace
* Reliability: valor configurable administrativamente

La ecuación para calcular la métrica de EIGRP puede apreciarse en la ecuación 3:



como puede verse en la ecuación el cálculo final de la métrica depende de los valores K, estos valores son lo que puede ser configurado por el diseñador o administrador de la red para influir en la forma como EIGRP toma la decisión del mejor camino hacia los destinos. Por defecto el protocolo utiliza los siguientes valores para las variables K.

* K1=1
* K2=0
* K3=1
* K4=0
* K5=0

Por lo que reemplazando estos valores en la fórmula se obtiene la ecuación 4 para el cálculo de la métrica en EIGRP al utilizar los valores K por defecto:

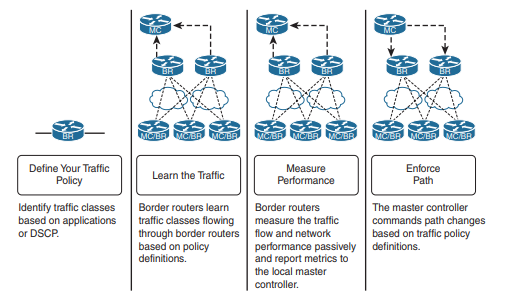
Por lo que por defecto EIGRP solamente utiliza los valores de ancho de banda y retardo para el cálculo de la métrica compuesta, a menos que se especifiquen valores K diferentes a los que utilizan los routers por defecto.

**4.2.1 PfR**

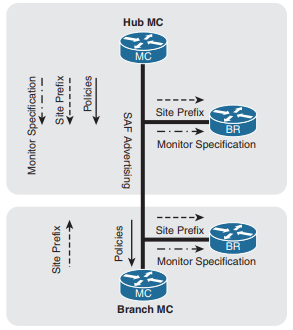
PfR es parte integral de la solución de IWAN, y es la mayor responsable de la inteligencia de la solución, su objetivo es mejorar el rendimiento y disponibilidad de las aplicaciones realizando una optimización del control de enrutamiento basándose en los requerimientos de cada aplicación. PfR monitorea 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. La imagen X 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, los 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 imagen detalla este flujo de información entre los elementos de IWAN.



https://www.cisco.com/c/en/us/td/docs/app\_ntwk\_services/waas/waas/v413/configuration/guide/cnfg/intro.html

Programming and Automating cisco Networks

Cisco Intelligent WAN (IWAN), Cisco Press

# 5. **Glosario de términos**

# 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.

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 a la nube con SD-WAN, la tabla X 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.

|  |  |  |  |
| --- | --- | --- | --- |
| **Tipo de oficina** | **Tienda** | **Regional** | **Oficina Nacional** |
| **Usuarios promedio** | 3 | 25 | 60 |
| **Sesiones de video simultaneas** | 1 | 8 | 20 |
| **Tráfico de datos actual** | 5MB | 10MB | 20MB |
| **BW servicio actual** | 10MB | 7MB | 14MB |
| **BW requerido** | 9MB | 25MB | 84MB |
| **Costo actual** | 221.741 | 1'260,741 | 1'803,563 |
| **Costo mensual red legacy** | 221.741 | 3'607,126 | 6'782,000 |
| **Costo mensual con SD-WAN** | 221.741 | 1'842,102 | 3'972,361 |

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.

# 7. Objetivos

# 7.1. **General.**

# 7.2. **Específicos**

# 8. Requerimientos

# 8.1 Requerimientos funcionales

# 8.2 Requerimientos no funcionales

# 9. Metodología

# 10. Etapa Inicial del diseño

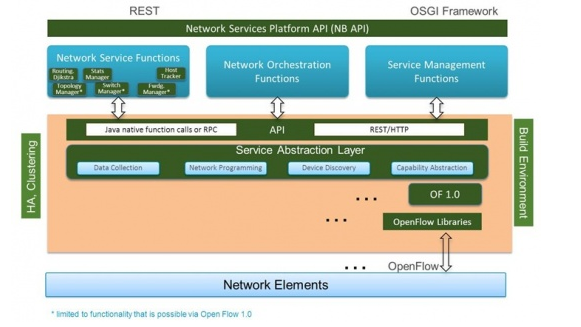
10.1 Selección de proveedor y tecnología.

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

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

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

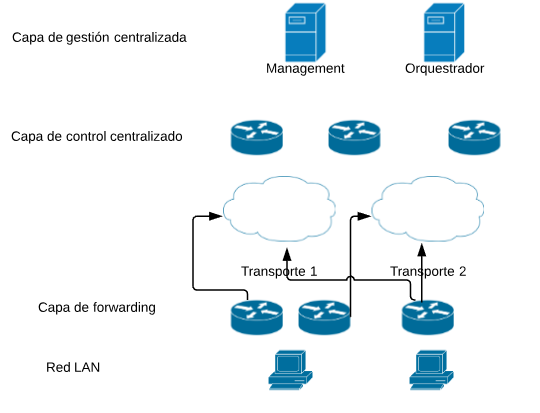
La primera opción que se consideró fue utilizar OpenDayLight como controlador SD-WAN ya que este utiliza totalmente software abierto para su funcionamiento, esta plataforma utiliza protocolos abiertos como Openflow y Netconf, la figura X muestra la arquitectura de esta solución:



<https://wiki.opendaylight.org/view/OpenDaylight_Controller:Architectural_Framework>

Esta arquitectura aunque al utilizar protocolos estándar permite que se conecte cualquier elemento de red que hable Openflow tiene la limitante de que los equipos de red tradicionales, incluyendo los que tiene el cliente no soportan OpenFlow por defecto, y por tanto los enrutadores que utiliza el cliente hoy en día no se integran con esta arquitectura de SDN, lo que significa que implementar esta solución requeriría cambiar todos los enrutadores por unos que soporten OpenFlow.

Se tuvieron en cuenta también soluciones de varios fabricantes para el proyecto, más precisamente las soluciones SD-WAN de Nokia(Nuage), Cisco(Viptela), vmware(Velo cloud) y Silverpeak, estas son las soluciones que dominan el mercado a la fecha de elaboración de este documento. Todas estas son soluciones SDN que desagregan completamente los planos de control y gestión de los enrutadores en las sedes Branch y los centralizan en controladoras y servidores de gestión, aunque todas las soluciones mencionadas utilizan protocolos diferentes su arquitectura y funcionamiento es muy similar.



Dentro de cada una de estas opciones se desagregan las capas de control y de gestión en un sitio centralizado, normalmente un centro de datos, y en los branch solamente se tiene la capa de envío de datos o forwarding, estas sedes remotas se comunican entre ellas en todos los casos mediante túneles que se forman automáticamente gracias al plano de control centralizado, sin embargo la tecnología con la que se forman dichos túneles y con la que se envía la información de enrutamiento del plano de control al plano de forwarding cambia considerablemente entre todas las soluciones, y por tanto son incompatibles entre ellos. Las siguientes son las tecnologías que cada una de las soluciones mencionadas utiliza para la comunicación contra los routers de borde:

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

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

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

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

10.2 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Proceso** | **IWAN** | **tiempo** | **Solución actual** | **tiempo** |
| Aprovisionamiento tienda nueva | Se ingresan datos básicos sobre el APIC-EM | 30 min | Se configura túnel en la tienda y en la regional y enrutamiento hacia internet y hacia las tiendas | 3 Horas |
| Aprovisionamiento regional nueva | Se ingresan datos básicos sobre el APIC-EM | 30 min | Se deben configurar túneles IPSEC contra todas las demàs regionales, ademàs de configurar protocolos de enrutamiento dinàmico contra el proveedor y contra las demàs regionales por medio del canal de internet | 2 Dìas |
| Cambio general de políticas | Se configura script y se agenda para ser aplicado en todos los equipos | 1 hora | Se ingresa equipo por equipo a realizar los cambios manualmente | 4 Meses |

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.

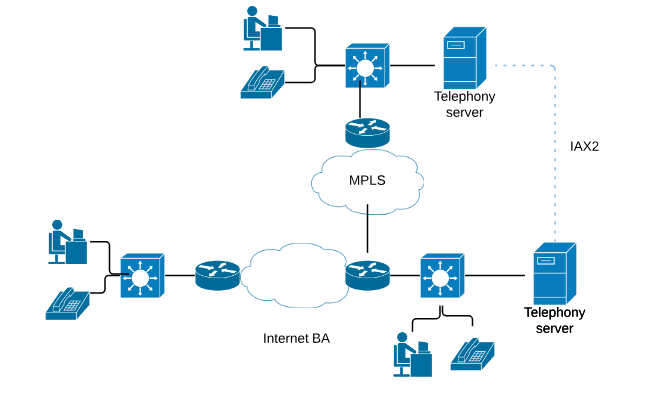
|  |  |  |
| --- | --- | --- |
| **Característica** | **IWAN** | **Solución Legacy** |
| Redundancia | 4 puntos concentradores de la solución, principal y backup de intranet y principal y backup de internet | 1 único punto de falla, si el internet de la regional cae, cae la conexión de todas las tiendas 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 |

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

10.3 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 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.



* 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.
* 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:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Aplicación** | **Bandwidth** | **Delay** | **Jitter** | **Packet loss** | **Description** |
| **Telefonía** | 80kbps per call | 150ms max | 30ms max | 1% max | Mission-critical |
| **Videoconferencia** | 3.2Mbps per conference | 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 |

[<http://www.ciscopress.com/articles/article.asp?p=471096&seqNum=6>]

10.4 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.

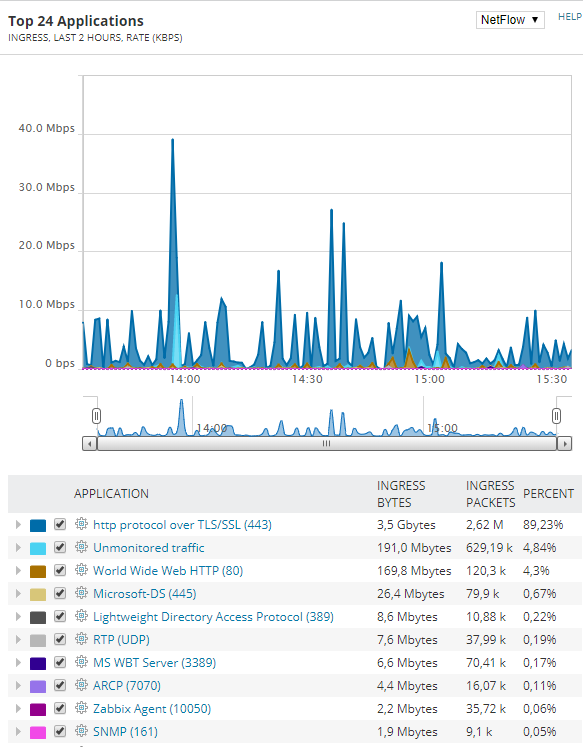
Se realiza un análisis del consumo actual de ancho de banda del cliente utilizando las herramientas de monitoreo disponibles y se obtienen los siguientes datos de consumo para cada una de las 11 sedes regionales y nacionales:

|  |  |  |
| --- | --- | --- |
| **Sede** | **Consumo promedio** | **BW contratado** |
| **Nacional Medellin** | 14Mbps | 14Mbps |
| **Antioquia Norte** | 20Mbps | 15Mbps |
| **Nacional Tocancipá** | 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 |

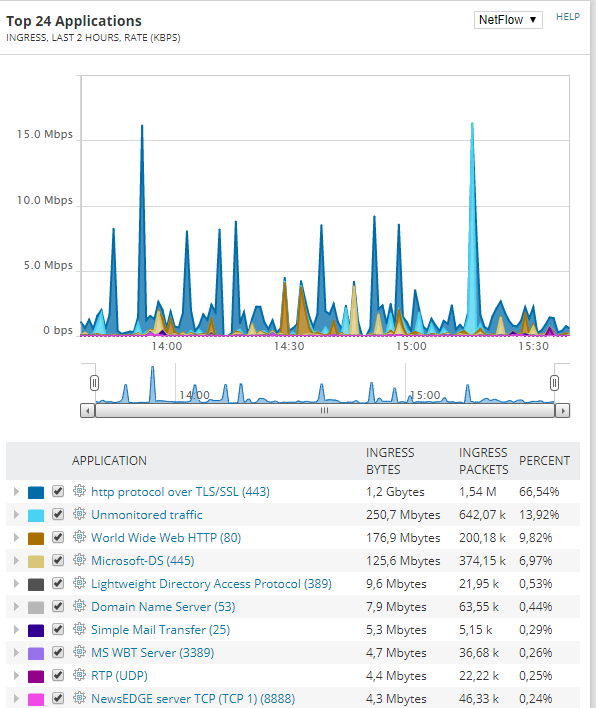
Con estos datos se puede concluir que ya hay saturación en las sedes, y que por tanto la solución actual está presentando retardos y pérdidas de paquetes en la comunicación.

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:

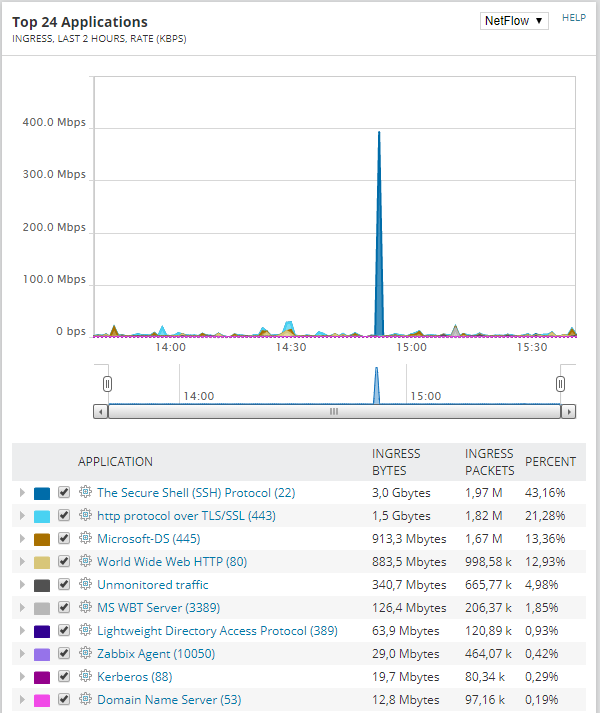
Sede nacional Tocancipá:



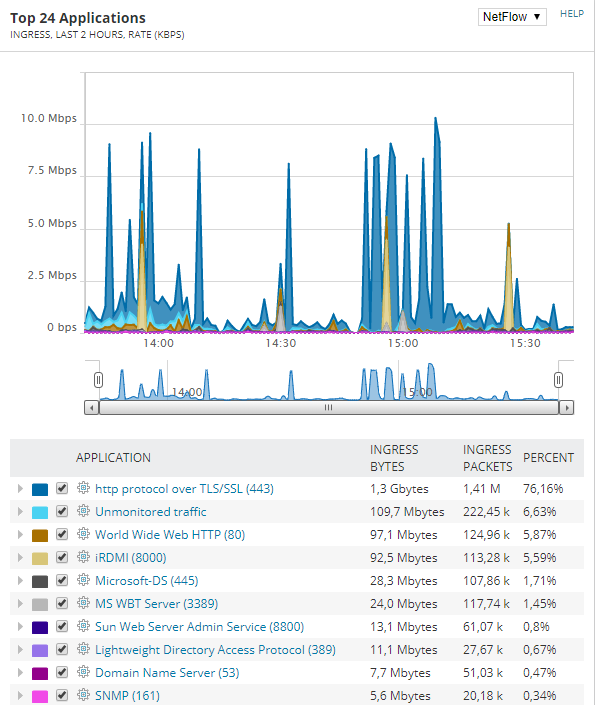
Sede Nacional Medellin:



Sede Regional Antioquia Norte:



Sede Regional Valle



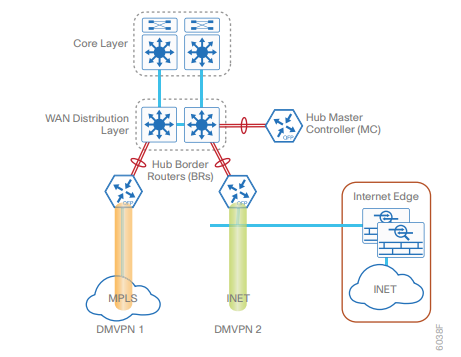
De estos resultados se concluye que para todos los casos el Tráfico Web representa la gran mayoría del tráfico que se genera tanto en las regionales como en las sedes nacionales

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:

|  |  |  |  |
| --- | --- | --- | --- |
| **Sede** | **Consumo promedio** | **BW MPLS** | **BW banda ancha** |
| Nacional Medellin | 14Mbps | 15Mbps | 20Mbps |
| Antioquia Norte | 20Mbps | 20Mbps | 50Mbps |
| Nacional Tocancipá | 20Mbps | 20Mbps | 50Mbps |
| 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 |

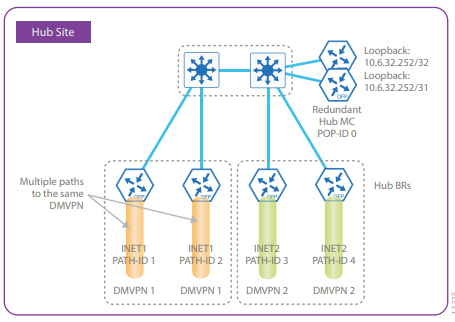
# 11. Diseño de datacenter

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.

  
[Intelligent WAN Design guide (CVD) - Septiembre 2017, pág 14 Fig 6]

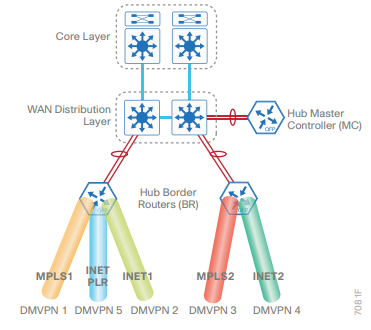
En este diseño se requiere acceso a los dos transportes desde el centro de datos, en el datacenter se encuentran los Hub Border routers que son quienes lo interconectan con las dos tecnologías de transporte y el Master controller, estos equipos estarán conectados mediante una infraestructura de switches(existente) 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:

  
[Intelligent WAN Design guide (CVD) - Septiembre 2017, pág 16 Fig 8]

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:

  
[Intelligent WAN Design guide (CVD) - Septiembre 2017, pág 20 Fig 12]

Por lo que al final el diseño utilizaría dos equipos para realizar la función de HBR, 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 el capítulo 10 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.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Aplicación** | **Bandwidth** | **Delay** | **Jitter** | **Packet loss** | **Grupo** |
| **Telefonía** | 80kbps per call | 150ms max | 30ms max | 1% max | Real Time |
| **Videoconferencia** | 3.2Mbps per conference | 150ms max | 30ms max | 1% max | Real Time |
| **FTP** | 3Mbps | tolerant | tolerant | 5% max | Business |
| **CCTV** | 2Mbps | 1s max | tolerant | 5% max | Business |
| **Web Privada** | 1Mbps | tolerant | tolerant | 5% max | Business |
| **Escritorio remoto** | 2Mbps | 200ms max | 30ms max | 3% max | Business |
| **Internet** | 1Mbps | tolerant | tolerant | 5% max | Best effort |
| **Correo** | 1Mbps | tolerant | tolerant | 5% max | Best effort |

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 resume los requerimientos de cada uno de los grupos que corresponden a los parámetros configurados en PfR.

|  |  |  |  |
| --- | --- | --- | --- |
| **Grupo** | **Delay** | **Jitter** | **Pérdida de paquetes** |
| ***Real-Time*** | 150ms | 20ms | 1% |
| ***Business-class*** | 250ms | 30ms | 2% |
| ***Best Effort*** | 500ms | N/A | 5% |
| ***Scavenger*** | 500ms | N/A | 10% |

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.

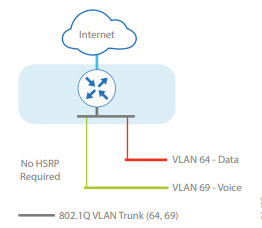
# 11. Diseño de sedes remotas

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.

11.1 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:

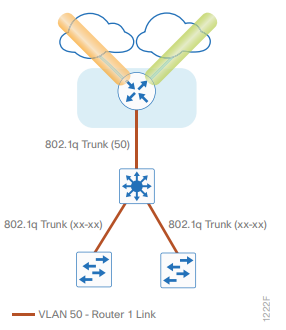


[Intelligent WAN Design guide (CVD) - Septiembre 2017, pág 25 Fig 15]

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.

11.2 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 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.



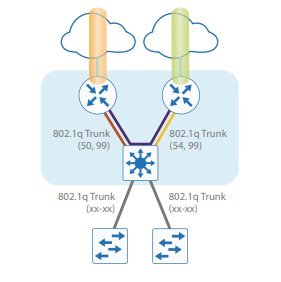
[Intelligent WAN Design guide (CVD) - Septiembre 2017, pág 26 Fig 11]

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.

11.2 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:



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.

11.3 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.

# 

# 12. 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.

12.1 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 se ilustra en la figura 12.1



Esta virtualización Anidada se realizó utilizando 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:

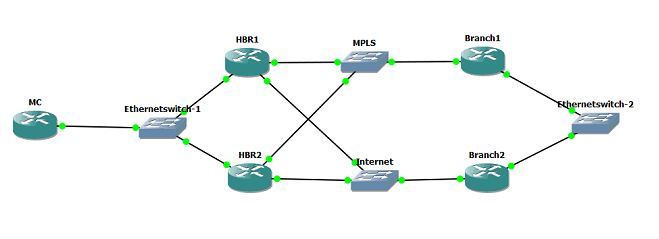
|  |  |
| --- | --- |
| Memoria RAM | 16 GB |
| CPU | intel core i7 7700HQ - 4 cores |
| Disco Duro | 1T HD + 128GB SSD |

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

12.2 Topologías y configuraciones realizadas

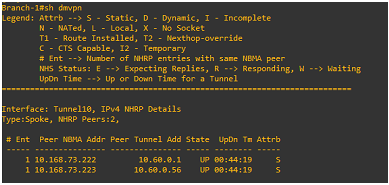
Dado el diseño planteado se realizaron pruebas con dos topologías diferentes, la primera siendo la topología de las sedes nacionales, es decir dos CPE en la sede cada uno recibiendo un hilo de fibra por un transporte diferente. Para esta topología se incluyeron un total de 5 enrutadores, dos realizando 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.

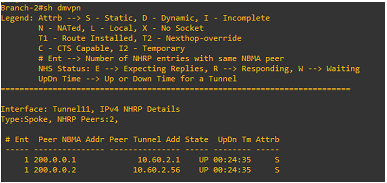
La topología configurada en GNS3 es ilustrada en la figura 12.2:



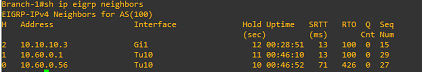
En la topología se simulan los diferentes transportes con switches, uno para la MPLS y otro para el transporte de internet, esto es una simplificación de las redes de transporte reales ya que estas son mucho más complejas, pero en este caso la simulación mantiene su validez ya que para establecer los 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.

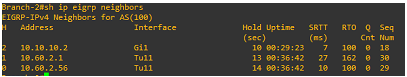
Como se mencionó anteriormente los HBR actúan como Hubs para la topología DMVPN y en esta topología los dos equipos Branch se registran contra dichos equipos como lo muestra la figura 12.3 para el Branch1 y 12.4 para el Branch2:



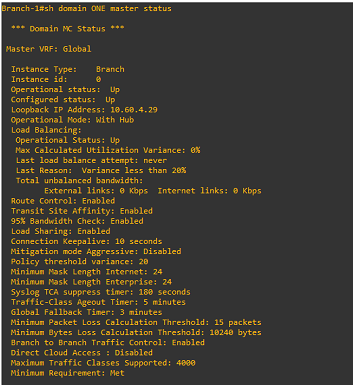


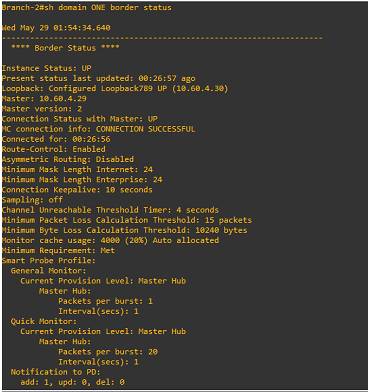
Además de estas adyacencias de DMVPN se configuró EIGRP como protocolo de enrutamiento utilizado tanto hacia los túneles como entre los routers Branch y en datacenter entre los HBR y el MC, las figuras 12.5 y 12.6 muestran los establecimientos de dichas adyacencias en el Branch.





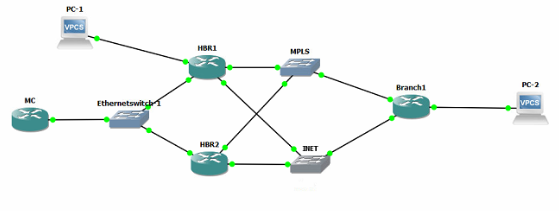
Finalmente el otro componente que hace parte de la solución de IWAN es PfR, en este caso uno de los routers (El activo en la configuración de HSRP) toma el rol de master en PFR encargándose de distribuir las políticas a los border router del Branch, las imagenes 12.7 y 12.8 muestran el registro de los dos routers con PfR.



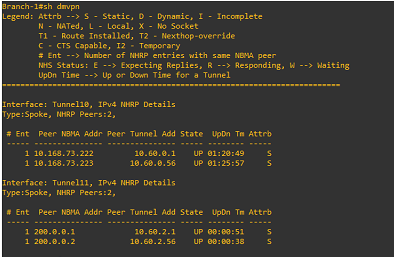


La configuración de los routers del Datacenter se encuentra en el Anexo 1, mientras que la de los routers del Branch se encuentran en el Anexo 2.

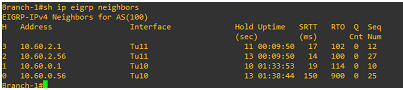
El diseño para las sedes regionales difiere de las sedes nacionales en cuanto a que por costos no se utilizan dos routers sino uno sólo con dos métodos de transporte independientes, en este sentido la distribución y configuración de la topología en datacenter se mantiene exactamente igual, el único cambio de configuración se realiza sobre el router Branch, la topología simulada para este caso es ilustrada en la figura 12.9



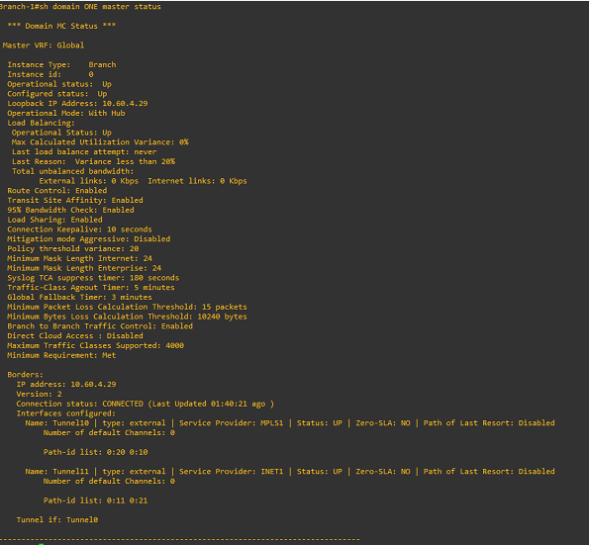
En este caso el único router branch contará con 4 adyacencias de DMVPN, dos por cada HBR, correspondientes a los diferentes tipos de transporte. Esto asegura que hay redundancia en caso de que alguno de los HBR falle o en caso de ruptura de fibra óptica para alguno de los canales de transporte. la imagen 12.10 ilustra la forma como se ve este 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 12.11.



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 12.12 muestra dicho registro.



# 12. Resultados

# 13. Conclusiones

# 14. Documentación de Referencia

# 15. Anexos