ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE UNA RED iWAN

DISEÑO DE UNA RED iWAN EMPRESARIAL

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TELECOMUNICACIONES

TIXE PAUCAR CRISTIAN JAVIER

cristian.tixe@epn.edu.ec

DIRECTOR: Msc. HERRERA MUÑOZ CARLOS ALFONSO

carlos.herrera@epn.edu.ec

Quito, marzo 2022

CERTIFICACIONES

Yo, CRISTIAN JAVIER TIXE PAUCAR declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

CRISTIAN JAVIER TIXE PAUCAR

Certifico que el presente trabajo de integración curricular fue desarrollado por CRISTIAN JAVIER TIXE PAUCAR, bajo mi supervisión.

Herrera Muñoz Carlos Alfonso
DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el producto resultante del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

CRISTIAN JAVIER TIXE PAUCAR

CARLOS ALFONSO HERRERA MUÑOZ

DEDICATORIA

A Dios, porque siempre ha estado a mi lado dándome fuerza para poder cumplir mis sueños. “Porque yo sé muy bien los planes que tengo para ustedes —afirma el Señor—, planes de bienestar y no de calamidad, a fin de darles un futuro y una esperanza.” Jeremías 29:11 (NVI)

A mi ama madre, porque gracias a su lucha y esfuerzo permanente me he convertido en la persona que soy, porque gracias a ella pude cumplir una etapa más de mi vida, porque es el mejor ejemplo de esfuerzo y lucha que puedo tener.

AGRADECIMIENTO

A Dios, porque me ha brindado vida, salud, fuerza y sabiduría para poder concluir una etapa más de mi vida “Él fortalece al cansado y acrecienta las fuerzas del débil. Aun los jóvenes se cansan, se fatigan, y los muchachos tropiezan y caen; pero los que confían en el Señor renovarán sus fuerzas; volarán como las águilas: correrán y no se fatigarán, caminarán y no se cansarán.” Isaías 40:29-31 (NVI)

A mi madre, porque me enseño que él esfuerzo y la humildad son la base para poder cumplir mis sueños, porque siempre confió en que yo podría llegar lejos, porque nunca me falto nada y siempre estuvo ahí cuando la necesitaba, por el apoyo incondicional que día a día me da, por todo su amor.

A mis hermanos Marco y Mónica, porque a pesar de las diferencias siempre han estado a mi lado, porque siempre hemos pasado momentos felices que los llevo guardados en mi corazón.

A toda mi familia por el apoyo y el amor que siempre me bridan, porque siempre confiaron en mí y me alentaban todos los días para ser mejor.

Al Msc. Carlos Herrera por la dedicación, el apoyo y las críticas constructivas que nos dio a lo largo del presente trabajo, porque más que un profesor fue un amigo.

A mis profesores por ser el pilar fundamental de esta etapa, por brindarme todos sus conocimientos y experiencia para forjarme como un buen profesional.

ÍNDICE DE CONTENIDO

RESUMEN

El presente Trabajado de Integración Curricular es el diseño de una red empresarial inteligente WAN (iWAN) con la utilización de Cisco Performance Routing (Cisco PfR) y Dynamic Multipoint VPN (DMVPN), tomando en cuenta que el enrutamiento es muy complejo, debido a la gran cantidad de trayectorias que debe cruzar un paquete antes de llegar al host destino, el diseño busca: optimizar el ancho de banda, reducir los costos de operación de las WAN sin afectar la seguridad, la confiabilidad o el rendimiento de las redes.

En el capítulo 1 se realiza el estudio de las tecnologías que intervienen en el diseño de la red iWAN empresarial.

En el capítulo 2 se realiza el estudio de DMVPN y dos de sus modelos de diseño. DMVPN es una solución que la empresa Cisco proporciona con arquitectura VPN que permite simplificar enormemente el enrutamiento, mediante el uso de un único dominio de enrutamiento que abarca ambos transportes. También se realiza el estudio de las características de Cisco PfR que permite mejorar la entrega de aplicaciones, supervisar el rendimiento de la red, controlar dinámicamente las decisiones de reenvió de paquetes y la eficiencia de la WAN.

En el capítulo 3 se realizará el diseño de la red iWAN empresarial, también se realiza la evaluación y el estudio de las diferentes fases de diseño de la red iWAN junto con sus configuraciones.

Por último, en el capítulo 4 se realiza el análisis de los resultados, también se realiza las conclusiones y recomendaciones del trabajo realizado.

PALABRAS CLAVE: iWAN, Cisco, PfR, DMVPN, Redes

ABSTRACT

The present Curriculum Integration Work is the design of an intelligent business network WAN (iWAN) with the use of Cisco Performance Routing (Cisco PfR) and Dynamic Multipoint VPN (DMVPN), taking into account that routing is very complex, due to the large number of paths that a packet must cross before reaching the destination host, the design seeks to: optimize bandwidth, reduce WAN operating costs without affecting network security, reliability or performance.

In chapter 1, the study of the technologies involved in the design of the corporate iWAN network is carried out.

In chapter 2, the study of DMVPN and two of its design models is carried out. DMVPN is a solution provided by Cisco company with VPN architecture that greatly simplifies routing by using a single routing domain that spans both transports. Cisco PfR features are also studied to improve application delivery, monitor network performance, dynamically control packet forwarding decisions, and WAN efficiency.

In chapter 3, the design of the iWAN network will be carried out, the study and evaluation of the different design phases of the iWAN business network will also be carried out along with its configurations.

Finally, in chapter 4 the analysis of the results is carried out, the conclusions and recommendations of the work carried out are also made.

KEYWORDS: iWAN, Cisco, PfR, DMVPN, Networks

1 INTRODUCCIÓN

En la actualidad, la falta de disponibilidad del ancho de banda, la latencia de la WAN y el costo de implementación no facilitan la ejecución de una red rentable y eficiente, esto evita que se pueda cumplir con los requerimientos de las organizaciones empresariales actuales. Sin embargo, a medida que la cantidad de aplicaciones y contenido que viajan a través de la red crecen exponencialmente, las organizaciones empresariales deben optimizar el costo de implementación de las redes. [1]

El enrutamiento se define como el proceso de descubrir una ruta hacia la dirección destino, esto es una problemática para el diseño de las redes WAN. En las grandes redes en enrutamiento es muy complejo, debido a la gran cantidad de destinos intermedios que debe atravesar un paquete antes de llegar a su destino. [2]

Una alternativa para mejorar el rendimiento y la eficiencia de la red es la utilización de la tecnología Cisco PfR desarrollada por la empresa Cisco. PfR es un control de ruta inteligente que selecciona una ruta en función de parámetros de rendimiento en tiempo real. Estos parámetros se receptan mediante la supervisión del rendimiento de la aplicación y el tráfico se recopila desde un centro de datos principal. Esto difiere de los protocolos de enrutamiento más clásicos, que no tienen la capacidad de monitorear problemas de rendimiento y cambiar a rutas alternativas en función de situaciones con el flujo de tráfico. PfR mide parámetros como la perdida de paquetes, el retaso, la accesibilidad y el rendimiento para encontrar la ruta de mejor rendimiento para enviar paquetes. [3]

Factores tales como, la falta de ancho de banda y la latencia de la WAN provocará un funcionamiento ineficiente de la red.

PfR permite a los administradores de red a optimizar el ancho de banda, para incluir opciones de conectividad de menor costo como el internet, perfecciona la eficiencia de la WAN y a la entrega de aplicaciones. Performance Routing controla de forma dinámica el reenvío de paquetes de datos al observar el rendimiento, el estado de ruta, el tipo de aplicación y sus políticas. [4]

Este Trabajo de Integración Curricular se enfoca en el diseño de una red empresarial iWAN utilizando Performance Routing que permita a las empresas tener la optimización de sus redes en los aspectos de, rendimiento, ancho de banda, y de esta manera tener una implementación de redes a menor costo, optimización del ancho de banda y con menor dificultad en su implementación. [5]

1.1 OBJETIVOS

Objetivo general:

- Diseñar una red iWAN empresarial utilizando Cisco Performance Routing.

Objetivos específicos:

- Estudiar dos alternativas de soluciones iWAN.
- Estudiar características de Performance Routing
- Estudiar las características del enrutamiento Cisco PfR.
- Diseñar una red iWAN empresarial utilizando DMVPN.
- Estudiar las diferentes fases del diseño DMVPN.
- Evaluar las diferentes fases de diseño DMVPN.

1.2 ALCANCE

Para el desarrollo del presente Trabajo de Integración Curricular se realiza el estudio de dos alternativas para solucionar problemas en las redes inteligentes WAN, el siguiente punto trata del estudio de características de PfR para determinar la forma de cómo mejorar el rendimiento de la red WAN, después, se realizara el estudio de las características de enrutamiento de Cisco PfR para realizar el diseño de una red inteligente WAN empresarial utilizando PfR y DMVPN, finalmente, se realizara el estudio y la evaluación de las diferentes fases del diseño de la red.

- Alternativas de soluciones iWAN: Se realiza el estudio de dos alternativas de soluciones de redes inteligentes WAN, para determinar la mejor solución que permita tener un mejor rendimiento en la red y, de esta manera, simplificar en gran medida el Routing el momento de implementar una red iWAN.
- Características de Performance Routing: Performance Routing es el control de ruta inteligente WAN, mediante el estudio de las características, se conoce la manera de como ayuda este componente a los administradores de red a poder mejorar el rendimiento de la red.
- Características del enrutamiento Cisco PfR: El estudio de las características del enrutamiento Cisco PfR, permite conocer los protocolos de enrutamiento y la manera de cómo se realiza él envió de paquetes en la red.
- Diseño de una red inteligente WAN: Se realiza el diseño de una red inteligente WAN empresarial utilizando Performance Routing.
- Fases del diseño de la red iWAN: Se realiza el estudio y la evaluación de las diferentes fases del diseño de la red iWAN diseñada.

El Trabajo de Integración curricular presenta el diseño de una red iWAN empresarial, la cual después de su estudio y diseño se concluye cuáles fueron los cambios que se realizaron para mejorar el rendimiento y la optimización de la red WAN el momento de su diseño.

1.3 MARCO TEÓRICO

1.3.1 iWAN VS WAN TRADICIONAL

En la actualidad el diseño de WAN híbridas se están volviendo cada vez más populares, debido a que permiten a las organizaciones elegir las mejores opciones de transporte para una situación particular, también pueden utilizar servicios de Internet cuando requieran más ancho de banda para requisitos de transporte de datos más grandes. Cuando las necesidades comerciales lo requieran las organizaciones pueden optar por utilizar Multiprotocol Label Switching (MPLS) que es un mecanismo de transporte de datos. Existen algunas diferencias clave entre iWAN y los diseños híbridos de WAN tradicionales, que se destacan en la Figura 1.1. [6]

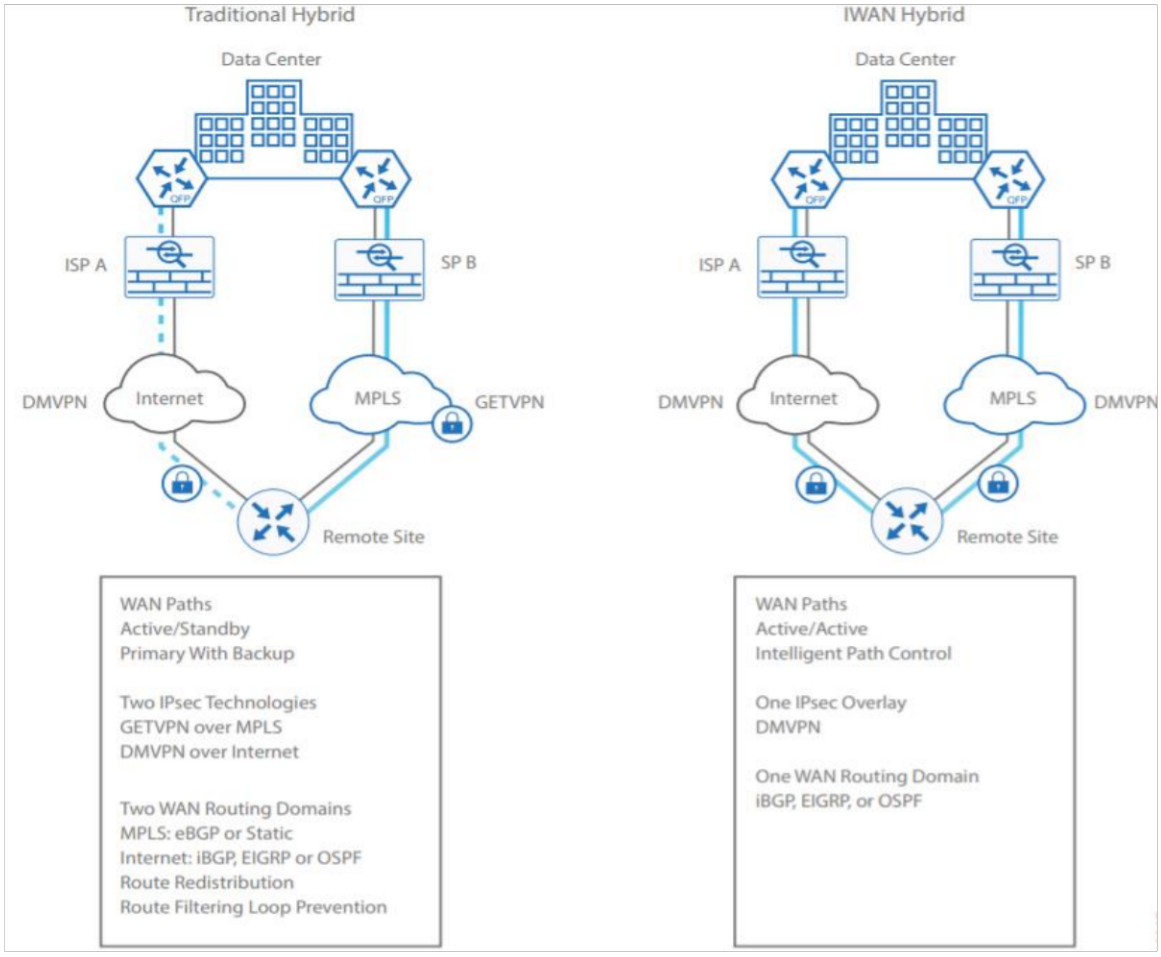

Figura 1.1. Diferencias entre las redes Hibrida WAN e Hibrida iWAN.

El diseño de iWAN proporciona una ruta activa / activa para todos los enlaces WAN y utiliza una sola tecnología Internet Protocol security (Ipsec). El diseño también utiliza un único dominio de enrutamiento WAN sin redistribución de rutas ni filtrado de rutas. El diseño de iWAN permite reducir el costo y la complejidad de implementación.

El diseño de una WAN hibrida tradicional entrega una ruta activa / en espera y dos tecnologías Ipsec según el tipo de transporte elegido. El diseño utiliza dos dominios de enrutamiento WAN, que requieren redistribución de rutas y filtrado de rutas para la prevención de bucles. Un diseño tradicional tiene más opciones de transporte para los clientes que tienen necesidades variadas, pero debido a la flexibilidad adicional, la complejidad es mayor.

1.3.2 CISCO INTELLIGENT WAN (Cisco iWAN)

Cisco iWAN es una tecnología que aporta soluciones de diseño e implementación para empresas que requieran implementar una red de área amplia independiente del transporte mediante un control de ruta inteligente.

iWAN disminuye el costo de implementación de una red WAN, aprovecha al máximo los servicios de transporte para optimizar el ancho de banda sin afectar la confiabilidad, el rendimiento o la seguridad de las aplicaciones basadas en la nube.

La Figura 1.2. muestra una red implementada con la tecnología iWAN

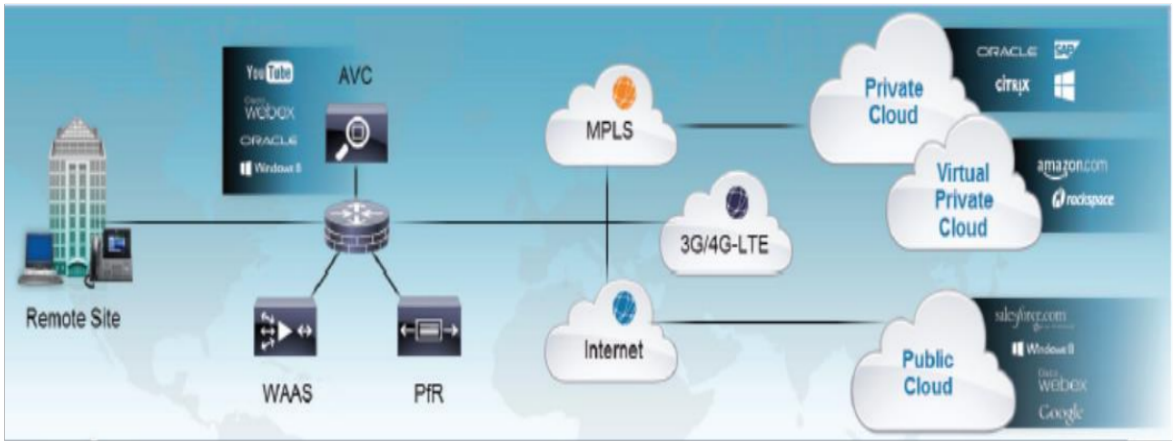

Figura 1.2. Ejemplo de una *Red implementada con la tecnología iWAN.*

La solución iWAN utiliza la tecnología Performance Routing v3 (PfRv3), además de la tecnología Dynamic Multipoint VPN(DMVPN), para entregar una WAN basada solo en Internet o WAN híbrida (MPLS + Internet).

LA tecnología iWAN se basa en cuatro componentes: control de ruta inteligente, independencia del transporte, conectividad segura y optimización de aplicaciones.

1.3.3 ARQUITECTURA iWAN

Con la llegada de la globalización, las WAN se han convertido en una parte importante para la comunicación entre oficinas remotas y clientes en cualquier rincón del mundo. Además, con la consolidación del centro de datos, las aplicaciones se están trasladando a centros de datos y nubes centralizados. Las WAN en la actualidad juegan un papel aún más crítico, porque la supervivencia de las empresas depende del rendimiento de la red y su disponibilidad.

Hoy en día, la manera de tener conectividad confiable con rendimiento predecible es aprovechar el servicio de línea alquilada o una WAN privada con MPLS. Sin embargo, los MPLS basados en el operador y los servicios de línea alquilada pueden ser muy costosos y no siempre son favorables o rentables para que una organización los utilice. Las organizaciones están buscando formas de reducir el presupuesto operativo y, al mismo tiempo, proporcionar adecuadamente el transporte de red para un sitio remoto. [4]

Con el incremento de la necesidad de las empresas de tener más ancho de banda, Internet se ha convertido en una solución rentable y con ganancias de precio-rendimiento más beneficiosas. Sin embargo, las organizaciones comenzaron a implementar "Internet como WAN" en sitios pequeños como una ruta de respaldo debido a los riesgos. Esta solución más rentable y de mejor rendimiento es utilizable en todas las sucursales de una organización con la tecnología Cisco iWAN.

Cisco iWAN permite que las empresas brinden experiencias libres de problemas a través cualquier tipo de conexión, también proporciona a las empresas de TI optimización del ancho de banda entre las conexiones de sus sucursales con el uso de opciones de transporte WAN de bajo costo sin afectar la seguridad, la confiabilidad o el rendimiento. Con iWAN, el tráfico se enruta dinámicamente según Service Level Agreement (SLA) de la aplicación, las condiciones de la red y el tipo de terminal brindan una mejor experiencia de calidad. Los ahorros en costo que se obtiene con la implementación de la iWAN permiten a las empresas cubrir los gastos de actualización de la infraestructura y, también permiten liberar recursos para la innovación empresarial. La Figura 1.3. muestra la arquitectura básica de la red iWAN. [6]

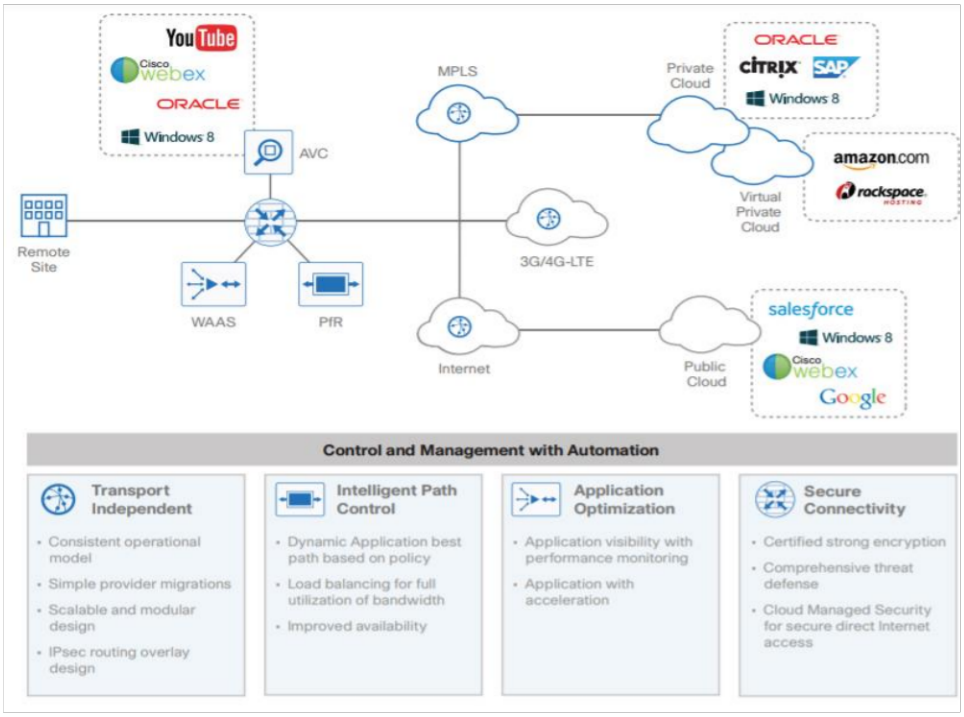

Figura 1.3. Arquitectura básica de la tecnología iWAN.

1.3.3.1 Independencia de transporte

La arquitectura Cisco iWAN utiliza DMVPN para proporcionar independencia de transporte mediante el uso de un único dominio de enrutamiento que abarca un trasporte hibrido. Este dominio provee independencia de trasporte de manera que un cliente tenga la opción de elegir cualquier tecnología WAN como: MPLS VPN (L2 o L3), metro Ethernet, Internet directo, banda ancha o celular 3G / 4G / LTE de alta velocidad.

El modelo de diseño DMVPN es una topología genérica "Hub and Spoke", crea túneles de forma estática con el router "Hub" cuya ubicación es el centro y sus "Spokes" unen las sucursales al edificio central. Para cada nuevo "Spoke" se necesita una configuración adicional en el “Hub" y el tráfico entre los "Spokes" se debe desviar por el "Hub" para que salga de un túnel y luego ingrese en otro.

Cisco DMVPN al disminuir la inestabilidad y la latencia mejora el rendimiento de la red, al mismo tiempo optimiza el ancho de banda del edificio central y permite que las sucursales se comuniquen de forma directa entre sí a través de internet o la WAN pública. [7] La Figura 1.4. muestra un ejemplo de la configuración de la iWAN DMVPN.

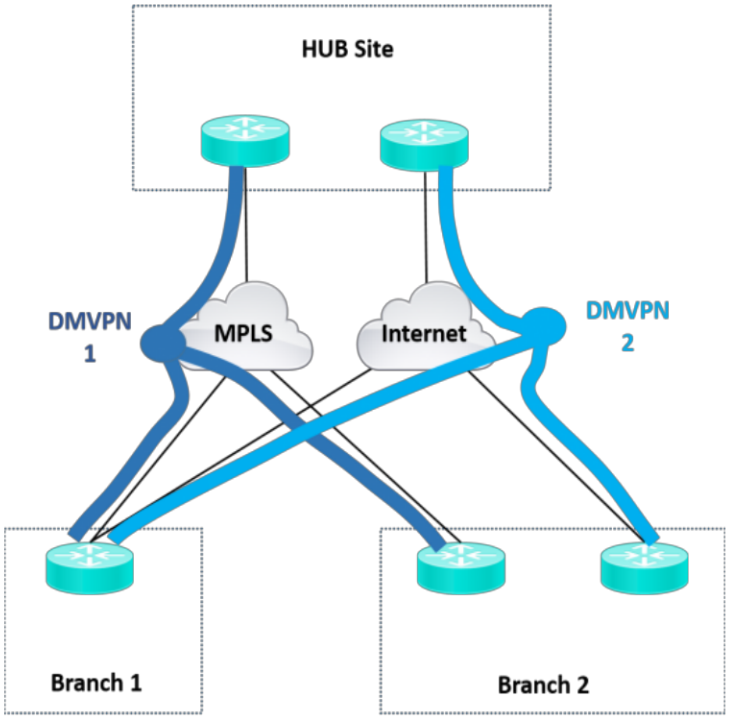

Figura 1.4. Ejemplo de la configuración Básica de iWAN DMVPN.

Las líneas azul y celeste muestran los túneles DMVPN, uno para el lado MPLS y otro para Internet. Cada uno proporciona conectividad segura y cifrada entre el edificio central y las sucursales. [8]

Un diseño independiente del transporte simplifica la implementación de WAN mediante el uso de una superposición de VPN GRE/IPsec sobre todas las opciones de transporte de WAN, incluidos MPLS, Internet y celular (3G/4G). Una única superposición de VPN reduce la complejidad y la seguridad del enrutamiento, de esta forma proporciona flexibilidad para elegir proveedores y opciones de transporte. Cisco DMVPN proporciona la superposición IWAN IPsec.

DMVPN utiliza túneles multipoint Generic Routing Encapsulation (mGRE) para conectar los hubs y todos los routers spokes. Estas redes de túneles mGRE también se denominan nubes DMVPN. [8]

1.3.3.2 Control de ruta inteligente

Cisco Performance Routing (PfR) provee control de ruta inteligente tomando en consideración los requerimientos de la aplicación, monitorea el rendimiento de la aplicación considerando el tipo de tráfico para y envía paquetes por la mejor ruta observando el estado de la ruta, el rendimiento, las políticas y el tipo de aplicación.

PfR supervisa el estado de la red (fluctuación, retrasos y perdida de paquetes) para tomar la decisión de volver a enviar las aplicaciones por la ruta de mejor rendimiento de acuerdo con las políticas de ampliación definida. En esencia, PfR asegura que la ruta tomada

cumplirá con los requisitos establecidos para esa aplicación. El control de ruta inteligente de la tecnología Cisco iWAN es parte fundamental para proveer una WAN de tipo empresarial sobre el transporte de Internet. [7] La Figura 1.5. muestra la topología básica PfR en iWAN.

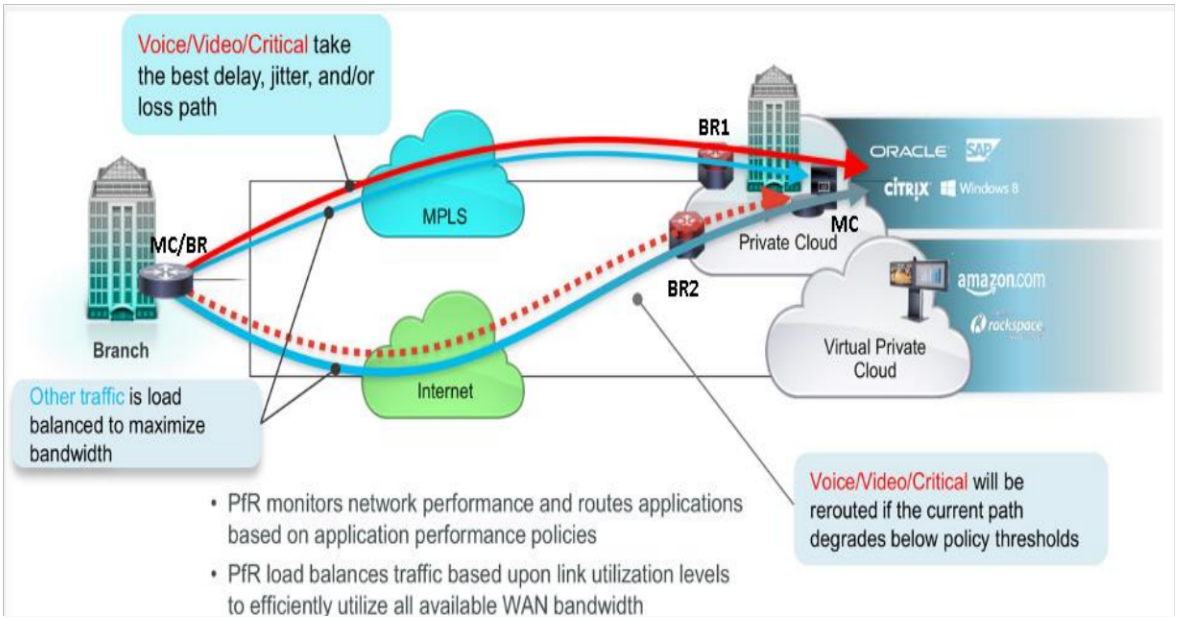

Figura 1.5. Topología PfR en iWAN.

Cisco PfR consta de Routers de Borde (BR) que se conectan a las redes superpuestas DMVPN para cada red de operador y un proceso de aplicación de Controlador Maestro (MC) que hace cumplir la política. El BR recopila datos sobre la ruta y el tráfico para posteriormente enviarlo al MC. [8]

- **Router de borde (BR):** los BR se encuentran en la ruta de reenvío de datos, realizan una recopilación de datos del caché del Monitor de rendimiento, poseen incidencia en la ruta de reenvío de paquetes como lo indica el Controlador Maestro (MC) para administrar el tráfico de usuarios.

  El router BR se encuentra en el plano de datos del router de borde con uno o más enlaces de salida al Internet Service Provider (ISP). El BR utiliza NetFlow que es un protocolo de red creado por Cisco Systems para recopilar información de forma pasiva sobre el rendimiento y el rendimiento de Transport Control Protocol (TCP). En el BR se aplican todas las decisiones de las políticas y cambios de enrutamiento en la red. El BR forma parte del monitoreo de prefijos y la optimización de rutas informando las mediciones del enlace de salida y prefijo al controlador maestro, luego se hace cumplir los cambios de política recibidos del controlador maestro. El BR exige cumplir los cambios de las políticas incluyendo una ruta preferida para

alterar el enrutamiento en la red. Se puede habilitar un proceso BR en el mismo router que un proceso de controlador maestro. [9]

- **Controlador maestro (MC):** el MC toma las decisiones en la red. En lugares grandes, como el data center o un campus, el MC es un componente independiente. Para sucursales más pequeñas por lo general la ubicación del MC suele estar en la misma plataforma que el BR. Como regla general, los lugares grandes administran más prefijos y aplicaciones de red, consumiendo así más recursos de CPU y memoria para la función del MC.

  El MC es un router que toma el papel de procesador central y base de datos para el sistema PfR. El componente MC no está ubicado en el plano de reenvío y, cuando se despliega de forma libre, no tiene vista de la información de encaminamiento incluida en la BR. El MC mantiene la comunicación y autentica las sesiones con los BR. El papel del MC es compilar información de los BR para determinar si las clases de tráfico están dentro o fuera de la política, e instruir a los BR sobre cómo se debe garantizar que las clases de tráfico permanezcan en la política utilizando la inserción de ruta. [9]

1.3.3.3 Optimización de aplicaciones

Cisco Wide Area Application Services (WASS) y Cisco Application Visibility and Control (AVC) contribuyen con optimización y visibilidad en el rendimiento de las aplicaciones sobre las WAN. Debido que las aplicaciones cada vez ocupan más espacio, se debe aumentar la reutilización de puertos HTTP (puerto 80).

WAAS provee conocimiento sobre las aplicaciones realizando una investigación de paquetes de tráfico para monitorear e identificar el rendimiento de las aplicaciones, también permite determinar qué tipo de tráfico se ejecuta en la red, de esta manera se puede ajustar la red para servicios críticos y resolver problemas de red. Con una mayor visibilidad de las aplicaciones en la red, se pueden habilitar mejores políticas de QoS y PfR que ayuda a garantizar que las aplicaciones críticas tengan la prioridad adecuada en toda la red.

Cisco AVC permite observar más de 1000 aplicaciones que se encuentran ejecutándose en los túneles, con diferencia entre las aplicaciones uniformes de políticas y las aplicaciones.

Cisco WAAS proporciona capacidades de aceleración específicas de la aplicación que permiten mejorar el tiempo de respuesta al tiempo que reducen los requisitos de ancho de banda WAN.

WAAS optimiza el tráfico y acelerar las aplicaciones en las redes inalámbricas y cableadas. La función del router fue redefinido por Cisco con Cisco ISR-AX. Cisco ISR-AX ofrece

actualmente un único Router para el sector de las capas 2 a 7 del Modelo OSI con servicios de aplicaciones y de red. [10]

Cisco ISR-AX permite garantizar el rendimiento de las aplicaciones sin tomar en cuenta su ubicación, los dispositivos que las ejecutan y el tipo de trasporte permiten ejecutar las aplicaciones con mayor rapidez, de esta forma se logra reducir la latencia en más de un 50%, de esta manera se puede simplificar las tareas de los encargados de la infraestructura de red. [10]

ISR-AX ofrece tiempos de respuesta mayores a los tiempos de las aplicaciones de los usuarios finales que utilizan aplicaciones públicas, como por ejemplo Microsoft 365 o CISCO WebEx, los usuarios finales también utilizan aplicaciones empresariales en la nube privada, incluido Citrix VDI y Microsoft Exchange.

Uno de los beneficios de la optimización WAAS es permitir a la TI postergar las actualizaciones que utilizan bastante ancho de banda de la WAN.

1.3.3.4 Conectividad segura

La conectividad segura protege la comunicación corporativa y descarga el tráfico de los usuarios de forma directa a internet. Se utiliza un cifrado IPsec sólido, firewalls basados en zonas y controles de acceso estrictos para proteger la WAN en la Internet pública. Para un mejor rendimiento de las aplicaciones en la nube pública se debe enrutar a los usuarios de sitios remotos directamente a Internet y, de esta manera se puede reducir al mismo tiempo el tráfico a través de la WAN.

Cisco Cloud Web Security (CWS) ofrece una nube basada en Web Proxy. CWS se basa en el manejo de tráfico del Usuario Seguro que accede a Internet. Una de las tecnologías que CISCO ofrece son los NGFW. NGFW son la siguiente generación de Intrusion Prevention System (IPS) o Firewalls.

2 METODOLOGÍA

2.1 ALTERNATIVAS DE SOLUCIONES iWAN

El presente trabajo de integración curricular describe dos modelos de diseño de soluciones iWAN: Hibrido iWAN y Dual Internet.

La Figura 2.1. ilustra los tres modelos de Cisco iWAN. Se observa la conectividad a Internet y las aplicaciones basadas en la nube para los tres modelos. La conectividad a Internet está disponible solo a través del modelo dual MPLS, mientras que los modelos híbrido y dual internet pueden proporcionar conectividad a Internet y a la nube directamente en la sucursal.

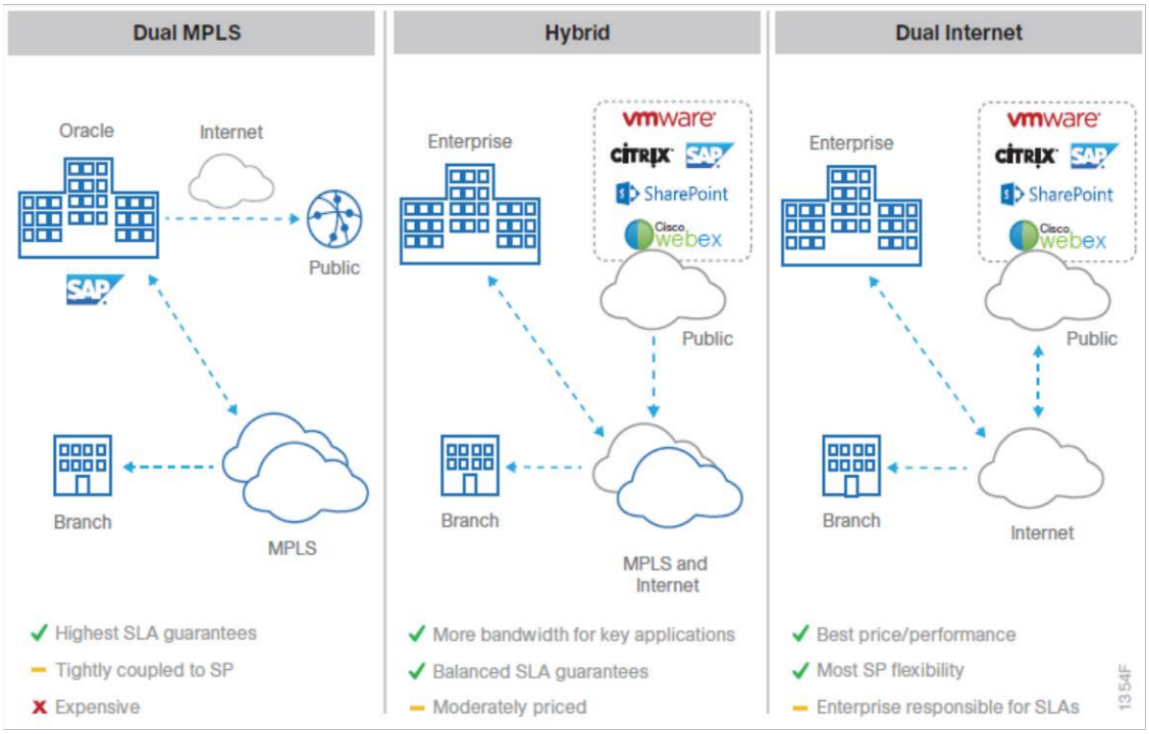

Figura 2.1. Modelos de diseño de Cisco iWAN.

El tercer modelo de diseño iWAN Dual MPLS, no será tratado en este trabajo. La configuración de MPLS dual sigue el mismo concepto que la de dual Internet, con la excepción de la base WAN, que usa MPLS en lugar de Internet para los transportes WAN.

Los diseños de agregación (hub) WAN de iWAN para el modelo de diseño incluyen dos routers de borde WAN.

Cuando se hace referencia a los routers de agregación WAN en el contexto de la conexión a un operador o proveedor de servicios, generalmente se les conoce como un router de borde del cliente (CE). Los routers WAN de agregación que terminan el tráfico de VPN se denominan routers hub VPN. En el contexto de iWAN, un router MPLS CE también se utiliza como router hub VPN. Independientemente del modelo de diseño, los routers de agregación WAN siempre se conectan a un par de switch de capa de distribución.

Cada modelo de diseño se muestra con conexiones LAN en un núcleo / capa de distribución colapsada o en una capa de distribución WAN dedicada. Desde la perspectiva de la agregación de WAN, no existen diferencias funcionales entre estos dos métodos.

En todos los diseños de agregación WAN, las tareas como el resumen de rutas IP se realizan en la capa de distribución. Hay otros dispositivos que admiten servicios de borde WAN, y estos dispositivos también deben conectarse a la capa de distribución. [6]

2.1.1 MODELO HIBRIDO iWAN

El primer modelo de diseño es el híbrido iWAN, que utiliza MPLS emparejado con Internet VPN como transportes WAN. En este modelo de diseño, MPLS WAN proporciona ancho de banda para las clases críticas de servicios necesarios para aplicaciones clave y puede proporcionar garantías SLA para estas aplicaciones. El segundo modelo de diseño es la Internet dual iWAN, que utiliza un par de Internet Service Providers (ISP) para reducir aún más los costos y, al mismo tiempo, mantener un alto nivel de resistencia para la WAN.

El modelo Hibrido iWAN usa dos enlaces activos de manera simultánea para optimizar el ancho de banda disponible en las aplicaciones. Posee la capacidad de balancear el tráfico entre los enlaces para garantizar los niveles de servicio SLA del proveedor de servicio a un bajo costo. [6]

En este modelo de diseño, MPLS proporciona ancho de banda a las clases críticas de servicios necesarios para aplicaciones clave y proporciona garantías SLA para estas aplicaciones. Las clases no críticas utilizan el ancho de banda de Internet o cualquier transporte adicional disponible en cada ubicación del sitio remoto. [8]

El modelo de diseño híbrido iWAN posee las siguientes características:

- Tiene un único operador de VPN MPLS.
- Utiliza un único proveedor de Internet.
- Utiliza enrutamiento y reenvío virtual de puerta de entrada (FVRF) en MPLS.
- Escala a 2000 sitios remotos.

En la Figura 2.2. se puede observar el diseño Hibrido iWAN.

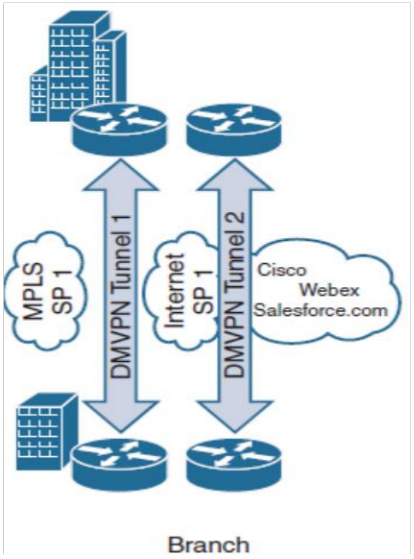

Figura 2.2. Modelo Hibrido iWAN.

El primer transporte es una VPN MPLS proporcionada por un SP y la conectividad a Internet es un segundo transporte. El transporte por Internet puede ser proporcionado por el mismo SP o por otro diferente. Idealmente, los SP utilizarían diferentes circuitos y routers de "última milla" para eliminar los SPOF. El circuito de Internet se utiliza para establecer un servicio VPN a otro sitio.

Este modelo proporciona conectividad para un modelo de Internet distribuido para todo el tráfico basado en Internet o selecto. Es posible permitir el acceso a Internet solo para aplicaciones en la nube aprobadas por TI.

La arquitectura iWAN no limita el diseño de la WAN a solo dos transportes. Es posible utilizar tres o más transportes para proporcionar una solución personalizada. Por ejemplo, puede utilizar dos SP diferentes que proporcionen transportes VPN MPLS y un tercer SP que proporcione conectividad a Internet para un transporte. Los tres transportes utilizarían DMVPN para mantener la coherencia del enrutamiento y la topología.

2.1.2 MODELO DE DISEÑO DUAL DE INTERNET iWAN

El primer transporte es la conectividad a Internet proporcionada por un SP, y la conectividad a Internet la proporciona un SP diferente para fines de resistencia. Este modelo también proporciona conectividad para un modelo de Internet distribuido y no tiene que estar restringido solo a túneles VPN.

El diseño dual de Internet tiene es menos costoso que el modelo Hibrido iWAN y proporciona la mayor flexibilidad a la hora de elegir proveedores de servicios. Depende de la empresa proporcionar el SLA, ya que no existen garantías de ancho de banda cuando se usa Internet.

Las características del modelo de diseño dual de Internet de iWAN:

- Utiliza dos operadores de servicio de internet.
- Escala a 2000 sitios remotos.

La Figura 2.3. muestra un ejemplo de diseño del modelo dual Internet.

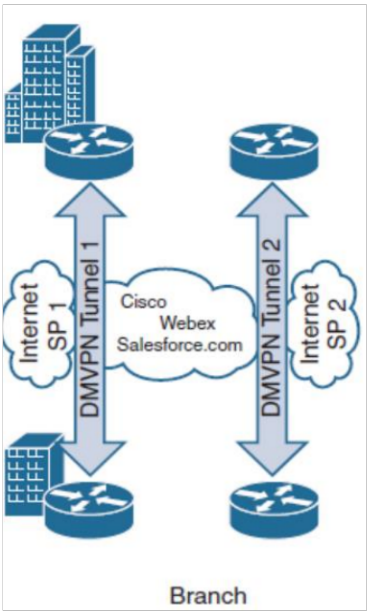

Figura 2.3. Modelo dual Internet.

En los modelos de diseño de Internet dual iWAN e iWAN híbrido, los routers de hub DMVPN se conectan a Internet indirectamente a través de una interfaz DMZ de firewall contenida dentro del perímetro de Internet. Los routers del hub VPN están conectados a la interfaz DMZ del firewall, en lugar de conectarse directamente con los routers del proveedor de servicios de Internet. Por lo general, no se usa una conexión de firewall cuando el router del hub VPN se conecta a un operador MPLS.

Este diseño, aún debe determinar una ruta preferida para sus clases críticas de tráfico. En casi todos los casos, la ruta preferida será el proveedor con el mayor ancho de banda, pero se puede elegir el que tenga los acuerdos de interconexión más favorables o aquel en el que la mayoría de sus sitios remotos tengan conexiones directas. Las clases no críticas pueden usar el ancho de banda de Internet secundario disponible en cada ubicación. [8]

2.2 CARACTERÍSTICAS DE PERFORMANCE ROUTING (PfR)

Cisco PfR permite enviar paquetes de red utilizando control de ruta inteligente. Por lo regular, se utiliza un protocolo de enrutamiento para determinar la ruta más corta entre un origen y un destino, pero el camino más corto podría estar muy transitado. En lugar de elegir la ruta más corta, Cisco PfR elige la mejor ruta en base a un mejor rendimiento.

PfR medide parámetros como la perdida de paquetes, el rendimiento y la accesibilidad para encontrar la ruta para enviar paquetes. Además de las métricas de rendimiento, PfR elegirá

rutas por estado de ruta, políticas y tipos de aplicación. PfR también se puede utilizar para mejorar la entrega de aplicaciones y la eficiencia de la WAN. [5]

Parámetros como la falta de latencia y ancho de banda de la WAN ocasionara que el rendimiento no sea eficiente. Cisco PfR ayuda a los administradores a abordar los problemas de rendimiento de la red al permitir que un router pueda elegir la mejor ruta mientras mantiene el rendimiento de la aplicación.

2.2.1 FUNCIONAMIENTO DE PERFORMANCE ROUTING

PfR selecciona una ruta en función del rendimiento de la red. Cuando una ruta comienza a tener problemas de rendimiento, debido a perdida de paquetes o accesibilidad, PfR mueve la ruta de acuerdo con las políticas definidas y configuradas por el usuario. Esto ayuda a mejorar la disponibilidad y el rendimiento de la aplicación. PfR utiliza el equilibrio de carga con el tráfico en las rutas disponibles.

PfR utiliza dos funciones de dispositivo diferentes en una red: BR y MC. Los BR son routers que tienen una o más interfaces conectadas a redes externas. Los BR envían parámetros de rendimiento a los MC. El MC se comunica con todos los diferentes BR para monitorear todo. El MC y BR se pueden configurar para que sean el mismo o diferentes routers.

PfR utiliza tres tipos de interfaz diferentes, local (que es lo que se usa para comunicarse entre, interna (que conecta las redes internas) y externa (que se conecta a redes externas). [5]

2.3 CARACTERÍSTICAS DEL ENRUTAMIENTO CISCO PfR

Cisco PfR parte del software Cisco IOS, proporciona control de ruta inteligente en la tecnología iWAN y complementa las tecnologías de enrutamiento tradicionales mediante el uso de inteligencia de infraestructura de Cisco IOS, esto permite mejorar la disponibilidad y el rendimiento de las aplicaciones.

2.3.1 CONFIGURACIÓN DEL ENRUTAMIENTO DE CISCO PfR [5]

Existen muchas formas en que un usuario puede configurar PfR, y puede hacerlo por una variedad de razones. Algunas configuraciones de ejemplo son las siguientes:

- El MC PfR puede ser configurado para aprender automáticamente los prefijos en función del tráfico de salida o el tiempo de demora mediante NetFlow Top Talker. El comando de aprendizaje se puede utilizar para ingresar a este modo desde el MC.
- El MC puede ser configurado para recopilar prefijos aprendidos por tipo. Esto se puede hacer mediante el comando de tipo de agregación (PfR) en PfR Top Talker y Delay learning.

- PfR se puede configurar para simplificar el aprendizaje de las clases de tráfico a través de un modo de configuración de lista de aprendizaje.
- Los usuarios pueden configurar manualmente PfR para crear clases de tráfico para monitoreo y optimización. Esto permite a los usuarios definir prefijos exactos.
- La configuración de la clase de tráfico de prefijo se puede utilizar para seleccionar un prefijo o un rango de prefijos para la supervisión.
- La accesibilidad, o el porcentaje / número máximo de hosts inalcanzables, se puede especificar en el controlador maestro mediante el comando inalcanzable (PfR).
- Los usuarios pueden configurar PfR para participar en monitoreo pasivo, activo o pasivo y activo.
- El rango de utilización de todos los enlaces se puede configurar y calcular, tanto para la salida como para la entrada.
- Para resolver posibles políticas superpuestas, los usuarios pueden ejecutar una función de resolución, que les permite establecer una prioridad para las políticas de PfR. Esto se puede hacer usando el comando *resolve* (PfR) en el modo de configuración del controlador maestro PfR.
- Los usuarios también pueden configurar políticas de PfR según el costo de cada enlace de salida en su red. Esto se puede hacer configurando el MC para enviar tráfico a través de enlaces de salida que son los más rentables en términos de ancho de banda.

2.3.2 BENEFICIOS DEL ENRUTAMIENTO DE CISCO PfR

Algunos de los beneficios del enrutamiento PfR de Cisco son los siguientes:

- Mejora el rendimiento de las aplicaciones y de la red.
- Puede mejorar la disponibilidad de la aplicación.
- Solo necesita pequeñas cantidades de configuración.
- Gran cantidad de opciones de políticas.
- Reduce los gastos de WAN en términos de operación.
- Distribuye de manera eficiente el tráfico en función de la carga, el rendimiento y otras métricas. [5]

2.3.3 VERSIONES DE ENRUTAMIENTO CISCO PfR

Cisco PfR ha tenido algunas funciones diferentes desde que se creó originalmente a partir de Optimized Edge Routing (OER). Cada versión se ha centrado en la facilidad de implementación.

La siguiente versión, PfRv2, agrego la capacidad de escalar hasta 500 sitios, selecciones de rutas de aplicaciones, simplificaciones de políticas y más opciones de configuración.

La versión actual, PfRv3, se enfoca en agregar escalabilidad a 2,000 sitios, aprovisionamiento centralizado, descubrimiento automático, soporte para múltiples centros de datos, así como múltiples próximos saltos por red DMVPN.

En la tabla 2.1. se indica la evolución y las características de las versiones de PfR.

Tabla 2.1. Evolución de las versiones y características de PfR.

VERSIÓN	CARACTERÍSTICAS
PfR / Borde optimizado Enrutamiento (REA)	Internet de borde. WAN básica. Aprovisionamiento por sitio por política. Miles de líneas de configuración.
PfRv2	Simplificación de políticas. Selección de ruta de aplicación. Escala 500 sitios. Decenas de líneas de configuración.
PfRv3	Aprovisionamiento centralizado. Infraestructura de control de visibilidad de aplicaciones (AVC). Conciencia de VRF. Escala 2000 sitios. Solo configuración del hub. Varios centros de datos. Varios saltos siguientes por red DMVPN.

2.3.4 PROTOCOLOS DE ENRUTAMIENTO

Es una buena práctica manipular los protocolos de enrutamiento para que el tráfico fluya a través del transporte preferido. Influir en la tabla de enrutamiento garantiza que cuando PfR esté deshabilitado, el tráfico seguirá la tabla de Cisco Express Forwarding derivada de la Base de información de enrutamiento (RIB) y reenviará el tráfico a DMVPN a través del túnel preferido.

PfRv3 siempre busca una ruta principal de cualquier prefijo de destino antes de crear un canal o controlar una clase de tráfico. PfR selecciona los próximos saltos según el siguiente orden de búsqueda:

- Ruta de atajo NHRP (solo sucursal).
- Si no, verifique en el orden de BGP, EIGRP, Static y RIB.
- Si en algún momento aparece una ruta de atajo de NHRP, PfRv3 la tomaría y abandonaría el uso de la ruta principal de ruta desde uno de los protocolos de enrutamiento.

Es esencial asegurarse de que todos los prefijos de destino sean accesibles a través de todas las rutas disponibles para que PfR pueda crear los canales correspondientes y controlar las clases de tráfico. Recuerde, PfR verificará dentro de la tabla de topología BGP o EIGRP.

El diseño tiene los siguientes objetivos de enrutamiento IP:

- Proporcione una conectividad de enrutamiento óptima desde los sitios principales de agregación de WAN a todas las ubicaciones remotas.
- Aísle los cambios de topología de enrutamiento WAN de otras partes de la red.
- Proporcionar una sólida topología de enrutamiento IP subyacente para admitir el control de ruta inteligente proporcionado por Cisco PfR.
- Proporcionar enrutamiento remoto de sitio a sitio a través del sitio principal de agregación de WAN (modelo hub-and-spoke).
- Permitir un enrutamiento remoto óptimo directo de sitio a sitio (modelo de spoke to spoke).
- Compatibilidad con multidifusión de IP procedente del sitio principal de agregación de WAN.

En los sitios remotos de WAN, no hay acceso local a Internet para navegar por la web o servicios en la nube. Este modelo se conoce como Internet centralizado. Vale la pena señalar que los sitios con Internet/DMVP podrían proporcionar capacidad de Internet local; sin embargo, para este diseño, solo el tráfico encriptado a otros sitios de DMVPN puede usar el enlace de Internet. En el modelo de Internet centralizado, se anuncia una ruta predeterminada a los sitios remotos de WAN además de las rutas internas desde el centro de datos y el campus.

La red debe tolerar condiciones de falla única, incluida la falla de cualquier enlace de transporte WAN único o un dispositivo de red único en el sitio de agregación WAN principal.

EIGRP y BGP son protocolos de enrutamiento para redes DMVPN.

2.3.4.1 EIGRP

El protocolo EIGRP reduce la configuración del stub en el spoke, mejora la estabilidad de la red y reduce la utilización de recursos. El enrutamiento EIGRP Stub se usa comúnmente en redes DMVPN que tienen múltiples sitios con un solo dispositivo en cada sitio. Los dispositivos del sitio que actúan como hub reducen el dominio de consulta y, por lo tanto, mejoran el rendimiento. Por otro lado, el enrutamiento de rama EIGRP es simple para un sitio de puerta de enlace predeterminada de un solo router. Cuando una sucursal agrega un segundo router o aumenta de tamaño y necesita enrutamiento dentro del campus, la configuración se vuelve compleja. [11]

Cisco usa EIGRP como el protocolo de enrutamiento principal para IWAN porque EIGRP es fácil de configurar, no requiere una gran cantidad de planificación, tiene resumen y filtrado flexibles y puede escalar a redes grandes. A medida que crecen las redes, también crece la cantidad de prefijos IP o rutas en las tablas de enrutamiento. Debe programar el resumen de IP en los enlaces donde existen límites lógicos, como los enlaces de la capa de distribución al área amplia o al núcleo. Al realizar el resumen de IP, puede reducir la cantidad de ancho de banda, procesador y memoria necesaria para transportar tablas de rutas grandes, así como reducir el tiempo de convergencia asociado con una falla de enlace.

Para un diseño iWAN se puede utilizar un solo sistema autónomo EIGRP (AS 400) para LAN, WAN y todos los sitios remotos. Todos los sitios remotos tienen una conexión dual para lograr resistencia. Sin embargo, debido a las múltiples rutas que existen dentro de esta topología, debe evitar los bucles de enrutamiento y evitar que los sitios remotos se conviertan en sitios de tránsito si se producen fallas en la WAN. El retraso de la interfaz se configura para garantizar que las interfaces WAN sean siempre preferidas y que MPLS sea la ruta WAN preferida en los modelos de diseño híbrido. [8]

Existen varias recomendaciones clave para cada tipo de sitio.

Hub y sitios de tránsito:

- **Anunciar el resumen del sitio, el resumen de la empresa y una ruta predeterminada a sitios remotos:** La escalabilidad del dominio de enrutamiento EIGRP depende del resumen. Resumir varias rutas en un agregado reduce el tamaño de la tabla de enrutamiento y crea un límite de consulta EIGRP. EIGRP resume los prefijos de red en función de la interfaz.
- **Resumen de métricas:** Las métricas de resumen se utilizan para reducir la carga computacional en el hub DMVPN y los routers de borde de tránsito.

- **Filtro de ingreso en túneles:** Se aplica un filtro de lista de prefijos de entrada en los routers hubs DMVPN para evitar que un router DMVPN aprenda una ruta predeterminada o resumida de un router hub par, lo que evita bucles de enrutamiento subóptimos.
- **Temporizadores de espera y saludo EIGRP:** Aumenta el intervalo de saludo de EIGRP a 20 segundos y el temporizador de espera a 60 segundos. El aumento de los temporizadores permite que los routers hub DMVPN manejen una gran cantidad de sitios remotos. Los temporizadores de saludo y espera deben coincidir en el hub DMVPN y en los routers del sitio remoto.

Sitios remotos:

- **Sitio auxiliar EIGRP:** La funcionalidad del sitio de código auxiliar se basa en la función de código auxiliar de EIGRP, que permite que un router se anuncie a sí mismo como un código auxiliar para los pares en interfaces WAN específicas. También permite que el router intercambie rutas aprendidas en la interfaz LAN.
- **Temporizadores de saludo y espera EIGRP:** Aumenta el intervalo de saludo de EIGRP a 20 segundos y el temporizador de espera a 60 segundos. El aumento de los temporizadores permite que los routers hub DMVPN manejen una gran cantidad de sitios remotos. Los temporizadores de saludo y espera deben coincidir en el hub DMVPN y en los routers del sitio remoto.

La función de sitio auxiliar de EIGRP proporciona los siguientes beneficios clave:

- Los vecinos EIGRP en enlaces WAN no envían consultas EIGRP al sitio remoto cuando una ruta se activa.
- Se pueden colocar routers adicionales más lejos en el sitio y seguir recibiendo rutas de la WAN a través del router del sitio auxiliar.
- Evita que el sitio auxiliar se convierta en un router de tránsito.
- Elimina la necesidad de una fuga de enrutamiento compleja con etiquetas de ruta y filtrado.

2.3.4.2 BGP

BGP establece sesiones con otros routers BGP. Si la sesión se forma con un router BGP dentro del mismo Autonomous System (AS), se conoce como sesión IBGP (BGP interno). Si la sesión se forma con un router BGP de un AS diferente, se conoce como sesión EBGP (BGP externo). Los cálculos y comportamientos de la mejor ruta en las sesiones de EBGP e IBGP son ligeramente diferentes. BGP adjunta Path Attributes (PA) asociados con cada

ruta de red. Los PA proporcionan a BGP granularidad y control de las políticas de enrutamiento. Las comunidades BGP brindan capacidad adicional para etiquetar rutas y modificar la política de enrutamiento BGP en routers ascendentes y descendentes. Las comunidades BGP se pueden agregar, eliminar o modificar de forma selectiva en cada atributo a medida que la ruta viaja de un router a otro. Las comunidades BGP son un atributo BGP transitivo opcional que puede atravesar de AS a AS y se puede utilizar para simplificar la política de enrutamiento de BGP. [12]

BGP se puede implementar en la superposición de la WAN como un protocolo de enrutamiento alternativo a EIGRP. BGP es una opción para los operadores de red que requieren un amplio conjunto de funciones para personalizar la selección de ruta en topologías complejas e implementaciones a gran escala. Aunque BGP se posiciona tradicionalmente en el borde de la WAN del proveedor de servicios, las mejoras recientes, como los vecinos dinámicos de BGP, lo convierten en una opción viable para la implementación de IWAN. La compatibilidad con vecinos dinámicos de BGP simplifica la configuración y permite emparejarse con un grupo de vecinos remotos que están definidos por un rango de dirección IP. Cada rango se puede configurar como una dirección IP de subred, lo que permite que los spokes iniciar el emparejamiento BGP sin tener que preconfigurar pares remotos en los reflectores de ruta. [8]

Para el diseño simple de una iWAN se utiliza un único proceso de enrutamiento iBGP para la superposición de WAN. OSPF se usa en las interfaces de LAN en el hub de tránsito y remotos.

Existen algunas recomendaciones para cada de sitio, se mencionan a continuación.

Hub y sitios de tránsito:

- **Reflectores de ruta BGP:** Los routers de tránsito y hub DMVPN funcionan como reflectores de ruta BGP para los spokes.
- **Emparejamiento BGP:** No se configura ningún emparejamiento BGP entre los reflectores de ruta.
- **Neighbors dinámicos BGP:** La compatibilidad con vecinos dinámicos de BGP está configurada en los reflectores de ruta.
- **Anuncio de ruta:** Los prefijos específicos del sitio, el prefijo de resumen empresarial y la ruta predeterminada se anuncian en los sitios remotos.
- **Preferencia local:** Establece la preferencia local para todos los prefijos en función de la jerarquía de transporte WAN.

- **Redistribución de rutas:** Redistribuya BGP en OSPF con un costo métrico definido para atraer tráfico desde los sitios centrales a los sitios remotos a través de MPLS.
- **Temporizadores de saludo y espera de BGP:** Aumenta el intervalo de saludo de BGP a 20 segundos y el temporizador de espera a 60 segundos. El aumento de los temporizadores permite que los routers hubs DMVPN manejen una gran cantidad de sitios remotos. Los temporizadores de saludo y espera deben coincidir en el hub DMVPN y en los routers del sitio remoto.
- **Área OSPF 0:** Configure un Área 0 OSPF para las interfaces LAN.

Sitios remotos:

- **Emparejamiento BGP:** Intercambio de tráfico con routers de borde de tránsito y hub para cada nube DMVPN.
- **Preferencia local:** La ruta preferida se elige de la preferencia local más alta.
- **Redistribución de rutas:** Realizar la redistribución mutua de las rutas OSPF y BGP.
- **Etiquetado de ruta:** Establecer una etiqueta de ruta local para identificar rutas en OSPF que se redistribuyeron desde BGP.
- **OSPF Área 0:** Configurar un Área 0 OSPF para las interfaces LAN de sitios remotos de router dual o sitios remotos con switches de capa de distribución.

3 DISEÑO DE LA iWAN EMPRESARIAL

3.1 CARACTERÍSTICAS DE LA RED EMPRESARIAL

La tecnología Cisco iWAN es una solución que proporciona mejoras el momento de utilizar enlaces WAN, la seguridad y el rendimiento son mejoras que se van a ver reflejados en el tiempo de respuesta de los servicios que serán utilizados por los usuarios. La red empresarial para mejorar permite conectar las ciudades de Quito, Guayaquil y Cuenca, siendo Quito la cede principal, Guayaquil y Cuenca las sucursales. La Figura 3.1. muestra la red empresarial a mejorar.

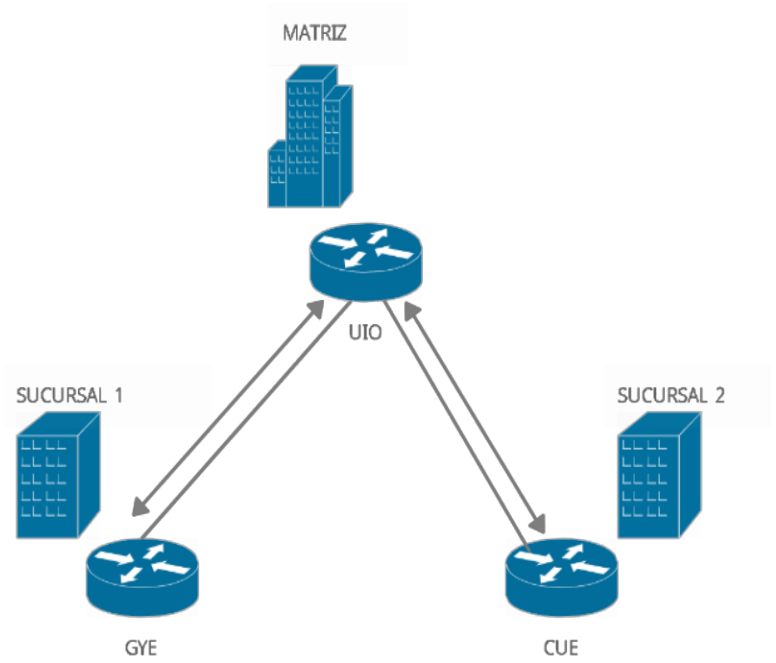

Figura 3.1. Diseño de la red empresarial.

La red diseñada posee enlaces WAN redundantes con el fin de disminuir el tiempo de inaccesibilidad en el caso de que falle uno de los enlaces. Para el diseño de la red empresarial se utiliza dos Proveedores de Servicio de Internet que llevan por nombre: Proveedor de servicio de internet 1 (ISP-1) y Proveedor de Servicio de Internet 2 (ISP-2).

El propósito de los dos ISP es dar servicios de Internet y de datos a para conectar diferentes lugares mediante una red basada en MPLS, la red tiene por finalidad enviar paquetes evitando realizar el análisis del campo de dirección IP destino. Con el etiquetado de los routers, se realiza el envío de paquetes de una manera más rápida y sin utilizar muchos recursos de los dispositivos. Como acotación, una red tradicional no es muy segura en comparación con la red basada en tecnología MPLS, esto se debe a que la tecnología MPLS tiene por objetivo principal la separación lógica de la información de los diferentes clientes que poseen un ISP gracias al uso de tablas de Virtual Routing and Forwarding (VRF). Gracias a las VRFs los clientes pueden manejar su propia tabla de rutas sin importar la presencia de otros clientes en los dispositivos del ISP. Esto garantiza que la seguridad de sus datos e información no sean compartidos con agentes externos a su infraestructura de red o con otros clientes que compartan la infraestructura del ISP. [13]

En el caso de una expansión de la empresa, la nueva sucursal debe tener el mismo diseño de redundancia para los enlaces WAN, de esta manera se garantiza la disponibilidad de los servicios. Para esto, la nueva sucursal debe poseer dos enlaces WAN, ambos deben

usar el servicio de transmisión de datos de ISP-2 ya que es considerado el ISP con mejores tiempos de respuesta ante problemas que se puedan suscitar en los enlaces. En este que el ISP-2 no funcione se debe utilizar el ISP-1, la sucursal cuenca por su ubicación solo tiene acceso al ISP-1.

La Figura 3.2. muestra el esquema de la Matriz Quito y las sucursales Guayaquil y Cuenca, también se puede observar los enlaces WAN principales y secundarios de cada localidad.

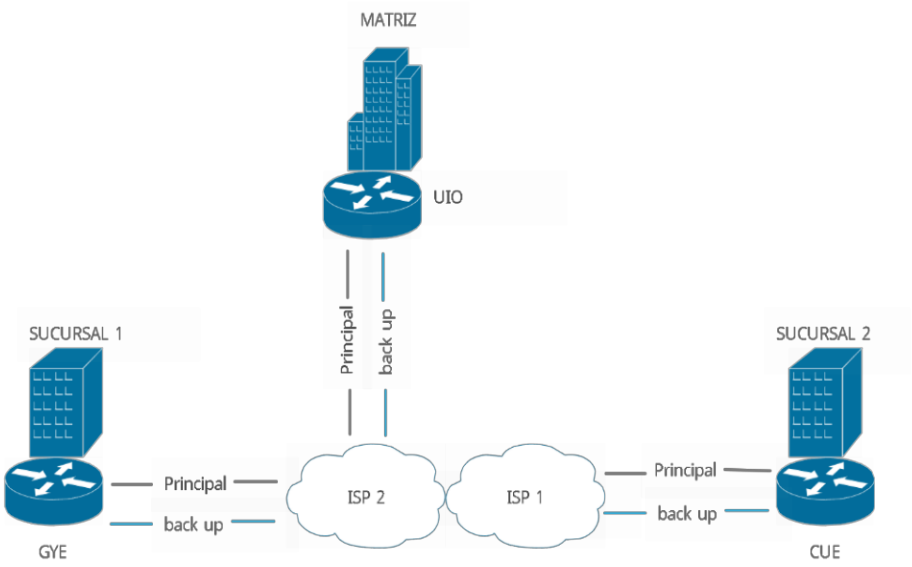

Figura 3.2. Diagrama de la matriz Quito y las sucursales Guayaquil y Cuenca con ISP.

La dirección que se utiliza para el diseño de la red es de clase C 192.168.0.0/16 y se encuentra distribuida como se puede observar en la Tabla 3.1.

Tabla 3.1. Información de las subredes de la red diseñada.

Router	Localización	Subred Primaria	Transporte
Quito	Matriz	192.168.0.0/24	MPLS
Guayaquil	Sucursal 1	192.168.1.0/24	MPLS
Cuenca	Sucursal 2	192.169.2.0/24	MPLS

En la Tabla 3.1 se puede observar la Matriz Quito con dirección de red de 192.168.0.0 y mascara de subred de 24 bits. Las sucursales Guayaquil y Cuenca tienen las subredes

192.168.1.0/24 para Guayaquil y 192.168.2.0/24 para Cuenca, se debe tomar en cuenta que las sucursales Guayaquil y Cuenca pueden tener comunicación entres si sin necesidad que el tráfico pase por la matriz, de esta manera se evita el uso innecesario de ancho de banda por causa de un mal enrutamiento.

3.2 ANALISIS PARA EL DISESEÑO DE RED iWAN

La comunicación de Guayaquil y Cuenca con los servidores de Quito, se realizan a través de enlaces WAN. La redundancia entre los enlaces de cada localidad se da de acuerdo con el esquema Activo/Pasivo, lo cual permite la utilización de un solo enlace a la vez, si existe una falla se deberá utilizar el enlace secundario. La Figura 3.3. muestra el esquema de redundancia de la red.

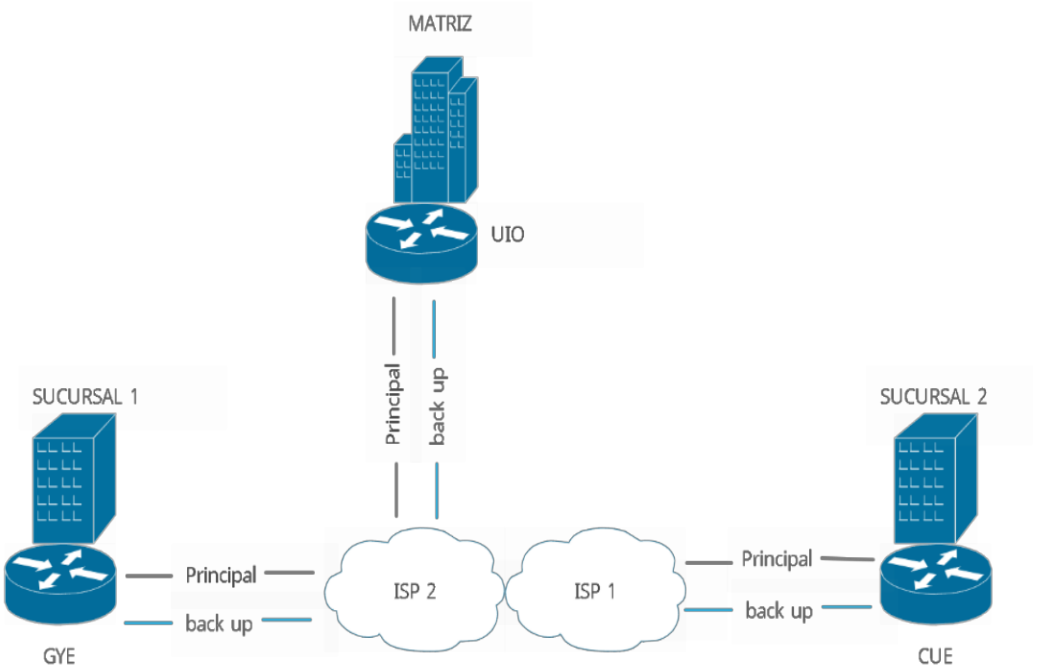

Figura 3.3. Esquema de enlace principal y enlace secundario.

En este caso se debe considerar que un enlace es utilizado hasta el momento en el que algo afecte la disponibilidad del enlace principal. En el caso que exista una falla la comunicación debe ser manejada con el protocolo de enrutamiento dinámico llamado BGP. BGP permite que la matriz y a las subredes de las sucursales sean intercambiadas, el enlace principal es cambiado por el enlace de enlace secundario. [14]

3.3 DISEÑO iWAN PROPUESTO

El diseño de iWAN propuesto está basado en el uso de la tecnología Cisco iWAN, con este diseño se puede establecer un adecuado uso de los enlaces en cada una de las localidades con el fin de evitar su subutilización, también se puede brindar una mejor seguridad de

información que atraviesa por la red. Con el mecanismo de cifrado en los paquetes se puede asegurar la confidencialidad y la integridad de la información.

La tecnología iWAN es aplicable en escenarios que presenten uno o más enlaces redundantes, de esta manera iWAN pueda evaluar cual es la mejor ruta para enviar el tráfico de acuerdo con los parámetros de calidad que se hayan especificado. Para el escenario de la red empresarial propuesta, cada una de las localidades posee dos enlaces redundantes, y se puede implementar esta solución como se observa en la Figura 3.4.

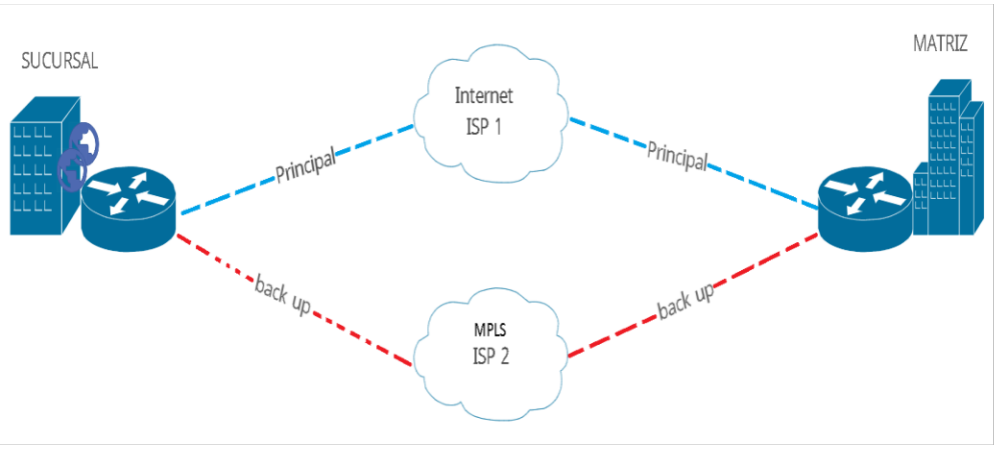

Figura 3.4. En laces redundantes.

La tecnología iWAN provee Independencia de Transporte gracias al uso de DMVPN, gracias a esto, no se requiere que un solo ISP provea del enlace principal y el enlace secundario, de esta manera se puede evitar una falla común en caso de que el ISP presente un daño. De acuerdo con esto, se debe mencionar que en el diseño del enlace secundario no se necesita contratar el mismo ISP que el enlace principal. El enlace principal puede ser de cualquier tipo de transporte como, por ejemplo: Internet, VPN (L2 o L3), metro Ethernet, banda ancha o celular 3G / 4G / LTE de alta velocidad. [15]

Para el diseño de la iWAN, cada una de las localidades tiene dos enlaces de diferente transporte. Quito y Guayaquil tienen un enlace de Internet mediante el ISP-1 y un enlace MPLS mediante el ISP-2. En el caso de Cuenca tiene dos enlaces de Internet a través del ISP 1 y 2.

Con el tipo de transporte establecido, se realiza la conectividad de Quito con las Sucursales Guayaquil y Cuenca utilizando la tecnología DMVPN.

3.3.1 ASPECTOS DEL DISEÑO DMVPN

Cada enlace posee una nube DMVPN, esto quiere decir, que cada infraestructura que comparta un transporte debe conectarse a través de una nube DMVPN privada, estas nubes son tuéneles multipunto que interconectan las infraestructuras. Para el diseño de la red iWAN. El servicio de Internet que ofrece el ISP-1 se le es asignado el túnel 100. El servicio MPLS que ofrece el ISP-2 se le da el nombre de túnel 200 y el otro servicio de Internet que ofrece el ISP-2 tiene por nombre túnel 300. En la Figura 3.5. se puede observar los túneles DMVPN entre la matriz y las sucursales.

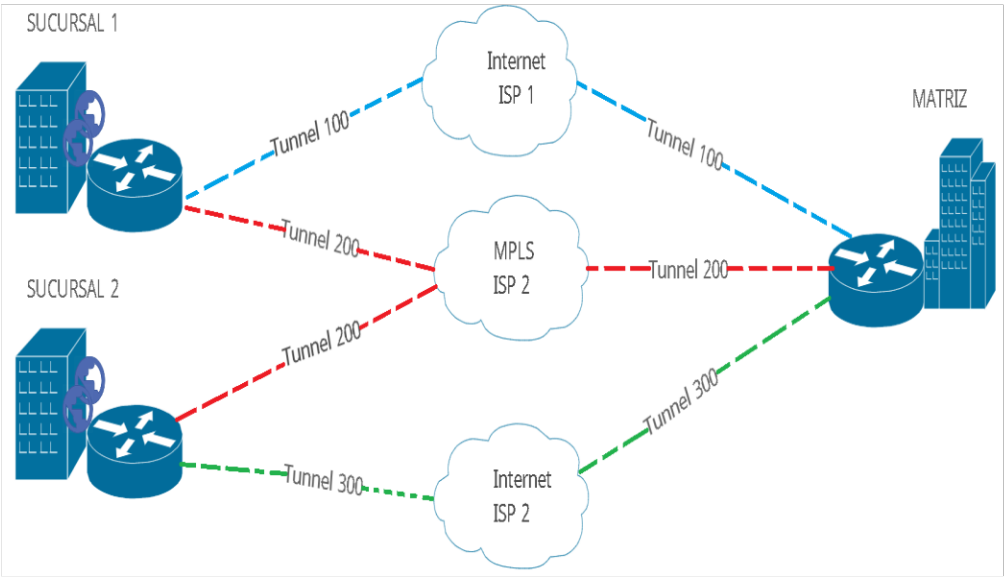

Figura 3.5. Representación de los túneles DMVPN.

Las sucursales Guayaquil y Cuenca deben realizar una conexión a la matriz Quito antes de encontrar la trayectoria más adecuada para volver a enviar el tráfico, esto ocasiona que la configuración inicial de la nueva sucursal se realice con parámetros previamente definidos por la matriz. Es necesario mencionar, que de existir tráfico de comunicación entre las sucursales Guayaquil y Cuenca, el tráfico de la sucursal de origen no debe pasar primero por la matriz y después por la sucursal destino, en el caso de que esto suceda, se generará un inadecuado enrutamiento y se tendrá un desperdicio de recursos del canal. Gracias al Next Hop Resolution Protocol (NHRP), el tráfico entre las sucursales se puede enviar de forma directa sin necesidad de pasar por la matriz. [16]

Por seguridad, el protocolo NHRP es protegido con una contraseña al ser utilizado en los túneles DMVPN, esta contraseña no permite establecer conexión con rauters que no pertenezcan a la empresa.

La sucursal Cuenca se diseñó de manera que posee dos tipos de transporte: Servicio de internet GEPON y servicio de internet Corporativo. El momento que el router decida por

cuál de los dos servicios enviar los paquetes se presentará un problema ya que son dos trasportes de similares características, dado este caso, el router debe tener una ruta activa por defecto en uno de los dos servicios, por tanto, el otro servicio quedara inactivo hasta que el primer servicio este afectado y pueda tomar su lugar. Con la finalidad de evitar este problema y poder obtener el beneficio que se busca para ambos enlaces, se define el router con un parámetro VRF, con el cual se puede separar los servicios que entregan cada ISP, y de esta manera mantener de forma separada el un enlace del otro. [17]

Al tener las nubes DMVPN funcionando de forma correcta, se debe elegir el adecuado protocolo de enrutamiento con el cual se pueda realizar la comunicación en tras las diferentes subredes de la red diseñada. La solución Cisco iWAN sugiere dos protocolos de enrutamiento: EIGRP o BGP. La decisión del protocolo a utilizar es determinada por el administrador de red, en este caso se optó por el uso de EIGRP que tiene las siguientes características:

- Es un protocolo de convergencia rápida.
- Envía actualizaciones el momento que existe un cambio de topología.
- Utiliza paquetes de saludo entre los vecinos para mantener una determinada caída de enlace.
- El ancho de banda y retardo es utilizado para realizar el calculo para elección de ruta.
- Resiste el balaceo de carga desigual.
- Mantiene una tabla de topología para guardar información de las distintas rutas disponibles.

Después de elegir el protocolo de enrutamiento EIGRP, se debe tener en cuenta las siguientes recomendaciones de diseño:

- Los sitios remotos no deben volver a enviarlas las rutas aprendidas de un router a otro router.
- Los routers de la matriz deben permitir la disminución del tamaño de la tabla de rutas. Esto quiere decir que una ruta por defecto debe ser anunciada para los prefijos que son utilizados por la matriz y sucursales, la ruta también debe ser anunciada para el tráfico de internet.

- Los parámetros del protocolo de enrutamiento deben ser manipulados con la finalidad que el tráfico sea enviado por el camino preferencial de transporte, para que, en caso de un problema de la tecnología PfR, el tráfico pueda seguir por su ruta normal con transporte de mayor calidad.

- Se debe tener un bajo número de variables de configuración con la finalidad que, en un futuro, sea más fácil la implementación de nuevas sucursales.

El diseño de funcionalidad de PfR posee dispositivos que cumplen un papel muy importante, a los cuales se les asigna diversas responsabilidades para el correcto funcionamiento de PfR. La red iWAN está compuesta por la central y los sitios remotos. Cada sitio remoto debe definir un router MC encargado de tomar las decisiones locales y controlar a lo BR que miden el rendimiento y toman un camino alternativo. [17]

El router de la Matriz tiene la función de MC del sitio Central y está encargado de asignar y distribuir políticas de PfR para todo el domino de la iWAN. [19]

Por simplicidad, cada sucursal tiene un solo router, de esta manera, el router tomará el papel de MC del sitio remoto y es el encargado de conservar la sincronización con el sitio central, de esta manera se puede tomar una decisión para que el tráfico tome un camino especifico en base al rendimiento.

3.3.2 REQUERIMIENTOS DE DISEÑO DE LA RED iWAN

iWAN requiere configuraciones de algunos protocolos y tecnologías. La Tabla 3.2. muestra las tecnologías que se utilizan en el diseño de la red iWAN.

TABLA 3.2. Tecnologías utilizadas en el diseño.

	TECNOLOGIA	ABREVIATURA	DESCRIPCION
1	Next Hop Resolution Protocol	NHRP	Esta encargado de realizar la identificación del dispositivo al cual se debe enviar un paquete en la subred.
2	Generic Routing Encapsulation	GRE	Permite encapsular toda la información que se requiere enviar entre los routers remotos.
3	Dynamic Multipoint VPN	DMVPN	Esta encargado de realizar la integración entre los

			túneles mGRE creados, haciendo uso de Next Hop Resolution Protocol.
4	Internet Protocol Security	IPSEC	Define los protocolos de seguridad que son utilizados en el diseño de la red.
5	Enhanced Interior Gateway Routing Protocol	EIGRP	Es el protocolo de enrutamiento que permite la conexión de las subredes para cada localidad de forma remota.
6	Detección de envío bidireccional	BDF	Es la tecnología que permite poseer una rápida detección en casa de falta de un enlace.
7	Performance routing v3	PfRv3	Es la tecnología que monitorea el estado de los enlaces y toma una decisión para un mejor camino para un tráfico determinado.

Los router requieren de un sistema operativo que se encargue del buen funcionamiento de las tecnologías mencionadas, no obstante, no todos los modelos de routers soportan todas las versiones de los sistemas operativos, esto dependerá en gran parte de las características de rendimiento del dispositivo a nivel de hardware. [17]

3.4 FASES DE DISEÑO DMVPN

3.4.1 RESUMEN DE LAS FASES DE DISEÑO DMVPN

Para el diseño de una red iWAN, DMVPN posee rutas WAN de modo activo/activo que maximizan el uso de la nube DMVPN para una superposición de IPsec consistente. Se puede utilizar un solo router para realizar las conexiones entre Internet y MPLS, o a su vez se puede utilizar dos routers separados para mayor resistencia. El mismo diseño de la red puede utilizar como transportes MPLS, 3G / 4G o Internet, etc., lo que permite al diseño ser independiente del transporte.

Es recomendable la utilización de un hub DMVPN (PfRv3 BR) por SP para facilitar la configuración del enrutamiento.

DMVPN requiere el uso de Internet Key Management Protocol version 2 (IKEv2) para la detección de actividad de Dead Peer Detection (DPD), que es parte fundamental para facilitar la convergencia rápida y para que el registro de los spokes funcionen de forma correcta en caso de que se vuelva a cargar un hub DMVPN.

DMVPN está compuesta por tres fases, la fase 2 fue creada a partir de la fase 1 pero con funciones adicionales, de igual manera la fase 3 fue creada en función de la fase 1 y fase 2 pero con más funciones. Cada una de las fases DMVPN requiere que el router tenga una interfaz túnel. Los Spokes DMVPN pueden utilizar direccionamiento estático o DHCP para las redes de superposición y transporte, también se puede localizar las direcciones IP de los otros spokes a través de NHRP. [4]

La Figura 3.6 muestra las diferencias de los estándares de tráfico de las tres fases DMVPN. Los modelos de las fases 1,2 y 3 permiten realizar una comunicación directa spoke a hub, esto se puede observar en R1 y R2. El flujo de paquetes spoke a spoke de la fase 1 DMVPN no es igual a la de las fases 2 y 3 DMVPN. El tráfico entre R3 y R4 debe pasar por el hub para la fase 1, durante la creación del túnel dinámico de spoke a spoke para la 2, la fase 3 permite la comunicación directa.

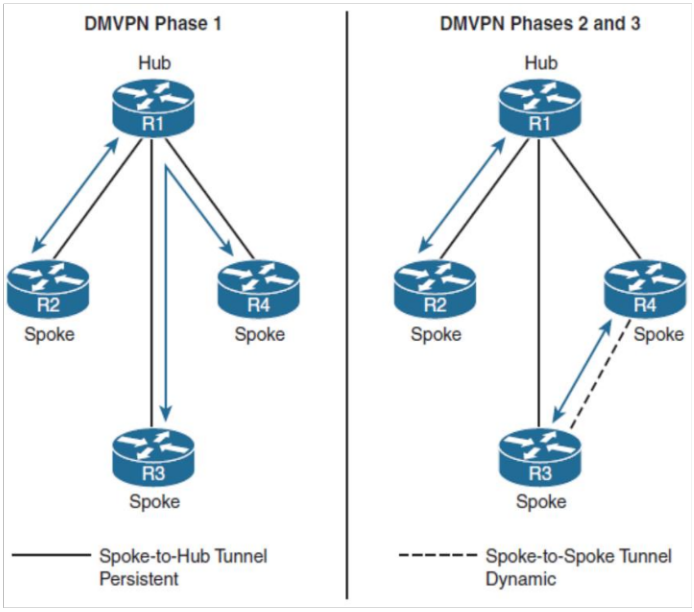

Figura 3.6. Patrones de tráfico de DMVPN en las diferentes fases de DMVPN.

La Figura 3.7 muestra la diferencia de los patrones de las fases 2 y 3 DMVPN con topología jerárquica (multinivel). En el diseño de dos niveles jerárquico, el hub es R2 para el túnel DMVPN 20 y el hub del túnel DMVPN 30 es R3. La conectividad de los túneles DMVPN 20 y 30 se crea utilizando el túnel DMVPN 10. Los tres túneles DMVPN utilizan el mismo túnel DMVPN ID a pesar de que se utilizan diferentes interfaces de túnel. Los túneles DMVP de

la fase 2, el tráfico de R5 fluyen por el hub R2, donde se envía a R3 y después vuelve R6 para que exista una comunicación entre sí. Para los túneles DMVPN de la fase 3, se establece un túnel de spoke a spoke R5 y R6 para su comunicación.

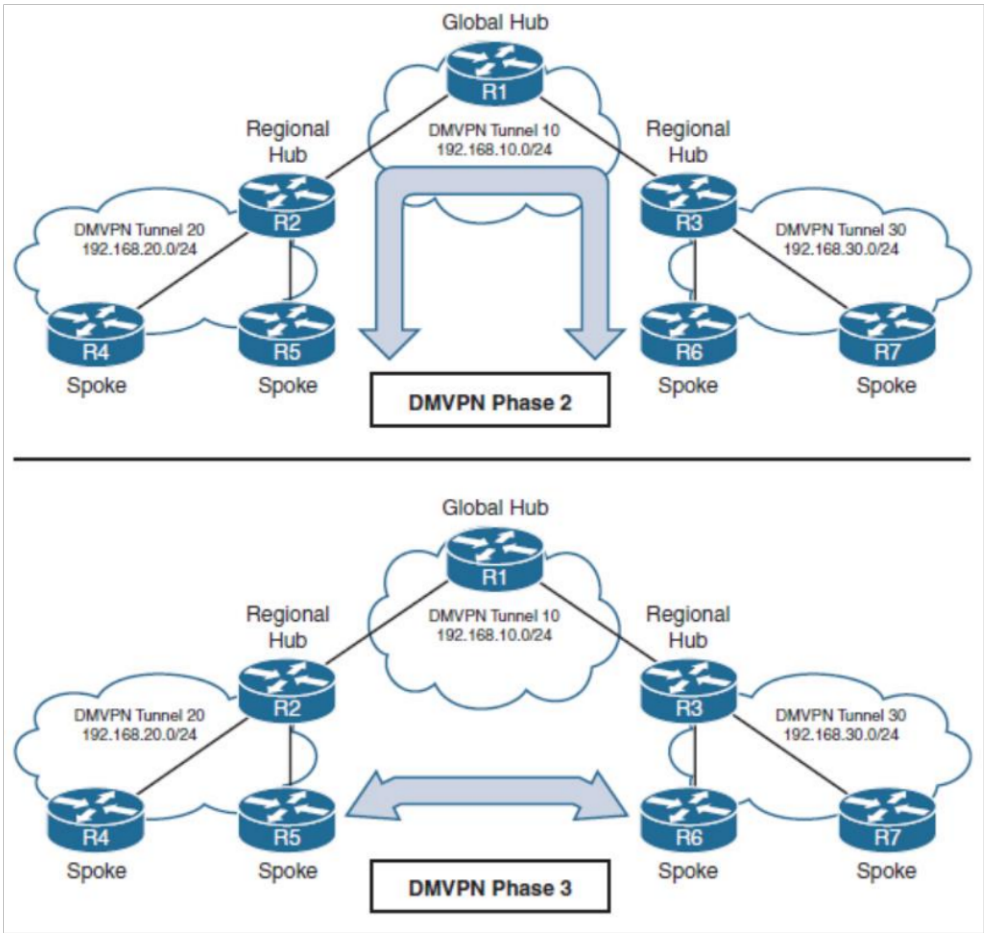

Figura 3.7. Diferencias de los patrones de tráfico entre la fase 2 y 3 de DMVPN.

Existen dos tipos de configuración DMVPN (hub o spoke), que varían de acuerdo a los requerimientos del router. El hub DMVPN es el NHRP NHS, y el spoke DMVPN es el NHRP NHC. Los Spokes deben ser configurados previamente con la dirección IP estática del hub, sin embargo, la dirección IP NBMA de un spoke puede ser asignada desde DHCP o de manera estática.

La Figura 3.8. muestra la primera topología que se utiliza para explicar la configuración y las funciones de DMVPN. R11 tiene la función de hub DMVPN y R31 con R41 son los Spokes DMVPN. Los 3 routers usan una ruta predeterminada estática al router SP que proporciona conectividad para las redes NBMA (transporte) con la red 172.16.0.0/16. Como ejemplo EIGRP se configura para operar en el túnel DMVPN.

.

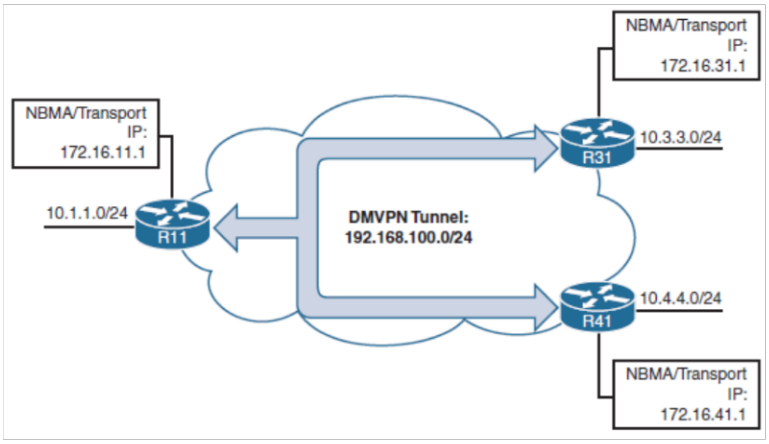

Figura 3.8. Topología simple DMVPN.

3.4.1.1.1 Configuración del Hub DMVPN.

Los pasos para configurar DMVPN en un router hub son:

- **Paso 1.** Crear la interfaz del túnel:
  Se debe utilizar el comando *interface tunnel tunnel-number*.
- **Paso 2.** Identificar la fuente del túnel:
  Para identificar la fuente local del túnel se de utilizar el comando *tunnel source {ip-address | interface-id}*.
- **Paso 3.** Convertir el túnel en una interfaz multipunto GRE:
  Para convertir el túnel en una interfaz multipunto GRE se debe configurar el túnel DMVPN como un túnel mGRE con el comando *tunnel mode gre multipoint*.
- **Paso 4.** Asignar una dirección IP para la red DMVPN (túnel):
  Utilizar el comando *ip address ip-address subnet-mask*.
- **Paso 5.** Habilitar NHRP en la interfaz del túnel.
  Para habilitar NHRP utilizar el comando *ip nhrp network-id*.
- **Paso 6.** Definir la clave del túnel (opcional).
  La clave del túnel se debe configurar con el comando *tunnel key*
- **Paso 7.** Habilitar la compatibilidad con multidifusión para NHRP (opcional).
  Esto debe habilitarse en los roters hub DMVPN con el comando de túnel *ip nhrp map multicast dynamic*.
- **Paso 8.** Habilitar la redirección NHRP (usado solo para la fase 3):
  Utilizar el comando *ip nhrp redirect*.
- **Paso 9.** Definir el ancho de banda del túnel (opcional):
  Se define con el comando *bandwidth que se mide en kilobits por segundo*.
- **Paso 10.** Definir la IP MTU para la interfaz de túnel (opcional):
  La IP MTU se debe configurar utilizando el comando *ip mtu mtu*. Por lo general, se usa una MTU de 1400 para los túneles DMVPN.

- **Paso 11.** Definir el tamaño de segmento máximo de TCP (MSS) (opcional):
  Utlizar el comando *ip tcp adjust-mss mss-size*.
  Por lo general, las interfaces DMVPN usan un valor de 1360 para acomodar los encabezados IP, GRE e IPsec.

Las tres fases de DMVPN se resumen a continuación:

3.4.1.2 Fase 1 DMVPN (Spoke a Hub)

La fase 1 DMVPN se basa en la funcionalidad Hub and Spoke:

- Es una configuración más pequeña y de forma simplificada en los hubs.
- Acepta CPE direccionados de forma dinámica (NAT).
- Posee soporte para los protocolos de enrutamiento y multidifusión.
- Los spokes se pueden resumir en el hub, sin la necesidad de una tabla completa de enrutamiento.

3.4.1.2.1 Configuración de la fase 1 spoke DMVPN (punto a punto) [20]

La configuración de la fase 1 de los spokes DMVPN es parecida a la configuración de un router hub, sin embargo, se tiene las siguientes sugerencias:

- No se debe utilizar un túnel mGRE. En su lugar, se debe especificar el destino del túnel.
- El mapeo de NHRP apunta al menos un NHS activo.

Proceso de configurar del router spoke DMVPN de la fase 1 es el siguiente:

- **Paso 1.** Crear la interfaz del túnel:
  Para crear la interfaz del túnel se debe utilizar el comando *tunnel-number*.
- **Paso 2.** Identificar la dirección IP del destino remoto:
  Para identificar la dirección IP del destino remoto se debe realizar la identificación del túnel con el comando *ip-address*.
- **Paso 3.** Identificar la fuente del túnel:
  Para identificar la fuente del túnel se debe utilizar el comando de parámetros de interfaz *{ip-address | interface-id}*.
- **Paso 4.** Definir el destino del túnel (hub):
  Para defnir el destino del túnel se debe utilizar el comanado *ip-address*.
- **Paso 5.** Asignar una dirección IP para la red DMVPN (túnel):
  Se utilizar el comando ip address {*ip-address subnet-mask | dhcp*} o el comando *ipv6 address*{*ipv6-address/prefix-length*}.

- **Paso 6.** Habilitar NHRP en la interfaz del túnel:
  Para habilitar NHRP en la interfaz del túnel se debe utilizar el comando *ip nhrp network-id*.
- **Paso 7.** Definir la clave del túnel NHRP (opcional):
  Para definir la clave del túnel NHRP se de configurar con el comando *tunnel key*.
- **Paso 8.** Especificar el NHRP NHS, la dirección NBMA y la asignación de multidifusión:
  Para poder specificar la dirección de uno o más servidores NHRP NHS se debe utilizar el comando *nhs-address o nbma-address* [multicast].
- **Paso 9.** Definir el ancho de banda del túnel (opcional):
  El ancho de banda se define con el comando *bandwidth y* se mide en kilobits por segundo.
- **Paso 10.** Definir la IP MTU para la interfaz de túnel (opcional):
  La IP MTU se configura con el comando *ip mtu mtu*. Por lo general, se utiliza una MTU de 1400 para túneles DMVPN.
- **Paso 11.** Definir el TCP MSS (opcional):
  El comando que se deb utilizar la definir el TCP MSS es *ip tcp adjust-mss mss-size*. Por lo general, las interfaces DMVPN usan un valor de 1360 para acomodar los encabezados IP, GRE e IPsec.

3.4.1.3 Fase 2 DMVPN (Spoke a Spoke)

La fase 2 de DMVPN no tiene resumen en el hub, esto quiere decir que cada spoke tiene el siguiente salto (dirección de spoke) para cada prefijo de destino. PfR tiene toda la información para hacer cumplir la ruta con PBR dinámico y la información correcta del siguiente salto. [4]

3.4.1.4 Fase 3 DMVPN (Árbol jerárquico Spoke a Spoke)

La fase 3 de DMVPN permite el resumen de rutas:

- Para realizar la búsqueda de la ruta principal, solo está disponible la ruta al hub.
- NHRP instala dinámicamente el túnel de acceso directo y, por lo tanto, completa RIB / CEF.
- PfR todavía tiene la información del siguiente salto del hub y actualmente no está al tanto del cambio del siguiente salto.
- PfRv3 admite todas las fases de DMVPN.

3.4.1.4.1 Configuración de la fase 3 DMVPN (multipunto) [15]

La configuración de la fase 3 DMVPN del router hub inserta el comando de parámetro de interfaz *ip nhrp redirect* en el router hub. Este comando verifica el flujo de paquetes en la

interfaz del túnel y envía un mensaje de redirección al router spoke de origen cuando detecta paquetes que salen de la nube DMVPN.

La configuración de la fase 3 de DMVPN para los routers spokes usa la interfaz de túnel GRE multipunto y usa el comando *ip nhrp shortcut* en la interfaz del túnel.

El proceso de configuracion del router Spoke de la fase 3 DMVP es el siguiente:

- **Paso 1.** Crear la interfaz del túnel:
  Para crear la interfaz del túnel se debe utilizar el comando *número-túnel*.
- **Paso2.** Identificar la fuente del túnel:
  Para identificar la fuente local del túnel se debe utilizar el comando *tunnel source* {*ip-address* | *interface-id*}.
- **Paso 3.** Convertir el túnel en una interfaz mGRE:
  Para configurar el túnel DMVPN como un túnel mGRE se debe utilizar el comando de parámetro de interfaz *tunnel mode gre multipoint*.
- **Paso 4.** Asignar una dirección IP para la red DMVPN (túnel):
  Para asignar una dirección IP para la red DMVPN se configura una dirección IP a la interfaz con el comando *ip address p-address subnet-mask*.
- **Paso 5.** Habilitar NHRP en la interfaz del túnel:
  Para habilitar NHRP y poder identificar de forma exclusiva el túnel DMVPN para la interfaz virtual se debe utilizar el comando *ip nhrp network-id*.
- **Paso 6.** Definir la clave del túnel (opcional):
  La clave del túnel se configura con el comando *tunnel key*. Las claves del túnel deben coincidir para que se establezca un túnel DMVPN entre dos routers.
- **Paso 7.** Habilitar el acceso directo NHRP:
  Para Habilitar la función de acceso directo de NHRP se debe utilizar el comando *ip nhrp shortcut*.

- **Paso 8.** Especificar el NHRP NHS, la dirección NBMA y la asignación de multidifusión:
  Para especificar la dirección de uno o más NHRP NHS se debe utilizar el comando *ip nhrp nhs nhs-address nbma nbma-address [multicast]*.
- **Paso 9.** Definir la IP MTU para la interfaz de túnel (opcional):
  MTU se debe configurar con el comando de parámetro de interfaz *ip mtu mtu*. Por lo general, se usa una MTU de 1400 para los túneles DMVPN.
- **Paso 10.** Definir el TCP MSS (opcional):
  El comando a utilizar es *ip tcp adjust-mss mss-size*. Por lo general, las interfaces DMVPN usan un valor de 1360 para acomodar los encabezados IP, GRE e IPsec.

3.5 EVALUACIÓN DE LAS FASES DE DISEÑO DMVPN

3.5.1 EVALUACIÓN DE LA FASE 1 DE DMVPN

La fase 1 es la primera implementación de DMVPN que provee de una implementación sin contacto para sitios VPN. Los túneles VPN se pueden crear solo en sitios spoke y hub. El tráfico que atraviesa los Spokes, primero pasa por el hub y de esta manera, este tráfico podrá llegar al otro spoke. [21]

3.5.2 EVALUACIÓN DE LA FASE 2 DE DMVPN

La fase 2 de DMVPN entrega una capacidad adicional a la fase1, esto permite que la comunicación sea spoke a spoke de manera dinámica, gracias a esto crear un túnel VPN con características solicitadas por le hub. En esta fase no se permite el next-hob preservation. En consecuencia, no se puede realizar la comunicación de spoke a spoke entre diferentes redes DMVPN. [21]

3.5.3 EVALUACIÓN DE LA FASE 3 DE DMVPN

Esta fase perfecciona la comunicación de spoke a spoke al mejorar la comunicación NHRP e interactuar con la tabla de enrutamiento. En la fase 3 el hub envía mensajes de redirección NHRP al spoke que origino el flujo de paquetes. El mensaje de redirección de NHRP proporciona la información requerida para que le spoke de origen inicie la resolución del host/red destino. PfR3 agrega soporte de API a la fase 3 DMVPN.

NHRP adiciona una entrada de ruta más explícita a la tabla de enrutamiento o instala rutas en la tabla para los accesos directos que modifican la entrega del siguiente salto de las rutas existentes. Debido a que los accesos directos de NHRP instalan rutas más explicitas en la tabla de enrutamiento, esta fase permite el resumen de redes en el hub y proporciona enrutamiento optimo en los routers Spokes. [21]

4 RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

4.1 RESUALTADOS

Las mejoras obtenidas con el diseño de la red iWAN se muestran en la Tabla 4.1

Tabla 4.1. Resultados del diseño de la red iWAN

Resultados	iWAN	WAN
Costo de implementación	El costo de implementación es bajo.	El costo de implementación es más costoso.

Implementación	Su implementación es más fácil y simplificada.	Su implementación es más complicada.
Redundancia	La redundancia entre los enlaces de las localidades se da de acuerdo con el esquema Activo/Activo.	La redundancia entre los enlaces de las localidades se da de acuerdo con el esquema Activo/Pasivo.
Control de ruta	Posee control de ruta inteligente	Posee un enlace principal y un enlace de backup
Ancho de banda	Optimiza el ancho de banda.	No utiliza el ancho de banda de forma adecuada.
Seguridad de la información	Permite tener control de ruta inteligente, mejor rendimiento, así como el cifrado del tráfico que pasa por los enlaces hacia cada destino	No posee una adecua seguridad de la información y puede ser vulnerable a diferentes tipos de ataques.
Tecnología que posee	Posee una superposición IPsec DMVPN	Posee dos tecnologías IPsec GETVPN sobre MPLS DMVPN por Internet.
Numero de dominios	Utiliza un solo dominio de enrutamiento WAN sin redistribución de rutas ni filtrado de rutas	Posee dos dominios de enrutamiento WAN.
Tipos de dominios	Para el dominio se utiliza protocolos de enrutamiento: iBGP, OSPF o EIGRP	Los dominios de enrutamiento son: MPLS: eBGP o Static

		Internet: iBGP, OSPF o EIGRP.
Conectividad	Posee una conectividad segura mediante un conjunto de protocolos IPsec	Posee conectividad que puede ser vulnerable.
Transporte de información	Posee independencia de transporte con el uso de la tecnología DMVPN.	La información se transmite mediante dos enlaces uno principal y uno de back up.
Diseño	El diseño de IWAN es prescriptivo para reducir las posibles combinaciones, lo que reduce la complejidad y el costo para los clientes que desean un enfoque simplificado.	Este diseño tiene más opciones de transporte para clientes que tienen necesidades variadas, pero debido a la flexibilidad adicional, la complejidad es mayor.

4.2 CONCLUSIONES

La tecnología iWAN permite elegir una trayectoria o ruta de manera inteligente optimizando el rendimiento de la red con la utilización de circuitos WAN cifrados que pasan por los enlaces y sus diferentes destinos.

La tecnología iWAN aporta soluciones de implementación para empresas que requieran una WAN independiente del transporte con costos más bajos, también permite aprovechar al máximo los servicios de transporte que optimizan el ancho de banda sin afectar la confiabilidad, el rendimiento o la seguridad de las aplicaciones basadas en la nube.

La tecnología DMVPN puede proporcionar independencia de trasporte, también se puede crear túneles privados desde un lugar remoto hasta una matriz o punto central, el transporte a utilizar no tiene importancia y puede ser: internet, una red brindada por ISP con MPLS, o incluso un acceso provisto por un celular.

La tecnología iWAN permite obtener ruta inteligente utilizando la tecnología PfR, con la cual se puede realizar el monitoreo del rendimiento en las WAN tomando en cuenta la utilización o el retardo de los enlaces, si se presenta una congestión, MC toma decisiones según las especificaciones del usuario para que el tráfico utilice un enlace menos utilizado y evitar la degradación del servicio.

PfR permite al administrador de red supervisar la fluctuación, retrasos y perdida de paquetes, para tomar la decisión de volver a enviar las aplicaciones por la ruta de mejor rendimiento de acuerdo con las políticas de ampliación definida. En esencia, PfR asegura que la ruta tomada cumplirá con los requisitos establecidos para esa aplicación.

Con la utilización de protocolos IPSec se puede obtener conectividad segura. IPSec se encarga de asegurar que los puntos remotos cumplan con los requerimientos de autenticación de la matriz, de esta manera se puede crear túneles cifrados y seguros, permitiendo así que el flujo de paquetes que pasan por aquí no puedan ser alterados en toda su trayectoria.

La tecnología iWAN optimiza el ancho de banda en todos los lugares que el usuario lo requiera, también puede obtener un mejor rendimiento para las diferentes aplicaciones que se requieran utilizar, en el caso de obstrucción, iWAN proporciona un mecanismo para entregar el tráfico con criterios de calidad de servicio, que permiten poseer prioridad de cierto tráfico sobre otros que el usuario considere de menor importancia.

Gracias a la fácil implementación de la infraestructura iWAN se puede reducir el costo de implementación y los gastos de prestación de servicios, los administradores de red tienen la opción de utilizar cualquier tipo de ISP, esto permite tener transportes de paquetes a menor costo sin afectar la seguridad, la confiabilidad y el rendimiento de la red.

IWAN al tener una red con reconocimiento de aplicaciones permite obtener el rendimiento óptimo de la red WAN, también se puede configurar la red para administrar servicios críticos para las empresas y resolver problemas de red de forma rápida.

PfR de Cisco mejora del rendimiento de las aplicaciones y de la red, mejora la disponibilidad de las aplicaciones, solo necesita pequeñas cantidades de configuración, reduce los gastos de WAN en términos de operación, distribuye de manera eficiente el tráfico en función de la carga, el rendimiento y otras métricas.

Tomando en cuenta que el enrutamiento es muy complejo, debido a la gran cantidad de trayectorias que debe cruzar un paquete antes de llegar a su destino, la tecnología iWAN

optimiza el ancho de banda reduciendo los costos de operación de las WAN sin afectar la seguridad, la confiabilidad o el rendimiento de las redes.

4.3 RECOMENDACIONES

Para la implementación de la red diseñada, se recomienda revisar el estado de arte de la tecnología iWAN, debido a que sebe elegir el tipo de protocolo de enrutamiento de acuerdo a los requerimientos de la empresa que desea realizar su implementación.

Se recomienda a la organización que desea implementar esta tecnología contrate enlaces WAN con diferentes ISP debido a que esto no afecta en la implementación ya que iWAN posee independencia de trasporte. La organización o empresa debe contratar un ISP que le garantice a los usuarios la entrega de sus servicios, de la misma manera, la organización debe hacer un análisis de la tecnología de transporte a utilizar, teniendo en consideración que los servicios corporativos tiene una mejor atención y resolución de problemas que un enlace residencial.

Para minimizar la carga de la WAN se recomienda utilizar una comprensión avanzada, de esta manera se reduce el consumo de nacho de banda de forma notablemente gracias a la utilización de una transferencia de datos redundante y comprensión avanzada, obteniendo de esta manera que el rendimiento sea mejor con la menor carga posible.

Para un adecuado diseño de la red se recomienda tener la documentación completa y disponible para la persona encargada de administrar la red, esta documentación debe tener la topología de la empresa, diagramas lógicos y físicos de cada enlace de red. Esta información es esencial sin importar el tamaño de la organización. Adicional, el inventario debe tener identificando las versiones de los routers, modelos, versiones del sistema operativo y licencias activas, esto ayuda a identificar con mayor facilidad las necesidades que se deben cumplir previo a la implementación de la iWAN.

Para la configuración de DMVPN se recomienda, en cualquier tipo de escenario se deben diferenciar los VPNs convencionales, y de esta manera la configuración de los Spokes y hubs se reduce significativamente, esto conlleva a que los equipos que son empleados no tengan que ser muy robustos para su funcionamiento. Cabe recalcar, que es posible comprobar que el spoke nuevo de la red no afecte la configuración del hub.

En el diseño de la red se recomienda utilizar dos routers en la central, de esta manera se puede separar las funciones del MC y RB que reciben los enlaces WAN. EN red pequeña con pocas localidades, un solo router puede cumplir con las dos funciones sin impactar de

forma significativa la capacidad de procesamiento, pero, a medida que la infraestructura crezca y aumente la utilización de routers o se agreguen más subredes aumenta el consumo de recursos del MC, para esto se recomienda que se maneje un router dedicado de manera específica al monitoreo del rendimiento de los enlaces.

5 REFERENCIAS BIBLIOGRÁFICAS

[1] J.-M. B. D. P. A. L. N. B.-D. Brad Edgeworth, «Performance Routing (Pfr),» de *Cisco Intelligent WAN (IWAN)*, Indianapolis, Cisco Press, 2017, p. 327.

[2] C. R. V. ABAD, «Estudio para optimizar los multi-objetivos para el enrutamiento multicast en redes superpuestas mediante algoritmos evolutivos en las redes de un,» Quito, 2014.

[3] J.-M. B. D. P. A. L. N. B.-D. Brad Edgeworth, «Path Control Used in Routing protocol,,» de *Cisco Intelligent WAN (IWAN)*, Indianapolis, Cisco Press, 2017, pp. 329-330.

[4] N. Garg, «cisco.com,» 19 febrero 2021. [En línea]. Available: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/performance-routing-pfr/200281-Introduction-To-IWAN-And-PfRv3.html#anc0. [Último acceso: 6 Diciembre 2021].

[5] A. S. Gillis, «techtarget.com,» 19 febrero 2021. [En línea]. Available: https://www.techtarget.com/searchnetworking/definition/Cisco-Performance-Routing-PfR. [Último acceso: 6 diciembre 2021].

[6] Cisco, Intelligent WAN Deployment Guide, indianaplois: cisco press, 2017.

[7] C. R. W. ECHEVERRIA, *DISEÑO E IMPLEMENTACIÓN DE LA TECNOLOGÍA IWAN Y SEGURIDAD NGFW EN LA ADUANA NACIONAL,* Bolivia, 2018.

[8] CISCO, *Intelligent WAN and WAN,* cisco.com, 2016.

[9] J.-M. B. D. P. A. L. N. B.-D. Brad Edgeworth, «Introduction to the IWAN Domain,» de *Cisco Intelligent WAN (IWAN)*, Indianapolis, Cisco Press, 2017, p. 339.

[10] Cisco, *El arte de las redes centradas en las aplicaciones,* cisco.com, 2011.

[11] J.-M. B. D. P. A. L. N. B.-D. Brad Edgeworth, «EIGRP for IWAN,» de *Cisco Intelligent WAN (IWAN)*, Indianapolis, ciscopress, 2017, p. 122.

[12] J.-M. B. D. P. A. L. N. B.-D. Brad Edgeworth, «Border Gateway Protocol (BGP),» de *Cisco Intelligent WAN (IWAN)*, Indianapolis, cisco.press, 2017, p. 151.

[13] A. F. ,. R. G. R. Brad Edgeworth, IP Routing on Cisco IOS,IOS XE, and IOS XR, Indianapolis: Cisco Press, 2014.

[14] Y. T. L. a. S. H. R. 4. Rekhter, «datatracker.ietf.org,» enero 2006. [En línea]. Available: https://datatracker.ietf.org/doc/html/rfc4271. [Último acceso: 7 11 2021].

[15] J.-M. B. D. P. A. L. N. B.-D. Brad Edgeworth, « Dynamic Multipoint VPN (DMVPN),» de *Cisco Intelligent WAN (IWAN)*, Indianapolis, Cisco Press, 2017, p. 8.

[16] Cisco, «cisco.com,» cisco, 19 enero 2018. [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nhrp/configuration/xe-3s/nhrp-xe-3s-book/config-nhrp.html. [Último acceso: 12 11 2021].

[17] N. Z. G. E. GARCÍA VARGAS JUAN FERNANDO, *MEJORAMIENTO EN EL USO DE LOS ENLACES WAN PARA CLIENTES CORPORATIVOS EN UNA EMPRESA DE TELECOMUNICACIONES USANDO LA SOLUCIÓN DE CISCO INTELLIGENT WAN,* Guayaquil –, 2018.

[18] J.-M. B. D. P. A. L. N. B.-D. Brad Edgeworth, «EIGRP for IWAN,» de *Cisco Intelligent WAN (IWAN)*, Indianapolis, Cisco Press, 2017, pp. 122-137.

[19] J.-M. B. D. P. A. L. N. B.-D. Brad Edgeworth, «Performance Routing (Pfr),» de *Cisco Intelligent WAN (IWAN)*, Indianapolis, Cisco Press, 2017, p. 328.

[20] J.-M. B. D. P. A. L. N. B.-D. Brad Edgeworth, «DMVPN Hub Configuration,» de *DMVPN Hub Configuration*, DMVPN Hub Configuration, Cisco Press, 2016, pp. 48-50.

[21] L. Carvajal, Metodología de la Investgación Científica. Curso general y aplicado, 28 ed., Santiago de Cali: U.S.C., 2006, p. 139.

[22] P. B. DAISSY MARÍA, «CONMUTACIÓN, ENRUTAMIENTO Y,» CARTAGENA DE INDIAS , 2004.

[23] Cisco, «Intelligent WAN,» abril 2017. [En línea]. Available: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Oct2016/CVD-IWANDesign-2016OCT.pdf. [Último acceso: 6 Diciembre 2021].