FACULTAD DE INGENIERÍA

MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

MENCIÓN REDES DE COMUNICACIONES

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE MÁSTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN REDES DE COMUNICACIONES

Tema: Diseño y prueba de concepto de DMVPN-MPLS sobre protocolo de internet IPv6 como red de transporte empresarial

AUTOR: MARYURI MARCELA OJEDA JORDAN

QUITO, 2021

CONTENIDO

CONTENIDO DE FIGURAS

CONTENIDO DE TABLAS

Resumen

La presente disertación se enfocó en un diseño y prueba de concepto de DMVPN-MPLS sobre protocolo de internet IPv6 como red de transporte empresarial. Para el alcance del objetivo se empleó pruebas experimentales, se utilizó para el diseño, topologías de red en base a los conocimientos obtenidos en DMVPN en IPv4. Adicional se analizó el protocolo mGRE y NHRP en IPv6 y su forma de operación en DMVPN fase 3. Durante el diseño, se incluyó los requisitos mínimos recomendados por Cisco, en lo que comprende a hardware y software, tanto para un ambiente de pruebas y un ambiente real en producción. Se realizó pruebas donde se evaluó indicadores como confiabilidad, escalabilidad y latencia para validar la funcionalidad y desempeño de DMVPN. Durante las pruebas de conectividad, se monitoreo la red donde se validó que DMVPN mantuvo valores promedios para una comunicación estable. Adicional, se incluyó una investigación de SD-WAN como red de transporte empresarial, su arquitectura lógica y física, y su forma de operar. Se incluyó el funcionamiento de protocolo de vector distancia EIGRP en IPv6 como protocolo dinámico para la comunicación entre sedes, su funcionamiento, configuración e integración con DMVPN. Se desarrolló un análisis de costos aportando de forma oportuna y permitiendo validar que la solución es viable sobre servicio de internet. Se validó con la prueba de concepto, que DMVPN-MPLS sobre protocolo de internet IPv6 fue viable y exitosa, tanto en la parte técnica y económica, siendo así, una solución innovadora para las redes WAN tradicionales.

Abstract

The present dissertation focused on a design and proof of concept of DMVPN-MPLS over IPv6 internet protocol as an enterprise transport network. To achieve the objective, experimental tests were used, it was used for the design, network topologies based on the knowledge obtained in DMVPN in IPv4. Additionally, the mGRE and NHRP protocol in IPv6 and its mode of operation in DMVPN phase 3 were analyzed. During the design, the minimum requirements recommended by Cisco were included, in terms of hardware and software, both for a test environment and a real environment in production. Tests were carried out where indicators such as reliability, scalability and latency were evaluated to validate the functionality and performance of DMVPN. During the connectivity tests, the network was monitored where it was validated that DMVPN maintained average values for stable communication. Additionally, an investigation of SD-WAN as an enterprise transport network, its logical and physical architecture, and its way of operating was included. The operation of the EIGRP distance vector protocol was included in IPv6 as a dynamic protocol for communication between sites, its operation, configuration and integration with DMVPN. A cost analysis was developed, contributing in a timely manner and allowing to validate that the solution is viable on internet service. It was validated with the proof of concept, that DMVPN-MPLS over IPv6 internet protocol was viable and successful, both in the technical and economic part, thus being an innovative solution for traditional WAN networks.

Introducción

En la actualidad, se ha producido un aumento substancial de tráfico de información, dado que, el cambio en la forma de comunicación de las empresas y el giro de negocio que han adaptado últimamente, ha generado que evolucione a pasos gigantescos la tecnología, este nuevo cambio ha permitido una búsqueda constante de diseños de red cada día más inteligentes y seguras, donde prevalezca características como: el alto rendimiento, la flexibilidad, la escalabilidad, la integridad y seguridad, sobre todo en lo que comprende su red privada y red pública. Por otra parte, este aumento de tráfico ha generado que las vulnerabilidades en las redes corporativas se presenten con mayor frecuencia y han obligado a los administradores de redes por soluciones integrales que permitan minimizar y asegurar la seguridad en la información.

La realidad que vive el país y a nivel mundial, ha permitido y obligado a generar nuevos modelos para realizar nuestras actividades, es así el caso de las funciones laborales. Para que las empresas sigan funcionando en una nueva realidad, donde todos deben estar conectados, es necesario y emergente migrar al proceso de digitalización y así mantenerse en el mercado, es decir, los empleados deben seguir cumpliendo sus funciones en espacios diferentes y con nuevas tecnologías y mantener así la continuidad del negocio.

El arrendamiento de espacios para una red dedicada tiene un alto costo, porque los proveedores de servicio de internet reservan espacios en sus infraestructuras de una forma exclusiva para sus clientes; por este servicio se cancela valores mensuales o anuales, lo que implicaría costos muy elevados al presupuesto de una empresa. La inestabilidad económica que atraviesan las pequeñas, medianas y grandes empresas, no permite que sigan invirtiendo en equipamiento, por ello es necesario aprovechar todos los recursos que se encuentra implementado actualmente en su infraestructura tecnológica.

El diseño de red en una empresa debe contar con un análisis inteligente, porque debe afrontar una gran demanda de los requerimientos de los usuarios y la posibilidad de adaptarse a nuevas tecnologías, por esto, se convierte en un reto para los administradores de una red, puesto que, deben analizar información, procesar datos, monitorear enlaces, gestionar tráfico, mantener la integridad, confidencialidad y flexibilidad en una red empresarial; todo ello para que una empresa tenga estabilidad y pueda mantenerse en el mercado.

El estudio planteado tendría un gran impacto en la evolución de las redes de área extensa WAN tradicionales que se encuentran implementadas en las redes corporativas

en el país, debido a que el aprovisionamiento de IPv4 es limitado y es emergente la migración a direccionamiento IPv6.

El gran desafío que presentan las redes empresariales, es contar con una solución integral, es decir, que cumpla con los nuevos desafíos de las telecomunicaciones y satisfaga las necesidades de los departamentos de tecnología de información, este gran objetivo se cumpliría con el diseño e implementación de una Red Privada Virtual Dinámica Multipunto DMVPN, por ello la investigación sería de gran aporte en el sector empresarial, que está creciendo e innovando en su forma de comunicación, en definitiva, el primer paso para este crecimiento es innovar en nuevas soluciones WAN.

La presente disertación tiene como propósito de investigación, el diseño y prueba de concepto de DMVPN-MPLS sobre protocolo de Internet IPv6 como red de transporte empresarial; para cumplir el objetivo se ha desarrollado cinco capítulos que se resumen a continuación:

El capítulo I, consta de los fundamentos teóricos de las tecnologías y protocolos, que son necesarias para el despliegue de una red de transporte DMVPN en IPv6.

El capítulo II, se detalla la arquitectura y los mecanismos que utiliza DMVPN como red de transporte; así como la evolución y mejora de cada una de sus fases. En este capítulo se incluye un estudio sobre las redes de área extensa definidas por software SD-WAN; donde se define su arquitectura y su forma de operar como red de transporte en las empresas corporativas.

El capítulo III, se plantea la solución propuesta con base en los capítulos I y II, se desarrolla mediante un diseño físico y un diseño lógico de la red DMVPN en IPv6. Durante este capítulo se especifica el equipamiento, las tecnologías y los protocolos de enrutamiento que se utiliza para la prueba de concepto.

El capítulo IV, consta del despliegue de la topología diseñada, donde se implementa las tecnologías y protocolos de red mencionados en los capítulos iniciales; por consiguiente, la configuración sobre los equipos.

Capítulo V, se ejecutan pruebas de conectividad; donde se afirmaría si la solución es factible o no; y de ser así, la posibilidad de ser considerada como una red de transporte en IPv6.

Justificación

La presente disertación tiene como propósito el estudio del concepto de diseño de DMVPN-MPLS sobre protocolo de internet IPv6 para comprobar su desempeño como red de transporte empresarial.

Los resultados obtenidos permitirán considerar el rendimiento de una red WAN y LAN aplicando DMVPN, con el fin de crear canales dinámicos de transmisión de datos. A su vez, con el análisis de costos permitirá ser considerada una opción técnica y económicamente factible en la implementación de enlaces confiables y estables para la transmisión de información en tiempo real entre varias sedes.

El presente estudio permitirá evaluar el desempeño de la técnica DMVPN para el diseño de una red WAN y LAN segura, confiable y con un alto grado de escalabilidad. Al mismo tiempo, la evolución de DMVPN permitirá tener mayor alcance en la comunicación tradicional, estableciendo canales dinámicos entre diferentes sedes, creando así una red con topología tipo malla.

Las pruebas de conectividad y verificación de resultados de la prueba de concepto aportarán datos teóricos y prácticos sobre el desempeño de DMVPN y permitirá a los administradores de redes obtener una solución comprobada para la transmisión de servicios, con una disminución de costos de sus comunicaciones al no requerir canales de datos dedicados y obtener un grado de independencia con relación a los proveedores de servicios de internet.

Objetivos

a) Objetivo General

I. Realizar una propuesta de diseño y prueba de concepto de DMVPN-MPLS sobre protocolo de Internet IPv6 como red de transporte empresarial en la ciudad de Quito.

b) Objetivos Específicos

I. Analizar la tecnología MPLS y conceptos de diseño que permitan mejorar la seguridad en el tratamiento de la información de las redes de empresariales.

II. Diseñar una red transporte DMVPN-MPLS sobre protocolo de internet IPv6, con los datos obtenidos en el análisis de la tecnología; para la optimización de los recursos de la red y se minimice las posibles vulnerabilidades en la seguridad de la información.

III. Implementar una solución de conectividad DMVPN-MPLS para que los recursos de la red siempre se encuentren accesibles a los usuarios y exista seguridad en la información.

IV. Realizar pruebas de conectividad y validación de resultados de la prueba de concepto de la red DMVPN sobre IPv6.

V. Realizar pruebas de diagnóstico del rendimiento de la red DMVPN, mediante analizadores de tráfico, con ello se demuestra que la nueva solución aporta en una comunicación estable y en seguridad de la información.

Capítulo 1: Marco Teórico

1.1 Antecedentes

El desarrollo del presente proyecto se enfoca en un diseño de mejora de una red MPLS, con una nueva propuesta de diseño y prueba de concepto de DMVPN. Las redes MPLS habían brindado rendimiento y confiabilidad; y, en la actualidad lo siguen brindando, sin embargo, la gran demanda de los requerimientos por parte de las micro, medianas y grandes empresas ha generado un crecimiento de forma exponencial en nuevas topologías de red, puesto que, deben ser aún más inteligentes, más estables y con un mayor grado en la seguridad durante la transmisión de información. Parte de ahí que las redes MPLS tuvieron la necesidad de ir innovando e ir integrando a nuevas tecnologías en las comunicaciones. Este es el caso de DMVPN, sobre esta tecnología han realizado varios estudios donde demuestran su funcionalidad y su alto rendimiento en las comunicaciones, habría decir que, lo consideran como un antecesor de SD-WAN, como lo indica (Seremet & Causevic, 2019), donde plantea un análisis entre las redes MPLS y SD-WAN.

En estudios realizados, señalaban que el año en curso, las grandes empresas triplicarían el uso de arquitecturas SD-WAN, esto debido al gran número de ventajas que ofrece la tecnología, como es, la optimización de los recursos de red y la calidad de servicio QoS de las aplicaciones distribuidas como lo indica (Kouicem et al., 2017). Con base en este estudio, se logra conocer cuál era la proyección que se tenía para el tráfico IP para el año 2020, según señala que sería de 2,3 ZB (zettabytes 1 ZB es igual a 1 trillón de GB), pero debido a la crisis mundial y las consecuencias de la nueva realidad, estos índices se vieron afectados de forma significativa, por lo que es necesario optar por soluciones rentables y escalables, donde se explotaría todos los recursos de una red nueva o que se encuentre desplegada en una pequeña y/o mediana empresa.

El artículo (Ghretli & Almukhtar, 2019), sirve de aporte para la elaboración de la prueba de concepto, donde se demuestra la escalabilidad y la fácil implementación de una red DMVPN donde la seguridad en la información prevalece sin interferencia del proveedor de servicios. Además, se demuestra, que los recursos de los enrutadores como cpu, memoria, ancho de banda no se ven afectados y se optimizan de forma significativa.

Apegados a la nueva realidad, el teletrabajo ha permitido mantener a la mayoría de los empleados un alto rendimiento y mejorar su productividad, pero el trabajo a larga distancia ha generado que utilicen nuevas plataformas para mantener la comunicación, de manera que, el uso de nuevas plataformas ha generado diversos tipos de tráfico que se han ido creando sobre el internet, es el caso de, Voz sobre IP VoIP, que consiste en la

transmisión de tráfico de voz sobre redes basadas en internet, puesto que, se ha convertido en una solución indiscutible sobre la redes de telefonía tradicional, las redes DMVPN garantizan y aseguran la prioridad en este tipo de transmisión de datos desde una sede remota hasta su sede principal, como lo da conocer la investigación (Radcliffe et al., 2019), en donde se cumple con el objetivo de la priorización de tráfico en una red DMVPN como lo menciona (Kouicem et al, 2017).

Con base en investigaciones, se ha ratificado que DMVPN, funciona de forma correcta en transportación de tráfico de video, como lo menciona el estudio, donde logran integrar diferentes tecnologías y como resultado brindan un servicio de videoconferencia de excelente calidad. DMVPN busca estos resultados, tener un alto rendimiento sobre todas las sedes que forman parte de la red privada virtual.

Según el Registro de Direcciones de Internet de América Latina y Caribe LACNIC, en su sitio oficial (Lacnic, 2020), revela que se encuentra en la fase 3 del agotamiento de direcciones IPv4, señalando que de los 5’548.288 de IP que forman este bloque, al mes de junio 2020 se encuentran disponibles únicamente 541.696 direcciones IP, esto es equivalente a un 9.8%, es decir una cantidad muy reducida para el aprovisionamiento de direcciones, por esto, la prioridad de todo el sector empresarial es la pronta migración de sus infraestructuras a direccionamiento IPv6. Dado que a las estadísticas son inquietantes, DMVPN se convierte en una solución rentable en las empresas que hoy se encuentran en proceso de migrar a direccionamiento IPv6

1.2 Fundamentos Teóricos

1.2.1 Red De Transporte Empresarial

Las redes de transporte conocidas como WAN tienen como función principal el transportar información de forma bidireccional y direccional en grandes áreas geográficas, esto de una forma segura, manteniendo la privacidad y seguridad de la información; siendo lo ideal desde el origen y toda la trayectoria de la comunicación hasta su destino final. Entre las principales características que deben prevalecer durante esta conexión WAN es la privacidad, fiabilidad y seguridad de la información en todo el proceso de comunicación.

Para lograr la comunicación entre las diferentes sedes de una compañía, el uso de tecnologías WAN y LAN juegan un rol importante durante el diseño de la arquitectura de red. La topología que desplieguen debe siempre mejorar la comunicación, mantener el rendimiento, la seguridad, la confiabilidad e integridad de toda la información. Las alternativas de comunicación WAN en la mayoría de los países se pueden clasificar en: privadas son aquellas que ofrecen los proveedores de servicios, ejemplo enlaces de datos arrendados dedicados; y las públicas, que hacen uso de internet a través de recursos de banda ancha, ejemplo Redes Privadas Virtuales VPN (Ruiz et al., 2018).

En la actualidad, el proceso de migración que se está desarrollando entre las redes de transporte WAN tradicionales a SD-WAN, es significativo, por ello es importante conocer que retos deben afrontar las empresas que están cambiando a esta nueva tecnología, que se basa principalmente, en la virtualización.

1.2.2 Arquitectura De Conmutación De Etiquetas Multiprotocolo MPLS

La red MPLS tiene sus orígenes aproximadamente tres décadas atrás, y su evolución fue creciendo exponencialmente ocupando y liderando en redes de comunicaciones por las diferentes ventajas que ofrecía. Se define como una técnica independiente del protocolo diseñada para redirigir los datos desde el origen al destino en función de las etiquetas en lugar de las direcciones IP.

La red MPLS, es un mecanismo que emplea la señalización de paquetes de datos, utilizando etiquetas en lugar de las direcciones IP, su forma de operar es indistinta del protocolo que se elija para el redireccionamiento del tráfico en una red, es decir, no interviene el protocolo de enrutamiento. Para realizar este intercambio se emplea el Protocolo de Distribución de Etiquetas LDP, es el encargado de que los enrutadores que se encuentran en una red MPLS puedan compartir información de etiquetas, siendo una gran ventaja para MPLS porque ha permitido que en la última década logre adaptarse a varios protocolos de enrutamiento, como son: Protocolo de Puerta de Enlace de Frontera

BGP, Protocolo de Red para Encaminamiento Jerárquico de Pasarela Interior OSPF, Protocolo de Puerta de Enlace Interior Mejorado EIGRP, Protocolo de Información de Enrutamiento RIP, que son los encargados de analizar de forma inteligente el redireccionamiento de paquetes en base a los algoritmos diseñados en cada uno de ellos.

El protocolo de distribución de etiquetas, opera como un protocolo de enrutamiento estándar, donde su función es almacenar las etiquetas en su Base de Información de Etiquetas LBI, para luego relacionar un prefijo de IP con la etiqueta del siguiente salto, opera como una tabla de enrutamiento, pero sobre MPLS (Garg, 2017).

1.2.3 Protocolos de Enrutamiento para la Capa de Red

Los protocolos de enrutamiento son aquellos que permiten redirigir el tráfico, de forma que mediante una tabla de rutas se defina el mejor salto siguiente. Entre ellos se tiene los protocolos dinámicos:

1.2.3.1 Protocolo de Puerta de Enlace de Frontera BGP

Permite que los sistemas autónomos puedan intercambiar información de tablas de ruteo entre sí. Un sistema autónomo es un conjunto de enrutadores bajo una sola administración técnica.

Los enrutadores logran establecer las sesiones BGP usando el protocolo TCP, mediante el puerto 179. Su forma de operación consiste en dos enrutadores BGP formando una conexión TCP entre ellos. Estos enrutadores son denominados, enrutadores pares. Los enrutadores pares intercambian mensajes para abrir y validar los parámetros de conexión. Los enrutadores BGP intercambian información sobre la posibilidad de alcance de una red, esta información es importante ya que muestra un camino completo, es decir una ruta que debe escoger para alcanzar la red de destino. Las trayectorias son números de AS BGP.

1.2.3.2 Protocolo de Enrutamiento de Puerta de Enlace Interior Mejorado EIGRP

Como lo menciona Cisco, EIGRP presenta las mismas ventajas en direccionamiento IPv4 e IPv6, sigue proporcionando la continuidad y familiaridad operativa (Cisco, 2011). Las características en IPv6 como lo indica (Cisco, 2011), se detallan a continuación:

Ancho de banda. Puede trabajar con un mayor ancho de banda en la red.

Rápida convergencia. El algoritmo dual permite que la información de enrutamiento converja de forma inmediata.

Actualizaciones parciales. Envía actualizaciones de forma parcial, en lugar de enviar todo el contenido de la tabla de rutas. Esta característica, minimiza el ancho de banda requerido para los paquetes EIGRP.

***Mecanismo de descubrimiento de vecinos*.** Este es un mecanismo de saludo simple, es empleado para conocer los dispositivos vecinos. Es independiente del protocolo.

Sumariza. Resumen de rutas arbitrarias.

Escalamiento. Tiene un alto grado de escalamiento.

La nueva característica de EIGRP para IPv6 es en su forma de anunciar, es decir, se configura sobre las interfaces que se pretende advertir, esta nueva característica permite configurar IPv6 sin el uso de una dirección IPv6 global. No hay una declaración de red en EIGRP para IPv6 (Cisco, 2011).

EIGRP, sin embargo, sigue ofertando un alto grado de confiabilidad y un alto grado de convergencia sobre otros protocolos de enrutamiento dinámicos, una de sus principales ventajas es el uso eficiente del ancho de banda como lo menciona (Patiño Sánchez, 2017).

1.2.4 Redes de Áreas Extensas Definidas por Software SD-WAN

La arquitectura SD-WAN es una solución integral que incluye el hardware, software y la integración servicios centralizados de una red, donde permite mejorar el rendimiento, la confiabilidad y la seguridad WAN a nivel empresarial. SD-WAN es capaz de gestionar una gran variedad de tipos de tráfico; basándose en políticas mediante varias redes WAN (Villas, 2019). Es también utilizada para crear unas conexiones WAN híbridas e inteligentes que puede incluir una red privada virtual para empresas, servicios de internet de banda ancha y servicios inalámbricos. Una de sus funciones es el monitoreo de los enlaces disponibles y al conocer las exigencias de cada aplicación o servicio, permite entonces en ese momento elegir el camino óptimo para enviar el tráfico de determinada aplicación.

Entre las funciones que nos ofrece SD-WAN mencionamos:

- Monitoreo de red.
- Ingeniería de tráfico.
- QoS garantizado.
- Administración centralizada (Yang et al., 2019).

En el capítulo 2, se desarrolla un análisis de SD-WAN, donde da a conocer su forma de operar y la arquitectura que emplean; así como el gran aporte que brinda a los desafíos en la nueva era de las telecomunicaciones.

1.2.5 Redes Privadas Virtuales VPN

"Las Redes Privadas Virtuales VPN se usan comúnmente para interconectar redes privadas a través de internet, permitiendo a los usuarios enviar y recibir datos de forma segura entre redes privadas remotas. Se pueden construir conexiones de red privadas virtuales, por ejemplo, entre dos sitios remotos de una organización denominadas VPN de punto a punto o entre los usuarios y la organización conocidas como VPN multipunto" (Korhonen, 2019,p.2).

Existen diferentes protocolos de seguridad que son utilizados por las redes privadas virtuales, entre ellos se menciona:

- PPTP (Protocolo de Túneles Punto a Punto).
- L2TP (Protocolo de Túneles de Capa 2).
- IPsec (Seguridad del Protocolo de Internet).

1.2.6 Red Privada Virtual Multipunto Dinámica DMVPN

La tecnología DMVPN tiene como función principal poder interconectar una gran cantidad de sitios de forma automática, dinámica y bajo demanda, lo que genera un aporte fundamental a las redes privadas virtuales con seguridad IPsec.

Los protocolos que emplea DMVPN son: Resolución de Próximo Salto (NHRP), Protocolo de Enrutamiento Multipunto de Encapsulamiento Genérico (mGRE) y cifrado IPsec para seguridad.

1.2.6.1 Características de DMVPN

La característica principal de DMVPN es permitir la unidifusión IP, multidifusión IP y protocolos de dinámicos de enrutamiento.

DMVPN se basa en una topología lógica tipo estrella, con nodos identificados como Hub y Spoke.

IPsec admite pares remotos con direcciones dinámicamente asignadas, y conecta sucursales a través de red pública como es internet, una red privada, o una red inalámbrica; todas ellas mediante túneles armados bajo demanda, incluye protocolos de seguridad como es IPsec.

1.2.6.2 Beneficios de DMVPN

A continuación, como lo menciona Fonseca (2017), los principales beneficios son:

Fácil aprovisionamiento. Cuando se incorpore un nuevo punto o sede, no es necesario incrementar líneas de configuración en los concentradores DMVPN.

Escalabilidad. Existe una configuración mínima en el router que cumple la función de Spoke, permitiendo que exista una escalabilidad de forma masiva. La escalabilidad de la red no se encuentra limitada por el dispositivo ya sea físico, virtual o lógico.

***Túnel de Spoke-Spoke*.** Debido a los túneles que se levantan entre el túnel inicial y el concentrador, se puede definir que DMVPN utiliza una topología de malla completa. Estos túneles se forman de manera que se genere la necesidad y desaparecen cuando ya no son útiles, es decir, funcionan bajo demanda.

Soporte multiprotocolo: DMVPN puede trabajar con direccionamiento IPv4, IPv6 y MPLS como protocolo de red de superposición de transporte.

Compatibilidad de multidifusión: DMVPN permite que el tráfico de multidifusión viaje a los diferentes destinos mediante las interfaces del túnel.

Conectividad adaptable: Soporta el Protocolo de Configuración Dinámica de Host DHCP en los túneles, tiene la capacidad de configurar dinámicamente las interfaces del Hub o el Spoke de las interfaces de GRE.

DMVPN ha logrado tener mejorías significativas, entre ellas se menciona a continuación en la **Tabla 1.**

Tabla 1

Características y Beneficios de CISCO DMVPN

Tipo de Mensaje	Descripción
Enrutamiento dinámico sobre VPN	• Permite que las tablas de enrutamiento IP se distribuyan de forma segura entre el sitio de la sucursal y la cabecera corporativa a través de túneles cifrados. Permite una mejor accesibilidad sin necesidad de definir manualmente las rutas permitidas. • Se admiten los protocolos de enrutamiento: EIGRP, OSPF, RIP Y BGP.
Sobrecarga de configuración reducida	• DMVPN elimina la necesidad de configurar mapas de cifrado vinculados a la interfaz física, lo que simplifica drásticamente la cantidad de líneas de configuración

	necesarias para una implementación de VPN (por ejemplo, para una implementación de 1000 sitios, DMVPN reduce el esfuerzo de configuración en el concentrador de 3900 líneas a 13 líneas). • Agregar nuevos Spoke a la DMVPN no requiere cambios en el concentrador. • Simplifica la configuración de túneles divididos. El cambio de configuración centralizado en el concentrador controla el comportamiento del túnel dividido. En IPsec tradicional, es necesario modificar todos los radios o Spoke.
Implementación sin intervención	• DMVPN se puede implementar en modelos de implementación sin intervención, mediante Easy Secure Device Deployment EzSDD, herramienta que sirve para el aprovisionamiento seguro de dispositivos basado en Infraestructura de Clave Pública PKI. Los dispositivos pueden arrancar de forma remota, evitando la necesidad de operaciones de configuración extensas.
Transversal de traducción de direcciones de red (NAT).	• DMVPN admite enrutadores radiales que ejecutan NAT o detrás de dispositivos NAT dinámicos, lo que permite una seguridad mejorada para las subredes de las sucursales.
Soporte de multidifusión IP	• DMVPN admite tráfico de multidifusión IP (entre el Hub y el Spoke); El IPsec nativo solo admite unidifusión IP. Esto proporciona una distribución eficiente y escalable de tráfico de uno a muchos y de muchos a muchos.
Soporte QoS	• Conformación del tráfico en las interfaces del concentrador por Spoke o por grupo de Spoke. • Políticas de QoS de Hub a Spoke y Spoke a Spoke. • Políticas de QoS dinámica en las que las plantillas de QoS se cargan automáticamente a los túneles a medida que surgen.

	• Vigilancia de QoS por Spoke, permite diferenciar los Spoke y protege la red de ser invadida por Spokes que consuman el ancho de banda.
Alta disponibilidad	• Cisco DMVPN habilita la conmutación por error basada en enrutamiento. • Los enlaces WAN duales y la redundancia del concentrador proporcionan una mayor disponibilidad. DMVPN admite diseños de dos concentradores, donde cada radio o Spoke se empareja con dos concentradores, lo que proporciona una rápida conmutación por error. • Las topologías de múltiples concentradores permiten una comunicación de Spoke a Spoke ininterrumpida en caso de que se produzca una falla en un solo concentrador.
Escalabilidad	• DMVPN escala a miles de Spoke utilizando el Equilibrio de Carga del Servidor SLB. El cifrado puede integrarse dentro del dispositivo SLB o distribuirse a enrutadores vpn de cabeceras dedicadas. Los túneles tienen carga equilibrada sobre los concentradores disponibles. • El rendimiento se puede escalar de forma incremental agregando Hub. • Las implementaciones de concentradores jerárquicos permiten una escalabilidad mejorada.
Manejabilidad	• El soporte de capacidad de administración se suministra a través de IPsec (incluido IPsec compatible con VRF) MIB, NHRP MIB e interfaz de línea de comandos (CLI).
Conciencia de VRF	• DMVPN vrf-aware implementada en los centros de borde del proveedor, permite la segregación del tráfico de clientes.
Compatibilidad con MPLS (2547º DMVPN)	• Las redes MPLS se pueden cifrar a través de túneles DMVPN

Nota. Fuente: Ojeda, M. Tomado de (Cisco, 2014)

1.2.6.3 Requerimientos de Sistemas

Hardware de Cisco que soporta DMVPN. En la **Figura 1** se detalla el equipamiento que soporta DMVPN y en qué fases pueden ser aplicadas.

Figura 1

Plataforma Hardware

Platform	VPN Acceleration Module
Cisco 870, 880, 890, 812, 819 Series Integrated Services Routers	Onboard encryption
Cisco 1801, 1802, 1803, 1811, 1812, 1841, 2800, 3825, and 3845 Integrated Services Routers	Onboard encryption
Cisco 1841 Integrated Services Routers	Advanced Integration Module (AIM)-VPN/SSL-1
Cisco 2800 Series Integrated Services Routers	AIM-VPN/SSL-2
Cisco 3825 Integrated Services Routers	AIM-VPN/SSL-3
Cisco 3845 Integrated Services Routers	AIM-VPN/SSL-3
Cisco 1900, 2900, and 3900 Next Generation Integrated Services Routers	Onboard encryption
Cisco 7200 Series Routers	VPN Acceleration Module 2+ (VAM2+)
Cisco 7200VXR Routers with Network Processing Engine NPE-G2	VPN Services Adapter (VSA)
Cisco 7301 Routers	VAM2+
Cisco 7600 Series Routers (Supports DMVPN phase 1 & 2 only)	IPsec VPN Shared Port Adapter (SPA)
Cisco Catalyst 6500 Series Switches (Supports DMVPN phase 1 & 2 only)	IPsec VPN SPA
Cisco ASR 1000 Series Routers	Onboard encryption
Cisco ISR 4000 Series Routers	Onboard encryption

Nota. Fuente Tomado de (Cisco, 2014)

***Software de Cisco que soporta DMVPN*.** En la **Figura 2**, se aprecia la versión del sistema operativo del router Cisco que debe tener como mínimo para la implementación de DMVPN. Adicional se observa características para los enrutadores de gama de Servicios de Agregación ASR y los enrutadores de Servicio Integrados ISR.

Figura 2.

Requisitos de Software

Hardware	Cisco 870, 1800, 1900, 2800, 2900, 3800, 3900, 7200 Series and Cisco 7301 routers
Cisco IOS Software Release	• Cisco IOS Software Release 12.3(2)T or later recommended for Cisco 870, 1800, 2800, 3800, and 7200 Series Routers and Cisco 7301 Routers • Cisco IOS Software Release 15.0 or later recommended for Cisco 1900, 2900 and 3900 Series Routers • Cisco IOS Software Release 12.2(18)SXE2 or later for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers • Cisco IOS XE Release 2.0.0 or later for Cisco ASR 1000 Series Routers • Cisco IOS XE release – 3.16.5S or later for Cisco ISR 4000 series routers
Cisco IOS Software Feature Set	• Advanced Security or higher • Cisco ASR 1000 Series Routers also require VPN license • Cisco ISR 4000 series routers need SECK9 license or higher

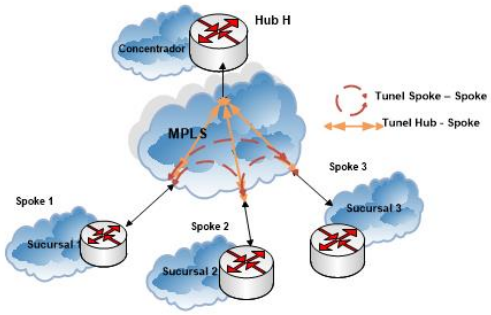
Nota. Fuente Tomado de (Cisco, 2014)

Para el despliegue de DMVPN se emplean varios componentes claves que son NHRP, mGRE e IPsec, todas ellas se integran y permiten construir una red de

superposición. En la **Figura 3** se logra apreciar un tradicional esquema de una nube DMVPN única.

Figura 3

Nube DMVPN única

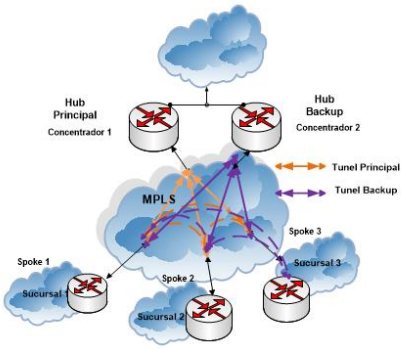


Nota. Fuente: Elaboración Propia

En la **Figura 4**, se logra apreciar una mejora en el tema de escalabilidad y disponibilidad; esto se debe a que la nube DMVPN trabaja de forma independiente para cada Hub, es decir, existe un Hub principal y a su vez un Hub backup, cada uno de ellos opera con su propia tunelización mGRE, así mismo, con su propio protocolo de seguridad IPsec, y su servidor NHRP. Acerca de, su forma operación es necesario la configuración de protocolos de enrutamiento dinámicos; que garanticen que exista la alta disponibilidad ante fallas, una característica que hoy se necesita a nivel de todas las empresas.

Figura 4

Nube DMVPN Redundante



Nota. Fuente: Elaboración Propia

1.2.7 Protocolo de Resolución del Siguiente Salto (NHRP)

El protocolo de NHRP fue definido en el RFC 2332, que ayuda a la creación de un túnel dinámico, es el que provee resoluciones de direcciones IP. El proceso inicia en los enrutadores clientes NHRP llamados Spoke, donde realizan una petición al servidor del siguiente salto, denominado NHS que es el enrutador HUB quien facilita la dirección física de otro router Spoke (Cisco, 2016).

NHRP es un protocolo cliente-servidor que permite que los dispositivos se registren a través de redes conectadas directamente o de forma indirecta. Los servidores del siguiente salto son responsables de registrar direcciones o redes, mantienen un repositorio NHRP y responden a cualquier consulta que se reciba por los clientes del siguiente salto NHC (Fonseca, 2017).

1.2.8 Descripción general de DMVPN para IPv6

Como lo menciona Cisco en (Jose, 2014,p. 49). “En DMVPN para IPv6, la red pública internet, es una red IPv4 pura, y la red privada la intranet, es compatible con IPv6. Las intranets podrían ser una combinación de nubes IPv4 o IPv6 conectadas entre sí, mediante tecnologías DMVPN, siendo el operador subyacente una red IPv4 tradicional”.

1.2.8.1 Direccionamiento IPv6 y Restricciones

Para la implementación de DMVPN sobre IPv6 existen ciertas restricciones, debido a que el direccionamiento IPv6 tiene una gran variedad de IP especiales. Se menciona lo indicado por Cisco (Cisco, 2016):

- Cada interfaz IPv6 NHRP está configurada con una dirección de unidifusión IPv6. La dirección puede ser una dirección local accesible o única.
- Cada interfaz IPv6 NHRP está configurada con una dirección local de enlace IPv6, que es única en todos los hosts en la nube DMVPN, es decir, los Hub y Spoke.
- Si ningún otro túnel del dispositivo utiliza la misma fuente de túnel, la dirección de origen del túnel se puede incrustar en una dirección IPv6.
- Si el dispositivo tiene solo un túnel DMVPN IPv6, entonces la configuración manual de la dirección del enlace local IPv6 no es necesaria. En su lugar, utiliza el comando ipv6 enable para generar automáticamente una dirección de enlace local.
- Si el dispositivo tiene más de un túnel DMVPN IPv6, entonces la dirección local de enlace debe ser manualmente configurada mediante el comando IPv6 address fe80 :: 2001 link-local (p.50).

1.2.9 Seguridad del Protocolo de Internet IPsec

Como indica Korhonen (2019), que “seguridad de protocolo de internet, es una pila de protocolos, que está oficialmente especificada por el Grupo de Trabajo de Ingeniería de Internet IETF, en varios documentos de solicitud de comentarios RFC. Se utiliza para proteger las comunicaciones del protocolo de internet IP, ya que puede cifrar, autenticar y verificar la integridad de los paquetes de datos de los flujos de datos” (p.3).

El protocolo IPsec, presenta un diseño basado en seguridad de extremo a extremo, con el principal objetivo, la protección de la información. La idea es que cada extremo cuente con su protocolo de seguridad, dado que, el medio donde se establezca la comunicación no sea del 100% fiable.

Capítulo 2: Arquitectura de DMVPN

2.1 Mecanismo de la Arquitectura DMVPN

La tecnología DMVPN puede ser implementada en tres fases:

Fase 1: Hub-Spoke.

Fase 2: Spoke-to-Spoke.

Fase 3: Árbol Jerárquico Spoke-a-Spoke.

2.1.1 Fase 1: Hub-Spoke

En la fase 1 se forman túneles IPsec de forma permanente entre el Hub y Spoke. La característica principal es que entre los Spoke no se configuran túneles IPsec. En este esquema, cada Spoke se lo conoce como estación cliente del servidor de NHRP, que se encuentra implementado en el router Hub.

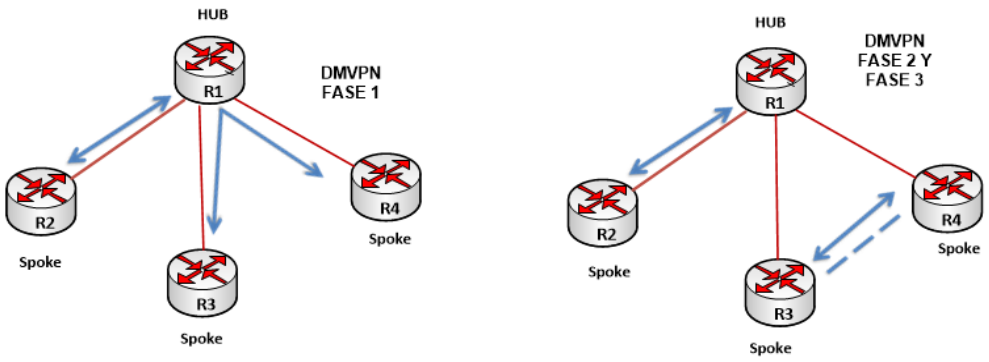
2.1.2 Fase 2: Spoke-Spoke

La fase Spoke-Spoke permite la comunicación de forma dinámica, mediante la creación de un túnel VPN por solicitud del router Hub. Durante la fase 2 no se permite conservar el siguiente salto, por ello no es compatible con la comunicación de Spoke a Spoke entre diferentes redes DMVPN jerárquica de varios niveles.

A continuación, se ilustra en la **Figura 5** las diferencias del flujo del tráfico entre la fase 1, fase 2 y fase 3 de DMVPN.

Figura 5

Flujo de Tráfico en fase 1, fase 2 y fase 3



Nota. Fuente Ojeda M. Tomado de (Guide, 2017)

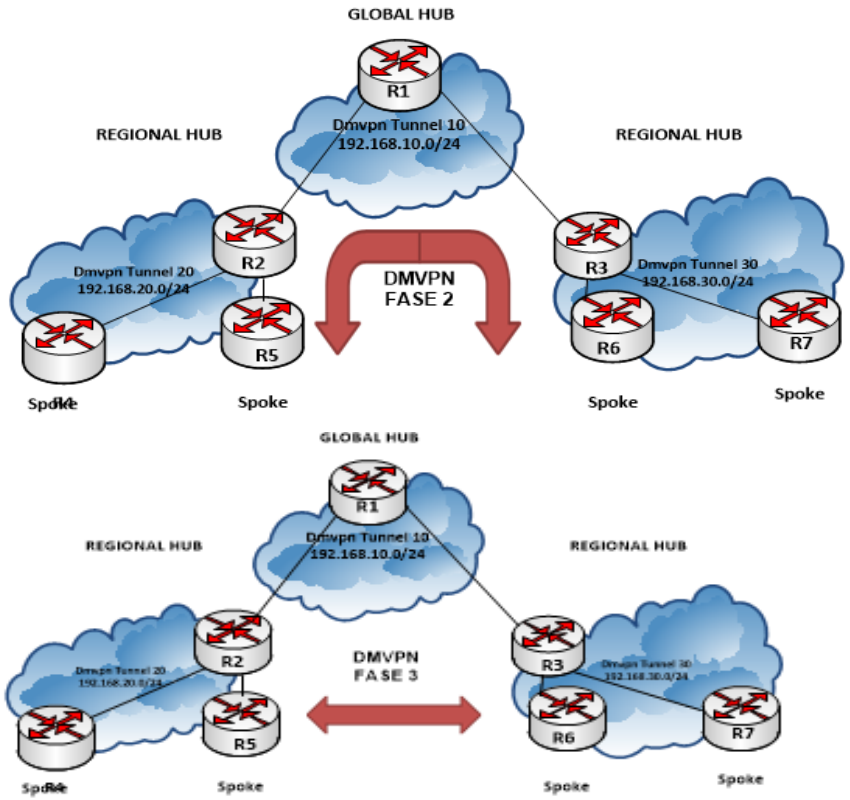
2.1.3 Fase 3: Árbol Jerárquico Spoke a Spoke

Cuando un Spoke necesita enviar un paquete sobre la red interna de otro Spoke, comienza a operar el servidor NHRP; el Spoke origen solicita la dirección externa del Spoke destino, se lleva a cabo una consulta donde el servidor NHRP, este busca en su tabla y anuncia la ubicación real del Spoke destino, y así el Spoke origen aprende la ubicación de su Spoke destino.

Entonces, el túnel Spoke a Spoke se forma sobre mGRE, la cual permite encapsular el protocolo de enrutamiento implementado. Se logra apreciar que este modo a diferencia de Hub and Spoke, se forman bajo demanda de los usuarios, en cualquier momento en que exista tráfico entre los mismos. Es muy importante mencionar que los paquetes pueden saltarse o evitar pasar por el Hub y usar el túnel que se arma entre los Spoke. Cisco en esta fase proporciona soporte a las Interfaces de Programación de Aplicaciones API, lo que la convierte en la fase más completa de DMVPN. En la **Figura 6,** se logra apreciar la diferencia en la dirección que se forma el túnel en la fase 3, con relación a la fase 2.

Figura 6

DMVPN fase 2 y fase 3



Nota. Fuente Elaboración Propia

Como se mencionó en el capítulo 2: DMVPN es una tecnología que permite integrar protocolos de seguridad, técnicas y protocolos de enrutamiento, entre ellos mencionamos:

- mGRE (Protocolo de Enrutamiento Multipunto de Encapsulamiento genérico).
- NHRP (Protocolo de resolución del siguiente salto).
- Encriptación dinámica IPsec.
- Protocolos de enrutamiento dinámico: EIGRP, RIP, OSPF, BGP.
- CEF (Cisco Express Forwarding).

A continuación, se detalla el mecanismo y la respectiva forma de operar de cada una de las técnicas y protocolos mencionados:

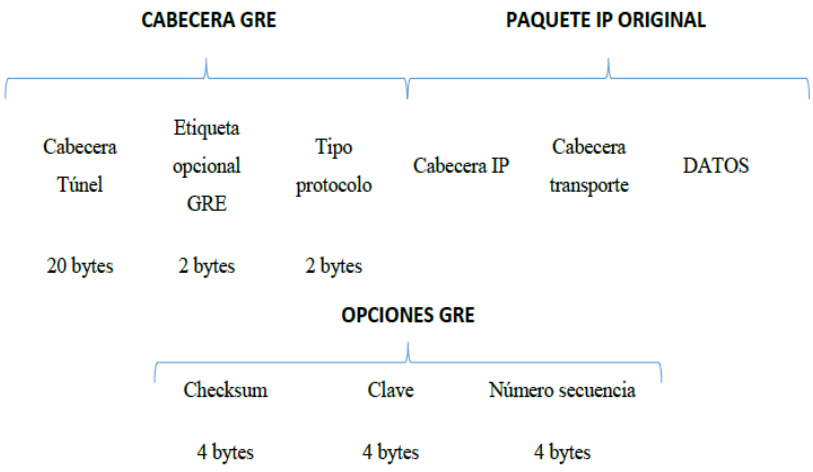
2.1.4 Modo de Operación de GRE

La cabecera GRE. El protocolo mGRE está descrito en la RFC 1701 y en el caso de IP sobre IP con GRE está en la RFC 1702. El protocolo GRE aumenta un mínimo de 24 bytes a la cabecera de los paquetes que cruzan por el túnel.

Los túneles de nivel 2, se establecen cuando el protocolo de pasajero pertenece a una trama de nivel 2 como es (Ethernet, PPP) y los paquetes pasajeros de nivel 3 como es (IP, OSPF, IS-IS, ARP, RARP, RIP, NAT etc) son denominados túneles de nivel 3.

Figura 7

Trama GRE



Nota. Tomado de (Ghretli & Almukhtar, 2019)

Se observa en la **Figura 8,** que los nuevos bytes se dividen de la siguiente forma, los primeros 20 bytes se ocupan para la nueva cabecera IP, donde se especifica la dirección origen y destino. De lo 4 bytes restantes, los dos primeros se usan para parámetros opcionales. Los dos últimos bytes indican el tipo de protocolo que está transportando el túnel.

Figura 8

Cabecera GRE

<table>
<tr><th colspan="5">Bits 0-4</th><th>5-7</th><th>8-12</th><th>13-15</th><th>16-31</th></tr>
<tr><td>C</td><td>R</td><td>K</td><td>S</td><td>S</td><td>Recur</td><td>Flags</td><td>Version</td><td>Tipo protocolo</td></tr>
<tr><td colspan="7">Checksum (opcional)</td><td>Offset (opcional)</td></tr>
<tr><td colspan="8">Key (opcional)</td></tr>
<tr><td colspan="8">Sequence number (opcional)</td></tr>
<tr><td colspan="8">Routing (opcional)</td></tr>
</table>

Nota. Tomado de (Ghretli & Almukhtar, 2019)

A continuación, en la **Tabla 2** se describe los campos de estos 4 bytes de la cabecera GRE a nivel de bits.

Tabla 2

Parámetros de la Cabecera GRE,

Tipo de Mensaje	Descripción
C (bit 0)	• Representa la opción checksum present. Si está en 1 quiere decir que se activa el campo opcional checksum de la cabecera GRE y también debe agregarse el campo offset. Normalmente no es necesario puesto los protocolos de capas superiores ya que realizan el checksum para detectar paquetes corruptos.

Tipo de Mensaje	Descripción
R (bit 1),	• Representa la opción routing. Por lo general ya no es usado, pero si se ubica en 1 deberá ser acompañado por los campos checksum y offset
K (bit 2),	• Representa la opción key. Si está en 1 añade el campo de seguridad y proporciona un sistema básico de seguridad comprobando que cada extremo del túnel tiene la misma clave.
S (bit 3),	• Representa la opción sequence number. Si se ubica en 1 quiere decir que el campo opcional del número de secuencia está presente.
s (bit 4),	• Representa el campo strict source route. Recomiendan ponerlo a 1 sólo si toda la información de enrutamiento está formada por rutas estrictas.
Recur (bits 5-7),	• Representa el campo de control de recursión. Contiene un entero positivo de 3 bits que indica el número de encapsulaciones adicionales que están permitidas. Siempre posee el valor 0.
Flags (bits 8-12),	• Es un campo reservado y se recomienda permanecerlo en 0.
Protocol type (bits 16-31),	• Representa el campo de protocolo. Permite identificar qué tipo de paquete está atravesando el túnel, siendo 0x0800 el usado para IP.
Checksum (2 bytes),	• Representa el campo opcional de la cabecera GRE. Contiene el checksum IP de la cabecera GRE y paquete interno.

Tipo de Mensaje	Descripción
Key (4 bytes),	• Representa un campo opcional de GRE. Contiene un número insertado por la parte encapsuladora del túnel que puede utilizarse en destino para propósitos de comprobación del remitente correcto.
Sequence number (4 bytes),	• Representa el campo opcional de GRE del número de secuencia. Corresponde al número usado por el receptor para asegurar el correcto orden de llegada de los paquetes.
Routing (variable),	• Representa un campo opcional que contiene una lista de rutas.

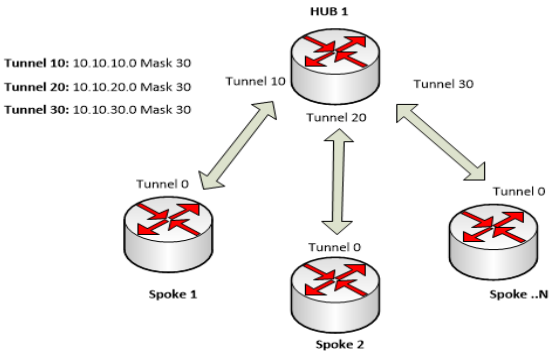
Nota. Fuente: Ojeda M. 2021, Tomado de (Jaramillo Zamora, 2018)

Túneles GRE Punto a Punto. Los túneles GRE punto a punto tienen exactamente dos extr**emos** y cada túnel en el router requiere una interfaz virtual separada con su propia configuración de manera independiente.

En la **Figura 9** se aprecia como los túneles son uno a uno, entre el Hub y el Spoke, no existe una comunicación directa entre los Spoke.

Figura 9

Túneles GRE Punto a Punto

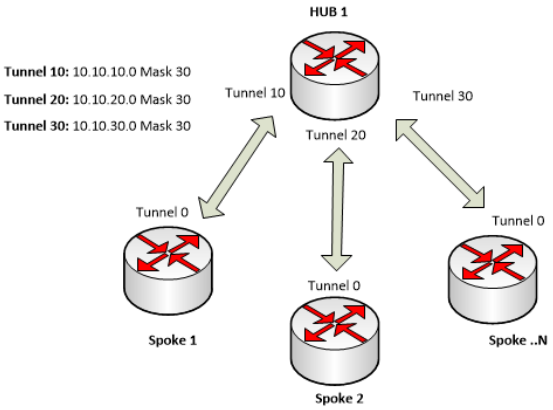


Nota. Fuente: Elaboración propia

Túnel GRE Punto Multipunto. La interfaz de túnel mGRE multipunto se emplea en DMVPN para permitir que una única interfaz GRE admita múltiples túneles IPsec, simplificando la complejidad y el tamaño de la configuración. En la **Figura 10** se logra apreciar cómo se levantan múltiples túneles IPsec entre el Hub y los Spoke.

Figura 10

Túneles mGRE



Nota. Fuente: Elaboración propia

DMPVN usa túneles multipunto y al integrarse con protocolos de enrutamiento dinámico se convierte en una gran ventaja; eliminando un gran número de los problemas de soporte asociados con otras tecnologías de VPN. Los GRE denominadas redes superpuestas, porque el túnel GRE se levanta sobre una red de transporte que se encuentra ya implementada.

Entre los principales elementos de los túneles GRE son:

Encabezado de entrega (Protocolo de transporte).

Encabezado GRE (Protocolo de operador).

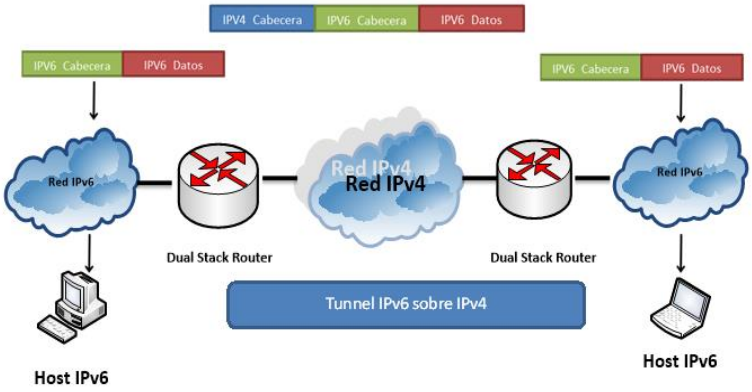
Paquete de carga útil (Protocolo de pasajeros).

Tunelización. El protocolo de pasajeros es todo aquello que será encapsulado, es enviado a la interfaz del túnel GRE donde está encapsulado por el encabezado GRE. El paquete resultante está encapsulado por el protocolo de transporte, que agrega el encabezado de entrega, que es utilizado para enrutar a través de la red subyacente. Por ejemplo, si IPv6 se va a tunelizar a través de una infraestructura IPv4, el dispositivo reenvía el paquete IPv6 a la interfaz del túnel GRE. La interfaz del túnel GRE agrega su encabezado y utiliza la pila de protocolos IPv4 para encapsular y entregar a través de la infraestructura de red IPv4 subyacente (Sarah Anand, 2020).

GRE se puede utilizar con una gran variedad de combinaciones diferentes de protocolos de transporte y pasajeros. Sin embargo, IPv4 e IPv6 son los protocolos de transporte más populares para GRE. En la **Figura 11** se logra apreciar como la comunicación de IPv6 transporta la información encapsulada en IPv4.

Figura 11

Túnel GRE de IPv6 sobre IPv4



Nota. Fuente: Elaboración propia

Entre las combinaciones de protocolos pasajeros y protocolo de transporte se tiene:

- GRE puede usar IPv4 como protocolo de transporte para canalizar un paquete IPv4 a través de la infraestructura de red subyacente.

- GRE puede usar IPv4 como protocolo de transporte para canalizar un paquete IPv6 a través de la infraestructura de red subyacente.

- GRE puede usar IPv6 como protocolo de transporte para canalizar un paquete IPv4 a través de la infraestructura de red subyacente.

- GRE puede usar IPv6 como protocolo de transporte para canalizar un paquete IPv6 a través de la infraestructura de red subyacente.

2.1.5 Modo de Operación de IPsec

IPsec proporciona una variedad de servicios de seguridad para el tráfico en la capa IP; emplea dos protocolos para garantizar la seguridad al tráfico; estos son, la Cabecera de Autentificación AH y la Carga de Seguridad Encapsulada ESP.

Los protocolos aportan con varios beneficios como indica (RODRIGUEZ, 2011):

- La AH provee integridad sin conexión, autentificación del origen de datos, y un servicio opcional de protección antireplay.

- La ESP puede proporcionar confidencialidad (encriptación), y confidencialidad limitada de flujo de tráfico. También puede proporcionar integridad sin conexión, autentificación del origen de datos, y un servicio de protección antireplay.

- AH y ESP son herramientas para el control y limitar el acceso, basados en el prorrateo de claves criptográficas y en el manejo de flujo de tráfico referente a estos protocolos de seguridad (p.27).

- AH y ESP pueden aplicarse de forma individual o en conjunto con otros protocolos, para proveer un conjunto de servicios de seguridad en IPv4 e IPv6.

2.1.6 Protocolo de Gestión de Claves Internet IKE

El protocolo de gestión de claves es un requisito fundamental en el funcionamiento de ESP y AH, porque permite la distribución de claves con un mayor grado de seguridad. Es indispensable que ambos miembros, emisor y receptor configuren los mismos parámetros para que este opere correctamente.

IKE logra la integración de dos protocolos, asociación de seguridad del internet y protocolo de administración de claves (ISAKMP) y Oakley, se lo podría considerar un protocolo híbrido.

ISAKMP es el encargado de la sintaxis de los mensajes que se emplean mientras se configura en IKE.

OAKLEY es el encargado de especificar el algoritmo de cómo llevar a cabo el intercambio de una clave de forma segura entre dos partes que son desconocidas.

2.1.7 Modos de Funcionamiento IPSEC

Los protocolos AH y ESP trabajan mediante dos modos de uso:

- Modo transporte proporciona protección a los protocolos de capas superiores.
- Modo túnel, los protocolos son aplicados a paquetes (a los que se hizo un túnel a través de IP).

2.1.8 Modo de Operación NHRP

En DMVPN se establecido mejoras por parte de Cisco, han sido agregado diferentes tipos de mensajes NHRP, a los ya especificados en RFC 2332.

El paquete de registro NHRP proporciona la información para el enrutador de eje de conexión que permite crear una correspondencia NHRP para este router radial. Con

esta correspondencia, el router de eje de conexión puede reenviar paquetes de datos IP de unidifusión a este router de radio por el túnel mGRE e IPsec.

En la **Tabla 3** se observa los tipos de mensajes NHRP como mejora en DMVPN.

Tabla 3

Mensajes NHRP

Tipo de Mensaje	Descripción
Registro	• El NHS (centros de DMVPN) reciben los mensajes de registro que fueron enviados por el NHC. El mensaje de registro ayuda a los concentradores a identificar la información NMBA del Spoke. En el NHC se especifican los parámetros del tiempo que el NHS debe permanecer el estado registro junto a otras características.
Resolución	• Los mensajes de resolución son mensajes NHRP que permiten ubicar y proporcionar la información de resolución de dirección del enrutador de salida hacia el destino. Se envía una solicitud de resolución durante la consulta real, y una respuesta de resolución proporcionada por la dirección IP del túnel y la dirección IP NBMA del Spoke remoto.
Redirección	• Los mensajes de redireccionamiento son un componente esencial de la Fase 3 de DMVPN. Permiten a un enrutador intermedio notificar al encapsulador (un enrutador) que se puede llegar a una red específica por una ruta óptima (túnel de Spoke a Spoke). El encapsulador puede enviar un mensaje de supresión de redirección para suprimir las solicitudes de redireccionamiento durante un periodo de tiempo específico. Esto se hace normalmente si una ruta óptima no es factible o la política no lo permite.

Tipo de Mensaje	Descripción
Purga	• SLA predecible para voz, nube y otras aplicaciones empresariales críticas. Políticas de aplicación con aplicación en tiempo real sobre problemas de red. Múltiples enlaces híbridos activo-activo para todos los escenarios. Los mensajes de purga se envían para eliminar una entrada NHRP en caché. Los mensajes de purga notifican a los enrutadores, la pérdida de una ruta utilizada por el NHRP. Por lo general, las purgas son enviadas por un NHS a los NHC (a las que contestó) para indicar que la asignación de una dirección/red a la que respondió ya no es válida (por ejemplo, si la red no es accesible desde la estación original o se ha movido). Los mensajes de purga toman la ruta más directa (túnel de Spoke a Spoke) si es posible. Si no, se establece un túnel de Spoke a Spoke, y así los mensajes de purga se reenvían a través del concentrador o Hub.
Error	• Los mensajes de error se utilizan para notificar al remitente de un paquete NHRP que se ha producido un error.

Nota. Fuente Ojeda M. 2021, Tomado de (Fonseca, 2017)

2.1.9 Enrutamiento NHRP IPv6

NHRP resuelve una dirección IPv4 o IPv6 de una determinada intranet en una dirección de internet IPv4 sin una Red de Acceso Múltiple sin Difusión NBMA.

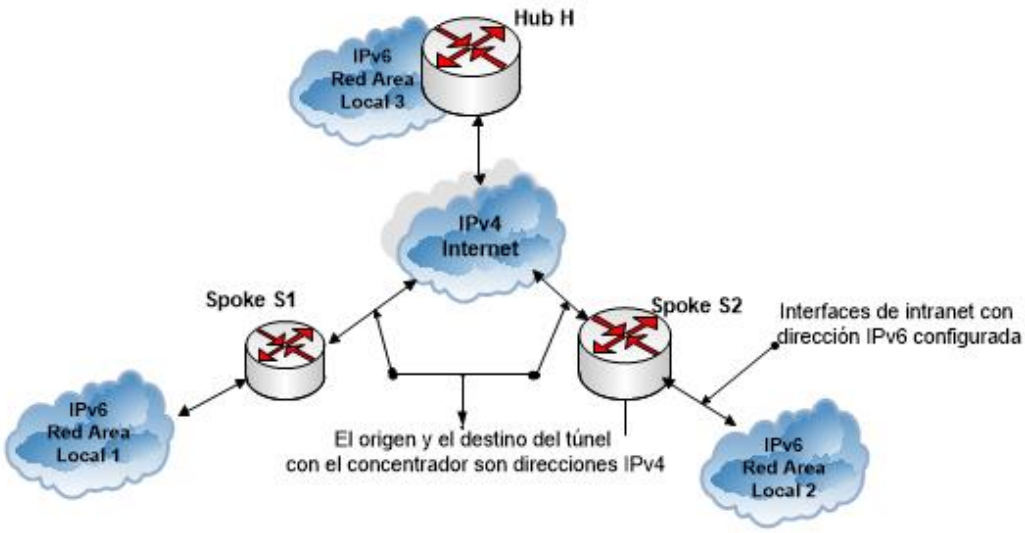
A continuación, en la **Figura 12**, las intranets que están conectadas a través de la red DMVPN son nubes IPv6; y la nube de internet es una nube IPv4 pura. Los Spoke S1 y S2, están conectados al Hub H a través de internet mediante un túnel. La dirección del túnel en sí es el dominio IPv6, porque es otro nodo de la intranet. La dirección de origen y destino del túnel están en IPv4, en el dominio de internet. El túnel mGRE es consciente de la red IPv6 porque el protocolo de pasajeros GRE es un paquete IPv6, y el protocolo de transporte GRE o portadora es un paquete IPv4.

Cuando un host IPv6 en LAN L1 envía un paquete destinado a un host IPv6 en LAN L2, el paquete se enruta primero a la puerta de enlace (que es Spoke S1) en LAN L1. Spoke S1

es un dispositivo de doble pila, lo que significa que tanto IPv4 como IPv6 está configurado en él. La tabla de enrutamiento IPv6 en S1 apunta a un próximo salto, que es la dirección IPv6 del túnel en Spoke S2. Esta es una dirección VPN que debe asignarse a una dirección NBMA, lo que activa NHRP.

Figura 12

Enrutamiento NHRP en IPV6



Nota. Fuente: Ojeda M. 2021, Tomado de (Jose, 2014)

2.2 Redes de Área Extensa Definidas por Software SD-WAN

El internet como la red de redes, ha jugado un rol importante en las últimas dos décadas a nivel de medio de transmisión y comunicación; esto ha generado que los requerimientos de los administradores de tecnologías de información y usuarios finales, sean más exigentes en el momento de necesitar algún tipo de transmisión de tráfico de voz, video y datos, ya sea que este se genere en un centro de red, en una red inalámbrica, en redes corporativas, en nubes privadas o públicas; este nuevo tráfico es el resultado de la actividades diarias de cada uno de los seres humanos, como son el teletrabajo, la telemedicina, las comunicaciones unificadas, resultado de un sin número de operaciones que se han logrado en los últimos años desarrollarlas de forma virtual. Por todas estas nuevas actividades, existe en la actualidad un proceso acelerado en la expansión de redes WAN tradicionales y de ello parte la necesidad de una solución integral, como lo pretende ser SD-WAN.

Las redes de área extensa tradicionales fueron inicialmente diseñadas para que puedan rendir al máximo en empresas pequeñas, medianas o grandes; pero las nuevas necesidades, como, mejoras en los tiempos de latencia en servicios de video y voz, una administración centralizada, ser más escalables, todo ello ha generado en los proveedores de servicio de internet, que busquen e implementen nuevas alternativas, es así que, ubican a SD-WAN como una arquitectura WAN prometedora de próxima generación, ofreciendo a los administradores de red una nueva visión para el diseño y construcción de una red. El libre acceso al internet mediante las diferentes aplicaciones y servicios que la nube ofrece, ha logrado que la red del cliente se viera expuesta a amenazas, es así, el desafío indiscutible de cualquier nueva tecnología es la seguridad de la información, siendo considerada como activo en el interior de una empresa, debido a que los operadores, empleados, socios, gerentes, usuarios invitados, administradores de TI en sí, quienes integran una empresa están en constante tratamiento y generando cada vez nueva información digital, por ello, mantener la privacidad y confidencialidad se vuelve parte fundamental en una empresa, otra característica ofrece SD-WAN.

Se define a SD-WAN, como la aplicación de tecnologías de red basadas en software a conexiones de redes área extensa para proporcionar acceso rentable y de alto rendimiento a servicios cloud, centros de datos privados y aplicaciones empresariales basadas en Software como Servicio (SaaS)". Las soluciones SD-WAN reemplazarían a las redes de área extensa tradicionales para entregar tráfico basado en políticas a través de "n" conexiones WAN. Entre ellos podríamos observar en la **Tabla 4** ¿Por qué elegir SD-WAN?, como lo menciona Cisco uno de los líderes mundiales de esta tecnología:

Tabla 4

Ventajas de SD-WAN proveedor Cisco

Ventajas	Descripción
Experiencia en Aplicaciones	• SLA predecible para voz, nube y otras aplicaciones empresariales críticas. • Políticas de aplicación con aplicación en tiempo real sobre problemas de red. Múltiples enlaces híbridos activo-activo para todos los escenarios.
Seguridad total para aplicaciones de Internet y en la nube	• Pila de seguridad integrada completa, tanto en las instalaciones como en la nube. • Base de confianza cero con autenticación, cifrado y segmentación Seguridad web, firewall empresarial, IPS, AMP NGAV, aplicación de la capa DNS, filtrado de URL y proxy de descifrado SS
Multinube Optimizado	• SD-WAN se extiende a las principales nubes públicas y colocación proveedores. Rendimiento optimizado en tiempo real para Office 365, Salesforce y otras aplicaciones SaaS importantes. Integración de flujo de trabajo para AWS, Azure y Google Cloud.
Simplificación en la operación	• Integración total de comunicación unificada, multicloud y seguridad. Panel de administración único para configuración y gestión automatizada de seguridad WAN. • Automatización con aprovisionamiento zero touch basado en plantillas e integración restfull.
Error	• La visibilidad granular de aplicaciones e infraestructura, permite correlación y mitigación rápida de fallas.

- Pronóstico sofisticado y análisis hipotético para una planeación de recursos
- Recomendaciones perspicaces para cambios de políticas basadas en patrones de tráfico.

Nota. Fuente: Tomado de (SD-WAN, 2020)

2.2.1 Arquitectura de SD-WAN

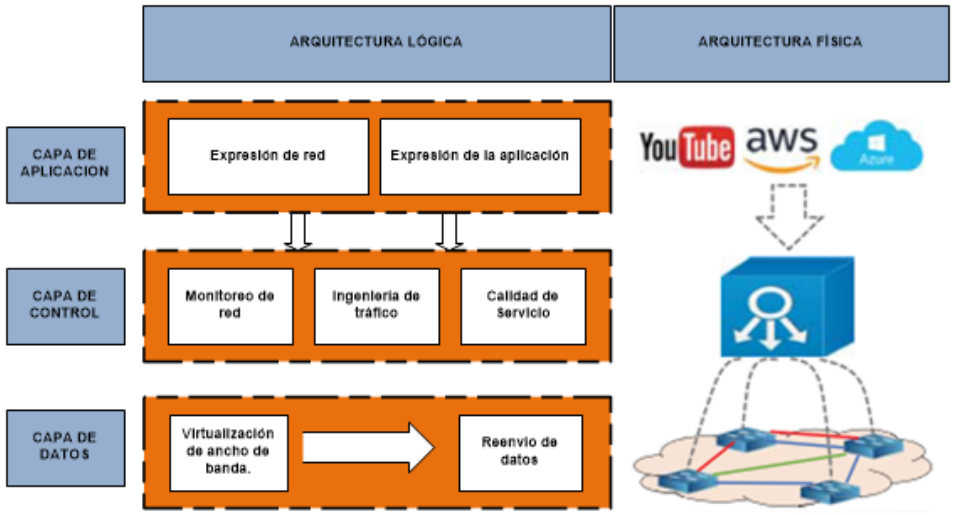
A continuación, se brindará una descripción de la arquitectura desde un punto de vista lógico y físico.

2.2.1.1 Arquitectura Lógica

En la **Figura 13** se observa que existen tres capas en el diseño lógico de una red SD-WAN.

Figura 13

Arquitectura Lógica y Física de SD-WAN



Nota. Fuente: Ojeda M, 2021 Tomado de (Yang et al., 2019)

Capa de Datos. La función de la capa de datos se subdivide en dos aspectos fundamentales como lo menciona (Yang et al., 2019):

Virtualización de ancho de banda. Esta combina diferente enlaces de red como son (MPLS, 4G, Internet etc), que sirven a una ubicación en un grupo de recursos disponibles para todas las aplicaciones y servicios.

Reenvío de datos. Es un conjunto distribuido de elementos de red de reenvío, principalmente conmutadores, su función es de reenviar paquetes empleando el ancho de

banda, facilitando el proceso por la virtualización; este proceso lo llevan mediante el protocolo de interfaz como OpenFlow, que se encarga de recibir comandos del controlador de red de la capa de control.

Capa de control. La capa de control tiene un número extenso de funciones, pero cada función opera de forma independiente, al igual que su implementación. Estas funciones han logrado que el personal de TI pueda administrarlas, de forma, que puedan desarrollar, modificar, depurar y de ser posible eliminar, sin afectar la una de la otra.

Una característica relevante de esta capa es que permite que sus funciones se puedan conectar o relacionar, para crear múltiples servicios y así incrementar la flexibilidad de SD-WAN.

Capa de Aplicación. La capa de aplicación da apertura a los proveedores de red y desarrolladores de aplicaciones, para que participen de una forma que puedan controlar mejor la red. Todo esto parte de las necesidades de los usuarios, convirtiéndose en requisitos, un ejemplo, son los usuarios que deben tener grandes transmisiones en vivo o el uso de telefonía IP, los tiempos de la latencia en estos servicios deben ser óptimos, para que pueda existir una comunicación exitosa. Mientras los requisitos de menor prioridad puedan ser tratados de forma que no tengan algún grado de afectación.

2.2.1.2 Arquitectura Física

A diferencia de la arquitectura lógica, en la arquitectura física, la capa de datos se encuentra integrada por un conjunto de conmutadores de Redes Definidas por Software SDN, interconectados entre sí, proceso que se lleva a cabo mediante enlaces físicos, como lo es un controlador de red, este suele ser un servidor o un clúster, dependiendo de la dimensión de la red y complejidad de esta. En la parte superior del controlador de red, se encuentran aplicaciones específicas, estas fueron diseñadas por los desarrolladores de aplicaciones y desarrolladores de red; de esta forma los proveedores pueden expresar sus requisitos al controlador de red, y el controlador de red los convierte en políticas y configuraciones compatibles.

Los controladores de red pueden operar de dos formas, el uno puede tomar el rol como controlador maestro y otros como controladores de respaldo, la forma de operar es que cuando falla el controlador maestro, uno de los controladores de respaldo ejecutará las tareas de forma inmediata.

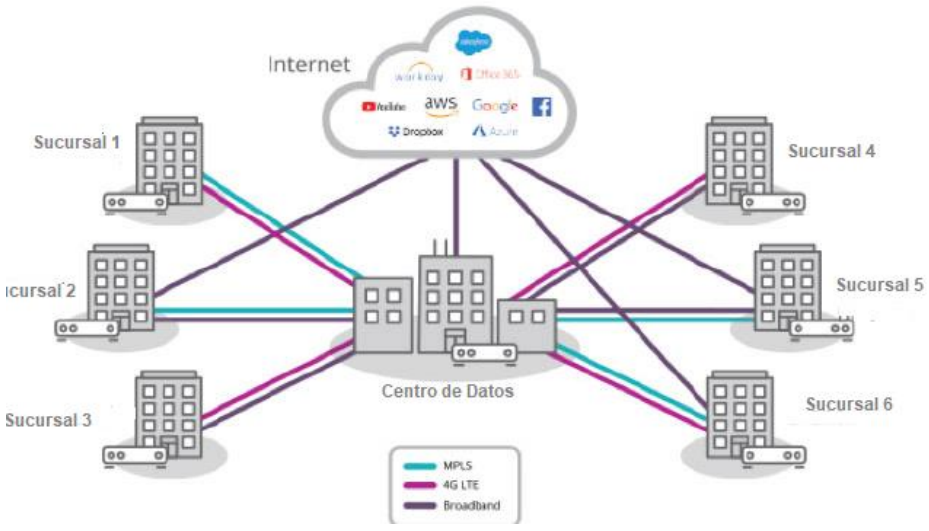
2.2.2 Modo de Operación de SD-WAN

SD-WAN aprovecha los principios de SDN y extiende los beneficios fuera del centro de datos, separando la red WAN en un plano de datos y un plano de control. La administración central de SD-WAN puede estar basada en la nube o alojada en las instalaciones. Durante la implementación, la automatización y la replicación de la configuración, puede ejecutarse sin contacto de los dispositivos de borde, lo que lo hace ideal para desplegarlo en sucursales y hasta en pequeñas oficinas como son las que se han creado en el hogar en la actualidad.

Como lo indica (Radcliffe et al., 2019), SD-WAN crea una superposición de red diferente de la infraestructura WAN subyacente. La superposición de red es una arquitectura de software, siendo la responsable de elegir la toma de decisiones en el enrutamiento y la señalización del tráfico; esto es, independiente de la red de transporte física. La capa de transporte WAN puede ser MPLS, Internet, LTE o incluso, en el caso de un usuario a domicilio que usa un enlace de banda ancha. Además, todos los métodos de transporte WAN, se pueden agregar mediante el plano de control, lo que proporciona una conexión más ágil y resistente. El tráfico de red en el plano de datos puede atravesar los múltiples enlaces WAN y la ruta que toman los datos puede moverse a la ruta alternativa de forma muy rápida. En la **Figura 14**, se logra apreciar la arquitectura de una solución SD-WAN, corriendo sobre diferentes redes de transporte WAN.

Figura 14

Capas de Transporte de Redes de Área Extensa



Nota. Fuente: Ojeda M. 2021, Tomado de (Acacia, n.d.)

Capítulo 3: Diseño de DMVPN-MPLS sobre Protocolo de Internet IPv6 como Red de Transporte Empresarial

3.1 Diseño de la Red DMVPN-MPLS

El diseño de la red piloto DMPVN sobre una red MPLS, se implementa en la fase 3, esto debido a que durante esta fase cuenta con las siguientes mejoras, en relación con la fase 1 y fase 2.

No requiere que el Hub conserve los valores del siguiente salto en las actualizaciones del enrutamiento, permitiendo sumarizar las rutas de los protocolos de enrutamiento del Hub y anunciando a los Spoke las mejores.

Los Spoke pueden utilizar rutas sumarizadas, donde el próximo salto pude ser la IP de la dirección IP del túnel del Hub y, aun así, poder construir túneles de Spoke a Spoke.

3.1.1 Diseño de Topología Física

El equipamiento empleado para la prueba de concepto comprende en tecnología CISCO, esto a que es una solución propietaria.

A continuación, se detalla las características de los equipos ruteadores, tanto en el Hub y los Spoke.

Router. Los ISR de la serie Cisco® 880 integran acceso a internet, seguridad a servicios de voz y a servicios inalámbricos, mediante un único dispositivo, ideal para administrar pequeñas sucursales e ideales para enlaces domiciliarios como son los de teletrabajadores de empresas. En la **Figura 15**, se observa el router CISCO 881-K9.

Figura 15

Router Cisco 881-K9

Nota. Fuente: Elaboración propia

A continuación, en la **Tabla 5** se aprecia las características técnicas del router 881-K9.

Tabla 5

Características Enrutador 881-K9

Router	Características
Hub / Spoke **Cisco 881-K9**	• Soportan 20 túneles • Algoritmo Cifrado: AES de 128 bits, 192 bits AES, 256-bit AES, DES, LEAP, PEAP, PKI, SSL, TKIP, Triple DES. • Puertos WAN: 1 • Protocolo de enrutamiento: BGP, EIGRP, GRE, HSRP, PNDH, OSPF, PIM-SM, RIP-1, RIP-2, VRRP. • Transferencia de Datos: 100 Mbps

Nota. Fuente: Elaboración propia

Últimas millas. La red de acceso o las últimas millas entregadas por el ISP permiten la conexión entre los dispositivos CE y PE, en el caso del Hub y los Spoke, el proveedor entrega fibra óptica. En la **Figura 16,** se observa una última milla de fibra óptica.

Figura 16

Transceptor y Cable de Fibra Óptica

Nota. Fuente: Elaboración propia

3.1.2 Diseño de Topología Lógica

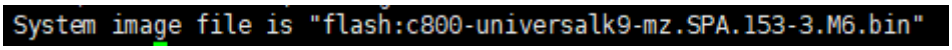
3.1.2.1 Red del Proveedor de Servicios.

El backbone del ISP, es una red diseñada bajo el modelo jerárquico de tres capas core, distribución y acceso, que la integran un conjunto de equipos de conmutación y enrutamiento de marca Cisco. En su capa de core y distribución, está configurado MPLS, para trabajar como enrutador de conmutación de etiquetas LSRs y ruteador de frontera de etiquetado (LERs), siendo los responsables de enrutar el tráfico entrante a la red MPLS.

El IOS utilizado en el Hub y los Spoke es, flash:c800-universalk9-mz.SPA.153-3.M6.bin", como se logra apreciar en le **Figura 17.**

Figura 17

IOS de router Cisco 881-K9.



Nota. Fuente: Elaboración propia

3.1.3 Diseño Propuesto sobre DMVPN-MPLS

La topología consiste en permitir la conexión de tres agencias, la agencia principal es denominada matriz, y es denominado, como router Hub y los Spoke, son sitios alternos o agencias que se enlazan hacia el Hub.

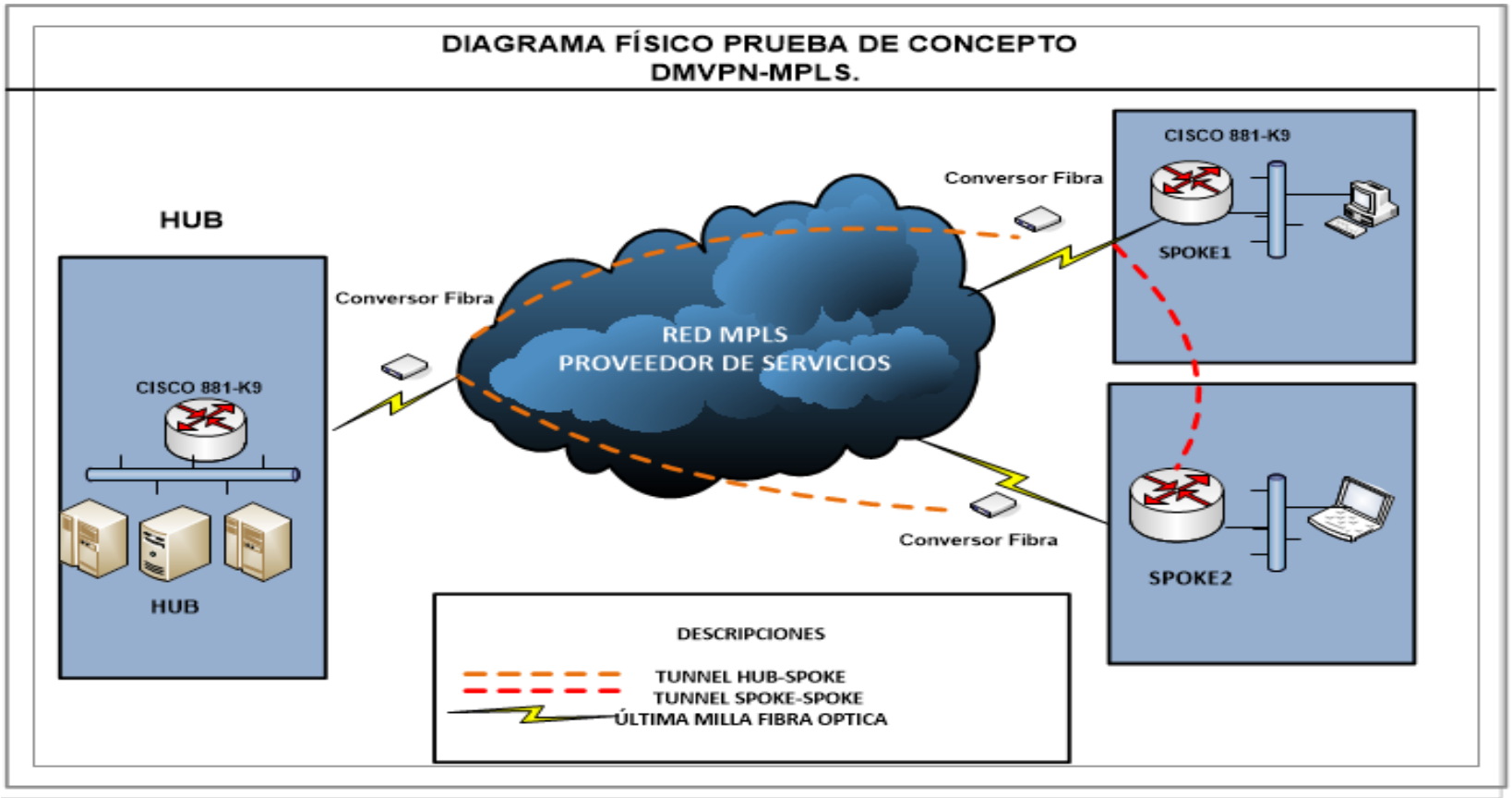
La fase que se propone es fase 3, esto debido a su gran ventana de creación de túneles entre Spoke, sin necesidad de pasar por el Hub. Su formación es de forma automática y bajo demanda.

En la **Figura 18,** se observa la topología física del escenario propuesto. En este escenario, se utiliza router Cisco 881-K9 en las tres agencias.

En la **Figura 19,** se logra apreciar la topología lógica, donde se aprecia los protocolos de enrutamientos, el direccionamiento IPv6 que formaran parte de los túneles y la red interna de las agencias. Así como la nube MPLS, que es administración del ISP.

Figura 18

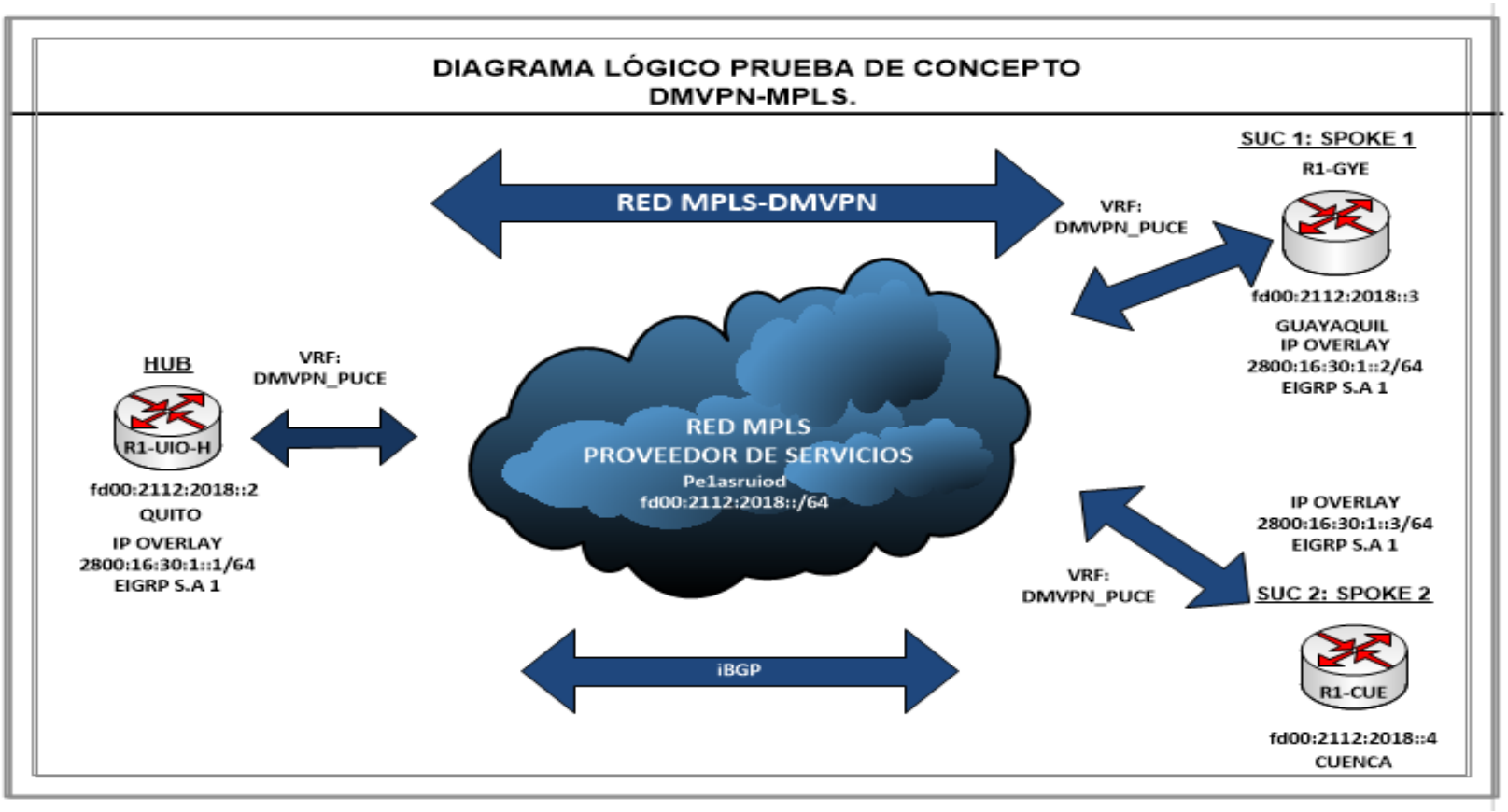
Topología Física Propuesta DMVPN-MPLS



Nota. Fuente: Elaboración propia

Figura 19

Topología Lógica Propuesta DMVPN-MPLS



Nota. Fuente: Elaboración propia

A continuación, se detalla las especificaciones técnicas del router Hub y los Spoke de las tres agencias, como se aprecia en la **Figura 20, Figura 21** y **Figura 22.**

Figura 20

Router Cisco 881-K9 HUB-QUITO

```
Cisco C881-K9 (revision 1.0) with 488524K/35763K bytes of memory.
Processor board ID FJC2108L22W
5 FastEthernet interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 32 bits wide
255K bytes of non-volatile configuration memory.
250880K bytes of ATA System CompactFlash (Read/Write)
```

Nota. Fuente: Elaboración propia

Figura 21

Router Cisco 881-K9 SPOKE-GUAYAQUIL

```
Cisco C881-K9 (revision 1.0) with 488524K/35763K bytes of memory.
Processor board ID FJC2108L1PV
5 FastEthernet interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 32 bits wide
255K bytes of non-volatile configuration memory.
250880K bytes of ATA System CompactFlash (Read/Write)
```

Nota. Fuente: Elaboración propia

Figura 22

Router Cisco 881-K9 SPOKE-CUENCA

```
Cisco C881-K9 (revision 1.0) with 488524K/35763K bytes of memory.
Processor board ID FJC2108L1NV
5 FastEthernet interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 32 bits wide
255K bytes of non-volatile configuration memory.
250880K bytes of ATA System CompactFlash (Read/Write)
```

Nota. Fuente: Elaboración propia

3.1.4 Direccionamiento de la Red MPLS

El escenario propuesto contempla que el core del proveedor corre sobre una red MPLS en IPv4. En la **Tabla 6** se especifica el direccionamiento IP de las interfaces WAN que comprende; Quito, Guayaquil y Cuenca. Adicional se detalla las interfaces de los equipos enrutadores.

Tabla 6

Direccionamiento IP de interfaces WAN del Hub y los Spoke

Equipo	Interfaz	Dirección de Subred	Dirección IP	Mascara
HUB-QUITO	FastEthernet4	fd00:2112:2018::	fd00:2112:2018::2	/64
SPOKE-GYE	FastEthernet4	fd00:2112:2018::	fd00:2112:2018::3	/64
SPOKE-CUE	FastEthernet4	fd00:2112:2018::	fd00:2112:2018::4	/64

Nota. Fuente: Elaboración propia

3.1.5 Direccionamiento IP Overlays de los Túneles

La red asignada para las IP overlay de los túneles, se asigna en el segmento 2800:16:30:1::/64 de forma ascendente, como se logra apreciar en la **Tabla 7.**

Tabla 7

Direccionamiento IP Overlays

Equipo	Interfaz	Dirección de Subred	Dirección IP	Máscara
HUB-QUITO	Tunnel100	2800:16:30:1::	2800:16:30:1::1	/64
SPOKE-GYE	Tunnel100	2800:16:30:1::	2800:16:30:1::2	/64
SPOKE-CUE	Tunnel100	2800:16:30:1::	2800:16:30:1::3	/64

Nota. Fuente: Elaboración propia

3.1.6 Direccionamiento de Enlace Local

Las direcciones de enlace local del equipo Hub y los enrutadores Spoke, se asignan en el segmento FE80::, se detalla en la **Tabla 8.**

Tabla 8

Direccionamiento IP de enlace local.

Equipo	Interfaz	Dirección de Subred	Dirección IP
HUB-QUITO	Tunnel100	FE80::1	link-local
SPOKE-GYE	Tunnel100	FE80::2	link-local
SPOKE-CUE	Tunnel100	FE80::3	link-local

Nota. Fuente: Elaboración propia

3.1.7 Direccionamiento de Interfaces Loopback

La red asignada para interfaces loopback de los túneles, se asigna en el segmento 2800:16:30:1::/64, de forma ascendente cómo se logra apreciar en la **Tabla 9**.

Tabla 9

Direccionamiento IP de Interfaces Loopback

R1-HUB-UIO	Loopback1	2800:16:10:1::1	64
SPOKE-GYE	Loopback1	2800:16:11:1::1	64
SPOKE-CUE	Loopback1	2800:16:12:1::1	64

Nota. Fuente: Elaboración propia

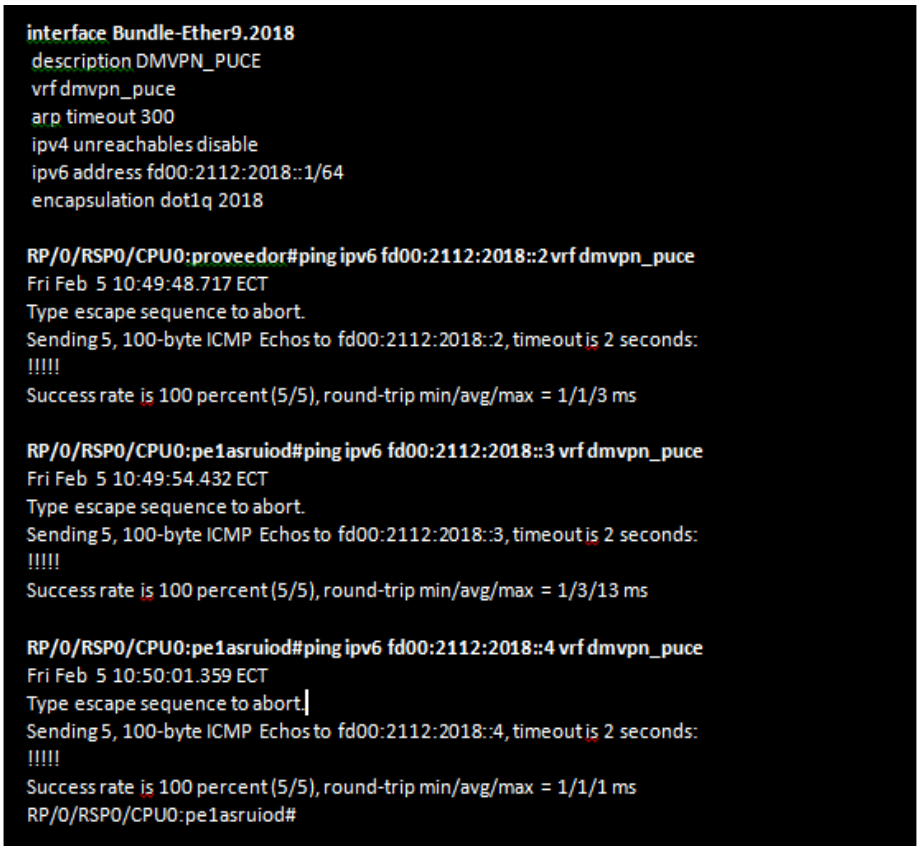
3.1.8 La Red MPLS

La troncal del proveedor de servicios, utiliza protocolos OSPF y BGP para la comunicación entre el P y los PE, la misma se encuentre implementada en IPv4.

Para iniciar con la solución planteada se debe tener conectividad entre las interfaces WAN de las tres agencias. El router de borde del proveedor de servicio utiliza la IP de enganche FD00:2112:2018::1/64, el Hub y los Spoke contarán con direccionamiento en este segmento de forma ascendente.

Figura 23

Conexión entre el PE-HUB-QUITO y PE-SPOKE

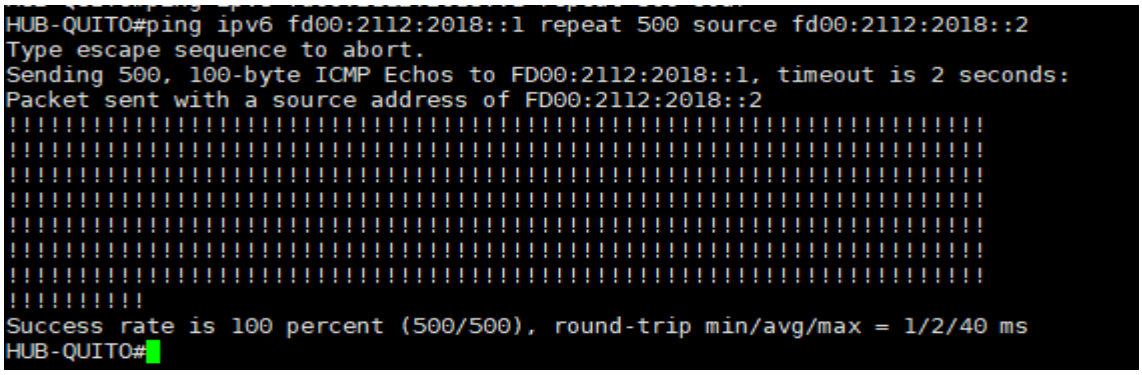


Nota. Fuente: Elaboración propia

A continuación, en la **Figura 24, Figura 25 y Figura 26** se valida que existe conexión entre las interfaces WAN del Hub y de los Spoke hacia el PE.

Figura 24

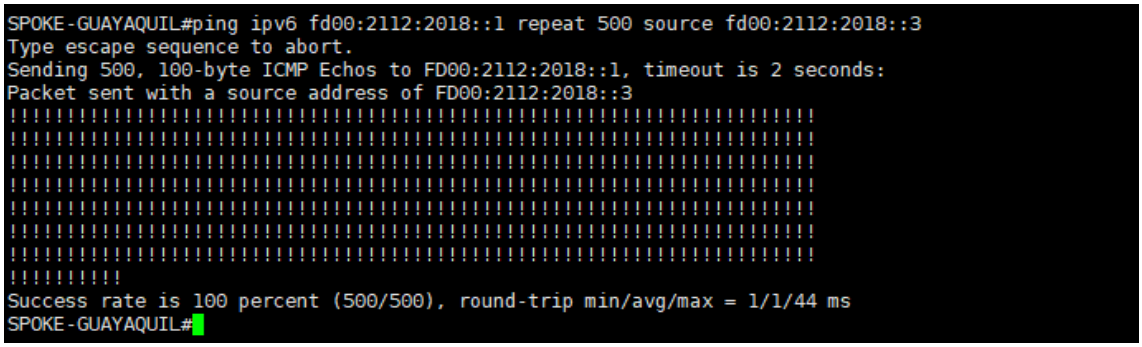
Conexión entre HUB-QUITO y PE



Nota. Fuente: Elaboración propia

Figura 25

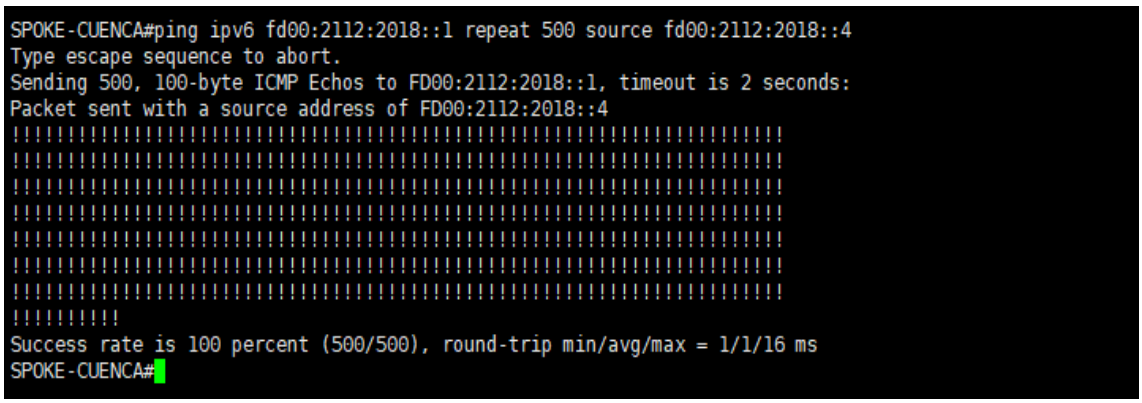
Conexión entre SPOKE-GUAYAQUIL y PE



Nota. Fuente: Elaboración propia

Figura 26

Conexión entre SPOKE-CUENCA y PE



Nota. Fuente: Elaboración propia

Con las pruebas de conectividad realizadas, se valida que el proveedor de servicios asegura conectividad entre las diferentes agencias a nivel interfaces WAN.

Capítulo 4: Implementación de Red DMVPN-MPLS sobre Protocolo de Internet IPv6 como Red de Transporte Empresarial

4.1 Implementación de la Solución Propuesta

Para despliegue y prueba de concepto de DMVPN-MPLS sobre protocolo de internet IPv6 como red de transporte empresarial, se da inicio con el despliegue de la red DMVPN, entre el Hub que representa la matriz y los Spoke a la ciudad de Guayaquil y Cuenca respectivamente.

4.1.1 Configuración de Seguridad

Uno de los beneficios de DMVPN, es la seguridad que se implementa en la comunicación entre túneles, mediante IPsec, que son algoritmos que protegen la información, se incluye dentro de la solución un perfil de seguridad IPsec.

A continuación; se detalla la sintaxis de IKE aplicada a la solución, véase **Anexo 1.** Luego de aplicar la sintaxis, se aprecia la configuración de la política IKE, véase **Anexo 2,** esta se aplicaría en el Hub y los Spoke.

Para el escenario se aplica claves pre-compartidas, se puede apreciar en el **Anexo 3** la respectiva sintaxis. En el **Anexo 4,** se observa la configuración IPsec y la creación de nuestro perfil IPsec en el **Anexo 5.** La configuración del perfil de IPsec se replica en el Hub y los Spoke, véase **Anexo 6, Anexo 7 y Anexo 8.**

4.1.2 Configuración de Interfaces WAN

En base al direccionamiento de la **Tabla 4**, se configura el Hub y los Spoke respectivamente; véase en el **Anexo 9** la sintaxis para configurar las interfaces WAN. Véase **Anexo 10, Anexo 11 y Anexo 12** se configura las interfaces WAN de Quito, Guayaquil y Cuenca respectivamente.

4.1.3 Configuración de IP Overlays de los Túneles

Para la configuración de los túneles, se ha utilizado el direccionamiento de la **Tabla 5,** el número de la interfaz tipo túnel es 100. Se debe ingresar en modo de configuración global en la interfaz tipo túnel. Véase **Anexo 13** donde se detalla los pasos para configurar. La configuración del router Hub y de los Spokes, véase en **Anexo 14, Anexo 15** y **Anexo 16** respectivamente.

4.1.4 Configuración de Protocolo de Enrutamiento EIGRP

El protocolo de enrutamiento que se utiliza para anunciar de forma dinámica las interfaces loopback del router Hub y de los Spoke, es EIGRP en IPv6. En el **Anexo 17**,

se detallan los pasos para configurar EIGRP. El número sistema autónomo ID es 1, para las tres agencias. Véase en **Anexo 18, Anexo 19 y Anexo 20.**

4.1.5 Configuración de DMVPN

El escenario propuesto consta de las tres agencias: Quito, Guayaquil y Cuenca, las tres funcionan en una topología en fase 3 DMVPN, donde Quito representa el Hub, y los Spoke son representados como las agencias remotas.

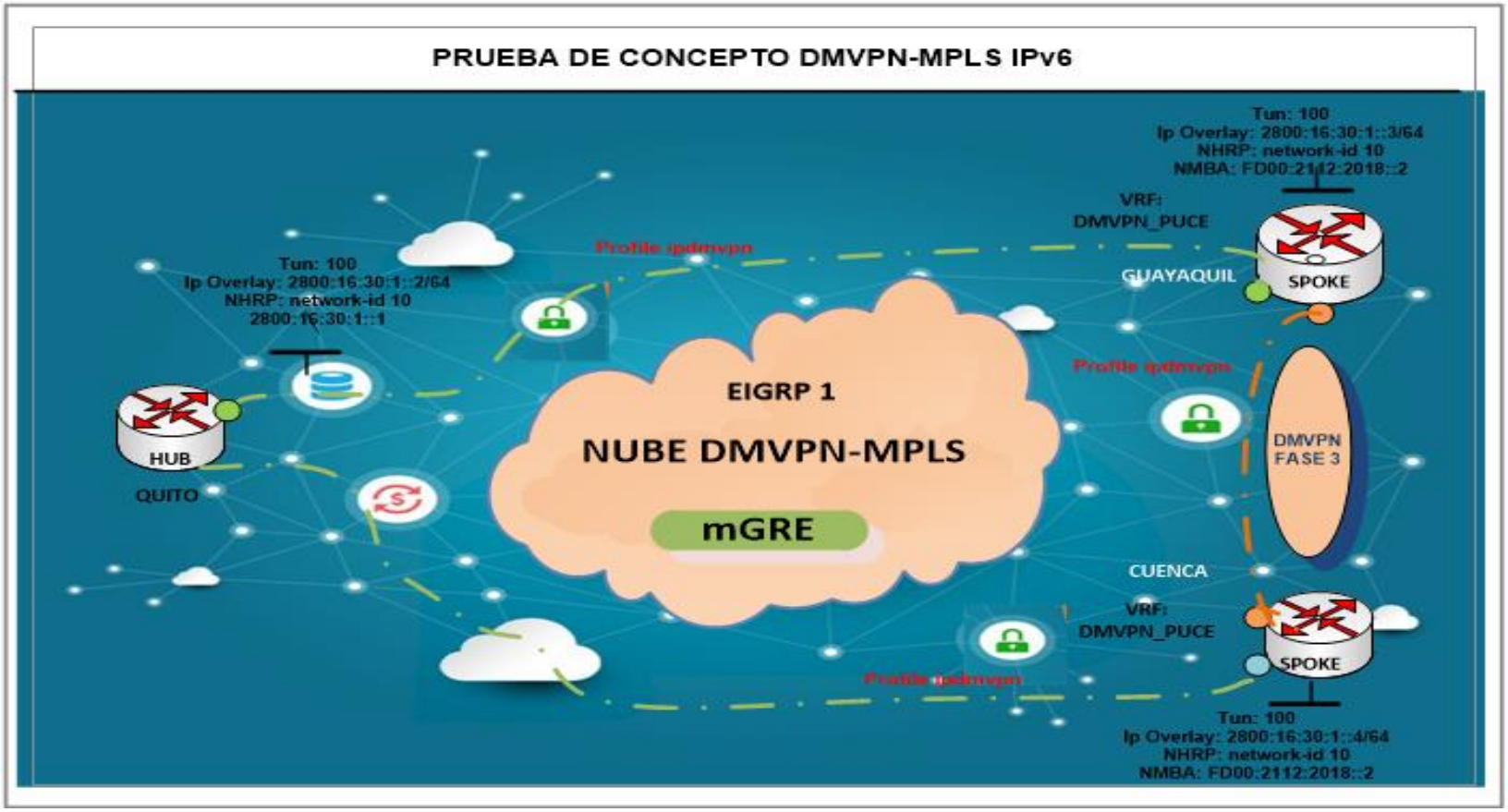
Véase en el **Anexo 21,** los pasos para configurar un router Hub. En el **Anexo 22**, se especifica como configurar el router HUB-QUITO. Para la configuración se utilizará las direcciones IPv6 descritas anteriormente en la **Tabla 4.**

Luego de configurar el router Hub, se detallan los pasos a configurar de los enrutadores Spoke, véase **Anexo 23.** Como se aprecia, la configuración tiene ciertas variaciones entre el Hub y los Spoke, esto se debe a que el Hub tendrá la función de una base de datos NHRP; donde se almacenan las direcciones IP o direcciones de redes de los otros Spoke; esta forma de operar es muy similar al protocolo de resolución de dirección ARP, este almacenamiento proporciona un mecanismo para que los dispositivos aprendan el protocolo y la red NBMA, lo que genera la creación de túneles dinámicos entre los Spoke, sin necesidad de pasar por el concentrador. A continuación; se procede con la configuración del Spoke Guayaquil y Spoke Cuenca con su perfil de seguridad ipdmvpn**,** véase **Anexo 24 y Anexo 25** respectivamente.

La configuración del router Cuenca es muy similar que el router de Guayaquil; cabe mencionar que, si fuese una nueva agencia, la configuración sería la misma, los cambios son mínimos. A diferencia de que, en el Hub, no se debe realizar ningún cambio en la configuración. En la **Figura 27,** se logra apreciar la solución DMVPN-MPLS sobre protocolo de internet IPv6 implementada, donde se aprecia la red de superposición creada sobre la red MPLS del ISP.

Figura 27

Red DMVPN-MPLS sobre Protocolo de Internet IPv6 como Red de Transporte Empresarial



Nota. Fuente: Elaboración propia

Capítulo 5: Análisis de Resultados de la Solución

5.1 Pruebas de Conectividad de la Solución Propuesta

Luego de la implementación de la red DMVPN, y sobre ella configurar IPsec, mGRE, NHRP e EIGRP, se confirma que la solución es viable y rentable, tanto en la parte técnica y económica.

DMVPN, es una solución que opera y trabaja de forma correcta, siempre y cuando la red MPLS del proveedor no tenga algún bloqueo de tráfico multicast, en las últimas millas de donde dependan las agencias, por lo que se recomienda validar con su ISP, los requisitos previos a la configuración de los enrutadores.

Adicional, validar la versión correcta de los IOS de los router esto debido a que partir de la versión m6, se puede configurar mGRE para tráfico IPv6.

A continuación, se detallan las diferentes pruebas de conectividad y el análisis de la solución técnica y un enfoque en la parte económica:

5.1.1 Pruebas de Conectividad

A continuación, se valida que existe conexión desde el HUB-QUITO hacia los SPOKE-GUAYAQUIL y SPOKE-CUENCA, se logra apreciar en la **Figura 28 y Figura 29** que existe conectividad con tiempos estables y sin pérdidas.

Figura 28

Conectividad entre el HUB-QUITO y SPOKE-GUAYAQUIL

```
HUB-QUITO#pin ipv6 2800:16:30:1::2 repeat 100 source 2800:16:30:1::1
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 2800:16:30:1::2, timeout is 2 seconds:
Packet sent with a source address of 2800:16:30:1::1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/16 ms
HUB-QUITO#
```

Nota. Fuente: Elaboración propia

Figura 29

Conectividad entre el HUB-QUITO y SPOKE-CUENCA

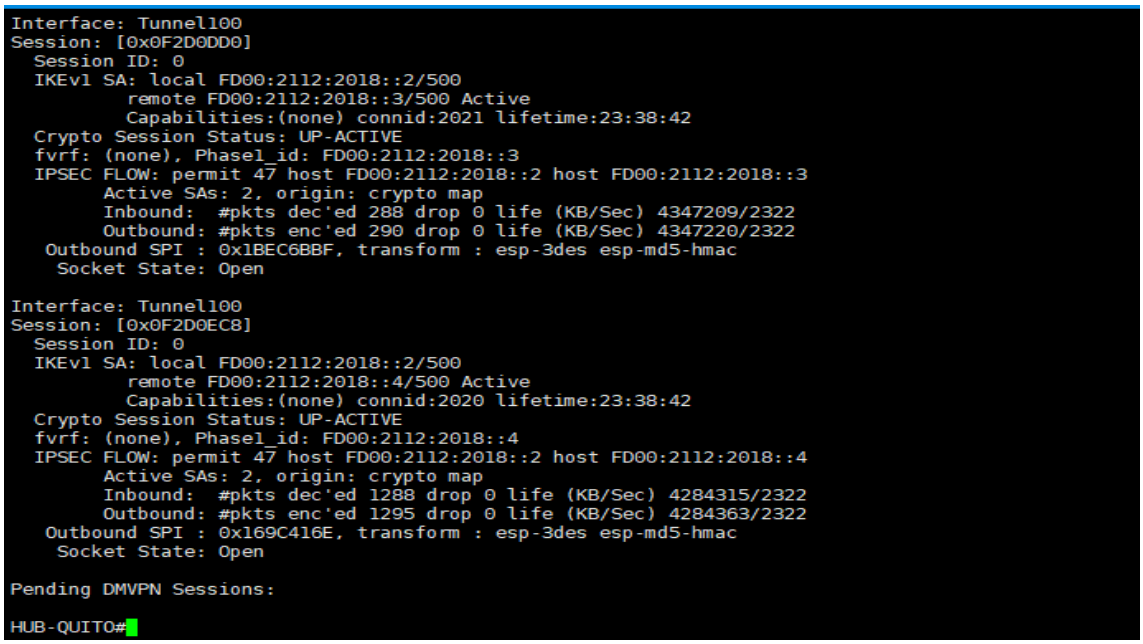
```
HUB-QUITO#pin ipv6 2800:16:30:1::3 repeat 100 source 2800:16:30:1::1
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 2800:16:30:1::3, timeout is 2 seconds:
Packet sent with a source address of 2800:16:30:1::1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/16 ms
HUB-QUITO#
```

Nota. Fuente: Elaboración propia

En la **Figura 30** se aprecia las sesiones IPsec entre el Hub y los Spoke.

Figura 30

Sesiones IPsec



Nota. Fuente: Elaboración propia

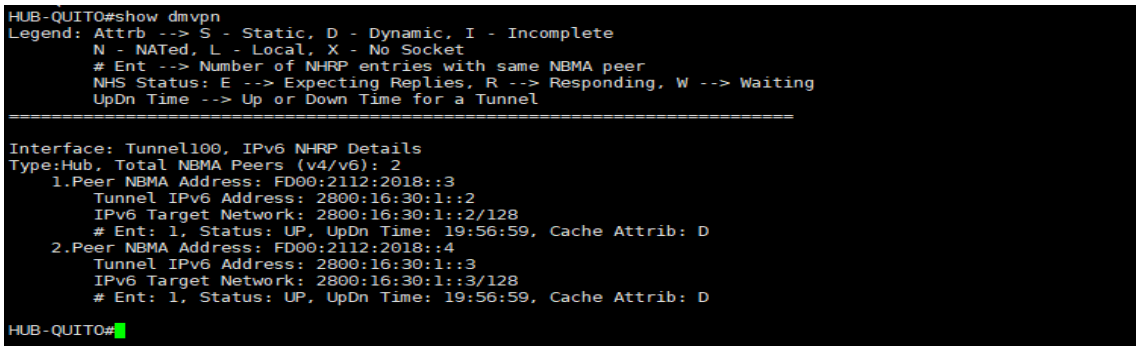
5.1.2 Sesiones DMVPN

DMVPN HUB-QUITO. Las sesiones DMVPN se encuentran UP, se puede apreciar en la **Figura 31** que existen dos sesiones UP, y fueron aprendidas de forma dinámica.

- Sesión 1: D00:2112:2018::3- Spoke-Guayaquil.
- Sesión 2: D00:2112:2018::4- Spoke-Cuenca.

Figura 31

Conectividad entre el SPOKE-GUAYAQUIL y SPOKE-CUENCA



Nota. Fuente: Elaboración propia

Tabla de enrutamiento en HUB-QUITO. En la **Figura 32**, se puede apreciar que se encuentran establecidas dos sesiones EIGRP IPv6, contra los dos Spoke mediante la interfaz del túnel 100.

Figura 32

Sesiones EIGRP IPv6.

```
HUB-QUITO#show ipv6 eigrp neighbors
EIGRP-IPv6 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   Link-local address:     Tu100                    10 20:04:29   44  1470  0  938
    FE80::3
1   Link-local address:     Tu100                    14 1w0d        6  1470  0  43
    FE80::2
HUB-QUITO#
```

Nota. Fuente: Elaboración propia

A continuación, en la **Figura 33,** se observa que se aprende las interfaces loopback del SPOKE-GUAYAQUIL y SPOKE-CUENCA mediante EIGRP.

Figura 33

Tabla de enrutamiento EIGRP IPv6

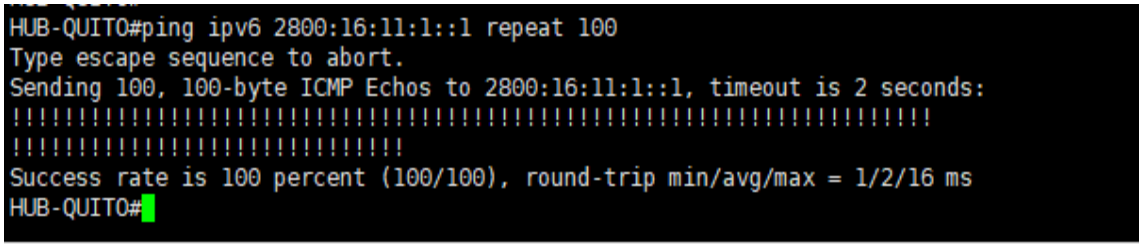
```
HUB-QUITO#show ipv6 route eigrp
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, D - EIGRP, EX - EIGRP external, ND - ND Default
       NDp - ND Prefix, DCE - Destination, NDr - Redirect, O - OSPF Intra
       OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, ls - LISP site, ld - LISP dyn-EID, a - Application
D   2800:16:11:1::/64 [90/27008000]
     via FE80::2, Tunnel100
D   2800:16:12:1::/64 [90/27008000]
     via FE80::3, Tunnel100
HUB-QUITO#
```

Nota. Fuente: Elaboración propia

Pruebas de conectividad desde HUB-QUITO hacia SPOKE-GUAYAQUIL A continuación, se aprecia en la **Figura 34**, la comunicación hacia la interfaz loopback en SPOKE-GUAYAQUIL, la misma fue aprendida por EIGRP

Figura 34

Conexión hacia interfaz loopback de SPOKE-GUAYAQUIL.

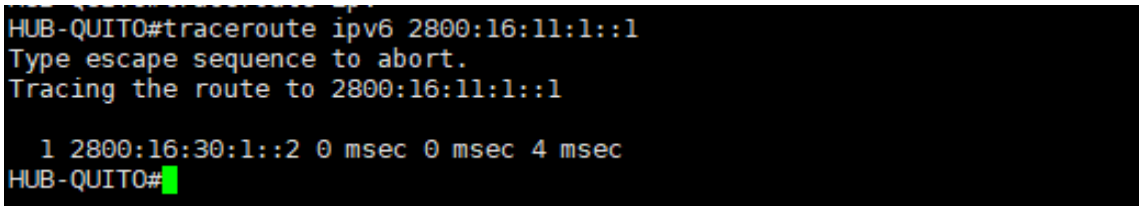


Nota. Fuente: Elaboración propia

A continuación, en la **Figura 35** se observa que la IP 2800:16:30:1::2 es la IP overlay del tunnel 100 del SPOKE-GUAYAQUIL, es decir que su conexión es mediante DMVPN.

Figura 35

Traza hacia SPOKE-GUAYAQUIL

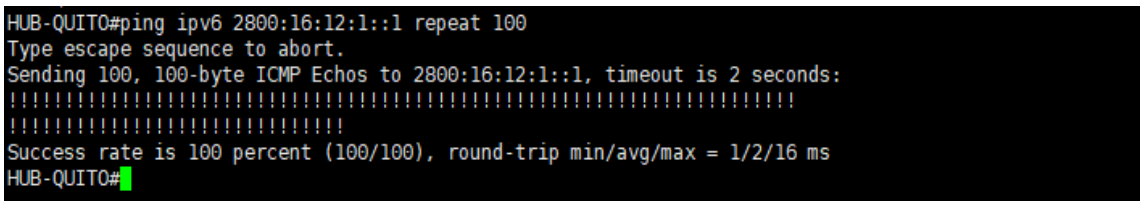


Nota. Fuente: Elaboración propia

Se observa en la **Figura 36 y Figura 37**, la conexión hacia el router de Cuenca mediante DMVPN.

Figura 36

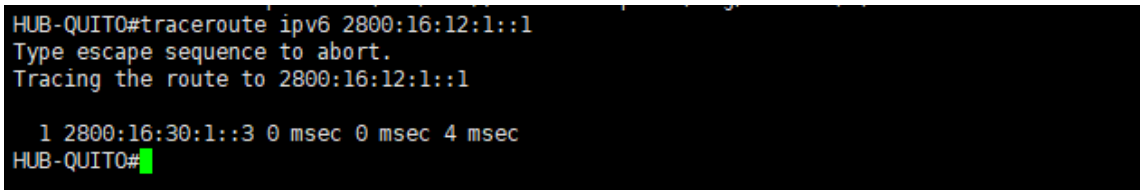
Conexión interfaz loopback de SPOKE-CUENCA



Nota. Fuente: Elaboración propia

Figura 37

Traza hacia interfaz loopback de SPOKE-CUENCA.

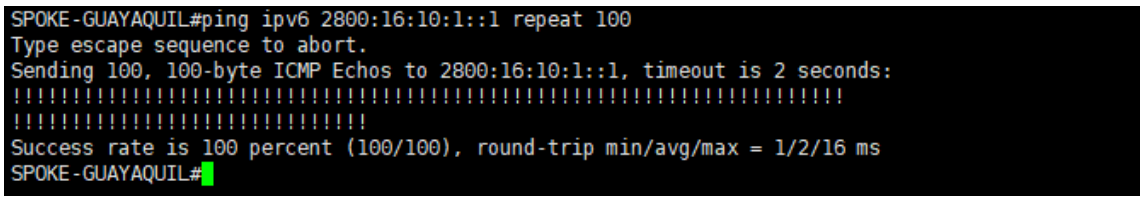


Nota. Fuente: Elaboración propia

DMVPN SPOKE-GUAYAQUIL. La comunicación entre el SPOKE-GUAYAQUIL y el HUB-QUITO, se puede apreciar en la **Figura 38.**

Figura 38

Conexión hacia interfaz loopback de HUB-QUITO



Nota. Fuente: Elaboración propia

DT1, indica que estás sesiones se crean de forma dinámica entre los Spoke, sin necesidad de pasar por el enrutador Hub. Esta característica es propia de la fase 3 de DMVPN. A continuación, en la **Figura 39,** se logra apreciar las sesiones DMVPN.

Figura 39

Traza hacia interfaz loopback 2800:16:11:1::1 (SPOKE-GUAYAQUIL)

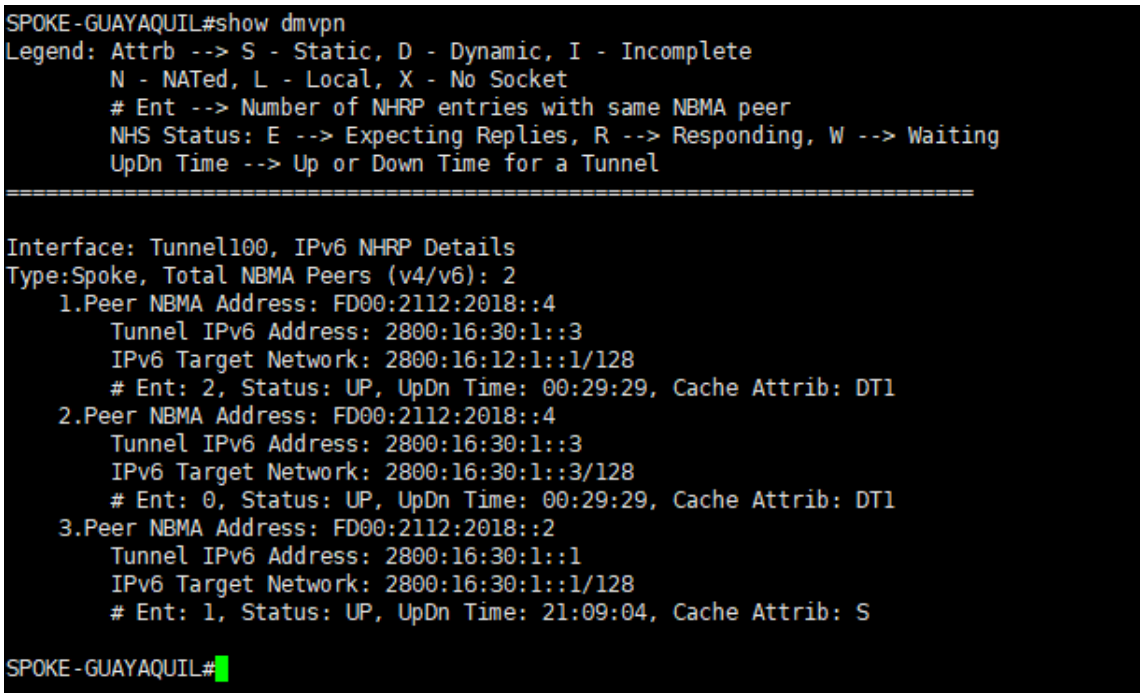
Nota. Fuente: Elaboración propia

DMVPN SPOKE-CUENCA. En la **Figura 40,** se logra apreciar, el comportamiento de los túneles que se arman de forma dinámica. Al realizar una traza en primera instancia hacia la interfaz loopback (2800:16:11:1::1) que es SPOKE-GUAYAQUIL, primero realiza un salto en el HUB-QUITO, este luego enviará un mensaje de redireccionamiento a los Spoke para informarles de su tabla de NHRP, debido a que

ambos son Spoke de DMVPN y con ello tendría una mejor ruta; y así puede construir un túnel directo entre Spoke y Spoke.

Figura 40

Sesiones DMVPN Spoke Guayaquil

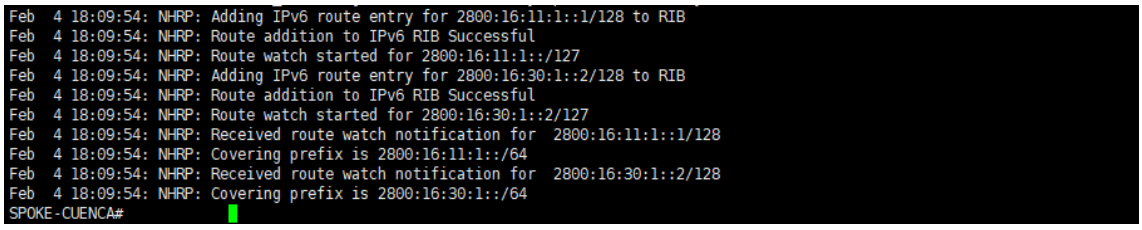


Nota. Fuente: Elaboración propia

A continuación, luego de que el Hub anuncia cual es la mejor ruta en su tabla NHRP de forma automática, se crea el túnel de forma directa con el SPOKE-GUAYAQUIL como se aprecia en la **Figura 41.**

Figura 41

Servidor NHRP

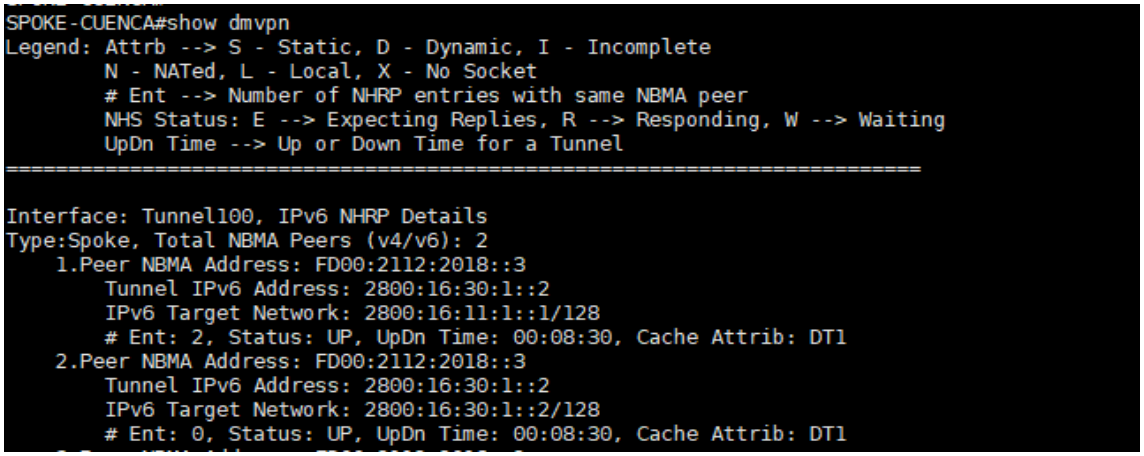


Nota. Fuente: Elaboración propia

Se aprecia en la **Figura 42,** la creación de forma dinámica de los túneles entre los Spoke.

Figura 42

Túnel dinámico entre Spoke



Nota. Fuente: Elaboración propia

Luego de la creación del túnel, se logra apreciar que existe una conectividad directa entre los Spoke, sin necesidad de pasar por el HUB-QUITO, se aprecia en la **Figura 43**.

Figura 43

Traza hacia SPOKE-GUAYAQUIL (Redirect)

Nota. Fuente: Elaboración propia

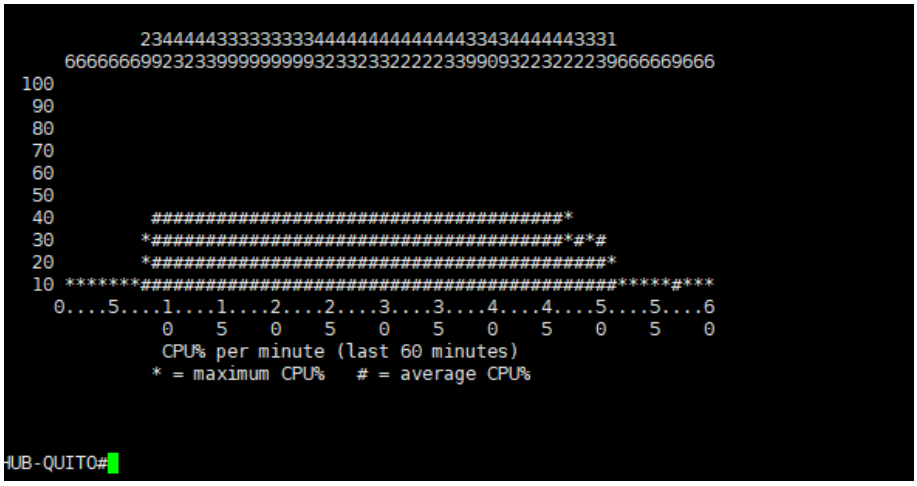
5.1.3 Análisis de la Solución Propuesta DMVPN-MPLS

Con base en los resultados obtenidos en las pruebas de conectividad y el monitoreo que se realizó sobre los enlaces durante la fase de pruebas, se pudo determinar que:

La solución DMVPN, no generó algún sobreprocesamiento de CPU en el enrutador Cisco 881-K9 en ninguna de las tres agencias. En la **Figura 44**, se puede apreciar el procesamiento del equipo Hub.

Figura 44

Procesamiento de enrutador HUB-QUITO



Nota. Fuente: Elaboración propia

Durante las pruebas de conectividad, en la agencia HUB-QUITO y SPOKE-CUENCA, se mantuvo en monitoreo las últimas millas para determinar los tiempos de respuesta; los mismos se mantuvieron sobre el promedio de una red sobre fibra óptica que son 1 ms., como se aprecia en la **Figura 45** y **Figura 46.**

Figura 45

Tiempos de respuesta de SPOKE-CUENCA

Nota. Fuente: Elaboración propia

Figura 46

Tiempos de respuesta de HUB-QUITO

Nota. Fuente: Elaboración propia

Se generó tráfico promedio de 2048 Kbps a 3072 Kbps, desde la agencia SPOKE-CUENCA hacia el HUB-QUITO, donde se aprecia que los tiempos estables, como se aprecia en la **Figura 47**.

Figura 47

Tráfico promedio durante las pruebas HUB-QUITO y SPOKE-CUENCA.

Nota. Fuente: Elaboración propia

No se identificó algún error de CRcs sobre la interfaz tunnel 100 en el HUB-QUITO, como se observa en la **Figura 48**.

Figura 48

Interfaz tunnel 100 HUB-QUITO

Nota. Fuente: Elaboración propia

En la prueba de conectividad desde el enrutador SPOKE-CUENCA hacia el enrutador SPOKE-GUAYAQUIL, se logra apreciar que no existen pérdidas de paquetes, es decir que la comunicación se mantiene estable durante la conexión entre agencias, como se aprecia en la **Figura 49**.

Figura 49

Tiempos durante comunicación SPOKE-CUENCA y SPOKE-GUAYAQUIL

Nota. Fuente: Elaboración propia

-

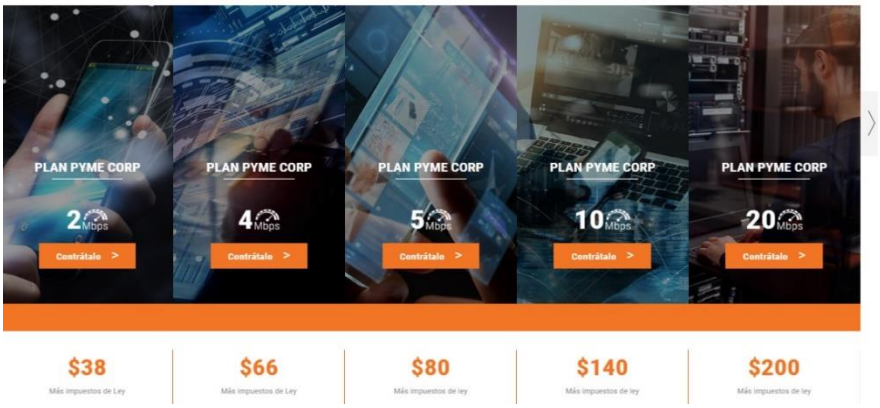
5.1.4 Análisis de Costos sobre Soluciones de Internet

En el mercado, existen varios proveedores de servicios de internet, se tomará como referencia a Telconet, Netlife, Corporación Nacional de Telecomunicaciones y Grupo TvCable, que cuentan ya desplegada su red sobre tecnología MPLS. El análisis se realizará sobre un enlace de 10 Mbps, sobre enlaces corporativos 1:1.

En la **Figura 50,** se logra apreciar los planes corporativos que ofrece Netlife, estos enlaces son dedicados 1 a 1.

Figura 50

Costo de servicio de internet Netlife



Nota. Fuente: Tomado de (Netlife, 2021)

En la **Figura 51,** se aprecia el precio del servicio Internet de la Corporación Nacional de Telecomunicaciones CNT, tomar en consideración que es un enlace asimétrico.

Figura 51

Costo de servicio de internet CNT

Tarifas

Planes	Tarifa mensual	Medio de transmisión
Hasta 10 x 5 Mbps	$70,00	Fibra Óptica / GPON
Hasta 20 x 10 Mbps	$90,00	Fibra Óptica / GPON
Hasta 35 x 15 Mbps	$133,70	Fibra Óptica / GPON
Hasta 45 x 20 Mbps	$149,85	Fibra Óptica / GPON
Hasta 55 x 25 Mbps	$198,25	Fibra Óptica / GPON

Nota. Fuente Tomado de (Corporación Nacional de Telecomunicaciones, 2021)

En la **Figura 52,** se aprecia el precio del servicio internet de Grupo TvCable tomar en consideración que es un enlace 1:1, de 10 Mbps.

Figura 52

Costo de servicio de internet Grupo TvCable

Nota. Fuente: Tomado de (Corporativas, 2012)

Con base en los tres proveedores, se tomará como referencia los que ofertan servicios dedicados, es decir Netlife y Grupo Tv Cable. A continuación, se determina un precio promedio, donde se suma la oferta de ambos proveedores y se divide para dos:

Ecuación 1:

$140.00 + $173.49 =313.49/2

Valor promedio de servicio de Internet de 10 Mbps= $**156.75**

El resultado de la ecuación 1, es el valor promedio del servicio de internet de dos proveedores.

A continuación, en la **Figura 53** se aprecia la cotización de un enlace de datos ofertado por la Corporación Nacional de Telecomunicaciones CNT.

Figura 53

Costo de Enlaces Servicio de Datos CNT

Enlace Principal

Plan (Mbps)	Medio de transmisión	Inscripción	Tarifa mensual
0,256 Mbps	Cobre	$50,00	$36,00
0,512 Mbps	Cobre	$50,00	$47,00
1 Mbps	FO: PTP / GPON	$60,00	$125,00
2 Mbps	FO: PTP / GPON	$60,00	$148,00
3 Mbps	FO: PTP / GPON	$75,00	$166,00
4 Mbps	FO: PTP / GPON	$80,00	$185,00
5 Mbps	FO: PTP / GPON	$80,00	$199,00
6 Mbps	FO: PTP / GPON	$115,00	$206,50
7 Mbps	FO: PTP / GPON	$115,00	$214,25
8 Mbps	FO: PTP / GPON	$115,00	$222,00
9 Mbps	FO: PTP / GPON	$115,00	$230,00
10 Mbps	FO: PTP / GPON	$115,00	$237,25

Nota. Fuente: Tomado de (Corporación Nacional de Telecomunicaciones, 2021)

Como referencia se tiene un enlace de Tv Cable de 512 Kbps, como se aprecia en la **Figura 54.**

Figura 54

Costo de servicio de datos Grupo TV Cable

Nota. Fuente: Tomado de (Grupo TVCABLE, 2012)

El proveedor como Telconet oferta un enlace de 10 Mbps de un canal dedicado capa 3 mpls de datos, como referencia a $250.00 dólares.

Se aplica la misma ecuación 1, para determinar un costo promedio de servicio de datos de 10 Mbps, con los proveedores de CNT y Telconet.

Ecuación 2:

$237.25 + $250 =487.25/2

Valor promedio de servicio de datos de 10 Mbps= $**243.63**

Con los valores obtenidos, es claramente visible que un canal de datos tiene un costo superior con relación a un servicio de Internet.

Para conocer el porcentaje que tiene un enlace de datos, se aplica la siguiente ecuación:

Ecuación 3:

Valor de servicio de internet promedio= $**156.75** equivale a "X-Desconoce**"**

Valor de servicio de datos promedio= **$243.63** equivale al 100%

Se Aplica regla de tres, para determinar el porcentaje que es superior el canal de datos.

Ecuación 4:

(156.75*100) /243.63 = 64.33%

Ecuación 5:

100% - 64.33% = 35.67 %

Con este valor determinamos que el canal de enlace de datos tiene un costo superior de **35,67%** sobre un enlace de enlace de internet.

Con los valores obtenidos de ambos servicios, el servicio de internet puede funcionar de forma exitosa con la solución propuesta, existiendo un valor menor de un 35.67% sobre los enlaces de dedicados de datos. Por lo que con DMVPN, se podría aplicar QoS para priorizar tráfico, y el servicio de internet podría ser una solución completa para gestionar diferentes tipos de tráfico.

CONCLUSIONES

- La prueba de concepto diseñada e implementada en el capítulo 3 y capítulo 4, se confirma que DMVPN en fase 3 es factible y funciona exitosamente como red privada y pública en IPv6, y con ello se observa el funcionamiento del protocolo NHRP entre Hub y los Spoke.
- El funcionamiento de mGRE, opera de forma exitosa en IPv6, pero para ello se debe contar con el equipamiento y plataforma correcta; es así como los enrutadores deben contar con el IOS adecuado para que puedan soportar mGRE en IPv6 nativo.
- mGRE sigue aportando ventajas para la configuración de DMVPN, esto se debe a que logra minimizar líneas de configuración entre el Hub y los Spoke y, aun así, seguir manteniendo la seguridad en el transporte de tráfico de red IPv6, mediante los perfiles de IPsec implementados.
- El protocolo de enrutamiento de vector distancia EIGRP en IPv6, se mantiene entre los más confiables protocolos dinámicos, debido a su mecanismo de sucesor factible, siendo así, garantiza un alto grado de confianza en la transmisión de datos.
- SD-WAN es una solución que cumple con un gran número de indicadores como es costo, seguridad, administración centralizada, gran escalabilidad, alto rendimiento; pensada y diseñada para los nuevos desafíos que presentan los administradores de red. El gran proceso de transformación digital obliga a una mejora continua de arquitecturas de red y aplicaciones de las redes WAN tradicional, convirtiendo a SD-WAN como el mejor protagonista para empresas que manejan principalmente aplicaciones sobre la nube digital.

RECOMENDACIONES

- DMVPN, al operar con mecanismos mGRE se debe tomar en consideración todas las observaciones con respecto al hardware y versión de IOS sobre el equipamiento Cisco.
- La prueba de concepto de DMVPN desarrollada, nos indica la forma de operar e integrarse NHRP, mGRE e IPsec en IPv6: pero se recomienda realizar un análisis de tráfico con equipos finales a nivel de usuarios reales para validar la calidad del servicio.
- El estudio para SD-WAN nos sirve como referencia para la elección de una elección de red de transporte empresarial, aunque es visible el gran aporte de redes definidas por software a las nuevas necesidades de comunicación e integración de servicios, pero cabe destacar que DMVPN sigue aportando grandes funcionalidades a la comunicación en ámbitos empresariales, que podría funcionar como un enlace alterno de forma exitosa. Por lo que se recomienda realizar un análisis previo para una migración de DMVPN hacia SD-WAN.
- SD-WAN, nace como una solución verdaderamente eficaz, permitiéndole integrarse con herramientas de seguridad y así poder trabajar en modelo abierto de interoperabilidad y colaboración, donde simplifique y automatice de forma significativa las operaciones y mejora de la experiencia de los administradores de red y de los usuarios; pero para migrar una red tradicional a esta nueva tecnología; se debe considerar y realizar un análisis previo con variables a considerar como costos, independización de tráfico, protección de aplicaciones y la principal, una WAN que realmente tenga una conexión con la nube; con ello se podría realmente determinar si es una solución ideal para el giro de negocio de ciertas empresas.

REFERENCIAS BIBLIOGRÁFICAS

Bahnasse, A., Louhab, F. E., Khiat, A., Badri, A., Talea, M., & Sahel, A. (2019). Dynamic Multipoint Virtual Private Network influence on Video Conferencing Quality of Service. *2nd International Conference on Computer Applications and Information Security, ICCAIS 2019*, 1–6. https://doi.org/10.1109/CAIS.2019.8769447

Cisco. (2011). *Cisco IOS IPv6 Configuration Guide*. *6387*. http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_4/ipv6_12_4_book.pdf

Cisco. (2014). Cisco Dynamic Multipoint VPN: Simple and Secure Branch-to-Branch Communications. *Cisco.Com*, 8. http://www.cisco.com/c/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/data_sheet_c78-468520.html

Cisco. (2016). *Conociendo Dynamic Multipoint VPN (DMVPN)*. https://community.cisco.com/t5/blogs-routing-y-switching/conociendo-dynamic-multipoint-vpn-dmvpn/ba-p/3101118

Cizmie, S., & Vukeliü, M. (2019). *Employee wellbeing int the digital age*. 100–102.

Corporación Nacional de Telecomunicaciones. (2021). *Soluciones de conectividad – datos - Datos Locales - CNT Empresas Ecuador*. https://empresas.cnt.com.ec/solucion/datos-locales

Corporativas, G. Tvc. » V. (2012). *Grupo TVCable » Ventas Corporativas*. https://www.grupotvcable.com/ventas-corporativas/

Fonseca, R. (2017). Universidad Politécnica Salesiana Sede Quito. *Tesis*, *6*, 1–100. http://dspace.ups.edu.ec/bitstream/123456789/5081/1/UPS-CYT00109.pdf

Garg, S. (2017). *A Study of Performance Analysis of Signaling Protocols in MPLS*.

Ghretli, M., & Almukhtar, A. (2019). *Implementation of Dynamic Multipoint VPN over Multiprotocol Label Switching Infrastructure*. *March*, 4–6.

Grupo TVCABLE. (2012). *Soluciones de conectividad – datos - Datos Locales - CNT Empresas Ecuador*. https://empresas.cnt.com.ec/solucion/datos-locales

Jaramillo Zamora, A. W. (2018). *Análisis comparativo entre VPN IPSEC y DMVPN (Dynamic Multipoint Virtual Private Network) para mejorar el desempeño de redes privadas sobre internet.* https://doi.org/UDCTIPEC;20T01119

Jose, S. (2014). *Dynamic Multipoint VPN Configuration Guide , Cisco IOS XE Release 3S*. *6387*.

Korhonen, V. (2019). *Ville Korhonen FUTURE AFTER OPENVPN AND IPSEC*. *August*.

Kouicem, D. E., Fajjari, I., & Aitsaadi, N. (2017). An enhanced Path Computation for Wide Area Networks based on Software Defined Networking. *Proceedings of the IM 2017 - 2017 IFIP/IEEE International Symposium on Integrated Network and Service Management*, 664–667. https://doi.org/10.23919/INM.2017.7987355

Lacnic. (2020). *Fases de Agotamiento de IPv4*. https://www.lacnic.net/1001/1/lacnic/fases-de-agotamiento-de-ipv4

Netlife. (2021). *Planes PYMES - Netlife*. https://www.netlife.ec/planes-pymes/#3

Patiño Sánchez, J. (2017). Análisis del direccionamiento IPv6 y estudio de los Protocolos de Enrutamiento orientados a IPv6. *Maskana*, *7*(Supl.), 221–226.

Radcliffe, D., Blue, J., & Ireland, N. (2019). *An SD - WAN Solution Assuring Business Quality VoIP Communication for Home Based Employees*.

RODRIGUEZ, C. A. R. (2011). *VPNS A TRAVÉS DEL PROTOCOLO IPSEC Y ADMINISTRACIÓN DE SEGURIDAD EN ROUTERS CISCO*.

Ruiz, M., Masache, P., & Dominguez, J. (2018). High availability network for critical communications on smart grids. *CEUR Workshop Proceedings*, *2178*(Ssn), 13–17.

Sarah Anand. (2020, January 21). *Anatomy Of GRE Tunnels - Packet Pushers*. https://packetpushers.net/anatomy-of-gre-tunnels/

Sd-wan, C. (2020). *Cisco SD-WAN*.

Seremet, I., & Causevic, S. (2019). Advancing IP/IMPLS with Software Defined Network in Wide Area Network. *2019 International Workshop on Fiber Optics in Access Networks, FOAN 2019*, 56–61. https://doi.org/10.1109/FOAN.2019.8933726

Villas, A. D. Las. (2019). *Combinación de mecanismos mpls en una arquitectura sdn*. *18*(1), 1–10.

Yang, Z., Cui, Y., Li, B., Liu, Y., & Xu, Y. (2019). Software-defined wide area network (SD-WAN): architecture, advances and opportunities. *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, *2019-July*. https://doi.org/10.1109/ICCCN.2019.8847124

ANEXOS

Anexo 1

crypto isakmp policy 100	Creación de la política de seguridad isakmp (Internet Security Association and Key Management Protocol). El ID es el mismo en todos los enrutadores.
encripta 3des	Algoritmo de cifrado Triple Data Encryption Standard (3DES)
authentication pre-share	Es clave secreta compartida.
group 2	Especifica el grupo Diffie-Hellman de 1024 bits.
crypto isakmp key eMi$0r3s address ipv6 ::/0	El tunnel local especifica la clave local compartida, y agrega la dirección del tunnel remoto.
crypto IPsec transform-set ipdmvpn esp-3des esp-md5-hmac	Define un conjunto de transformación, que es una combinación aceptable de protocolos y algoritmos de seguridad, y entra en el modo de configuración de transformación criptográfica.
tunnel transport	Mode transporte del túnel.
crypto IPsec profile ipdmvpn	Se define los parámetros de seguridad IP (IPsec) que se usarán para el cifrado IPsec entre dos enrutadores IPsec (HUB Y SPOKE)
set transform-set ipdmvpn	Especifica una lista de conjuntos de transformación en orden de prioridad.

Anexo 2

Configuración Políticas IKE

```
crypto isakmp policy 100
 encr 3des
 authentication pre-share
 group 2
```

Anexo 3

Configuración de Claves Precompartidas

```
crypto isakmp key eMi$0r3s address ipv6 ::/0
```

Anexo 4

Configuración IPSEC Transform-Set

```
crypto ipsec transform-set ipdmvpn esp-3des esp-md5-hmac
 mode tunnel
```

Anexo 5

Configuración IPSEC Profile

```
crypto ipsec profile ipdmvpn
 set transform-set ipdmvpn
```

Anexo 6

Configuración de IPSEC Profile HUB-QUITO

```
HUB-QUITO(config)#crypto isakmp policy 100
HUB-QUITO(config-isakmp)# encr 3des
HUB-QUITO(config-isakmp)# authentication pre-share
HUB-QUITO(config-isakmp)# group 2
HUB-QUITO(config-isakmp)#crypto isakmp key eMi$0r3s address ipv6 ::/0
A pre-shared key for address ::/0 already exists!

HUB-QUITO(config)#!
HUB-QUITO(config)#!
HUB-QUITO(config)#crypto ipsec transform-set ipdmvpn esp-3des esp-md5-hmac
HUB-QUITO(cfg-crypto-trans)# mode tunnel
HUB-QUITO(cfg-crypto-trans)#!
HUB-QUITO(cfg-crypto-trans)#!
HUB-QUITO(cfg-crypto-trans)#crypto ipsec profile ipdmvpn
HUB-QUITO(ipsec-profile)# set transform-set ipdmvpn
HUB-QUITO(ipsec-profile)#
```

Anexo 7

Configuración de IPSEC Profile SPOKE-GUAYAQUIL

```
SPOKE-GUAYAQUIL#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SPOKE-GUAYAQUIL(config)#crypto isakmp policy 100
SPOKE-GUAYAQUIL(config-isakmp)# encr 3des
SPOKE-GUAYAQUIL(config-isakmp)# authentication pre-share
SPOKE-GUAYAQUIL(config-isakmp)# group 2
SPOKE-GUAYAQUIL(config-isakmp)#crypto isakmp key eMi$0r3s address ipv6 ::/0
A pre-shared key for address ::/0 already exists!

SPOKE-GUAYAQUIL(config)#!
SPOKE-GUAYAQUIL(config)#!
SPOKE-GUAYAQUIL(config)#crypto ipsec transform-set ipdmvpn esp-3des esp-md5-hmac
SPOKE-GUAYAQUIL(cfg-crypto-trans)# mode tunnel
SPOKE-GUAYAQUIL(cfg-crypto-trans)#!
SPOKE-GUAYAQUIL(cfg-crypto-trans)#!
SPOKE-GUAYAQUIL(cfg-crypto-trans)#crypto ipsec profile ipdmvpn
SPOKE-GUAYAQUIL(ipsec-profile)# set transform-set ipdmvpn
SPOKE-GUAYAQUIL(ipsec-profile)#
```

Anexo 8

Configuración de IPSEC Profile SPOKE-CUENCA

```
SPOKE-CUENCA(config)#crypto isakmp policy 100
SPOKE-CUENCA(config-isakmp)# encr 3des
SPOKE-CUENCA(config-isakmp)# authentication pre-share
SPOKE-CUENCA(config-isakmp)# group 2
SPOKE-CUENCA(config-isakmp)#crypto isakmp key eMi$0r3s address ipv6 ::/0
A pre-shared key for address ::/0 already exists!

SPOKE-CUENCA(config)#!
SPOKE-CUENCA(config)#!
SPOKE-CUENCA(config)#crypto ipsec transform-set ipdmvpn esp-3des esp-md5-hmac
SPOKE-CUENCA(cfg-crypto-trans)# mode tunnel
SPOKE-CUENCA(cfg-crypto-trans)#!
SPOKE-CUENCA(cfg-crypto-trans)#!
SPOKE-CUENCA(cfg-crypto-trans)#crypto ipsec profile ipdmvpn
SPOKE-CUENCA(ipsec-profile)# set transform-set ipdmvpn
SPOKE-CUENCA(ipsec-profile)#
```

Anexo 9

Pasos configuración Interfaz WAN

Router> enable	Habilita el modo EXEC privilegiado.
Router# configure terminal	Ingrese en modo de configuración global
Router(config)#interface fastethernet 4	Ingrese a la interfaz Wan (fa4)
Router(config)#interface4 **ipv6 address** {*ipv6-address* **/** *prefix-length* | *prefix-name sub-bits* **/** *prefix-length*	Configura una dirección IPv6 basada en un prefijo general IPv6
Router(config)#interface4 **ipv6 address enable**	Habilite la dirección IPv6

Anexo 10

Configuración Interfaz WAN HUB-QUITO

```
HUB-QUITO#show run int fa4 | i ipv6
 ipv6 address FD00:2112:2018::2/64
 ipv6 enable
HUB-QUITO#
```

Anexo 11

Configuración Interfaz WAN SPOKE-GUAYAQUIL

```
SPOKE-GUAYAQUIL#show run int fa4 | i ipv6
 ipv6 address FD00:2112:2018::3/64
 ipv6 enable
SPOKE-GUAYAQUIL#
```

Anexo 12

Configuración Interfaz WAN SPOKE-CUENCA

```
SPOKE-CUENCA#show run int fa4 | i ipv6
 ipv6 address FD00:2112:2018::4/64
 ipv6 enable
SPOKE-CUENCA#
```

Anexo 13

Pasos configuración IP Overlays Tunnel

Router> enable	Habilita el modo EXEC privilegiado.
Router# configure terminal	Ingrese en modo de configuración global
interface tunnel *number*	Configura una interfaz de túnel e 100
ipv6 address {*ipv6-address* **/** *prefix-length* | *prefix-name* *sub-bits* **/** *prefix-length*	Configura una dirección IPv6 basada en un prefijo general IPv6
Router(config)#interface4 **ipv6 address enable**	Habilite la dirección IPv6

Anexo 14

Configuración IP Overlays Tunnel HUB-QUITO

```
HUB-QUITO#show run interface tunnel 100 |  i 2800
 ipv6 address 2800:16:30:1::1/64
HUB-QUITO#
```

Anexo 15

Configuración IP Overlays Tunnel SPOKE-GUAYAQUIL

```
SPOKE-GUAYAQUIL#show run interface tunnel 100 |  i 2800:16:30:1::2
 ipv6 address 2800:16:30:1::2/64
SPOKE-GUAYAQUIL#
```

Anexo 16

Configuración IP Overlays Tunnel SPOKE-CUENCA

```
SPOKE-CUENCA#show run int tunnel 100 | i 2800:16:30:1::3
 ipv6 address 2800:16:30:1::3/64
SPOKE-CUENCA#
```

Anexo 17

Pasos para configurar EIGRP IPV6

Router> enable	Habilita el modo EXEC privilegiado.
Router# configure terminal	Ingrese en modo de configuración global
Router (config)# ipv6 unicast-routing Enables	Habilita el reenvío de datagramas de unidifusión IPv6
Router (config)# ipv6 router eigrp as-number	Ingresa al modo de configuración del enrutador y crea un proceso de enrutamiento EIGRP IPv6.
Router (config)# router-id ip-address	Habilita el uso de una ID de enrutador fija.
Router(config)# interface loopback #	Especifica un tipo y número de interfaz
Router(config-if)# ipv6 address {ipv6-address/prefix-length | prefix-name sub-bits / prefix-length	Configura una dirección IPv6 basada en un prefijo general IPv6
Router(config-if)# ipv6 eigrp ID	Habilite EIGRP ipv6 sobre la interfaz loopback
Router(config-if)# no shut	Habilite la interfaz

Anexo 18

Configuración EIGRP/Loopback 2 (LAN CLIENTE) HUB-QUITO

```
ipv6 router eigrp 1
 eigrp router-id 2.2.2.2
HUB-QUITO#
interface Loopback2
 no ip address
 ipv6 address 2800:16:10:1::1/64
 ipv6 enable
 ipv6 eigrp 1
```

Anexo 19

Configuración EIGRP/Loopback 2 (LAN CLIENTE) SPOKE-GUAYAQUIL

.

Anexo 20

Configuración EIGRP/Loopback 2 (LAN CLIENTE) SPOKE-CUENCA

Anexo 21

Pasos para configurar DMVPN HUB

Configure terminal	Ingreso en modo de configuración global
ipv6 address FE80::1 link-local	Configuración del a IP link -local
ipv6 address 2800:16:30:1::1/64	Configuración de la IP Overlays
ipv6 eigrp 1	Se habilita EIGRP en el túnel DMVPN
no ipv6 split-horizon eigrp 1	Desactiva el horizonte dividido en la interfaz del túnel mGRE; de lo contrario, EIGRP no anunciará las rutas que se aprenden a través de la interfaz mGRE vuelven a salir de esa interfaz.
ipv6 nhrp map multicast dynamic	Permite el uso de un protocolo de enrutamiento dinámico entre SPOKE y HUB, y envía paquetes de multidifusión al concentrador enrutador.
ipv6 nhrp network-id 10	Habilita NHRP en una interfaz. El ID specifica un único identificador global de red de 32 bits. El rango es de 1 al 4294967295.
ipv6 nhrp redirect	Habilita el reenvío NHRP.
tunnel source FD00:2112:2018::2	Establece la dirección de origen para una interfaz de túnel.
tunnel mode gre multipoint ipv6	Esablece el modo de encapsulación en mGRE para la interfaz túnel en IPV6

Anexo 22

Configuración DMVPN HUB-QUITO

```
interface Tunnel100
 no ip address
 ipv6 address FE80::1 link-local
 ipv6 address 2800:16:30:1::1/64
 ipv6 eigrp 1
 no ipv6 split-horizon eigrp 1
 ipv6 nhrp map multicast dynamic
 ipv6 nhrp network-id 10
 ipv6 nhrp redirect
 tunnel source FD00:2112:2018::2
 tunnel mode gre multipoint ipv6
 tunnel protection ipsec profile ipdmvpn
end

HUB-QUITO#
```

Anexo 23

Pasos para configurar DMVPN SPOKE

Configure terminal	Ingreso en modo de configuración global
ipv6 address FE80::2 link-local	Configuración del a IP link -local
ipv6 address 2800:16:30:1::2/64	Configuración de la IP Overlays
ipv6 eigrp 1	Se habilita EIGRP en el túnel DMVPN
ipv6 nhrp map multicast FD00:2112:2018::2	Permite el uso de un protocolo de enrutamiento dinámico entre SPOKE y HUB, y envía paquetes de multidifusión al concentrador enrutador.
ipv6 nhrp map FE80::1/128 FD00:2112:2018::2	Configura estáticamente la asignación de direcciones IPv6 a NBMA de destinos IPv6 conectados a una red NBMA

ipv6 nhrp nhs 2800:16:30:1::1 **nbma** FD00:2112:2018::2	Especifica la dirección de uno o más servidores IPv6 NHRP.
ipv6 nhrp network-id 10	Habilita NHRP en una interfaz. El ID specifica un único identificador global de red de 32 bits. El rango es de 1 al 4294967295.
ipv6 nhrp shortcut	Activa la comunicación de acceso directo entre los Spoke
tunnel source FD00:2112:2018::3	Establece la dirección de origen para una interfaz de túnel
tunnel mode gre multipoint ipv6	Establece el modo de encapsulación en mGRE para la interfaz túnel. IPV6

Anexo 24

Configuración DMVPN SPOKE-GUAYAQUIL

```
interface Tunnel100
 no ip address
 ipv6 address FE80::2 link-local
 ipv6 address 2800:16:30:1::2/64
 ipv6 eigrp 1
 ipv6 nhrp map multicast FD00:2112:2018::2
 ipv6 nhrp map FE80::1/128 FD00:2112:2018::2
 ipv6 nhrp network-id 10
 ipv6 nhrp nhs 2800:16:30:1::1 nbma FD00:2112:2018::2
 ipv6 nhrp shortcut
 tunnel source FD00:2112:2018::3
 tunnel mode gre multipoint ipv6
 tunnel protection ipsec profile ipdmvpn
end

SPOKE-GUAYAQUIL#
```

Anexo 25

Configuración DMVPN SPOKE-CUENCA

```
SPOKE-CUENCA#show run interface tunnel 100
Building configuration...

Current configuration : 416 bytes
!
interface Tunnel100
 no ip address
 ipv6 address FE80::3 link-local
 ipv6 address 2800:16:30:1::3/64
 ipv6 eigrp 1
 ipv6 nhrp map multicast FD00:2112:2018::2
 ipv6 nhrp map FE80::1/128 FD00:2112:2018::2
 ipv6 nhrp network-id 10
 ipv6 nhrp nhs 2800:16:30:1::1 nbma FD00:2112:2018::2
 ipv6 nhrp shortcut
 tunnel source FD00:2112:2018::4
 tunnel mode gre multipoint ipv6
 tunnel protection ipsec profile ipdmvpn
end

SPOKE-CUENCA#
```