UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:
INGENIERÍA ELECTRÓNICA

Trabajo de titulación previo a la obtención del título de:
INGENIERA ELECTRÓNICA E INGENIERO ELECTRÓNICO

TEMA:
DISEÑO DE UNA RED DMVPN SOBRE PROTOCOLO DE INTERNET VERSIÓN 6 (IPV6) PARA LA UNIVERSIDAD POLITÉCNICA SALESIANA

AUTORES:
VERÓNICA RAQUEL ORTIZ PALOMINO
DENNIS OMAR LÓPEZ CADENA

TUTOR:
JUAN CARLOS DOMÍNGUEZ AYALA

Quito, julio del 2019

CESIÓN DE DERECHOS DE AUTOR

Nosotros, Ortiz Palomino Verónica Raquel con documento de identificación N°171320637-1 y López Cadena Dennis Omar con documento de identificación N°171794533-9, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación: "DISEÑO DE UNA RED DMVPN SOBRE PROTOCOLO DE INTERNET VERSIÓN 6 (IPV6) PARA LA UNIVERSIDAD POLITÉCNICA SALESIANA", mismo que ha sido desarrollado para optar por el título de Ingeniera Electrónica e Ingeniero Electrónico, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribimos este documento en el momento que hacemos entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

Verónica Raquel Ortiz Palomino
CI:171320637-1

Dennis Omar López Cadena
CI:171794533-9

Quito, julio del 2019

DECLARATORIA DE COUATORIA DEL DOCENTE TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el Proyecto Técnico: "DISEÑO DE UNA RED DMVPN SOBRE PROTOCOLO DE INTERNET VERSIÓN 6 (IPV6) PARA LA UNIVERSIDAD POLITÉCNICA SALESIANA", realizado por Ortiz Palomino Verónica Raquel y López Cadena Dennis Omar, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerado como trabajo final de titulación.

Quito, julio del 2019

Juan Carlos Domínguez Ayala

CI: 1713195590

AGRADECIMIENTOS

A Dios, principalmente, por permitirme culminar este proyecto. Gracias por darme la fuerza y el coraje para poder hacer este sueño realidad.

A mis padres por haber confiado en mí y apoyarme, incondicionalmente, cada paso que he dado, y por ser una inspiración para seguir adelante.

Un agradecimiento especial para el Ingeniero Juan Carlos Domínguez Ayala, MSc. por su ayuda y guía para el desarrollo de este trabajo.

Verónica

Quiero expresar mi gratitud a Dios, quien con su bendición ha llenado mi vida, dándome la perseverancia para lograr culminar esta meta.

Agradecer a mi familia por estar siempre presentes en mis logros brindándome su apoyo y comprensión.

A la Universidad Politécnica Salesiana por haberme brindado la oportunidad del conocimiento durante todo este proceso.

Dennis

DEDICATORIAS

A mi hijo Damián que a pesar de no estar a mi lado ha sido mi guía, mi inspiración, mi fuerza día con día; y que a pesar de las adversidades fue el motor para la culminación de este trabajo.

A mis padres porque sin su apoyo y esfuerzo no hubiese podido culminar este meta propuesta… Gracias a su ejemplo y consejos.

Verónica

A mis padres Jorge y Mariana quienes con su paciencia, apoyo y esfuerzo me han permitido culminar este sueño enseñándome lo que es la perseverancia y la constancia, con su ejemplo.

A mi hijo Damián quien con su llegada me enseñó el sueño de una vida mejor, a pesar de su pronta partida, no lo hubiera logrado. Las promesas que estuvieron presentes entre los dos fueron las que me impulsaron a la culminación de este sueño.

A mis hermanos que con sus palabras y apoyo me hicieron sentir orgulloso de todo mi esfuerzo y de lo que soy.

Dennis

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

En el presente proyecto de Titulación se desarrolló debido la necesidad de tener un servicio de interconexión de dos o más sedes de la Universidad Politécnica Salesiana ubicadas en lugares geográficamente distintos, si este tipo de interconexiones fuesen echas por cableado se requeriría mayor inversión tanto en recursos humanos, infraestructura y financiamiento, ya que se consideran distancias muy extensas. Tomando en cuenta que la Universidad Politécnica Salesiana pretende su expansión territorial a largo plazo, las conexiones alámbricas en su totalidad se considerarían no favorables para la institución. El objetivo del diseño de una red piloto DMVPN SOBRE IPV6 para la Universidad Politécnica Salesiana el cual fue simulado en el software GNS3 que permitirá cargar los IOS en los routers reales cisco, el cual permitirá construir la topología con todos los dispositivos que se van a emplear para el diseño de la red piloto a futuro teniendo como objetivo fundamental complementar la red existente sobre IPV4 hacia la Confidencialidad, Integridad, Autenticación y Anti-Repudio que son factores necesarios para el buen funcionamiento para integrar a nuevas tendencias, características e implementación de nuevas sedes o instalaciones. El diseño de la red implementada en el software mencionado demostró que la red piloto DMVPN es factible y dispone de recursos necesarios para la conectividad entre sedes a larga o corta distancia y posee los requerimientos necesarios para transmitir información ya sea pública o privada

ABSTRACT

In the present project of Titling was developed due to the need to have an interconnection service of two or more offices of the Universidad Politécnica Salesiana located in geographically different places, if this type of interconnections were made by cabling it would require more investment in human resources , infrastructure and financing, since they are considered very long distances. Taking into account that the Salesian Polytechnic University intends its territorial expansion in the long term, the wired connections in their entirety would be considered unfavorable for the institution. The aim of the design of a pilot network DMVPN ON IPV6 for the Polytechnic University Salesiana which was simulated in the GNS3 software that will allow to load the IOS in the real routers cisco, which will allow to build the topology with all the devices that are going to be used for the design of the pilot network in the future with the fundamental objective of complementing the existing network over IPV4 towards Confidentiality, Integrity, Authentication and Anti-Repudiation, which are necessary factors for the proper functioning to integrate new trends, features and implementation of new venues or facilities. The design of the network implemented in the aforementioned software showed that the DMVPN pilot network is feasible and has the necessary resources for connectivity between long and short distance centers and has the necessary requirements to transmit information, whether public or private.

INTRODUCCIÓN

Con la constante evolución de las telecomunicaciones se han ido creando entornos para muchas aplicaciones empresariales, La necesidad de acceso remoto a la infraestructura de una organización se las puede realizar a través de VPN. Esta solución se basa en ubicaciones fijas, aquí los usuarios pueden crear enlaces privados para tener acceso a los recursos de una organización. Una limitante importante para las conexiones VPN clásicas son el número de conexiones al aumentar la demanda, así como la administración de las conexiones existente. Una solución a este problema es el DMVPN (protocolo dinámico multipunto VPN). La arquitectura que ofrece DMVPN está basado en la implementación de redes de tipo *Hub* y también *spoke.*

La ventaja principal de la implementación de DMVPN es que crea enlaces privados entre las diferentes estaciones remotas según los requerimientos de cada una de ellas, pero no *enruta* todo el tráfico en el concentrador. El protocolo propuesto consta de tres fases que son posibles en la implementación. La primera consta de la comunicación entre el *hub* y la estación remota. La segunda consta de un túnel entre estaciones remotas. La tercera consta de un túnel entre estaciones remotas, pero con las características mejoradas. DMVPN es un protocolo que construye GRE, el cual es escalable sobre los sitios IPSEC a túneles en los diferentes sitios. Esto es una característica muy importante porque dentro del DMVPN se puede ejecutar protocolos de enrutamiento dinámico como lo son OPSF (Primero abre la ruta más corta), BGP (Protocolo de puerta de enlace de frontera) y EIGRP (Protocolo de enrutamiento de puerta de enlace mejorada).

Es por lo que existe la necesidad de actualizar las redes de comunicación de la Universidad Politécnica Salesiana (UPS), puesto que posee diferentes requerimientos, con la infraestructura que posee actualmente. Pero esto es una oportunidad para la mejora de estos, contribuyendo de esta forma al servicio de la comunidad educativa de las diferentes sedes de la UPS.

CAPÍTULO 1

1.1 Antecedentes del problema de estudio

La UPS consta de varias sedes a nivel nacional y en algunas provincias. En Quito posee 3 campus, el Campus Kennedy (Rafael Bustamante), el Campus Sur (Rumichaca y Moran Valverde), el Campus El Girón (Católica N 23-52 y Madrid).

En los últimos años los campus que conforman la Sede de Quito han solicitado la mejora en cuanto a las comunicaciones usadas. Esto implica una mejora en la tecnología que posee la UPS. Todas las peticiones han sido tratadas y tomadas en cuenta dentro del plan de mejora institucional que posee la UPS. Una de las principales razones para la mejora de la infraestructura tecnológica es por las exigencias de la SENESCYT (Secretaria de Educación Superior, ciencia, tecnología e innovación). Las exigencias de esta entidad las Instituciones de educación superior deben tener a su servicio una infraestructura tecnológica con alta funcionalidad.

Se identifica posibles soluciones y se asigna prioridades a cada una de ellas, de esto se encarga las Dirección técnica de tecnologías de la información, la misma que funciona en la sede Quito. Con la medida tomada anteriormente de migrar de un protocolo IPV4 a un protocolo IPV6. Se abren nuevas soluciones y prioridades, que consiste en un plan para el diseño de una red DMVPN que se basara en el protocolo IPV6 implementado anteriormente para aprovechar todas las ventajas que nos ofrece la implementación de este.

1.2 Justificación (importancia y alcances)

El presente proyecto técnico se desarrolla debido a la necesidad de mantener interconectadas varias sedes de la Universidad Politécnica Salesiana, por dicha razón se busca una nueva solución que se encuentre enfocado a introducir una nueva forma de estructurar las redes de comunicación, mediante el desarrollo del diseño que integra varias tecnologías de despliegues rápidos como el multipunto dinámico a través de túneles de conexión privada entre Routers lejanos para IPv6(Protocolo de internet versión 6), que transmiten la información a través de internet, encapsulando los datos en un protocolo llamado GRE(Encapsulación de enrutamiento genérico) e *IPSec* (Protocolo de seguridad de internet), ayudando al crecimiento progresivo de dicha

institución. El desarrollo de este proyecto podrá asegurar el funcionamiento de forma eficiente de una red DMVPN (multipunto dinámico VPN) para IPV6. Para asegurar que la información enviada se encuentre segura de cualquier tipo de ataque en la red de internet, DMVPN mantiene una conexión de forma mallada al interconectar las diferentes sedes de la institución permitiendo la utilización de forma segura de la red pública.

El presente proyecto técnico será dirigido para la población de la Universidad Politécnica Salesiana como son docentes, estudiantes, personal administrativo y/o de Apoyo.

1.3 Objetivos

1.1.3 Objetivo general

Diseñar una Red para DMVPN sobre IPv6 utilizando el protocolo OSFP para la Universidad Politécnica Salesiana y sus diferentes sedes.

1.2.3 Objetivos específicos

- Determinar los requerimientos del software a ser utilizado y técnicas necesarias para que los modelos de equipos que van a ser utilizados en la simulación sean identificados.

- Establecer el modelo transición heredable que va a complementar la red existente sobre IPv4 para integrarse a nuevas tendencias, características, instalaciones de la Universidad Politécnica Salesiana.

- Simular la red DMVPN en OSPF sobre IPv6 a partir del diseño que ya se encuentra establecida dentro de la Universidad Politécnica Salesiana sobre IPv4, para que sea complementada en su funcionamiento y desarrollo.

- Verificar el correcto funcionamiento de la DMVPN en OSPF sobre IPv6 para que se logre la interconexión de todas las sucursales y transmitir información de forma rápida, eficiente y segura.

1.4 Formulación del problema

El principal problema que se detectó para la realización del presente proyecto en la Universidad Politécnica Salesiana es que en el futuro se tendrá problemas de conexión entre sedes ya que el pool de direcciones de IPv4 cada vez resultan más escasas para la conectividad, la necesidad de un modelo que permita la transición suave a IPV6 donde la red sea escalable es decir la integración de nuevas sedes o el uso de la misma desde puntos remotos por usuarios de la universidad, que la red sea tolerante a fallos permitiendo que las interconexiones no establecidas se puedan mantener con una conexión a través de la creación de túneles privados y tenga seguridad en la entrega de información, dicha red tiene como requisito soportar el aumento en el volumen de transmisión de datos manteniéndose lista para las nuevas instalaciones en el crecimiento de la universidad, con la mejora de la red DMVPN existente en la universidad sobre ipv4 e introduciendo el concepto IPv6 se tendrá un pool de direcciones que va a permitir la conectividad a futuro cuando la comunidad de la Universidad Politécnica Salesiana vaya en aumento teniendo en cuenta que en el mundo, la tecnología está tomado tanta importancia para los usuarios y la necesidad de estos para mantenerse conectados a la red sin importar la ubicación geográfica, ya sea dicha red pública o privada, poniendo a prueba nuevas tecnologías que faciliten el desarrollo de redes futuras como la implementación de redes virtuales multipunto para interconectar varias sedes entre si desde cualquier punto sobre el Protocolo IPv6.

En las redes de última tecnología para mantener una administración total de las redes se debe tener convergencia, control de los dispositivos electrónicos y mantenerlos comunicados entre sí, procurando seguridad y escalabilidad. Para satisfacer estas necesidades se hace necesaria la realización de este proyecto dando una solución diferente a las que ofrece las VPNs tradicionales enfocándolas a la utilización del protocolo IPv6 dando soporte para redes futuras.

El problema se origina en la necesidad de tener un servicio de interconexión de dos o más sedes de la Universidad Politécnica Salesiana ubicadas en lugares geográficamente distintos, si este tipo de interconexiones fuesen echas por cableado se requeriría mayor inversión tanto en recursos humanos, infraestructura y financiamiento, ya que se consideran distancias muy extensas. Tomando en cuenta que

la Universidad Politécnica Salesiana pretende su expansión territorial a largo plazo, las conexiones alámbricas en su totalidad se considerarían no favorables para la institución.

Como solución alternativa para las interconexiones entre las sedes de la Universidad Politécnica Salesiana aparecen las VPNs que permiten entablar conexiones utilizando la red pública o Internet, en relación con los enlaces dedicados tiene un costo menor.

Las redes privadas virtuales (VPN) permiten tener una extensión de la red LAN, he incluso a usuarios remotos ya sea ésta la necesidad de las sedes de la universidad, lógicamente se tiene una sola red que utiliza como medio de transmisión la red de Internet, por tanto la inserción a las redes privadas virtuales multipunto dinámicas (DMVPNs) presentadas en este proyecto son una versión más completa de las VPNs tradicionales, resolviendo las falencias que estas últimas mantienen y añaden características importantes a la hora de decidir la forma de transmitir información en una red haciendo que la transmisión de datos mantenga la seguridad y confiabilidad esperada.

Las DMVPN sobre IPv6 que se desea diseñar para la Universidad no puede ser concebida sin seguridad en la transmisión de información, por lo que, dentro de la DMVPN, IPSec es parte fundamental de esta forma de conexión, ya que permite dar a la red Confidencialidad, Integridad, Autenticación y Anti-repudio (CIA), factores que son necesarios para su buen funcionamiento.

Las DMVPN sobre IPv6 soporta QoS al utilizar políticas para el desempeño dinámico donde las plantillas de QoS se unen automáticamente a los túneles que vayan surgiendo entre las conexiones de las diferentes sedes de la universidad.

La alta disponibilidad de servicios depende mucho de los equipos Cisco utilizados para la implementación de la red DMVPN sobre IPv6 que permite el enrutamiento basado en conmutación por error.
La escalabilidad que provee la DMVPN sobre IPv6 necesaria para la universidad se basa en el despliegue de *hubs* jerárquicos gracias a los túneles que se forman en las

interconexiones, equilibran la carga sobre los HUB disponibles permitiendo la creación de nuevas conexiones.

La red DMVPN sobre IPv6 diseñada para la Universidad Politécnica Salesiana es una excelente opción al momento de escoger una forma segura y escalable de transmitir información entre sitios a larga distancia.

CAPÍTULO 2

2.1 Multipunto Dinámico VPN

La llamada función Dinámica multipunto VPN(DMVPN) permite una mejora substancial a gran escala de redes privadas virtuales (VPN) con seguridad IP (Ipsec), tanto como de grandes como pequeñas magnitudes, se logra mediante la combinación de túneles de encapsulación de enrutamiento genérico (GRE), cifrado IPsec y el protocolo de resolución de salto próximo (NHRP).

La DMVPN proporciona varios beneficios a los administradores de red, entre los cuales se destacan:

- **Aprovisionamiento de fácil aprovisionamiento:** Los concentradores de los DMVPN no requiere configuraciones extras cuando se agregan spoke adicionales. Los spoke de DMVPN pueden ser configurados como túnel con plantilla.

- **Escalabilidad:** El estado permanente mínimo de los spoke enrutadores permite una escalabilidad masiva. La escala de la red no está limitada por el dispositivo (físico, virtual, o lógico).

- **Túnel de spoke-spoke:** DMVPN proporciona conectividad de malla completa al configurar el túnel inicial hacía el spoke y hacia el concentrador. Los túneles de spoke-spoke se crean según sea necesario y desaparecen cuando ya no son necesarios. No existe perdidas del paquete mientras se construye el túnel dinámico hacia el spoke, una vez que se establecen los túneles iniciales de un spoke hacia un concentrador. Uno de los spoke mantiene el reenvió hacia los demás spoke con los que está conectado.

- **Topologías de red flexibles:** la operación de DMVPN no realiza suposiciones sobre la topología de superposición del plano de control o del plano de datos. El plano de control de DMVPN puede usar un modelo distribuido y resistente que permite una gran escala masiva y evita puntos de falla o congestión. En el

otro extremo se puede emplear otro modelo centralizado para obtener un único punto de control.

- **Soporte multiprotocolo:** DMVPN es compatible con IPV4, IPV6 y MPLS como protocolo de red de superposición de transporte.

- **Compatibilidad de multidifusión:** DMVPN permite que el tráfico de multidifusión fluya en las interfaces del túnel.

- **Conectividad adaptable:** los enrutadores DMVPN pueden establecer conectividad NAT. Los enrutadores de los spoke pueden usar direcciones IP dinámicas, como el Protocolo de configuración dinámica de host (DHCP).

- **Bloques de construcción estandarizados:** DMVPN usa tecnologías que están estandarizadas en la industria como NHRP, GRE e IPsec, para construir una red de superposición. Esto propaga la familiaridad y al mismo tiempo, minimiza los tiempos de aprendizaje, además que facilita la resolución de problemas.

2.2 Túnel de encapsulación de enrutamiento genérico (GRE)

Un GRE proporciona una conectividad a una amplia variedad de protocolos de capa de red, esto lo hace al encapsular y reenviar los paquetes a través de una red basada en la IP. El uso original que se le dio a los GRE fue el de proporcionar un mecanismo de transporte para protocolos heredados no enrutables como DECnet, Systems Network Architecture (SNA) o IPX. Además, los túneles GRE se han usado como una solución rápida, para el diseño de enrutamientos correctos o como un método para pasar el tráfico a través de un firewall o ACL. DMPVN usa la encapsulación GRE multipunto y admite protocolos de enrutamiento dinámico, esto elimina mucho de los problemas de soporte asociados con otras tecnologías de VPN. Los GRE se clasifican como una red superpuesta porque el túnel GRE se construye sobre una red de transporte existente.

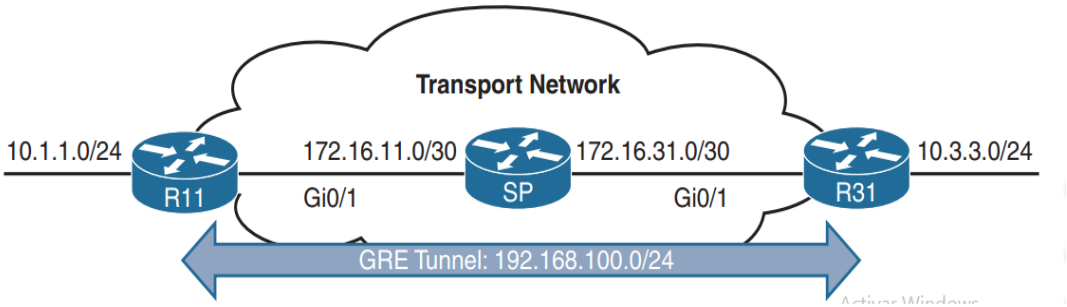
La información adicional del encabezado se agrega al paquete cuando el enrutador encapsula el paquete para el túnel GRE. La nueva información consta de nueva

información como la dirección IP del punto final remoto como destino. Los nuevos encabezados IP permiten que el paquete se enrute entre los dos puntos finales del túnel sin inspeccionar la carga útil del paquete. Una vez que el paquete llega al punto final remoto, se eliminan los encabezados GRE y el paquete original se reenvía fuera del enrutador remoto.

A continuación, se describe el proceso para la configuración de un túnel GRE.

2.1.2 Configuración de túnel GRE

Figura2. 1. Topología de túnel GRE (Guide, 2017)



En la Figura2.1 se ilustra la configuración de un túnel GRE, El rango de red es 172.16.0.0/16 corresponde a la red de transporte subyacente y 192.168.100.0/24 se utiliza para el túnel GRE, es decir la red de superposición.
Para configurar el túnel GRE se siguen los siguientes pasos.

- **Paso 1 Crear la interface del túnel:**

Crea la interface del túnel con el número del túnel de la interfaz del comando de la configuración global.

- **Paso 2 Identificar la fuente del túnel:**

Identificación local del túnel con el comando de parámetro de interfaz fuente de túnel {dirección IP| ID de interfaz}. La interfaz de origen del túnel indica la interfaz que se utiliza para la encapsulación y la des encapsulación del túnel GRE. La fuente del túnel puede ser una interfaz física o una interfaz de bucle retorno. Una interfaz de bucle invertido puede proporcionar accesibilidad si una de las interfaces de transporte fallara.

2.3.2.1 Paso 3 Identifique la dirección IP de destino remoto:

Identifique el destino del túnel con la dirección IP del destino del túnel del comando del parámetro de la interfaz. El destino del túnel es la dirección IP subyacente del enrutador remoto hacia la cual el enrutador local envía paquetes GRE.

- **Paso 4 Asigne una dirección IP a la interfaz del túnel:**

Se asigna una dirección IP a la interfaz con el comando *ip address ip-address subred-mask.*

- **Paso 5 Definir el ancho de banda del túnel (opcional):**

Las interfaces virtuales no tienen el concepto de latencia, por ello necesitan tener configurado un ancho de banda de referencia para que los protocolos de enrutamiento que usan el ancho de banda, para el cálculo de la mejor ruta puedan toman una decisión inteligente. El ancho de banda también se utiliza para la configuración de *QoS* en la interfaz. El ancho de banda se define con el parámetro de interfaz, comando ancho de banda [1 -1000000], que se mide en *kbits* por segundo.

- **Paso 6 Especifique un túnel GRE keepalive (opcional):**

Las interfaces de túnel son GRE punto a punto (P2P) de manera predeterminada, y el protocolo de la línea entra en estado activo cuando el enrutador detecta que existe unan ruta hacia el destino del túnel en la tabla de enrutamiento. Si el destino del túnel no está en la tabla de enrutamiento, la interfaz del túnel (protocolo de línea) entra en un estado inactivo. Los *keepalive* del túnel aseguran que exista una comunicación bidireccional entre los puntos finales del túnel para mantener el protocolo de enrutamiento, para detectar un punto final remoto muerto. Los *keepalive* se configuran con el comando de parámetros de la interfaz *keepalive* [segundos | reintentos]. El temporizador predeterminado es de 10 segundos y tres reintentos.

- **Paso 7 Definir la unidad de transmisión máxima (MTU) de IP para la interfaz de túnel (opcional):**

El túnel agrega un mínimo de 24 bytes al tamaño del paquete para acomodar los encabezados que se agregan al paquete. Al especificar la MTU de IP en la interfaz del túnel, el enrutador realiza la fragmentación antes de que el host tenga que detectar y

especificar la MTU del paquete. IP MTU se configura con el comando de parámetros de la interfaz *ip mtu*.

A continuación, en la tabla 1 se muestra la cantidad de sobrecarga de encapsulación para varias técnicas de túnel. El tamaño del encabezado puede cambiar en función de las opciones de configuración utilizadas.

Tabla2.1. Encapsulación general para túneles

Tipo de túnel	Tamaño de la cabecera del túnel
GRE sin IPsec	24 bytes
DES/3DES Ipsec (modo de transporte)	18-25 bytes
DES/3DES Ipsec (modo túnel)	38-45 bytes
GRE/DMVPN+DES/3DES	42-49 bytes
GRE/DMVPN+AES+SHA-1	62-77bytes

Elaborado por: Verónica Ortiz y Dennis López

2.2.2 Protocolo de resolución del próximo salto (NHRP)

El protocolo de resolución de próximo salto NHRP se define en RFC 2332 como un método para proporcionar resolución de direcciones para hosts o redes (capacidad similar ARP) para redes de acceso múltiple sin transmisión (NBMA) *como Frame Relay y ATM. NHRP* proporciona un método para que los dispositivos aprendan el protocolo y la red *NBMA*, lo que les permite comunicarse directamente entre sí.

NHRP es un protocolo cliente-servidor que permite que los dispositivos se registren a través de redes conectadas directamente o dispares. Los servidores de salto siguiente *NHRP* son responsables de registrar direcciones o redes, mantener un repositorio *NHRP* y responder a cualquier consulta que se reciba por los clientes del siguiente salto (*NHC*). El *NHC* y *NHS* son transacciones usuales.

DMVPN usa túneles *GRE* multipunto, que requieren un método para asignar las direcciones IP del túnel a la dirección IP de transporte (subyacente). El NHRP proporciona la tecnología para asignar esas direcciones IP. Los spoke DMVPN se configuran estáticamente con la dirección IP de los concentradores (NHS) para que

puedan registrar su túnel y la dirección IP NBMA (transporte) con los concentradores (NHS). Cuando se establece un túnel de spoke a spoke, los mensajes de NHRP proporcionan la información necesaria para que los spoke se localicen entre sí, de modo que puedan construir un túnel de DMVPN de *spoke* a *spoke*. Los mensajes NHRP también permiten que un *spoke* localice una red remota. Cisco ha agregado tipos de mensajes NHRP adicionales a los definidos en *RFC2332* para proporcionar algunas de las mejoras recientes en DMVPN.

Todos los paquetes NHRP deben incluir la dirección NBMA de origen, la dirección del protocolo de origen, la dirección del protocolo de destino y el tipo de mensaje NHRP. Los tipos de mensajes NHRP se detallan a continuación.

Tabla 2.2 Tipos de mensajes NHRP

Tipo de mensaje	Descripción
Registro	Los mensajes de registro son enviados por el NHC (spoke de DMVPN) hacia el HNS (centros de DMVPN). El registro les permite a los concentradores conocer la información NBMA del spoke. El NHC también especifica la cantidad de tiempo que el NHS debe mantenerse el registro junto con otros atributos.
Resolución	Los mensajes de resolución son mensajes NHRP para ubicar y proporcionar la información de resolución de direcciones 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 más 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 más óptima no es factible o la política no lo permite.
Purga	Los mensajes de purga se envían para eliminar una entrada NHRP en cache. Los mensajes de purga notifican a los enrutadores, la perdida de una ruta utilizada por el NHRP. Por lo general, las purgas son enviadas por un NHS a los NHC (a las que contesto) 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, los mensajes de purga se reenvían a través del concentrador.
Error	Los mensajes de error se utilizan para notificar al remitente de un paquete NHRP que se ha producido un error.

Elaborado por: Verónica Ortiz y Dennis López

Los mensajes NHRP pueden contener información adicional que se incluyen en la parte de extensión de un mensaje. A continuación, se presenta las extensiones comunes de los mensajes NHRP.

Tabla 2.3 Extensiones de mensajes NHRP

Extensión NHRP	Descripción
Dirección de respuesta	Esto se utiliza para determinar la dirección del nodo que responde para los mensajes de respuesta.
Registro de transito de NHS hacia adelante.	Esto contiene una lista de NHS que el paquete de solicitud NHRP puede haber atravesado.
Registro NHS de transito inverso.	Esto contiene una lista de NHS que el paquete de respuesta NHRP puede haber atravesado.
Autentificación	Esto transmite información de autentificación entre los altavoces NHRP. La autentificación se realiza por pares en una base de salto por salto. Este campo se transmite en texto plano.
Vendedor privado	Esto transmite información privada del proveedor entre los altavoces del NHRP.
NAT	DMVPN funciona cuando un concentrador o spoke reside detrás de un dispositivo que realiza NAT y cuando el túnel esta encapsulado en Ipsec. Esta extensión NHRP es capaz de detectar la dirección NBMA reclamada (dentro de la dirección local) utilizando la dirección de protocolo de origen del paquete NHRP y la dirección IP global interna de los encabezados IP del paquete NHRP.

Elaborado por: Verónica Ortiz y Dennis López

2.3 VPN Multipunto Dinámico DMVPN

DMVPN proporciona conectividad completa mientras simplifica la configuración a medida que se implementan nuevos sitios. Se considera una tecnología de cero toques porque no se necesita configuración en los enrutadores centrales de DMVPN a medida que se agregan nuevos spoke a la red DMVPN. Esto facilita una configuración consistente en la que todos los spoke pueden usar una configuración de túnel idéntica (es decir, se puede templar) para simplificar el soporte y la implementación con sistemas de aprovisionamiento de red como Cisco Prime infraestructura.

Los sitios de spoke inician una conexión VPN persistente al enrutador concentrador. El tráfico de red entre los sitios de spoke no tiene que viajar a través de los centros. DMVPN construye dinámicamente un túnel VPN entre sitios de spoke según sea

necesario. Esto permite que el tráfico de la red, como para *VoIP*, tome una ruta directa, lo que reduce la demora y el *jitter* sin consumir ancho de banda en el sitio central.

DMVPN se lanzó en tres fases, y cada fase se construyó sobre la anterior con funciones adicionales. Las tres fases de DMVPN necesitan solo una interfaz de túnel en un enrutador, y el tamaño de la red de DMVPN debe acomodar todos los puntos finales asociados a esa red de túnel. Los spoke DMVPN pueden usar DHCP o direccionamiento estático para las redes de transporte y superposición. Localización de las direcciones IP de los otros spoke (protocolos y NBMA) a través del NHRP.

- **Fase 1 spoke-a-hub:**

La primera fase consiste en la implementación de DMVPN, además de proporcionar la implementación de cero toques para los sitios VPN. Los túneles VPN solamente se crean entre los spoke y concentradores. El tráfico entre los spoke debe atravesar el hub para alcanzar otro spoke.

- **Fase 2 spoke-a-spoke:**

La fase dos proporciona una capacidad adicional a la fase 1, que permite la comunicación de spoke a spoke de forma dinámica mediante la creación de un túnel VPN a petición del hub. En la fase 2 no se permite la preservación del siguiente salto, por ello no es compatible con la comunicación de spoke a spoke entre diferentes redes DMVPN jerárquica multinivel.

- **Fase 3 Árbol jerárquico Spoke-a-spoke:**

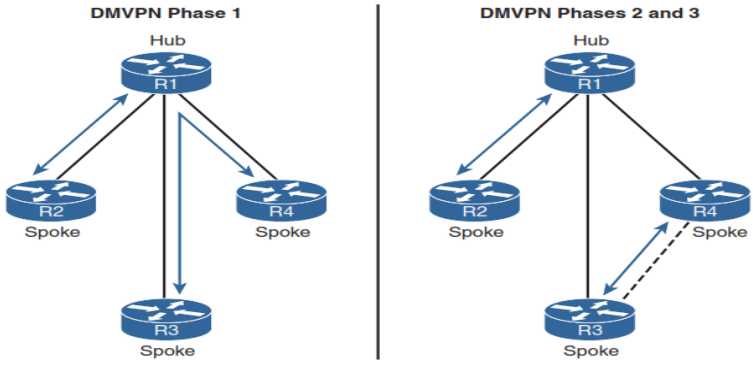
En la fase 3 se refina la conectividad de spoke a spoke mejorando los mensajes del NHRP e interactúa con la tabla de enrutamiento. En esta fase el concentrador envía un mensaje de re direccionamiento NHRP al spoke que origino el flujo de paquetes. El mensaje de re direccionamiento de NHRP proporciona la información necesaria para que el spoke de origen pueda iniciar una resolución del host/red de destino. Cisco proporciona soporte API para la fase 3 de DMVPN.

NHRP instala rutas en la tabla de enrutamiento para los accesos directos que crea. Los accesos directos de NHRP modifican la entrada del siguiente salto, para las rutas existentes o agregan una entrada de ruta más explícita a la tabla de enrutamiento. Debido a que los accesos directos de NHRP instalan rutas más explicitas en la tabla de

enrutamiento, la fase 3 admite el resumen de las redes en el concentrador mientras proporciona un enrutamiento óptimo entre los enrutadores de los spoke. Los accesos directos de NHRP permiten una topología jerárquica de árbol de modo que un centro regional es responsable de administrar el tráfico y las subredes de NHRP dentro de esa región, pero se puede establecer túneles de spoke a spoke fuera de esa región.

A continuación, se ilustra la diferencia entre los patrones de tráfico para las 3 fases DMVPN.

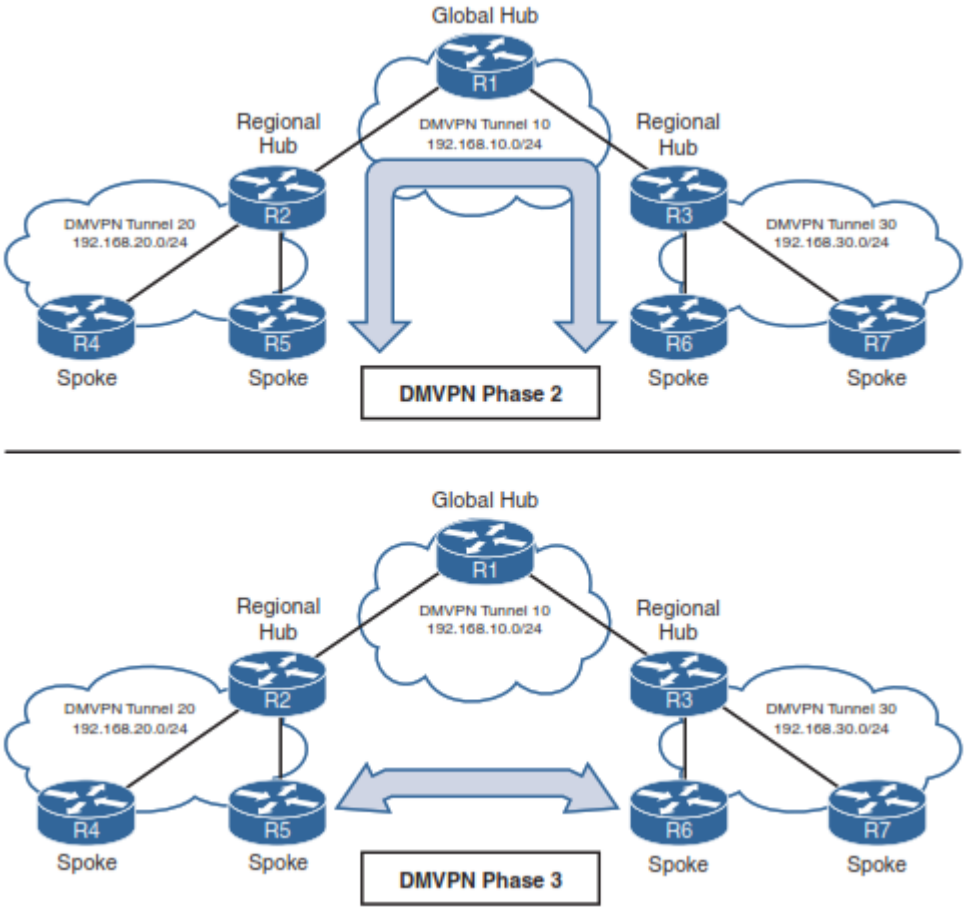
Figura 1.2. Patrones de tráfico DMVPN (Guide, 2017)



Los tres modelos presentados admiten la comunicación directa de spoke a concentradores, como se muestra en R1 y R2. El flujo de paquetes de spoke a spoke en la fase 1 de DMVPN es diferente del flujo de paquetes en las fases 2 y 3 de DMVPN. El tráfico entre R3 y R4 debe atravesar el centro para la fase 1, mientras que se crea un túnel dinámico de spoke a spoke para DMVPN fase2 y fase 3 que permiten la comunicación directa.

A continuación, se ilustra la diferencia en los patrones de tráfico entre DMVPN de la fase 2 y fase 3 con topologías jerárquicas.

Figura 2. 2 Comparación DMVPN fase 2 y fase 3 (Guide, 2017).



En el diseño jerárquico de dos niveles, R2 es el centro para el túnel 20 de DMVPN, y R3 es el centro para el túnel 30 de DMVPN. La conectividad entre los túneles 20 y 30 de DMVPN se establece mediante el túnel 10 de DMVPN. Los tres túneles de DMVPN usan el mismo túnel. La identificación a pesar de que utilizan diferentes interfaces de túnel. Para los túneles DMVPN de la fase 2, el tráfico de R5 debe fluir al hub R2, donde se envía a R3 y luego a R6. Para los túneles DMVPN de la fase 3, se establece un túnel de spoke a spoke entre R5 y R6 y los dos enrutadores pueden comunicarse directamente.

Cada fase DMVPN posee su propia configuración específica. No es recomendable mezclar fases DMVPN en la misma red de túneles. Si se necesita admitir varias fases DMVPN para una migración se debe usar una segunda red DMVPN.

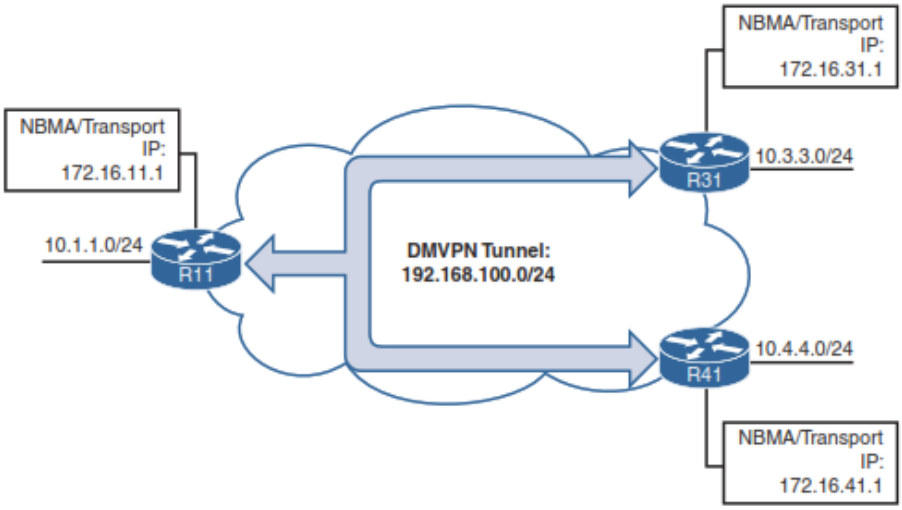
2.4 Configuración DMVPN

Existen dos tipos de configuraciones de DMVPN (concentrador o spoke), varían según la función del enrutador. El centro de DMVPN es el NHRP NHS y el spoke de

DMVPN es el NHRP NHC. Los spoke deben estar pre configurados con la dirección IP estática del concentrador, pero la dirección IP NBMA de un spoke puede ser estática o asignada desde DHCP.

En la siguiente figura se muestra la primera topología utilizada para explicar la configuración y las funciones DMVPN.

Figura 1 Topología DMVPN simple (Guide, 2017).



R11 actúa como el centro de DMVPN, R31 y R41 son los spoke de DMVPN. Los tres enrutadores utilizan una ruta estática predeterminada l enrutador SP que proporciona conectividad para las redes NBMA en el rango de red 172.16.0.0/16. EIGRP se ha configurado para operar en el túnel DMVPN y para anunciar las redes LAN locales.

2.4.1 Configuración del concentrador DMVPN

Para configurar un concentrador DMVPN se desarrolla los siguientes pasos:

- **Paso 1. Crear la interfaz del túnel:** Crear la interfaz del túnel con el número de túnel de la interfaz del comando de configuración global.

- **Paso 2. Identificar la fuente del túnel:** Identificar la fuente local del túnel con el comando de parámetro de interfaz fuente de túnel {dirección ip | ID de interfaz}. La fuente del túnel depende del tipo de transporte. La interfaz gráfica de encapsulación puede ser una interfaz lógica, como un bucle de retorno o una subinterfaz.

- **Paso 3. Convertir el túnel en una interfaz multipunto GRE**: Configurar el túnel DMVPN como un túnel multipunto GRE con el comando de parámetros de la interfaz modo túnel GRE multipunto.

- **Paso 4. Asignar una dirección IP para la red DMVPN (túnel)**: Se configura una dirección IP para la interfaz con el comando *ip address ip-address suberd-mask.*

- **Paso 5. Habilitar NHRP en la interfaz del túnel:**Activar NHRP e identificar de forma exclusiva el túnel DMVPN para la interfaz virtual con el comando de parámetros de la interfaz ip nhrp network-id 1-4294967295.

  La ID de la red de NHRP es importante a nivel local y se la utiliza para identificar una nube DMVPN en un enrutador porque varias interfaces de túnel pueden pertenecer a la misma nube DMVPN. Se recomienda que la identificación de la red NHRP coincida con los enrutadores que participan en la misma red DMVPN.

- **Paso 6. Definir la llave del túnel (opcional):**La clave del túnel ayuda a identificar la interfaz de túnel virtual DMVPN, si varias interfaces del túnel usan las mismas interfaces de origen de túnel como se detalló en el paso 3.

  Las claves del túnel deben coincidir para que un túnel DMVPN se establezca entre dos enrutadores. La clave del túnel agrega 4 bytes al encabezado DMVPN.

  La clave del túnel se configura con la clave de túnel de comando 0-4294967295.

- **Paso 7. Habilitar el soporte de multidifusión para NHRP (opcional):** NHRP proporciona un servicio de mapeo de la dirección del protocolo (túnel IP) a la dirección NBMA (transporte) para paquetes de multidifusión también. Para admitir los protocolos de enrutamiento o multidifusión que utilizan en

multidifusión, esto debe estar habilitado en los enrutadores centrales de DMVPN, con el *comando tunnel ip nhrp map multicast Dynamic.*

- **Paso 8. Habilitar la redirección NHRP (usada solo para fase 3):** Habilitar las funciones de redirección NHRP con el comando *ip nhrp redirect.*

- **Paso 9. Definir ancho de banda del túnel (opcional):** Las interfaces virtuales no tienen el concepto de latencia y la necesidad de tener un ancho de banda de referencia configurado, para que los protocolos de enrutamiento que usan ancho de banda, para el cálculo de la mejor ruta que pueden tomar una decisión inteligente. El ancho de banda también se utiliza para la configuración QoS en la interfaz. El ancho de banda se define con el parámetro de interfaz comando ancho de banda [1-10000000], se mide en kilobits por segundo.

- **Paso 10. Definir la MTU IP para la interfaz del túnel (opcional):** La MTU IP se configura con el comando de parámetros de interfaz ip mtu mtu. Normalmente se usa una MTU de 1400 para túneles DMVPN, teniendo en cuenta la sobrecarga de encapsulación adicional.

- **Paso 11. Definir el tamaño máximo de segmento TCP (MSS) (opcional):** La función TCP Adjust MSS garantiza que el enrutador editara la carga útil de un protocolo de enlace de tres vías TCP si el MSS excede el valor configurado. El comando es ip tcp adjust-mss mss size.

  Normalmente las interfaces DMVPN usan el valor de 1360 para acomodar los encabezados IP, GRE e IPsec.

2.4.2 Configuración de spoke DMVPN para fase 1(punto-punto).

La configuración de spoke en la fase 1 de DMVPN es similar a la configuración de un enrutador con la excepción:

- No utiliza un túnel GRE multipunto, en su lugar se especifica el destino del túnel.
- El mapeo NHRP apunta al menos un NHS activo.

El proceso para configurar un enrutador de spoke de fase 1 DMVPN es:

- **Paso 1. Crear la interfaz del túnel:** Crear la interfaz del túnel con el número de túnel de la interfaz del comando de la configuración global.

- **Paso 2. Identificar la dirección IP del destino remoto:** Identifica el destino del túnel con el parámetro de la interfaz comando *tunnel address ip address.*

- **Paso 3. Identificar la fuente del túnel:** Identifique la fuente local del túnel con la fuente del túnel del comando del parámetro de la interfaz {ip-address | ID de interfaz}

- **Paso 4. Definir el destino del túnel (hub):** Identifique el destino del túnel con el parámetro de interfaz *comando tunnel address ip address*. El destino del túnel es la dirección IP del concentrador DMVPN (NBMA) que usa el enrutador local para estableces el túnel DMVPN.

- **Paso 5. Asignar una dirección IP para la red DMVPN (túnel):** Se configura una dirección IP para la interfaz con el comando ip address {mascara de subred de la dirección ip | dhcp} o con el comando ipv6 address ipv6-address/prefix-length.

- **Paso 6. Habilitar NHRP en la interfaz del túnel:**Activar NHRP e identificar de forma exclusiva el túnel DMVPN para la interfaz virtual con el comando de parámetros de la interfaz ip nhrp network-id 1-4294967295.

- **Paso 7. Definir una clave para el túnel NHRP (opcional):** La clave del túnel NHRP ayuda a identificar la interfaz del túnel virtual DMVPN, si varios túneles terminan en la misma interfaz que se define en el paso 3. Las claves del túnel deben coincidir para que un túnel DMVPN se establezca entre dos enrutadores. La clave del túnel agreda 4 bytes al encabezado DMVPN.

  La clave del túnel se puede configurar con el comando clave 0-4294967295.

- **Paso 8. Especificar el NHRP NHS, la dirección NBMA y la asignación de multidifusión:** Especifique la dirección de uno o más servidores NHRP NHS con el comando *ip nhrp nhs, nhs-address nbma nbma-address* [multidifusión]. La palabra clave de multidifusión proporciona funciones de asignación de multidifusión en NHRP y requiere que admita los siguientes protocolos de enrutamiento: RIP, EIGRP y OSPF.

  Este comando es el método más simple para definir la configuración NHRP. En la siguiente tabla se presentan comandos alternativos de mapeo NHRP, que se necesitan solo en los casos en que se necesite un mapa estático de *unicast* o *multicast* para un nodo que no es un NHS.

Tabla.2.4 Comandos alternativo mapeo NHRP

Comando	Función
Ip nhrp nhs nbs-address	Crea una entrada NHS y la asigna a la dirección IP del túnel.
Ip nhrp map ip-address nbma-address	Asigna la dirección NBMA a la dirección IP del túnel.
Ip nhrp map multicast [nbma-address | dynamic]	Asigna las direcciones NBMA utilizadas como destinos para los paquetes de difusión o multidifusión que se enviaran a través de la red.

Elaborado por: Verónica Ortiz y Dennis López

- **Paso 9. Definir el ancho de banda del túnel (opcional):** Las interfaces virtuales no tienen el concepto de latencia y necesitan tener configurado un ancho de banda de referencia para que los protocolos de enrutamiento que usan el ancho de banda para el cálculo de la mejor ruta que pueda tomar una decisión inteligente. El ancho de banda también se utiliza para la configuración de *QoS* en la interfaz. El ancho de banda se define con el parámetro de interfaz comando de banda [1-100000000], que se mide en kilobits por segundo.

- **Paso 10. Defina la MTU IP para la interfaz del túnel (opcional):** La MTU IP se configura con el comando de parámetros de interfaz mtu. Normalmente se usa una MTU de 1400 para túneles de DMVPN para tener en cuenta la sobrecarga de encapsulación adicional.

- **Paso 11. Definir el TCP MSS (opcional):** La función TCP Adjust MSS garantiza que el enrutador edite la carga útil de un protocolo de enlace de tres vías TCP si el MSS excede el valor configurado. El comando es ip tcp adjust-mss mss size. Normalmente las interfaces DMVPN usa el valor de 1360 para acomodar encabezados IP, GRE e Ipsec.

2.4.3 Verificando el estado del túnel DMVPN.

Al configurar una red DMVPN, es de mucha utilidad verificar que los túneles se hayan establecido y que el NHRP esté funcionando correctamente. El comando show dmvpn(detalle) proporciona la interfaz del túnel, la función del túnel, el estado del túnel y los pares del túnel con el tiempo de actividad. Cuando la interfaz del túnel DMVPN se apaga administrativamente, no hay entradas asociadas a esa interfaz del túnel. Los estados del túnel son:

- **INTF:** El protocolo de línea del túnel DMVPN está inactivo.
- **IKE:** Los túneles DMVPN configurados con Ipsec aún no han establecido con éxito una sesión IKE.
- **Ipsec:** se ha establecido una sesión IKE, pero aún no se ha establecido una asociación de seguridad (SA) Ipsec.
- **NHRP:** el enrutador de spoke DMVPN aún no se ha registrado correctamente.
- **Arriba**: el enrutador de spoke DMVPN se ha registrado en el concentrador DMVPN y recibió un ACK (respuesta de registro positiva) del concentrador.

2.4.4 Visualizando el cache de NHRP

La información que proporciona NHRP es un componente vital de la operación de DMVPN. Cada enrutador mantiene un cache de solicitudes que recibe o está procesando. El comando show ip nhrp [brief] muestra el cache NHRP local en un enrutador. El cache NHRP contiene los siguientes campos:

- Entrada de red para hosts (IPv4:/32 o IPv6:/128) o para una red / x y la dirección IP del túnel a la dirección IP NBMA (transporte).
- El número de interfaz, la duración de la existencia y cuando expiran (horas: minutos: segundos). Solo las entradas dinámicas caducan.
- El tipo de entrada de mapeo NHRP. En la tabla 5 se muestra una lista de las entradas de mapeo NHRP en el cache local.

Tabla 2.5 Entradas de mapeo NHRP

Entrada de mapeo NHRP	Descripción
Static	Una entrada creada estáticamente en una interfaz DMVPN.
Incomplete	Una entrada temporal colocada localmente mientras se procesa una solicitud de resolución NHRP. Una entrada incompleta evita las solicitudes repetitivas de NHRP para la misa entrada, evitando el consumo innecesario de recursos del enrutador. Eventualmente, esto dejará de funcionar y permitirá otra solicitud de resolución NHRP para la misma red.
Local	Muestra información de mapeo local. Una entrada típica representa una red local que fue anunciada para una respuesta de resolución NHRP. Esta entrada registra qué nodos recibieron esta asignación de red local a través de una respuesta de resolución NHRP.
(no-socket)	Estas entradas de asignación no tienen un socket Ipsec asociado y el cifrado no se activa.
NBMA address	Dirección de acceso múltiple sin transmisión, o la dirección IP de transporte donde se recibió la entrada.

Elaborado por: Verónica Ortiz y Dennis López

CAPÍTULO 3

3.1 Diseño de la red

El diseño lógico de la red piloto se simulará en el software GNS3, este nos permite cargar IOS de routers reales de CISCO, para construir la topología con todos los dispositivos que se emplearan para el diseño de la red piloto.

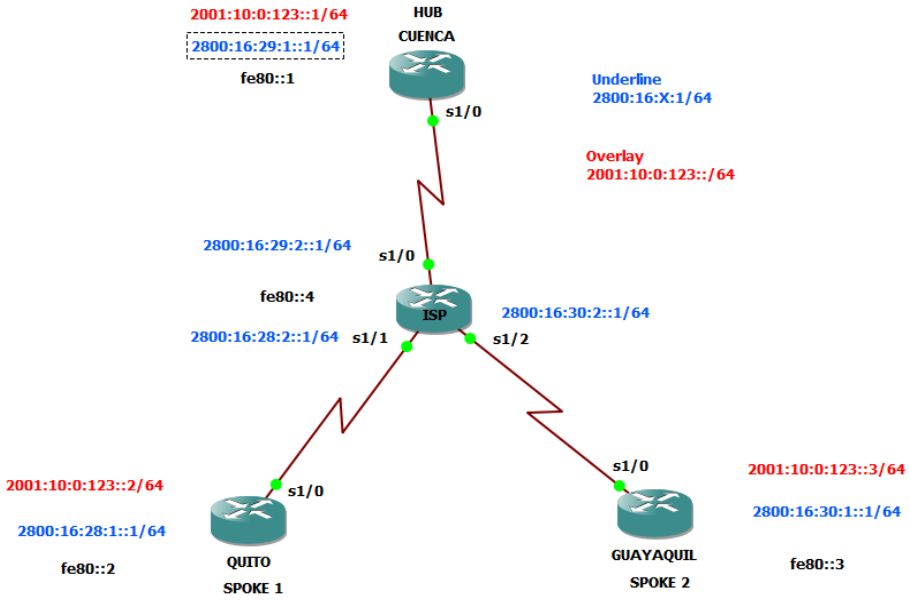
3.1.1 Diseño De La Red Piloto

La red piloto consta de 4 routers base, como se observa en la Figura 3.1. Uno de los routers servirá como proveedor de servicio de internet, los routers restantes representan a las sedes de la Universidad Politécnica Salesiana que se encuentran en Quito, Guayaquil y Cuenca. Para la conexión de la topología se emplearán routers Cisco 7200.

La red está compuesta por los siguientes elementos:

- Router Cisco 7200
- Switch

Figura 3. 1 Red Piloto



Elaborado por: Verónica Ortiz y Dennis López

3.2.1 Direcciones IPS.

Para el direccionamiento de la ISP de la red piloto se escogió las direcciones 2800, debido a que la ISP CEDIA (Fundación Consorcio Ecuatoriano para el desarrollo de Internet Avanzado) asigno segmentos de redes Ipv6 para los campus de la UPS.
Lo que define la topología de la red es el prefijo ISP o RIR, estos prefijos son proporcionados por las empresas.

Tabla 3.6 Direccionamiento IPV6 red piloto

Direccionamiento IPV6 ISP					
Red	Host	Prefijo	Red	Host	Prefijo
2800:16:28:1	::1	/64	2800:16:28:2	::1	/64
2800:16:29:1	::1	/64	2800:16:29:2	::1	/64
2800:16:30:1	::1	/64	2800:16:30:2	::1	/64
2800:16:31:1	::1	/64	2800:16:31:2	::1	/64
2800:16:32:1	::1	/64	2800:16:32:2	::1	/64

Elaborado por: Verónica Ortiz y Dennis López

3.3.1 Direccionamiento de overlay

Para la configuración de los túneles correspondientes a la Overlay se asigna direcciones IPV6 2001:10:0:123::/64, con la terminación ascendente para un túnel diferente, como se observa en la tabla 4. Si se requiere agregar nuevos túneles es necesario seguir la secuencia mencionada anteriormente.

Tabla 3.7 Direccionamiento IPV6 túneles DMVPN

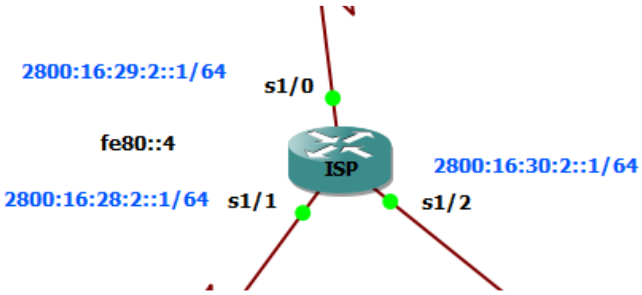
Direccionamiento para túneles			
2001:10:0:123	::1	/64	Cuenca Hub-Tunel 0
2001:10:0:123	::2	/64	Guayaquil Spoke-Tunel 0
2001:10:0:123	::3	/64	Quito Spoke- Tunel0

3.2 Configuraciones

3.1.2 Configuración del router isp.

Como primer paso se debe configurar la red ISP en GNS3, para ello se debe añadir la IOS del router 7200. Una vez añadido la IOS del router se procede configurar cada interfaz con las respectivas direcciones presentadas en la tabla 6, posterior a ellos se configurar el enrutamiento a usar para este caso es OSPF.

Figura 3. 2 Router ISP



Elaborado por: Verónica Ortiz y Dennis López

A continuación, se muestra la configuración del router ISP, correspondiente al router 2 en GNS3.

Tabla 3.8 Configuración router ISP

Configuración	Explicación
Configure terminal	Ingresa a la configuración del terminal
ipv6 unicast-routing	Habilita el ruteo unicast para IPV6
int s1/0	Ingresa a la interfaz serial s1/0 del router 2
ipv6 address 2001: acad:1234: acde: aaaa: abcd: a1b1:abc2/64	Asigna la dirección IPV6 a la interfaz s1/0.
ipv6 address fe80::4 link-local	Asigna la dirección IPV6 link local a la interfaz s1/0
no shutdown	Enciende la interfaz s1/0
Exit	Sale de la interface s1/0
ipv6 router ospf 1	habilita el enrutamiento OSPF para IPV6
router-id 2.2.2.2	Identifica el R2 con OSPF
Exit	Sale del enrutamiento OSPF
int s1/0	Ingresa a la interfaz serial s1/0
ipv6 ospf 1 area 0	Asigna el área OSPF del ipv6
Exit	Sale de la interfaz s1/0
int s1/1	Ingresa a la interfaz serial s1/1 del router 2
ipv6 address 2001 :aaaa: bbbb: cccc: acad:cada:3421:dfe8/64	Asigna la dirección IPV6 a la interfaz s1/1.
ipv6 address fe80::4 link-local	asigna la dirección IPV6 link local a la interfaz s1/1
no shutdown	Enciende la interfaz s1/1
Exit	Sale de la interfaz s1/1

Elaborado por: Verónica Ortiz y Dennis López

Tabla 3.9 Configuración router ISP (continuación)

Configuración	Explicación
int s1/1	Ingresa a la interfaz serial s1/1
ipv6 ospf 1 area 0	Asigna el área OSPF del ipv6
Exit	Sale de la interfaz s1/1
int s1/2	Ingresa a la interfaz serial s1/2 del router 2
ipv6 address 2001: dbac:1234: acad :1234 :5678:a123:cca8/64	Asigna la dirección IPV6 a la interfaz s1/2
ipv6 address fe80::4 link-local	Asigna la dirección IPV6 link local a la interfaz s1/2
no shutdown	Enciende la interfaz s1/2
Exit	Sale de la interfaz s1/2
int s1/2	Ingresa a la interfaz serial s1/2
ipv6 ospf 1 area 0	Asigna el área OSPF del ipv6
Exit	Sale de la interfaz s1/2

Elaborado por: Verónica Ortiz y Dennis López

Nota: Los pasos descritos anteriormente se deberán emplear para cada interfaz que se desee configurar con enrutamiento OSPF.

A continuación, se muestra la configuración de OSPF en el router de Cuenca.

Tabla 3.11 Configuración OSPF router Cuenca

Configuración	Explicación
configure terminal	Ingresa a la configuración del terminal
ipv6 unicast-routing	Habilita el ruteo unicast para IPV6
int s1/0	Ingresa a la interfaz serial s1/0 del router 1 correspondiente a Cuenca
ipv6 address 2001: acad: 1234: acde: aaaa:abcd:a1b1:abc1/64	Asigna la dirección IPV6 a la interfaz s1/0.
ipv6 address fe80::1 link-local	Asigna la dirección IPV6 link local a la interfaz s1/0
no shutdown	Enciende la interfaz s1/0
exit	Sale de la interfaz s1/0

Elaborado por: Verónica Ortiz y Dennis López

Tabla 3.10 Configuración OSPF router Cuenca (continuación)

Configuración	Explicación
ipv6 router ospf 1	Habilita el enrutamiento OSPF para IPV6
router-id 1.1.1.1	Identifica el router con OSPF
Exit	Sale del enrutamiento OSPF
int s1/0	Ingresa a la interfaz serial s1/0
ipv6 ospf 1 area 0	Asigna el área OSPF del ipv6
Exit	Sale de la interfaz s1/0

Elaborado por: Verónica Ortiz y Dennis López

A continuación, se muestra la configuración de OSPF en el router de Guayaquil.

Tabla 3. 12 Configuración OSPF router Guayaquil

Configuración	Explicación
configure terminal	Ingresa a la configuración del terminal
ipv6 unicast-routing	Habilita el ruteo unicast para IPV6
int s1/0	Ingresa a la interfaz serial s1/0 del router 1 correspondiente a Guayaquil
ipv6 address 2001 :aaaa: bbbb: cccc: acad:cada:3421:dfe7/64	Asigna la dirección IPV6 a la interfaz s1/0.
ipv6 address fe80::2 link-local	Asigna la dirección IPV6 link local a la interfaz s1/0
no shutdown	Enciende la interfaz s1/0
exit	Sale de la interface s1/0
ipv6 router ospf 1	Habilita el enrutamiento OSPF para IPV6
router-id 3.3.3.3	Identifica el router con OSPF
Exit	Sale del enrutamiento OSPF
int s1/0	Ingresa a la interfaz serial s1/0
ipv6 ospf 1 area 0	Asigna el área OSPF del ipv6
Exit	Sale de la interfaz s1/0

Elaborado por: Verónica Ortiz y Dennis López

A continuación, se muestra la configuración de OSPF en el router de Quito.

Tabla 3.13 Configuración OSPF router Quito

Configuración	Explicación
configure terminal	Ingresa a la configuración del terminal
ipv6 unicast-routing	Habilita el ruteo unicast para IPV6
int s1/0	Ingresa a la interfaz serial s1/0 del router 1 correspondiente a Quito
ipv6 address 2001: dbac: 1234: acad: 1234: 5678:a123:cca7/64	Asigna la dirección IPV6 a la interfaz s1/0.
ipv6 address fe80::3 link-local	Asigna la dirección IPV6 link local a la interfaz s1/0
no shutdown	Enciende la interfaz s1/0
exit	Sale de la interface s1/0
ipv6 router ospf 1	Habilita el enrutamiento OSPF para IPV6
router-id 4.4.4.4	Identifica el router con OSPF
Exit	Sale del enrutamiento OSPF
int s1/0	Ingresa a la interfaz serial s1/0
ipv6 ospf 1 area 0	Asigna el área OSPF del ipv6
Exit	Sale de la interfaz s1/0

Elaborado por: Verónica Ortiz y Dennis López

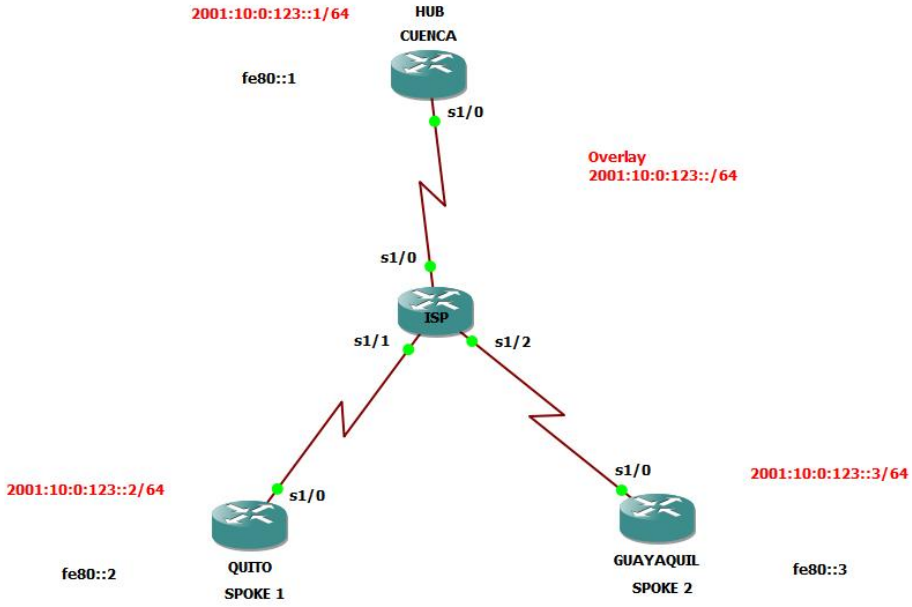
3.2.2 Configuración de mgre en los routers de Cuenca, Guayaquil y Quito.

Para configurar los túneles multipunto DMVPN se empleará una topología Hub-Spoke. El router principal será el de Cuenca, actuando como Hub, mientras que los routers de Guayaquil y Quito actúan como Spoke.

Para configurar mGRE se usó la ISO de Cisco 7200 que soporta mGRE para IPV6, es importante mencionar que no todas ISO soportan mGRE para IPV6.

Para la configuración se emplea las direcciones IPV6 descritas anteriormente en la Tabla 3.

Figura 3. 3 Diseño de DMVPN para IPV6



Elaborado por: Verónica Ortiz y Dennis López

A continuación, se muestra la configuración del Hub de la red propuesta:

Tabla 3.14 Configuración DMVPN router Cuenca (HUB)

Configuración	Explicación
config terminal	Ingresa a la configuración del terminal
int tun 0	Ingresa a la interfaz túnel 0
tunnel source 2001: acad: 1234: acde: aaaa: abcd:a1b1:abc1	Se configura la dirección de origen de la interfaz túnel 0, es posible colocar en lugar la dirección IPV6 la interfaz serial s1/0.
tunnel mode gre multipoint ipv6	Se establece el modo de encapsulamiento del túnel
ipv6 address fe80::1 link-local	Se configura la dirección del link local de la interfaz s1/0.
ipv6 address 2001:10:0:123::1/64	Se configura la dirección IPV6 que se le asigna al túnel 0.
ipv6 nhrp network-id 123	Se configura un identificador de res de 32 bits, como un identificador de una red no difusión de acceso múltiple.
ipv6 nhrp redirect	Activa el reenvió NHRP.

Elaborado por: Verónica Ortiz y Dennis López

A continuación, se presenta la configuración del Spoke 1:

Tabla 3.154 Configuración DMVPN router Quito (SPOKE 1)

Configuración	Explicación
config terminal	Ingresa a la configuración del terminal
int tun 0	Ingresa a la interfaz túnel 0
tunnel source 2001: aaaa: bbbb:cccc:acad:cada:3421:dfe7	Se configura la dirección de origen de la interfaz túnel 0, es posible colocar en lugar la dirección IPV6 la interfaz serial s1/0.
tunnel mode gre multipoint ipv6	Se establece el modo de encapsulamiento del túnel
ipv6 address fe80::2 link-local	Se configura la dirección del link local de la interfaz s1/0.
ipv6 address 2001:10:0:123::2/64	Se configura la dirección IPV6 que se le asigna al túnel 0.
ipv6 nhrp network-id 123	Se configura un identificador de res de 32 bits, como un identificador de una red no difusión de acceso múltiple.
ipv6 nhrp shortcut	Activa la conmutación de acceso directo.
ipv6 nhrp nhs 2001:10:0:123::1 nbma 2001: acad:1234: acde: aaaa : abcd: a1b1: abc1	Indica que todo el tráfico multicast que necesite enviar al Hub lo reencapsule con la dirección de la underline de la interfaz s1/0 del HUB.

Elaborado por: Verónica Ortiz y Dennis López

A continuación, se muestra la configuración del Spoke 2 de la red propuesta

Tabla 3.165 Configuración DMVPN router Guayaquil (SPOKE 2).

Configuración	Explicación
config terminal	Ingresa a la configuración del terminal
int tun 0	Ingresa a la interfaz túnel 0
tunnel source 2001: dbac: 1234: acad: 1234:5678:a123:cca7	Se configura la dirección de origen de la interfaz túnel 0, es posible colocar en lugar la dirección IPV6 la interfaz serial s1/0.
tunnel mode gre multipoint ipv6	Se establece el modo de encapsulamiento del túnel

Elaborado por: Verónica Ortiz y Dennis López

Tabla 3.17 Configuración DMVPN router Guayaquil (SPOKE 2 ccontinuación)

Configuración	Explicación
ipv6 address fe80::3 link-local	Se configura la dirección del link local de la interfaz s1/0.
ipv6 address 2001:10:0:123::3/64	Se configura la dirección IPV6 que se le asigna al túnel 0.
ipv6 nhrp network-id 123	Se configura un identificador de res de 32 bits, como un identificador de una red no difusión de acceso múltiple.
ipv6 nhrp shortcut	Activa la conmutación de acceso directo.
ipv6 nhrp nhs 2001:10:0:123::1 nbma 2001: acad:1234: acde: aaaa: abcd: a1b1: abc1	Indica que todo el tráfico multicast que necesite enviar al Hub lo reencapsule con la dirección de la Underline de la interfaz s1/0 del HUB.

Elaborado por: Verónica Ortiz y Dennis López

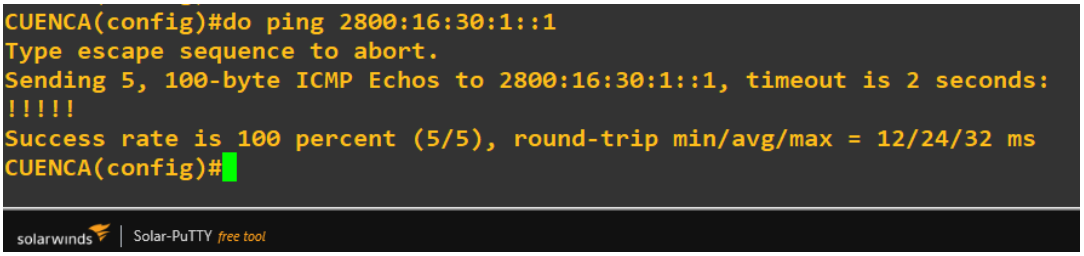
Nota: Para configurar un nuevo spoke basta con copiar la configuración de uno de los spokes existentes, cambiando el origen del túnel y la dirección.

3.1.2 Pruebas de conectividad

Como primer paso es necesario verificar la conectividad en la underline, es decir se debe comprobar la conectividad entre el Router de Cuenca- Router de Guayaquil, el Router de Guayaquil-Router de Quito y la conectividad entre el router de Guayaquil

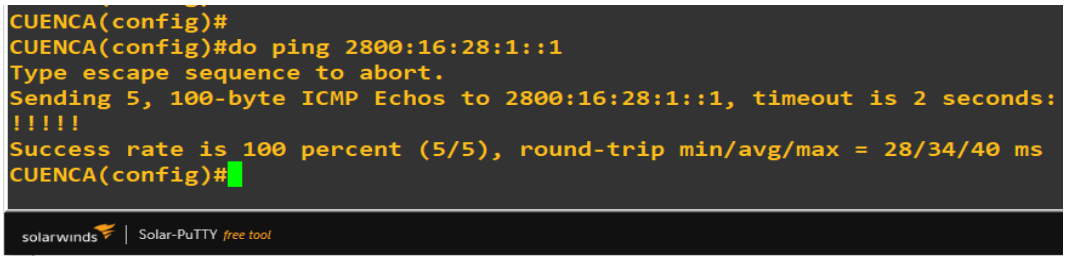
Router de Quito. Para ellos se procede a realizar pruebas de ping entre los routers descritos.

Figura 3. 4 Prueba de conexión entre router de Cuenca-Guayaquil



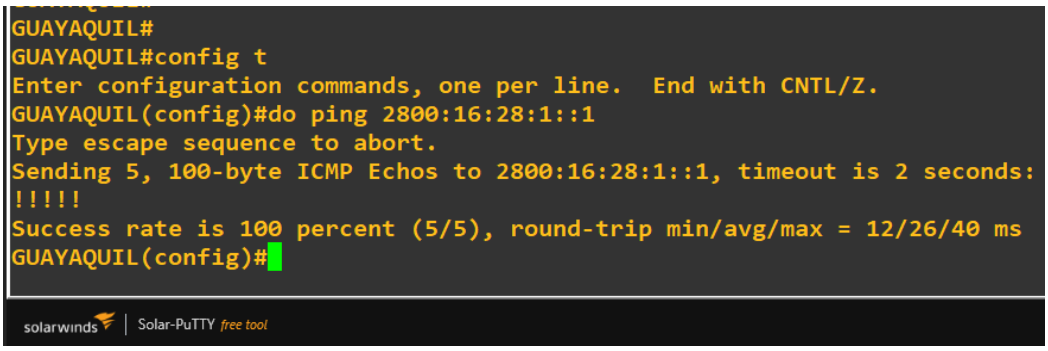
Elaborado por: Verónica Ortiz y Dennis López

.Figura 3. 5 Prueba de conexión entre router de Cuenca-Quito



Elaborado por: Verónica Ortiz y Dennis López

Figura 3. 6 Prueba de conexión entre router de Guayaquil-Quito



Elaborado por: Verónica Ortiz y Dennis López

Como se observa en las figuras 3.4, 3.5 y 3.6 existe conectividad entre todos los routers. Para comprobar el tipo de enrutamiento que se encuentra configurado se lo hace mediante dos comandos:

- Show run //Permite verificar la configuración de las interfaces del router.
- Do show ipv6 route //Permite verificar la direcciones de red que se encuentran conectadas bajo el protocolo OSPF.

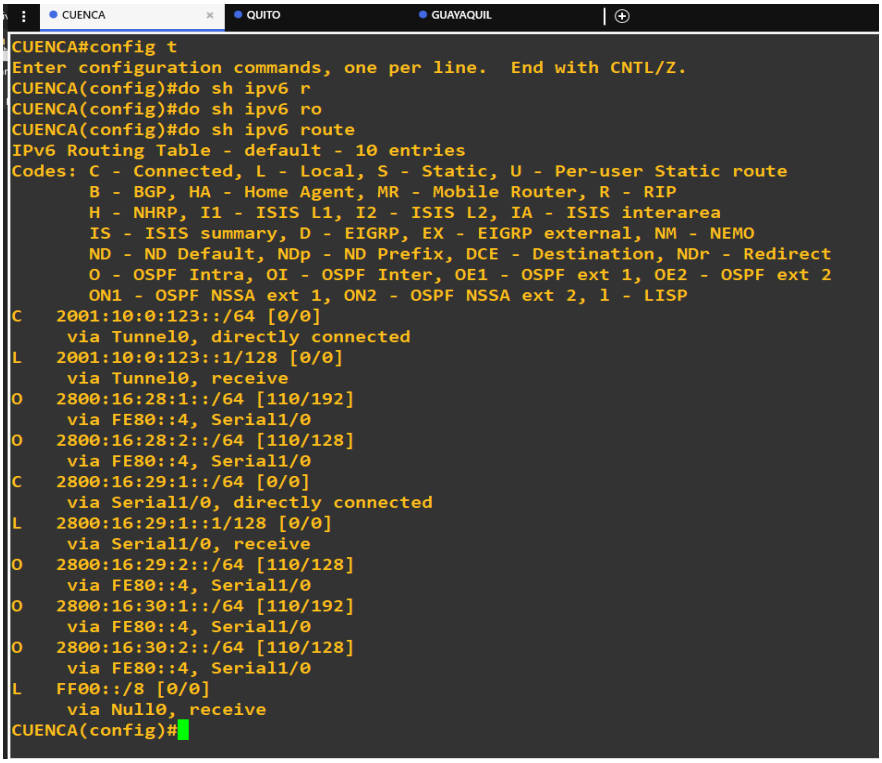
Figura 3. 7 Ejecución de comando show run.

Elaborado por: Verónica Ortiz y Dennis López

En la Figura 3.7 se puede apreciar la ejecución del comando show run, es posible verificar la configuración de las interfaces del router de Cuenca, en este caso es posible observar que la interfaz s1/0 tiene una dirección IPV6 correspondiente a la asignación según la Tabla 6, además que está configurado el enrutamiento OSPF.

Ahora si se ejecuta el comando Do show ipv6 route se tiene:

Figura 3. 8 Ejecución de comando Do show ipv6 route.



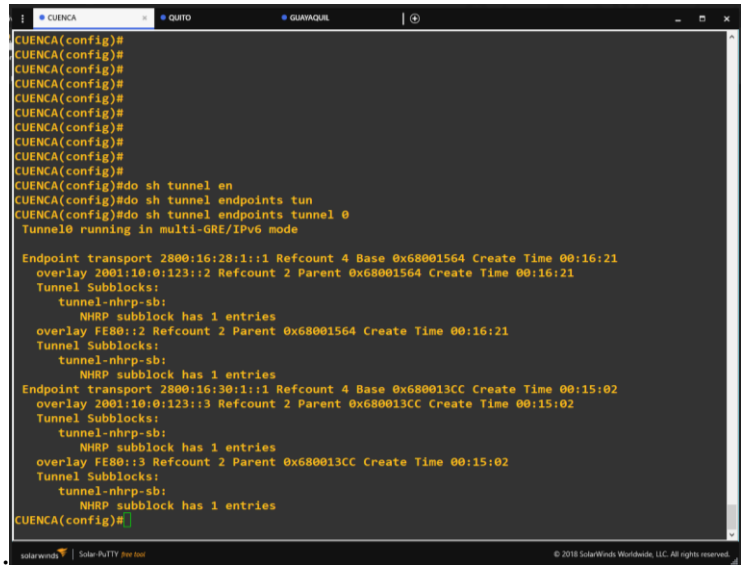
Fuente:GNS3

En la figura 3.8 es posible apreciar que la dirección 2800:16:28: 1:: se encuentra conectada bajo el protocolo de OSPF, correspondiente al router de Quito. También existe la dirección 2800:16:30::1 conectada bajo el protocolo OSPF, correspondiente al router de Guayaquil.

El siguiente paso consiste en demostrar que se encuentra configurado mGRE en el router de Cuenca, Guayaquil y Quito, para ello se hace empleo de los siguientes comandos.

- Do show tunnel endpoints tunnel [0-1-2-3-4-5-6---n] //Permite verificar que los puntos finales de los tuneles se levantaron de forma correcta.
- Do show dmvpn // Permite observer los tuneles dmvpn creados.

Figura 3. 9 Ejecución de comando Do show tunnel endpoints tunnel 0, router Cuenca



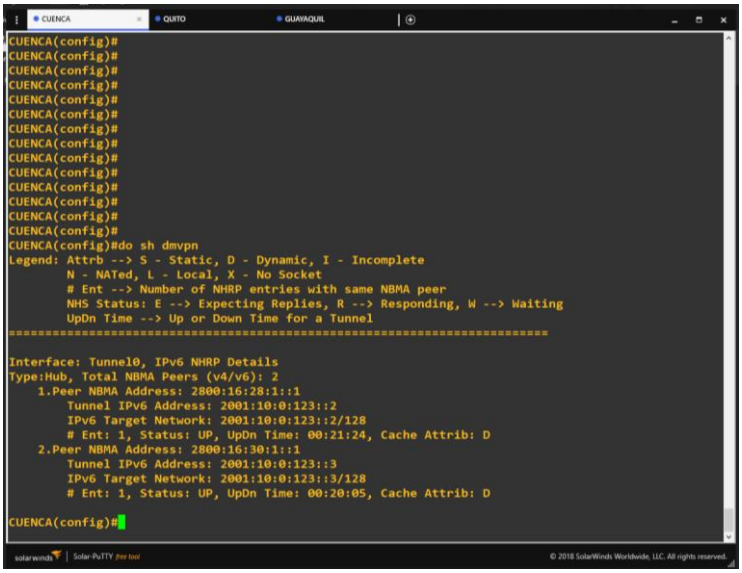
Fuente:GNS3

En la Figura 3.9 es posible observar que existen dos túneles creados correctamente.

El primero se transporta bajo la dirección Underline 2800:16:28:1::1, el túnel se encuentra funcionando 16 minutos y la dirección del túnel en la Overlay es 2001:10:0:123::2, dirección correspondiente al spoke de Quito.

El segundo se transporta bajo la dirección Underline 2800:16:30:1::1, el túnel se encuentra funcionando 15 minutos y la dirección del túnel en la Overlay es 2001:10:0:123::3, dirección correspondiente al Spoke de Guayaquil.

Figura 3. 10 Ejecución del comando do show dmvpn, router Cuenca.



Fuente:GNS3

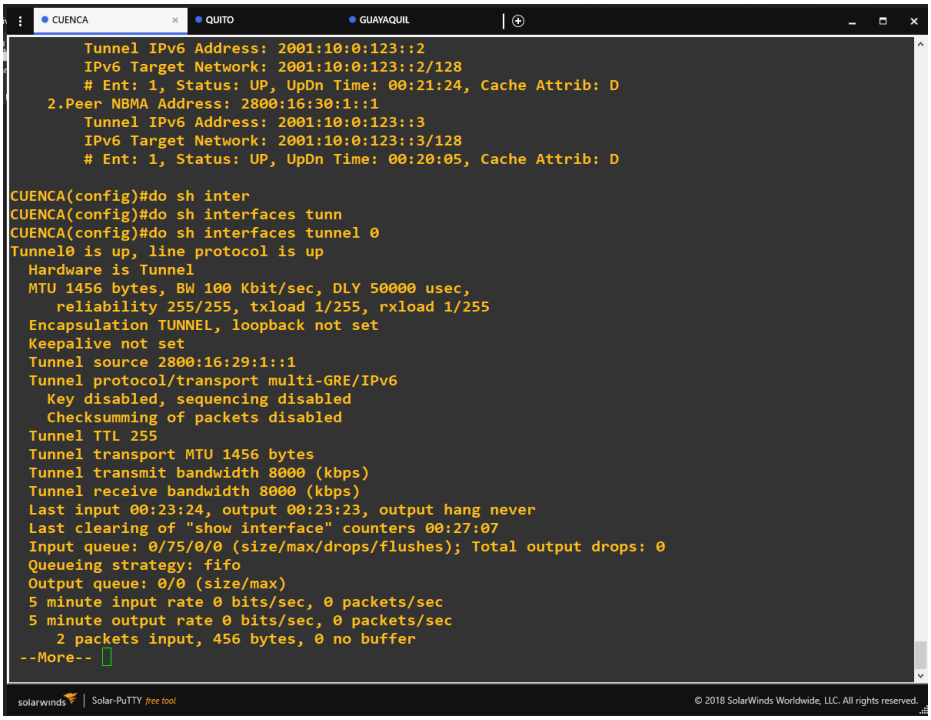
En la Figura 3.10 se observan operativos dos túneles dinámicos.

El primero tiene una dirección NBMA 2800:16:28:1::1 y la dirección del túnel es 2001:10:0:123::2, el estado de este es UP (el túnel se encuentra levantado) y tiene atributos dinámicos. Este túnel corresponde al Spoke 1, es decir Quito.

El segundo tiene una dirección NBMA 2800:16:30:1::1 y la dirección del túnel es 2001:10:0:123::3, el estado de este es UP (el túnel se encuentra levantado) y tiene atributos dinámicos. Este túnel corresponde al Spoke 2, es decir Guayaquil.

A continuación, se muestra el estado del túnel 0 correspondiente al HUB:

Figura 3. 11 Descripción estado del túnel 0.



Fuente:GNS3

En la Figura 3.11 se puede apreciar el estado del túnel, entre la información relevante proporciona la MTU (unidad máxima de transferencia) con un valor de 1456 bytes, el protocolo del túnel es GRE Multipunto y el ancho de banda de transmisión es 8000 kbps.

CAPÍTULO 4

La red que se configuro en el Capítulo 3, corresponde a la propuesta planteada sobre DMVPN, misma que consiste configurar túneles dinámicos para la interconexión de las diferentes sedes de Cuenca, Quito y Guayaquil. Pero la UPS dispone de más sucursales mismas que podrían ser configuradas de tal forma que sea posible la interconexión entre ellas. Para comprobar que la configuración de la red propuesta es funcional se propone dos escenarios.

- Escenario 1: Configuración de la red con enrutamiento OSPF sobre IPV6 y DMVPN sobre ipv6
- Escenario 2: Configuración de la red con enrutamiento EIGRP sobre IPV4 y DMVPN sobre ipv6.

Además, para demostrar la escalabilidad de la red propuesta, se configura un Spoke adicional, para comprobar la facilidad que brinda la implementación DMVPN en el ingreso de nuevos Spokes a la red.

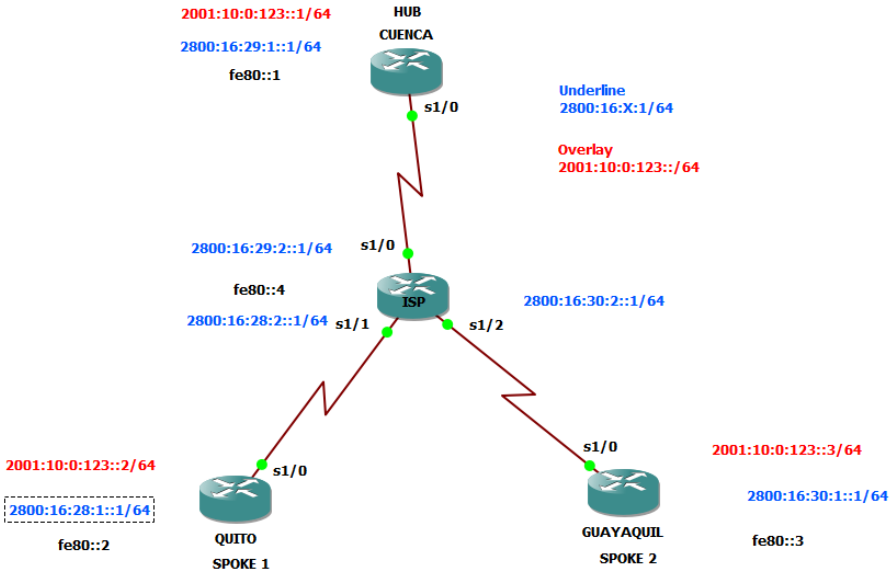
4.1 Escenario 1

4.1.1 Configuración de la red con enrutamiento OSPF sobre IPV6 y DMVPN

La red propuesta consta de 4 routers, los tres que representan a cada una de las sucursales de la UPS y un router que representa al proveedor de internet. Es posible configurar esta red con un protocolo de enrutamiento en la Underline, para sobre ese protocolo configurar DMVPN. En este caso se configuro OSPF para IPV6, para ello es necesario tomar en cuenta que se necesita un router con una IOS que soporte IPV6 de forma nativa. Además, los túneles multipunto se configuraron con direcciones IPV6, es decir que se tiene la configuración de la Underline con IPV6 y la configuración de la Overlay también con IPV6 (IPv6 sobre IPV6). Esta configuración es muy útil debido a que existe el estudio (Ayala, 2017) que proponen la migración de direcciones IPv4 a direcciones Ipv6.

La red Propuesta con las direcciones que se emplearon se presenta a continuación.

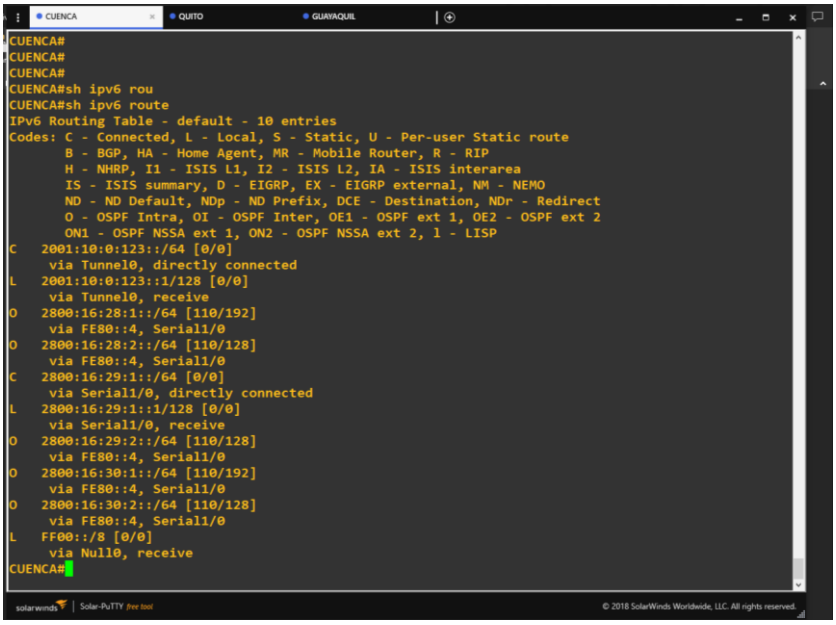
Figura 4. 1 Red propuesta y direccionamiento IPv6 sobre IPv6.



Elaborado por: Verónica Ortiz y Dennis López

En la Figura 4.1 se observa la red propuesta, el primer paso para comprobar que la red está configurada bajo el protocolo de enrutamiento OSPF es ingresar el comando sh ipv6 route.

Figura 4. 2 Comprobación de protocolo enrutamiento OSP sobre IPV6

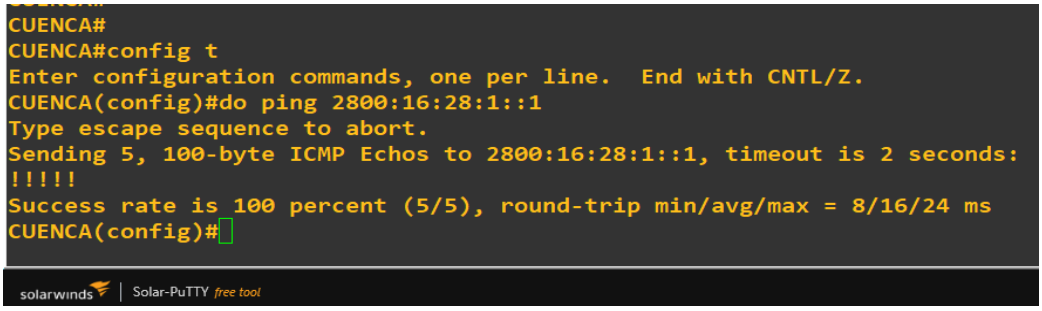


Fuente: GNS3

En la Figura 4.2 se presenta el resultado de la ejecución del comando show ipv6 *route* en el *router* 1, dando como resultado que las direcciones 2800:16:28:1::1/64 y 2800:16:30:1::1/64, correspondientes a los routers de Quito y Guayaquil respectivamente se encuentran conectados bajo un protocolo denominado O, que representa a OSPF como es posible apreciar en la parte superior de los códigos de la Figura 4.2.

El siguiente paso es verificar la conectividad de la *Underline*, debido a que, si no existe conectividad, los túneles DMVPN no pueden ser levantados. Para verificar dicha conectividad se envía paquetes desde las distintas sucursales de la UPS como se observa a continuación.

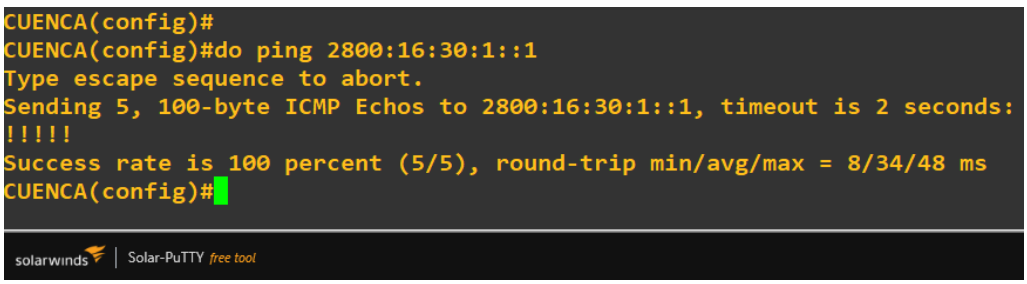
Figura 4.3 Verificación de conectividad Cuenca-Quito



Fuente: GNS3

En la Figura 4.3 se observa la conectividad de la Sede de Cuenca con la sede de Quito, para ello se ejecutó el comando do ping, seguido de la dirección que corresponde hacia donde se requiere realizar la verificación, en este caso es la dirección 2800:16:28:1::1, correspondiente a la sede Quito. Se observa que se envió 5 paquetes, mismos que llegaron al *router* de Quito completos.

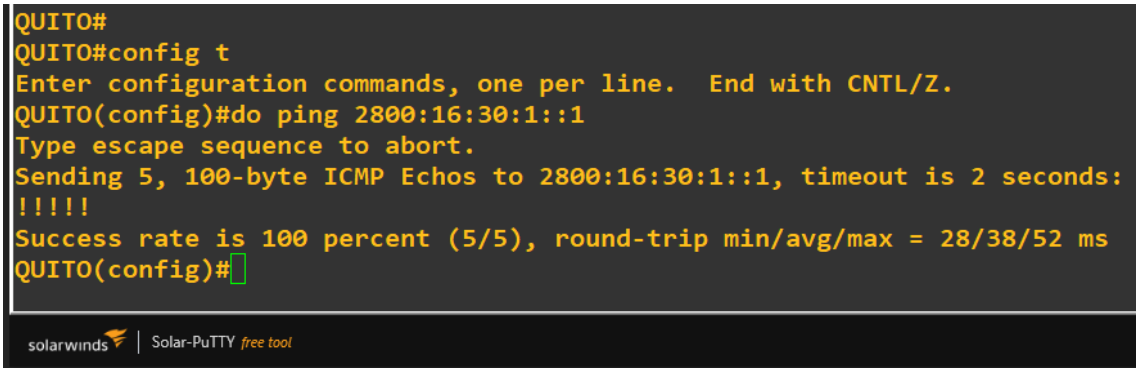
Figura 4.4 Verificación de conectividad Cuenca-Guayaquil



Fuente: GNS3

En la Figura 4.4 se observa la conectividad de la Sede de Cuenca con la sede de Guayaquil, para ello se ejecutó el comando do ping, seguido de la dirección que corresponde hacia donde se requiere realizar la verificación, en este caso es la dirección 2800:16:30:1::1, correspondiente a la sede Guayaquil. Se observa que se envió 5 paquetes, mismos que llegaron al *router* de Guayquil completos.

Figura 4.5 Verificación de conectividad Quito-Guayaquil



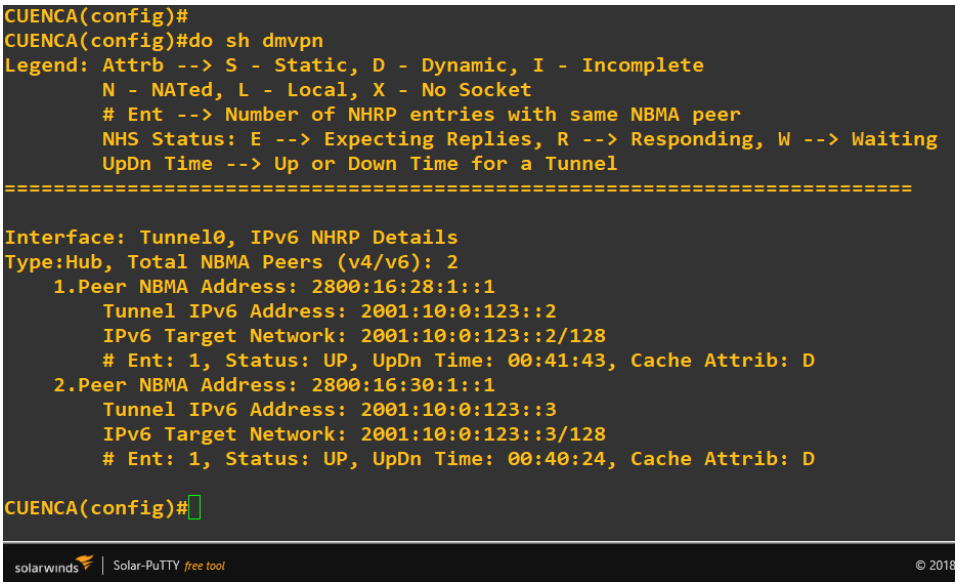
Fuente: GNS3

En la Figura 4.5 se observa la conectividad de la Sede de Quito con la sede de Guayaquil, para ello se ejecutó el comando do ping, seguido de la dirección que corresponde hacia donde se requiere realizar la verificación, en este caso es la dirección 2800:16:30:1::1, correspondiente a la sede Guayaquil. Se observa que se envió 5 paquetes, mismos que llegaron al router de Guayquil completos.

Una vez comprobada la conectividad en la Overlay se procede a verificar el funcionamiento de los túneles DMVPN entre sedes. En este caso el *router* que actúa como Hub es el de Cuenca, mientras que los *router* de Quito y Guayaquil son los *Spokes*.

En el hub se ejecuta el comando do *show dmvpn.*

Figura 4.6 Comprobación de túneles DMVPN HUB (Cuenca).

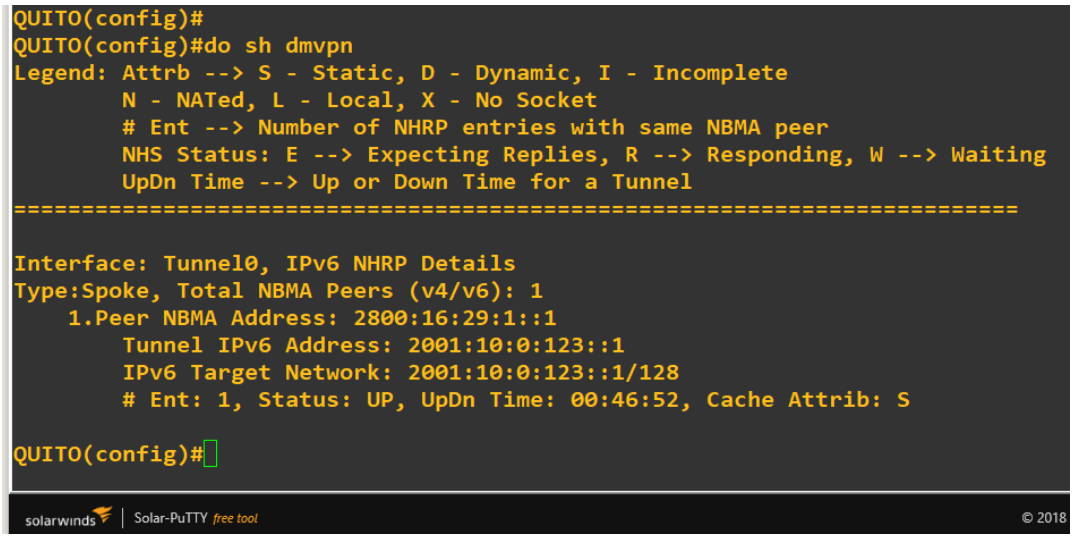


Fuente: GNS3

En la Figura 4.6 es posible constatar que se crean dos túneles de tipo D, la letra representa que el túnel es de tipo dinámico. Cada uno de los túneles con dirección 2001:10:0:123::2 y 2001:10:0:123::3, correspondientes a el *router* de Quito y Guayaquil respectivamente.

El siguiente paso es verificar los túneles creados en los *router* de Quito y Guayaquil. Para ello se ejecuta el comando do show *dmvpn* en cada *router* mencionado.

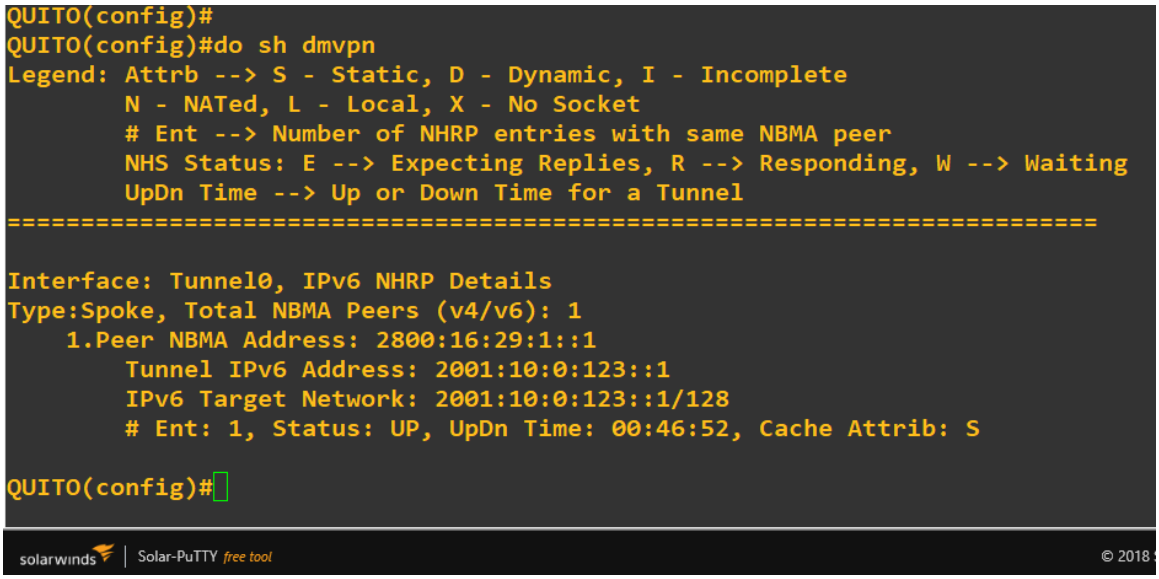
Figura 4.7 Comprobación de túnel DMVPN Spoke1 (Quito).



Fuente: GNS3

En la Figura 4.7 es posible comprobar que en el *router* de Quito se creó un túnel, pero con atributos S, la letra significa que es estático.

Figura 4.8 Comprobación de túnel DMVPN Spoke2 (Guayaquil).



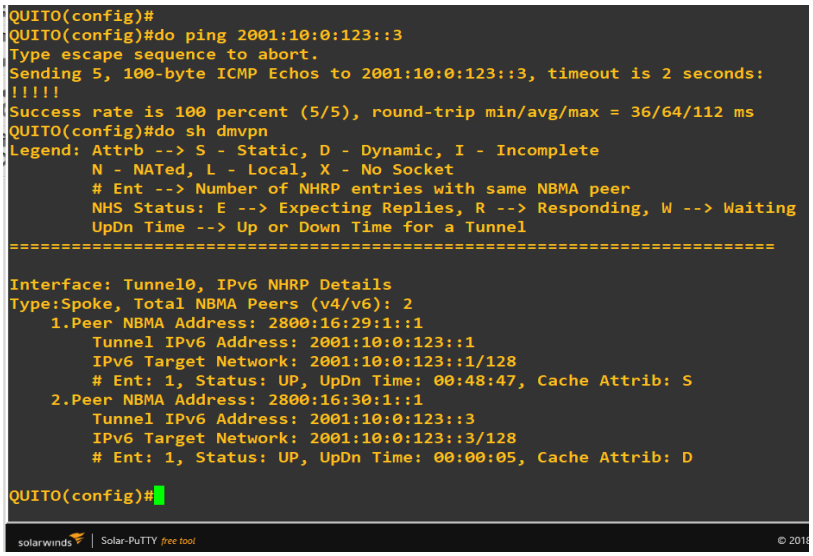
Fuente: GNS3

En la Figura 4.8 es posible comprobar que en el *router* de Guayaquil se creó un túnel, pero con atributos S, la letra significa que es estático.

Hasta este punto se comprobó que los túneles se encuentran levantados tanto en el Hub, como en los *Spokes*. Es similar a una configuración convencional de VPN. Sin embargo, la ventaja de configurar DMVPN es que los túneles se crean de forma dinámica y que es posible conectarse con cualquier *router* de la red de forma directa, sin pasar por el Hub.

Para comprobar esa funcionalidad es necesario enviar paquetes desde el router de Quito hacia el router de Guayaquil para que se establezca la conexión y se levante el túnel.

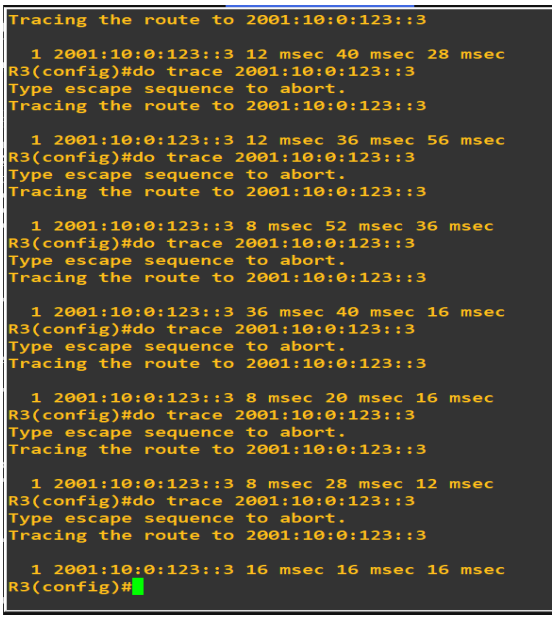
Figura 4.9 Comprobación de túnel entre Spoke1 (Quito) y Spoke2 (Guayaquil).



Fuente: GNS3

En la Figura 4.9 es posible observar que al momento de enviar tráfico desde el Spoke1 (Quito) al Spoke2 (Guayaquil) se crea un nuevo túnel, pero con características dinámicas. Es importante mencionar que no se realizó ninguna modificación en el Hub, tampoco en los *Spokes*. También es necesario comprobar los saltos que realiza la conexión para llegar desde el Spoke1 (Quito) al Spoke2 (Guayaquil), para ello se emplea el comando do trace seguido de la dirección del túnel de destino.

Figura 4.10 Comprobación de saltos entre Spoke1 (Quito) y Spoke2 (Guayaquil).

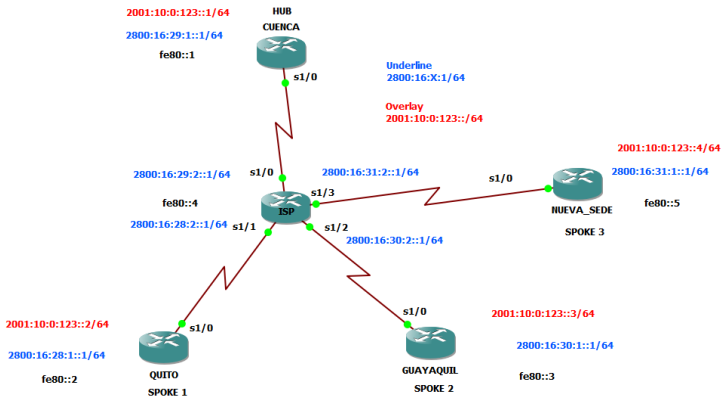


Fuente: GNS3

En la Figura 4.10 se observa que el siguiente salto para la conexión entre el Spoke1 (Quito) y Spoke2 (Guayaquil), es el Spoke2 (Guayaquil). Esto quiere decir que existe una comunicación directa entre *Spokes*, comprobando que él envió de tráfico no pasa por el Hub.

Es necesario comprobar que el ingreso de un nuevo Spoke, no afectara a la configuración del Hub para que el túnel funcione. Para ello se conecta un nuevo *Router* a la red.

Figura 4.11 Ingreso de un router (NUEVA SEDE) a la red.



Elaborado por: Verónica Ortiz y Dennis López

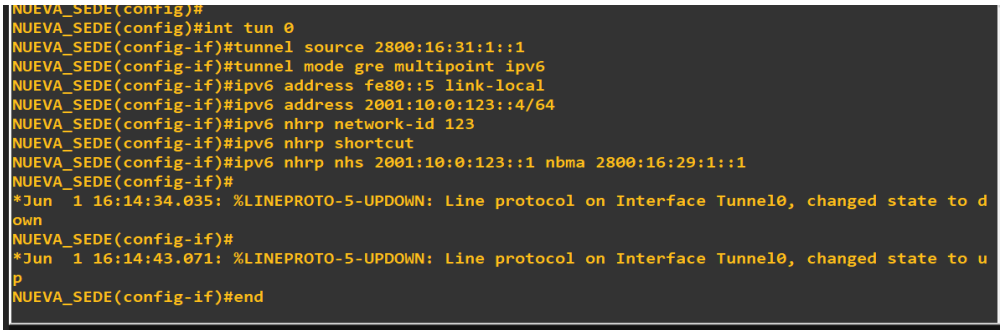
En la Figura 4.11 se observa que se conectó un nuevo router NUEVA SEDE a la red, para que este nuevo router pueda conectarse a la red y crear un túnel dinámico basta con configurar la Underline y la Overlay en el nuevo router.

Figura 4.12 Configuración underline R5 (NUEVA SEDE).

Fuente: GNS3

En la Figura 4.12 se observa la configuración de la Underline para el router 5 con su respectivo enrutamiento OSP.

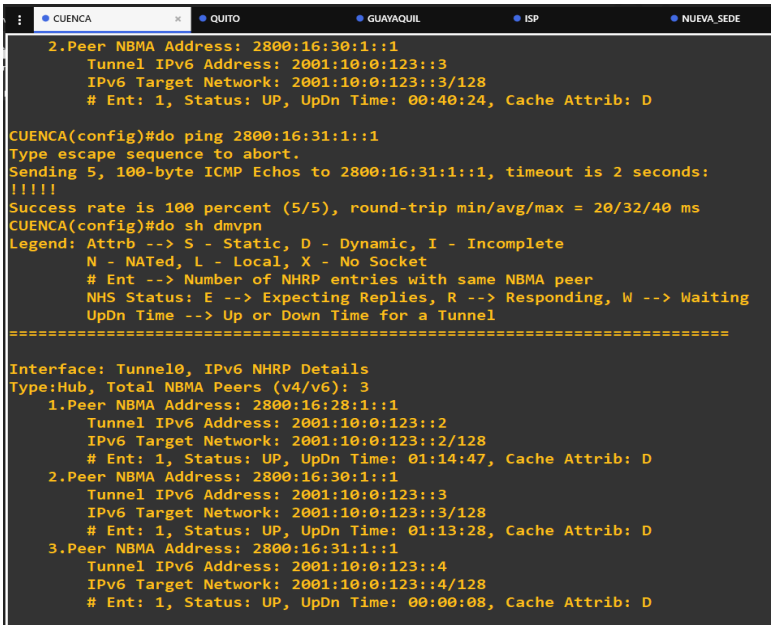
Figura 4.13 Configuración Overlay R5 (NUEVA SEDE).



Fuente: GNS3

En la Figura 4.13 se observa la configuración DMVPN del *router* 5 (NUEVA SEDE), es importante resaltar que para la configuración de este router únicamente se copió la configuración de cualquiera de los dos *Spokes* y se cambió la dirección del túnel y la dirección del recurso para la creación del mismo. Ahora es necesario comprobar que el túnel se creó de forma correcta, para ello se ejecutó el comando do *sh dmvpn* en el Hub y en la NUEVA SEDE.

Figura 4.14 Comprobación del Hub.



Fuente: GNS3

En la Figura 4.14 se observa que se creó un nuevo túnel con atributos dinámicos con la dirección 2001:10:0:123::4, correspondiente al nuevo *router* ingresado a la red. También es posible observar que los dos túneles antes creados siguen en funcionamiento de igual forma con atributos dinámicos.

A continuación, se procede a comprobar la conexión del *router* 5 (SEDE NUEVA), en este *router* se esperaría que se haya creado un túnel con atributos dinámicos, cuyo origen sea la dirección *Underline* del mismo *router* y que la dirección final sea la dirección del Hub.

Figura 4.15 Comprobación del Spoke 3.

```
NUEVA_SEDE(config)#
NUEVA_SEDE(config)#
NUEVA_SEDE(config)#do sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv6 NHRP Details
Type:Spoke, Total NBMA Peers (v4/v6): 1
    1.Peer NBMA Address: 2800:16:29:1::1
        Tunnel IPv6 Address: 2001:10:0:123::1
        IPv6 Target Network: 2001:10:0:123::1/128
        # Ent: 1, Status: UP, UpDn Time: 00:11:08, Cache Attrib: S

NUEVA_SEDE(config)#
```

Fuente: GNS3

En la Figura 4.15 es posible observa que efectivamente en el nuevo *router* conectado a la red se creó un túnel con atributos estáticos, que tiene como dirección final la dirección del HUB 2001:10:0:123::1/64. Ahora es necesario comprobar si es posible crear túneles dinámicos con los demás routers.

Figura 4.16 Comprobación de túnel entre Spoke3 (NUEVA SEDE) y Spoke1 (Quito).

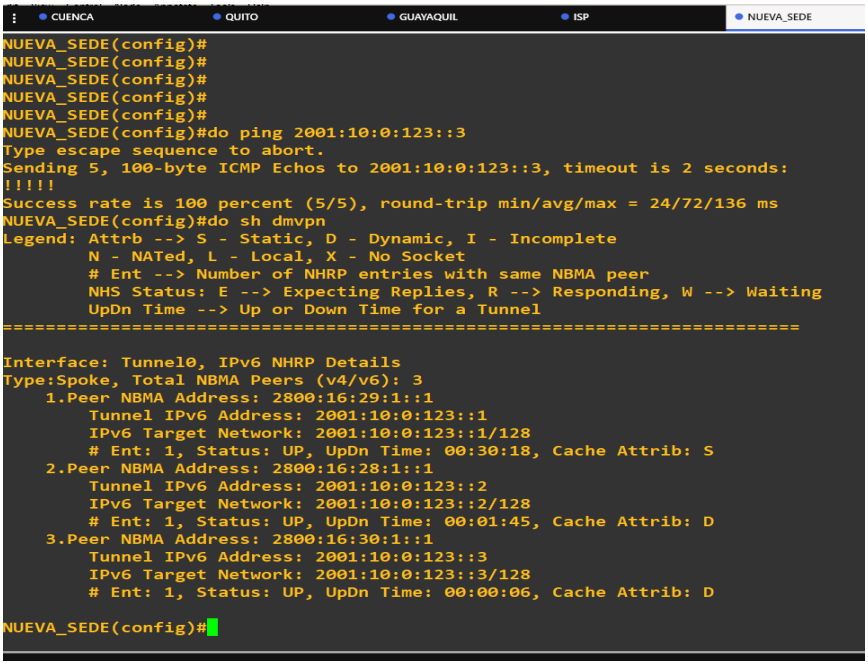
CUENCA | QUITO | GUAYAQUIL | ISP | NUEVA_SEDE

```
NUEVA_SEDE(config)#
NUEVA_SEDE(config)#
NUEVA_SEDE(config)#
NUEVA_SEDE(config)#
NUEVA_SEDE(config)#
NUEVA_SEDE(config)#
NUEVA_SEDE(config)#
NUEVA_SEDE(config)#
NUEVA_SEDE(config)#
NUEVA_SEDE(config)#do ping 2001:10:0:123::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:10:0:123::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/27/36 ms
NUEVA_SEDE(config)#do sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv6 NHRP Details
Type:Spoke, Total NBMA Peers (v4/v6): 2
    1.Peer NBMA Address: 2800:16:29:1::1
        Tunnel IPv6 Address: 2001:10:0:123::1
        IPv6 Target Network: 2001:10:0:123::1/128
        # Ent: 1, Status: UP, UpDn Time: 00:28:56, Cache Attrib: S
    2.Peer NBMA Address: 2800:16:28:1::1
        Tunnel IPv6 Address: 2001:10:0:123::2
        IPv6 Target Network: 2001:10:0:123::2/128
        # Ent: 1, Status: UP, UpDn Time: 00:00:23, Cache Attrib: D

NUEVA_SEDE(config)#
```

Fuente: GNS3

En la Figura 4.16 se observa que al enviar paquetes mediante el comando do ping hacia el spoke1 (Quito), se creó un túnel con características dinámicas. De igual forma se realizó el envío de paquetes hacia el Spoke2 (Guayaquil).

Figura 4.17 Comprobación de túnel entre Spoke3 (NUEVA SEDE) y Spoke2 (Guayaquil).



Fuente: GNS3

En la Figura 4.17 se observa que al enviar paquetes mediante el comando do ping desde el nuevo *router* R5(SEDE NUEVA) hacia el spoke2(Guayaquil), se creó un túnel con características dinámicas.

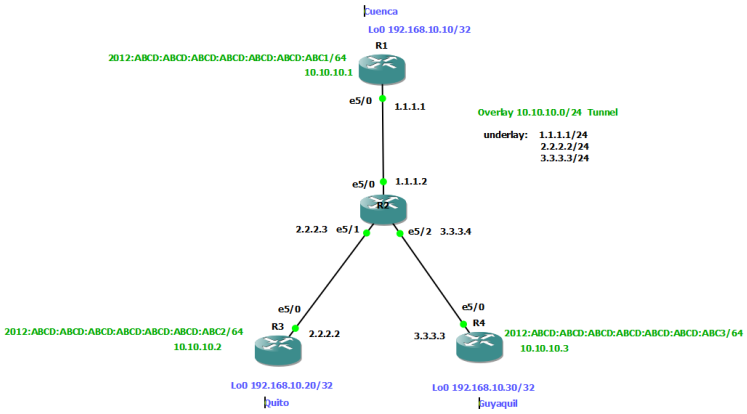
De esta forma se comprobó que, al ingresar un nuevo dispositivo a la red, es necesario configurar el nuevo dispositivo en base a la configuración de uno de los *Spokes* que se encuentra en funcionamiento. Es importante recalcar que no se requiere ninguna configuración extra en el Hub para que el nuevo dispositivo funcione.

4.2 Escenario 2

4.2.1 Configuración de la red con enrutamiento EIGRP sobre IPV4 y DVPN sobre ipv6.

La red propuesta consta de 4 routers, los tres que representan a cada una de las sucursales de la UPS y un *router* que representa al proveedor de internet. Es posible configurar esta red con un protocolo de enrutamiento en la *Underline*, para sobre ese protocolo configurar DMVPN. En este caso se configuro EIGRP para IPV4, para ello es necesario tomar en cuenta que se necesita un *router* con una IOS que soporte IPV4 de forma nativa. Además, los túneles multipunto se configuraron con direcciones IPV6, es decir que se tiene la configuración de la *Underline* con IPV4 y la configuración de la *Overlay* es IPV6 (IPv6 sobre IPV4).
La red Propuesta con las direcciones que se emplearon se presenta a continuación.

Figura 4.18 Red propuesta y direccionamiento IPv6 sobre IPv4.

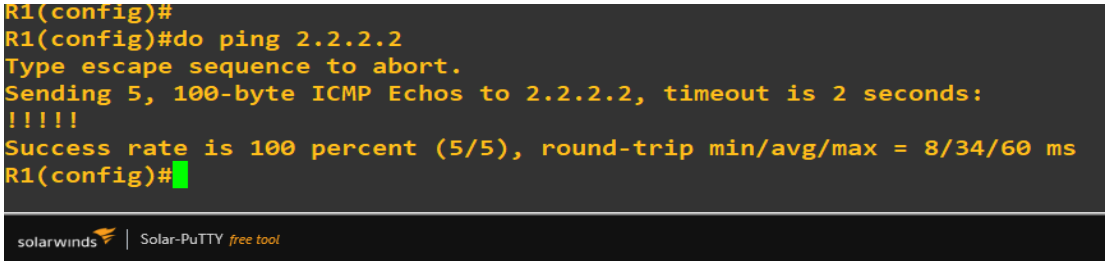


Elaborado por: Verónica Ortiz y Dennis López

En la Figura 4.18 se observa la red propuesta, para la configuración de EIGRP se la hace posterior a la configuración de los túneles DMVPN.

El primer paso es verificar la conectividad de la *Underline*, debido a que, si no existe conectividad, los túneles DMVPN no pueden ser levantados. Para verificar dicha conectividad se envía paquetes desde las distintas sucursales de la UPS como se observa a continuación.

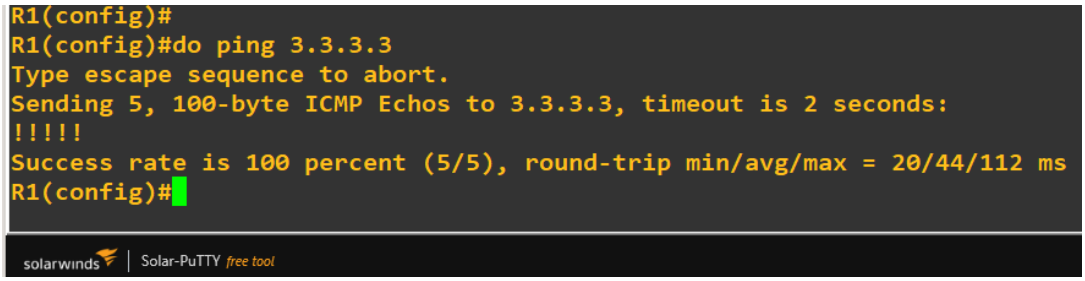
Figura 4.19 Verificación de conectividad Cuenca-Quito IPv4



Fuente: GNS3

En la Figura 4.19 se observa la conectividad de la Sede de Cuenca con la sede de Quito, para ello se ejecutó el comando do ping, seguido de la dirección que corresponde hacia donde se requiere realizar la verificación, en este caso es la dirección 2.2.2.2, correspondiente a la sede Quito. Se observa que se envió 5 paquetes, mismos que llegaron al *router* de Quito completos.

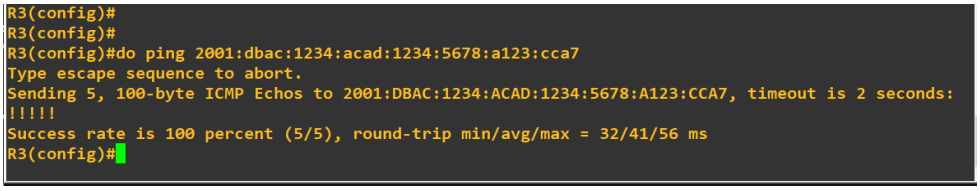
Figura 4.20 Verificación de conectividad Cuenca-Guayaquil IPv4



Fuente: GNS3

En la Figura 4.20 se observa la conectividad de la Sede de Cuenca con la Sede de Guayaquil, para ello se ejecutó el comando *do ping*, seguido de la dirección que corresponde hacia donde se requiere realizar la verificación, en este caso es la dirección 3.3.3.3, correspondiente a la Sede Guayaquil. Se observa que se envió 5 paquetes, mismos que llegaron al *router* de Guayaquil completos.

Figura 4.21 Verificación de conectividad Quito-Guayaquil IPv4



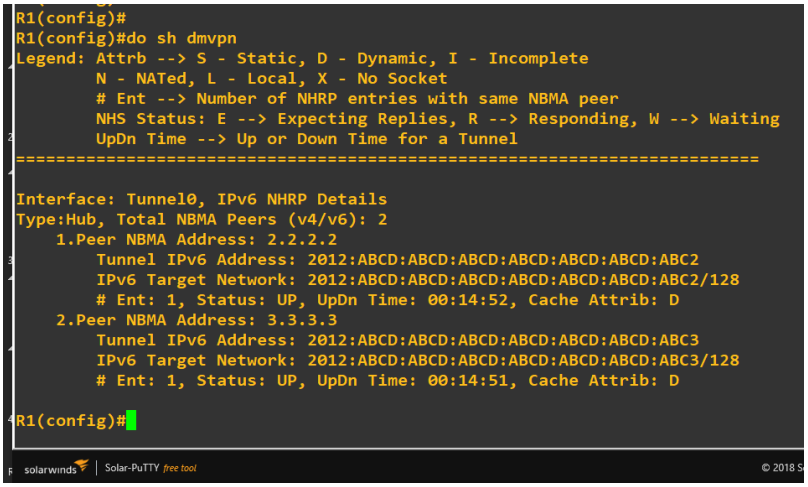
Fuente: GNS3

En la Figura 4.21 se observa la conectividad de la Sede de Quito con la Sede de Guayaquil, para ello se ejecutó el comando *do ping*, seguido de la dirección que corresponde hacia donde se requiere realizar la verificación, en este caso es la dirección 3.3.3.3, correspondiente a la Sede Guayaquil. Se observa que se envió 5 paquetes, mismos que llegaron al *router* de Guayaquil completos.

Una vez comprobada la conectividad en la *Overlay* se procede a verificar el funcionamiento de los túneles DMVPN entre sedes. En este caso el *router* que actúa como Hub es el de Cuenca, mientras que los *router* de Quito y Guayaquil son los *Spokes*.

En el hub se ejecuta el comando do show dmvpn.

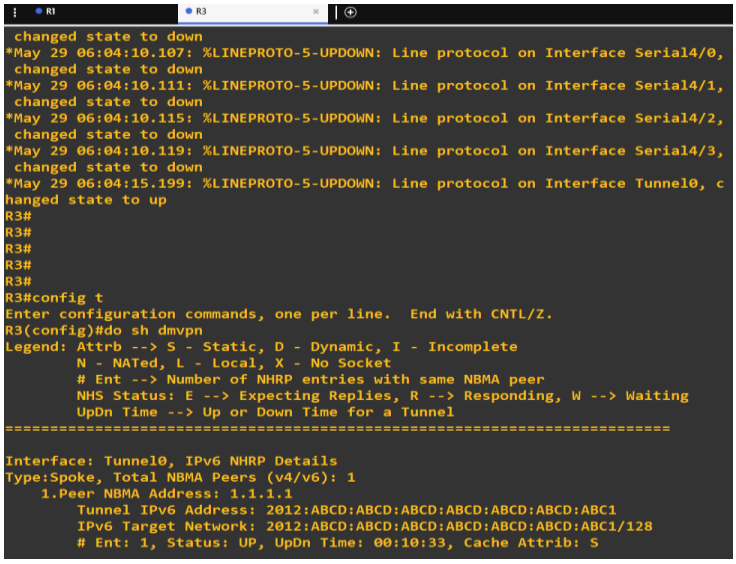
Figura 4.22 Comprobación de túneles DMVPN HUB (Cuenca).



Fuente: GNS3

En la Figura 4.22 es posible constatar que se crean dos túneles de tipo D, la letra quiere decir que son de tipo dinámico. Cada uno de los túneles con dirección 2012: ABCD: ABCD:ABCD:ABCD:ABCD:ABCD:ABC2 y 2012 :ABCD: ABCD: ABCD: ABCD:ABCD:ABCD:ABC3, correspondientes al *router* de Quito y Guayaquil respectivamente. Es importante notar que la dirección NBMA corresponde a direcciones IPv4. El siguiente paso es verificar los túneles creados en los *router* de Quito y Guayaquil. Para ello se ejecuta el comando *do show dmvpn* en cada *router* mencionado

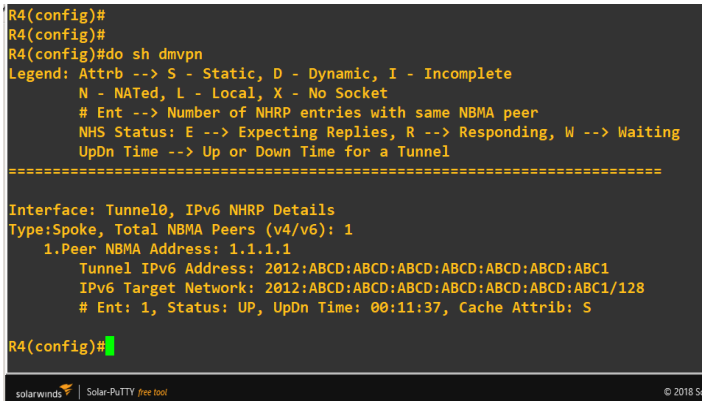
Figura 4.23 Comprobación de túnel DMVPN Spoke1 (Quito).



Fuente: GNS3

En la Figura 4.23 es posible comprobar que en el *router* de Quito se creó un túnel, pero con atributos S, la letra significa que es estático.

Figura 4.24 Comprobación de túnel DMVPN Spoke2 (Guayaquil)



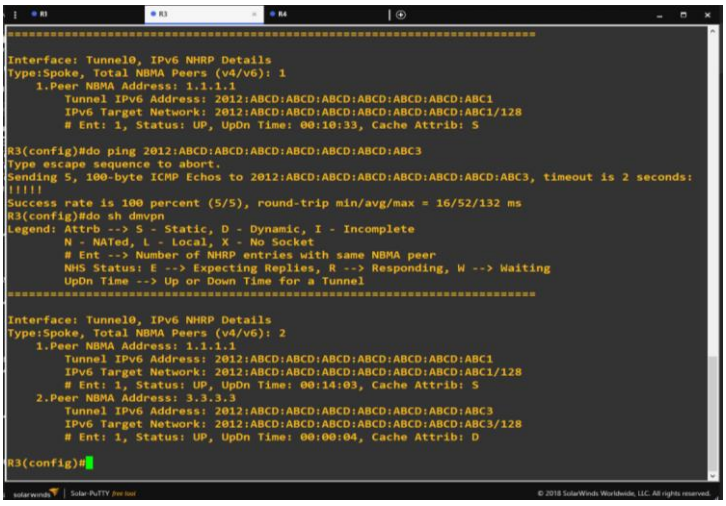
Fuente: GNS3

En la Figura 4.24 es posible comprobar que en el *router* de Guayaquil se creó un túnel, pero con atributos S, la letra significa que es estático.

Hasta este punto se comprobó que los túneles se encuentran levantados tanto en el Hub, como en las *Spokes*. Es similar a una configuración convencional de VPN. Sin embargo, la ventaja de configurar DMVPN es que los túneles se crean de forma dinámica y que es posible conectarse con cualquier router de la red de forma directa, es decir sin pasar por el Hub.

Para comprobar esa funcionalidad es necesario enviar paquetes desde el router de Quito hacia el router de Guayaquil para que se establezca la conexión y se levante el túnel.

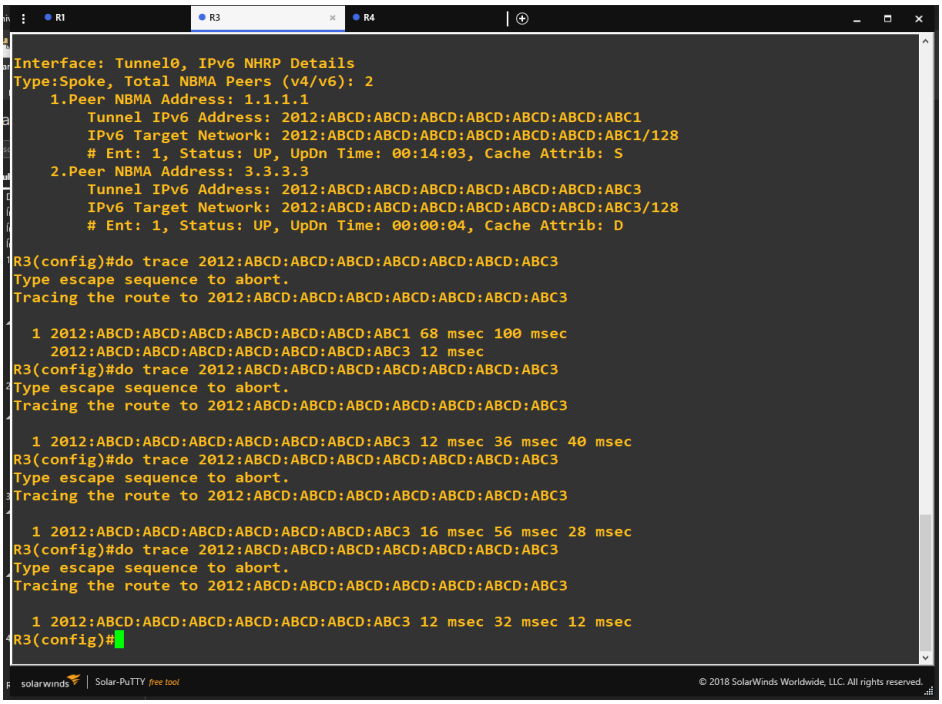
Figura 4.25 Comprobación de túnel entre Spoke1 (Quito) y Spoke2 (Guayaquil).



Fuente: GNS3

En la Figura 4.25 es posible observar que al momento de enviar tráfico desde el Spoke1 (Quito) al Spoke2 (Guayaquil) se crea un nuevo túnel, pero con características dinámicas. Es importante mencionar que no se realizó ninguna modificación en el Hub, tampoco en los *Spokes*, además que las direcciones NBMA son IPv4. También es necesario comprobar los saltos que realiza la conexión para llegar desde el Spoke1 (Quito) al Spoke2 (Guayaquil), para ellos se emplea el comando *do trace* seguido de la dirección del túnel de destino.

Figura 4.26 Comprobación de saltos entre Spoke1 (Quito) y Spoke2 (Guayaquil) IPv4.



Fuente: GNS3

En la Figura 4.26 se observa que el siguiente salto para la conexión entre el Spoke1 (Quito) y Spoke2 (Guayaquil), es el Hub en primera instancia, pero en el segundo trace que se ejecuta el siguiente salto es directamente el Spoke2 (Guayaquil). Esto quiere decir que existe una comunicación directa entre *Spokes*, es decir el envío de tráfico no pasa por el Hub.

CONCLUSIONES

Según los resultados obtenidos en el capítulo 4 y la configuración de la red en el capítulo 3, se demostró que la implementación de DMVPN sobre IPv6 es factible, puesto que se dispone de recursos necesarios para la comprobación del funcionamiento, entre los recursos mencionados se encuentra la IOS del *router* 7200, mismo que fue esencial para configurar la red mGRE con direccionamiento IPV6 y brindar la confidencialidad de los datos de la UPS. Además, él envió de paquetes usados para las pruebas de funcionamiento pueden ser datos personales o cualquier tipo de información sobre una institución Pública o Privada.

El primer escenario planteado para la implementación de DMVPN es posible realizarlo, siempre y cuando la red cuente con la infraestructura que posee los requerimientos mínimos, es decir que poseer un *router* que soporte *mGre* en IPv6 nativa

Al configurar DMVPN tanto en el escenario 1 como en el escenario 2, se comprobó que, a diferencia de los VPN convencionales, la configuración del Hub y los *Spokes* se reducen de forma significativa, lo que implica que los equipos que se emplean no tengan que ser tan robustos para su funcionamiento. Además, también fue posible comprobar que el ingresar un nuevo Spoke a la red, este no afecta a la configuración del Hub. Es necesario configurar el Spoke en base a uno de los *Spokes* operativos, lo que reduce tiempo y complejidad en la configuración.

Es posible configurar DMVPN IPv6 sobre IPv6, también IPv6 sobre IPv4, lo que permitió comprobar que, con el direccionamiento actual de algunas sedes de la UPS en IPv4 es posible implementar Ipv6 sobre IPv4, para no reemplazar los dispositivos existentes por unos que soporten mGRE de forma nativa.

La configuración de la red DMVPN permite una escalabilidad bastante notable como se lo comprobó en el escenario 1, puesto que al crear túneles de forma dinámica no se requiere una configuración compleja para un caso donde se tenga un número muy grande de *spokes.*

RECOMENDACIONES

DMVPN emplea un protocolo *mGRE* que no se ha explorado de forma completa, debido a que existe una limitante en cuanto a los equipos. En una red es necesario que los *routers* soporten el protocolo *mGRE,* adicionalmente la migración de entornos de IPv4 a IPv6 provoca una necesidad, en cuanto a los *routers* debido a que deberían soportar *mGRE* para ipv6 Nativa, por lo que se recomienda comprobar si para versiones más bajas a la 7200 de Cisco es posible implementar *mGRE* sobre IPv6, con la finalidad de comprobar si empresas pequeñas podrían implementar DMVPN, puesto que el uso de *routers* inferiores al 7200 implica un menor costo.

Se recomienda realizar un análisis de calidad de servicio *mGRE,* bajo un protocolo *MPLS,* de esta forma se tendría un escenario en donde existe una velocidad de transferencia alta, estrechamente ligado a la calidad del servicio.

REFERENCIAS BIBLIOGRAFICAS

Cisco.com. (s.f.). Obtenido de https://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/prod_presentation0900aecd80313c9d.pdf

Dominguez Ayala, J. C. (2017). *Diseño e implementación de un prototipo de transacción de direccionamiento IPV4 a IPV6 en la red de la Universidad Politécnica Salesiana*. Quito.

Estrada, A. (10 de 10 de 2014). *Protocolo TCP/IP de Internet*. Obtenido de Revista.unam.mx: http://www.revista.unam.mx/vol.5/num8/art51/sep_art51.pdf

Garcia, L. (2014). *IPSEC*. Obtenido de http://slideplayer.es/slide/159908/

IBM Knowledge Center. (s.f.). Obtenido de Ibm.com: https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_72/rzajw/rzajwosp f.htm

IGP: Definición. (s.f.). Obtenido de https://es.ccm.net/faq/9462-igp-definicion

IPSec - IPv6 - Proyectos. (10 de enero de 2014). Obtenido de Proyectos.ingeniovirtual.com.ar: https://proyectos.ingeniovirtual.com.ar/projects/ipv6/wiki/IPSec

IPsec. Volumen II : AH (Cabecera de autenticación). (20 de 11 de 2011). Obtenido de RedesZone: https://www.redeszone.net/2011/08/30/ipsec-volumen-ii-ah-cabecera-de-autenticacion/

Materias.fi.uba.ar. (s.f.). Obtenido de http://materias.fi.uba.ar/7543/download/conf_gre.pdf

Schertler, M. S. (Agosto de 2005). *Rfc-es.org*. Obtenido de Protocolo de Gestión de Claves y Asociaciones de Seguridad en Internet (ISAKMP): http://www.rfc-es.org/pendientes/rfc2408-es.txt

TCP/IP. (s.f.). Obtenido de CCM: https://es.ccm.net/contents/282-tcp-ip

Tejada Zúñiga, K. K., León Guerrero, S. K., & Astudillo Avila, C. R. (06 de 07 de 2018). *Diseño de una intranet usando tecnología VPN (Virtual Private Network), que comunique la matriz de SECOHI con sus oficinas sucursales y que además permita el acceso remoto de usuarios móviles.* Obtenido de http://www.dspace.espol.edu.ec/xmlui/handle/123456789/43982

What is Next Hop Resolution Protocol (NHRP)? - Definition from WhatIs.com. (s.f.). Obtenido de SearchNetworking: https://searchnetworking.techtarget.com/definition/Next-Hop-Resolution-Protocol