UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE ELECTROTECNIA Y COMPUTACIÓN

Trabajo monográfico para optar al título de Ingeniería Electrónica y Telecomunicaciones.

Tema:

“Diseño de una Red Privada Virtual Dinámica Multipunto (DMVPN) para renovar la tecnología WAN de la empresa Megabyte S.A”

Autores:

Br. Denis Alfonso Cruz Martínez **No. Carnet:** 2010-32602-Eo

Br. Cristhyan Javier Cardoza Latino **No. Carnet:** 2010-35149-Tc

Br. Katherine Sofía Espinoza Herrera **No. Carnet:** 2012-41118-Eo

Tutor:

Ing. Marlovio José Sevilla Hernández

Managua, Nicaragua, junio de 2023

Dedicatoria

A Dios principalmente, por la fuerza y sabiduría que nos brindó para poder culminar este trabajo.

A nuestras familias, quienes siempre confiaron y apoyaron de manera incondicional, en cada paso y decisión tomada.

Por último, queremos dedicar este trabajo a todos aquellos que han contribuido en nuestra formación académica y personal.

Resumen

En el presente trabajo, se tuvo como finalidad el diseño y emulación de la red DMVPN, para renovar y modernizar la tecnología WAN con la cual opera actualmente la empresa Megabyte S.A., la cual se encuentra ubicada en la ciudad de Managua. Esta empresa se encuentra en proceso de crecimiento y de aperturas de distintas sucursales a lo largo del país. Para dar solución a este tipo de problemas de conectar distintas sucursales ubicadas geográficamente distantes entre sí, los proveedores de ISP optan por la tecnología MPLS lo cual crea una limitante, ya que la mayoría de los ISP no poseen cobertura en todo el territorio nacional.

Con el fin de brindar una solución de conectividad a través de diferentes ISP, se propone realizar el diseño y creación de una topología de red por medio del software GNS3, en donde se instalaron las imágenes IOS de equipos cisco reales. El tipo de topología que se utilizo fue Hub-Spoke en la cual se implementó los protocolos de tunelización mGRE, que en conjunto con el protocolo NHRP nos permite tener una conexión dinámica, multipunto. La implementación del protocolo IPsec nos proporciona una conexión segura al momento del envío de datos a través de la red pública. Para el enrutamiento se utilizó el protocolo OSPF, ya que es un protocolo escalable el cual permite el intercambio de información de la topología entre los routers en la red.

Debido a que en este trabajo solo se abarca el diseño de la red DMVPN para la empresa Megabyte S.A, se evaluaron diferentes soluciones técnicas para la empresa. Por otra parte, se elaboró un plan o guía de implementación con el fin de que la empresa realice un correcto despliegue de la tecnología DMVPN, dicha guía de implementación esta detallada con los comandos utilizados, en conjunto con su funcionalidad, para cada router utilizado en el diseño de la red de la empresa.

Índice de contenido

1. Introducción 1

2. Objetivos 3

2.1 Objetivo General 3

2.2 Objetivos Específicos 3

3. Justificación 4

4. Marco Teórico 5

4.1 Definición de una red privada virtual (VPN) 5

4.1.1 Requerimientos para la implementación de VPN 5

4.1.2 Bases de Túnel. 6

4.1.3 Clasificación de una VPN. 7

4.1.4 Topología en las VPN. 9

4.1.5 Protocolos VPN. 10

4.1.5.1 Protocolo túnel punto a punto (PPTP)……...10

4.1.5.2 Protocolo de túnel de capa 2 (L2PT) ……10

4.1.5.3 Protocolo de seguridad de Internet (IPsec)……..……11

4.1.5.3.1 Servicios de seguridad de IPsec……11

4.1.5.3.2 Protocolos de seguridad usados por IPsec……12

4.1.5.3.3 Protocolo de control Internet Key Exchange – IKE..... 15

4.1.5.3.4 Estructura de IPsec……16

4.2 Red Privada Virtual Multipunto (DMVPN)..... 18

4.2.1 Características de DMVPN. 19

4.2.2 Topología de diseño DMVPN. 20

4.2.3 Arquitectura DMVPN 22

4.3 Protocolo de enrutamiento. 26
4.3.1 Enrutamiento estático. 26
4.3.2 Enrutamiento dinámico. 27
5. Diseño metodológico. 31
5.1. Metodología. 31
6. Análisis de la situación actual. 33
7. Diseño de la Red DMVPN. 37
7.1 Infraestructura de la red. 38
7.1.2 Diseño de la red física. 38
7.1.3 Diseño de la red lógica..... 41
7.2. Evaluación de costo financiero de la implementación de DMVPN. 43
8. Guía de implementación de la red DMVPN. 51
8.1 Instalación de software para la emulación. 51
8.2 Configuración de los equipos. 54
8.3 Cronograma de trabajo para la implementación de DMVPN. 82
9. Conclusiones 85
10. Recomendaciones 86
11. Bibliografía 87
12. Anexos 91
Código de la red DMVPN. 91

Índice de tablas

Tabla 1. Requerimientos implementación VPN 6

Tabla 2. Ventajas vs Desventajas OSPF. 29

Tabla 3. Listados de equipos. 39

Tabla 4. Características y Beneficios Router Cisco867. 40

Tabla 5. Tabla direccionamiento LAN. 42

Tabla 6. Tabla direccionamiento WAN. 42

Tabla 7. Tabla direccionamiento mGRE. 43

Tabla 8. Costo implementación MPLS 44

Tabla 9. Costo servicio de internet más alquiler de dispositivos 45

Tabla 10. Costo de servicio de internet. 46

Tabla 11. Inversión inicial, implementación DVMP……46

Tabla 12. Características de los routers. 47

Tabla 13. Características de los switches 48

Tabla 14. Servicio internet con equipos propios. 50

Tabla 15. Requerimientos GNS3. 52

Tabla 16. Requerimientos VMware Workstation. 53

Índice de figuras

Figura 1. Túnel punto a punto. 7

Figura 2. Encabezado IP túnel VPN. 9

Figura 3. Estructura de un datagrama 13

Figura 4. Estructura de datagrama ESP 14

Figura 5. Estructura de marco de trabajo 17

Figura 6. Encabezado IPsec. Modo transporte 17

Figura 7. Encabezado IPsec. Modo túnel 18

Figura 8. Modelo de Hub-Spoke. 21

Figura 9. Modelo de Spoke-Spoke. 22

Figura 10. Funcionamiento protocolo NHRP. 24

Figura 11. Protocolos de enrutamiento dinámico. 27

Figura 12. Datagrama OSPF. 30

Figura 13. Insatalaciones empresa Megabyte S.A 33

Figura 14. Oficinas empresa Megabyte S.A 33

Figura 15. Recepción empresa Megabyte S.A 34

Figura 16. Router de la empresa Megabyte S.A 35

Figura 17. Router cisco867 39

Figura 18. Cisco Catalyst 2960 Series Switches. 40

Figura 19. Topología Hub & Spoke empresa Megabyte. 41

Figura 20. Direcciones IP de la red DMVPN. 43

Figura 21. Presupuesto para la implementación DMVPN. 49

Figura 22. Configuración interfaz WAN Managua_Hub_1. 55

Figura 23. Configuración interfaz WAN Managua_Hub_2. 55

Figura 24. Configuración interfaz WAN Masaya_Spoke_1. 55

Figura 25. Configuración interfaz WAN Chinandega_Spoke_2. 55
Figura 26. Configuración interfaz WAN Matagalpa_Spoke_3. 56
Figura 27. Configuración de las interfaces WAN del ISP. 56
Figura 28. Conectividad Hub-Spoke_1. 57
Figura 29. Conectividad Hub-Spoke_2. 57
Figura 30. Conectividad Hub-Spoke_3. 57
Figura 31. Configuración interfaz LAN y NAT Managua_Hub_1. 58
Figura 32. Configuración interfaz LAN y NAT Managua_Hub_2. 59
Figura 33. Configuración interfaz LAN y NAT Masaya_Spoke_1. 59
Figura 34. Configuración interfaz LAN y NAT Chinandega_Spoke_2. .. 59
Figura 35. Configuración interfaz LAN y NAT Matagalpa_Spoke_3. 60
Figura 36. Configuración DHCP Managua_Hub_1. 60
Figura 37. Configuración DHCP Managua_Hub_2. 61
Figura 38. Configuración DHCP Masaya_Spoke_1. 61
Figura 39. Configuración DHCP Chinadega_Spoke_2. 61
Figura 40. Configuración DHCP Matagalpa_Spoke_3. 61
Figura 41. Configuración IP SLA Managua_Hub_1. 62
Figura 42. Configuración HSRP Managua_Hub_1. 63
Figura 43. Configuración HSRP Managua_Hub_2. 63
Figura 44. Validación alta disponibilidad Hub_1. 64
Figura 45. Validación alta disponibilidad Hub_2. 64
Figura 46. Configuración mGRE Managua_Hub_1. 65
Figura 47. Configuración mGRE Managua_Hub_2. 65
Figura 48. Configuración mGRE Masaya_Spoke_1. 65
Figura 49. Configuración mGRE Chinandega_Spoke_2. 65

Figura 50. Configuración mGRE Matagalpa_Spoke_3. 66
Figura 51. Configuración NHRP Managua_Hub_1. 67
Figura 52. Configuración mGRE Managua_Hub_2. 67
Figura 53. Configuración mGRE Masaya_Spoke_1. 68
Figura 54. Configuración mGRE Chinandega_Spoke_2. 68
Figura 55. Configuración mGRE Matagalpa_Spoke_3. 68
Figura 56. Configuración OSPF Managua_Hub_1. 69
Figura 57. Configuración OSPF Managua_Hub_2. 69
Figura 58. Configuración OSPF Masaya_Spoke_1. 69
Figura 59. Configuración OSPF Chinandega_Spoke_2. 70
Figura 60. Configuración OSPF Matagalpa_Spoke_3. 70
Figura 61. Configuración IPsec Managua_Hub_1. 71
Figura 62. Tunnel en función GRE multipunto. 72
Figura 63. Estado del tunnel. 72
Figura 64. Validación NHRP. 73
Figura 65. Validación NHRP spoke to spoke. 74
Figura 66. WAN Masaya paquete request. 74
Figura 67. WAN Managua paquete request. 75
Figura 68. WAN Matagalpa paquete reply, ... 75
Figura 69. WAN Masaya paquete reply. 76
Figura 70. Validación DMVPN. 76
Figura 71. Validación DMVPN en Spokes. 77
Figura 72. Validación DMVPN. 77
Figura 73. Validación OSPF y NHRP. 78
Figura 74. Tabla de enrutamiento OSPF. 79

Figura 75. Validación de adyacencia. 79
Figura 76. Estado del enlace enrutado. 79
Figura 77. Validación IPsec. 80
Figura 78. Primera fase IPsec. 80
Figura 79. Tráfico por tunnel en Managua_Hub_1. 81
Figura 80. Validación de los estados túneles IPsec. 81
Figura 81. Trafico interfaz WAN Managua_Hub_1. 82
Figura 82. Implementación casa matriz. 83
Figura 83. Implementación Masaya. 83
Figura 84. Implementación Chinandega. 83
Figura 85. Implementación Matagalpa 84

1. Introducción

En la actualidad los ISP (Internet Service Provider) en nuestro país ofertan diferentes tipos de tecnologías para ser implementadas como servicios de redes de área amplia (WAN) para las pequeñas y medianas empresas (PYMES) y clientes corporativos. Los ISP cuentan con una red desplegada y disponen de tecnologías como radioenlaces, cableado de fibra óptica, cobre, etc., con el fin de brindar soluciones WAN entre las cuales encontramos ofertas de línea arrendadas como enlaces punto a punto, redes de datos MPLS (Multiprotocol Label Switching) para conectar de dos o más sucursales PYMES o clientes corporativos. Este tipo de soluciones no suelen ser escalables, flexibles ni convergentes, lo que resulta un problema debido a que las empresas corporativas y las PYMES demandan en la actualidad una red escalable y centralizada. Por otra parte, las soluciones WAN punto a punto suelen ser más costosas ya que el precio del arrendamiento se incrementa al momento de añadir una nueva sucursal.

Debido a los altos costos que los proveedores de ISP han establecido en este mercado, muchas de las empresas optan por usar una red de acceso pública, como internet, para conectar sus sucursales, ya que el acceso a internet tiene un costo accesible y en la mayoría de los casos toda PYME o cliente corporativo cuentan con este servicio. Muchos de los Clientes corporativos ante la necesidad de obtener mayor seguridad en su red, optan por implementar túneles VPN estáticos tradicionales como punto a punto, pero esto genera problemas de administración de red al momento de agregar o retirar una sucursal, ya que esto implica realizar cambios en la configuración de la red.

Por ese motivo, este trabajo monográfico tiene como finalidad dar una solución diferente a las VPN punto a punto, y evaluar el desempeño de la técnica de una Red Privada Dinámica Virtual Multipunto (DMVPN) para la empresa Megabyte

S.A, dicha empresa se encuentra en crecimiento y están en proceso de apertura de nuevas sucursales a lo largo del país. Mediante este proyecto se comprobará y verificará por medio de emulación, que la tecnología DMVPN brindará datos teóricos y prácticos sobre el desempeño de la misma, como mejora de envío de paquetes con menor latencia y con mayor seguridad, esto mediante algoritmos de cifrado y descifrado, los cuales proporcionan confiabilidad, integridad y autenticación de datos enviados sobre la red pública de internet. Por otro lado, permitirá a los administradores de la red obtener una solución detallada y comprobada para la transmisión de los servicios en tiempo real.

2. Objetivos

2.1 Objetivo General

- Diseñar una Red Privada Virtual Dinámica Multipunto (DMVPN) con el propósito de renovar la tecnología WAN de la empresa Megabyte S.A.

2.2 Objetivos Específicos

- Analizar el estado de la red actual de la empresa Megabyte S.A, con el fin de modernizar su tecnología WAN, para proveer escalabilidad, seguridad y alta disponibilidad a la misma.

- Evaluar el costo financiero que tendrá el despliegue de la tecnología basada en túneles DMVPN, en comparación con la tecnología de arrendamiento dedicado MPLS.

- Realizar pruebas para verificar funcionalidad y alta disponibilidad del despliegue de la tecnología DMVPN usando el software GNS3, en función los protocolos resolución de siguiente salto NHRP, tunelización mGRE, seguridad IPsec y enrutamiento dinámico OSPF.

- Elaborar plan de implementación detallado para desplegar la tecnología DMVPN y sus funciones en un ambiente de alta disponibilidad.

3. Justificación

Los administradores de redes al implementar el diseño de DMVPN lograrán tener una interconexión entre todas sus sucursales, y de esta manera poder transmitir información de forma rápida, eficiente, segura y a un menor precio. Para la implementación de esta tecnología solo necesitaremos una conexión a internet, de esta manera se tendrá un ahorro económico significativo en comparativa con otras tecnologías WAN que se ofertan en el mercado.

La empresa Megabyte S.A. que se dedica a la venta de aparatos electrónicos, tiene su casa matriz ubicada en la ciudad de Managua, y tiene como proyecto realizar la apertura de nuevas sucursales en las ciudades de Masaya, Chinandega y Matagalpa. Con el uso de la tecnología DMVPN el administrador de red de la empresa, podrá crear túneles seguros de forma dinámica, de esta manera cuando se inaugure una sucursal no deberá de modificar toda la configuración de los routers, sino simplemente trabajar en los dispositivos de red que serán agregados.

Con el despliegue de la tecnología DMVPN se tendrá una mejora en el desempeño y disponibilidad de la red, disminuyendo la latencia y garantizando el tráfico de la información de manera segura, se evidenciará una agilización en la ejecución de procesos asociados a la casa matriz y sus sucursales para la empresa Megabyte S.A.

La ventaja principal de la implementación de DMVPN en la empresa Megabyte S.A., es que se crearan enlaces privados entre las diferentes estaciones remotas según los requerimientos de cada una de ellas, esto será independientemente del proveedor de internet que se utiliza en cada sucursal, ya que muchos casos los proveedores de internet no tienen el alcance geográfico que otros si tienen. A diferencia de MPLS, DMVPN no se limita a un solo proveedor.

4. Marco Teórico

4.1 Definición de una red privada virtual (VPN).

VPN es una infraestructura de red privada virtual que permite la comunicación a través de una red compartida [1] , publica como Internet. En base a este concepto, se puede decir que una red VPN es una tecnología de red que permite la extensión de la una red privada sobre una red pública o no controlada, para transmitir información de manera segura y confiable.

Por otra parte, podemos decir que una VPN combina los conceptos de red virtual y red privada. Se considera una red privada porque los enlaces de la red son lógicos y no físicos, es decir, que la topología de esta red es independiente de la topología física de la infraestructura utilizada para soportarla. En cambio, una red privada es definida como una red que pertenece dentro de la organización u empresa. De los conceptos de red privada y red virtual es como nace el concepto de red privada virtual [2].

4.1.1 Requerimientos para la implementación de VPN.

Al implementar una solución de red remota VPN, se necesita facilitar el acceso controlado a los recursos de la empresa. Esta solución debe permitir la libertar de conectar las oficinas remotas para compartir recursos e información de la empresa [3]; Por lo que una solución VPN debe de cumplir con los siguientes requerimientos:

Tabla 1. Requerimientos implementación VPN 1. [3]

Requerimientos para la implementación de VPN	
Autenticación del Usuario	Verifica la identidad del usuario y restringir el acceso a la VPN para que sólo permita a los usuarios autorizados
Manejo de Direcciones	Asigna una dirección de la red privada al usuario, y asegura que estas direcciones privadas se mantengan privadas.
Encriptación de Datos	Los datos que viajan en la red pública no podrán ser leídos por usuarios no autorizados en la red.
Administración de Llaves	Genera y renueva las llaves de encriptación entre el usuario y servidor.
Soporte de protocolo múltiple	Maneja protocolos comunes utilizados en la red pública.

4.1.2 Bases de Túnel.

El concepto de VPN se asocia frecuentemente con el túnel protegido; De esta manera solemos referirnos a una técnica que permite transitar en una red pública o compartida. El envió de datos a través de VPN utilizando túnel nos permite evitar que se filtren datos en la red del proveedor [4]. Por otra parte, ocultan a los dispositivos intermediarios, el origen o destino originales de ese contenido. El túnel tiene varias características:

- Los dispositivos que transportan el túnel solamente verifican el origen y destino del túnel. No acceden al origen y destino definitivos del tráfico.
- La existencia y operación del túnel es transparente para ambos extremos originales del tráfico.
- El túnel se logra agregando un nuevo encabezado al paquete por fuera del encabezado original existente.

- El encabezado agregado es llamado “encabezado externo y es único visible para la red que transporta el túnel.
- El tunelizado puede demandar una cantidad variable de procesamiento de acuerdo al grado de complejidad de la implementación.

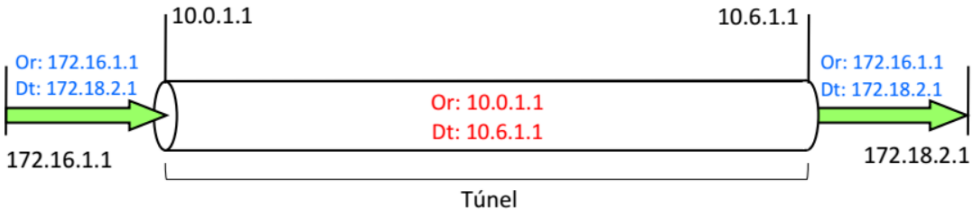

Figura 1.Túnel punto a punto. [4]

4.1.3 Clasificación de una VPN.

Las VPN se clasifican en:

- **VPN personales:** Son determinadas también como VPN de consumo o VPN comercial, este tipo de VPN es un servicio privado que se ofrece directamente a los usuarios individuales, generalmente a cambio de un costo [5]. Estas VPN proporcionan a sus usuarios una conexión a internet a través de una conexión cifrada, que permite ocultar tu identidad en línea y falsea tu ubicación geográfica. Por lo general se utilizan para ver películas que no están disponibles en tu área geográfica, ocultan dirección IP y protegerte de los ataques de denegación de servicio distribuido (DDoS).

- **VPN de acceso remoto:** Este tipo de VPN permiten la conexión de los empleados a distancia, los cuales pueden acceder a los recursos de la intranet privada de la empresa de manera remota por medio de una conexión a Internet. Este tipo de VPN resultan ser económicas para las empresas ya que los usuarios solo necesitan una conexión a internet.

Una VPN de acceso remoto se crea cuando la información de VPN no se configura de forma estática, pero permite el intercambio dinámico de información y permite habilitarla o deshabilitarla. Esto hace que el host o dispositivo logre comunicarse con la red de la empresa a través de la VPN. Cuando el host intenta enviar cualquier tipo de tráfico, el software Cliente VPN encapsula y cifra dicho tráfico. Después los datos cifrados se envían por Internet al Server VPN en el perímetro de la red de destino.

- **VPN móviles:** Este tipo de VPN se suelen utilizar al igual que las VPN de acceso remoto, para todos aquellos trabajadores que deseen acceder a la intranet privada de la organización de manera remota a través de una conexión a internet, con la única diferencia de que con una VPN de acceso remoto el trabajador debe de permanecer en una misma ubicación, ya que, si el trabajador se desconecta de la VPN, o tiene una conexión inestables de internet y no va a permanecer en la misma red toda la sesión, la conexión con el túnel IP se cerrara. En cambio, con las VPN móviles, la conexión se mantendrá, aunque el empleado cambie de conexión ya sea móvil o wifi, apaga el dispositivo durante el tiempo de la sesión.

- **VPN sitio a sitio:** Se utilizan para conectar sitios geográficamente separados. El costo de implementación es bajos debido que los clientes solo pagan su servicio de internet; sin embargo, el mecanismo de conexión es diferente a las VPNs de acceso remoto. Una VPN de punto a punto se crea cuando los dispositivos en ambos lados de la conexión VPN conocen la configuración de VPN con anticipación. La VPN permanece estática y los hosts internos no saben que existe una VPN.

  Las VPN de sitio a sitio conectan redes enteras entre sí. De esta forma se pueden crear redes WAN utilizando una VPN. Una Empresa puede hacer que sus redes se conecten utilizando un ISP local y establezcan una conexión de sitio a sitio a través de Internet [6].

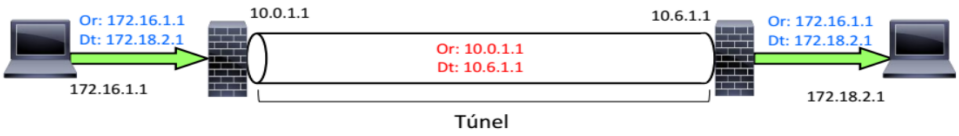

Figura 2. Encabezado IP túnel VPN. [6]

4.1.4 Topología en las VPN.

Para las VPN de sitio a sitio: La topología en las VPN se decide en función de los problemas que va a resolver. Una misma topología puede ofrecer distintas soluciones en diferentes compañías u organizaciones. En una VPN podemos encontrar las siguientes topologías:

4.1.4.1 Topología estrella.

La topología estrella es la más común en las VPN de punto a punto. Las sucursales remotas se conectan a un punto central, intercambiando información entre ellas y siempre pasando a través del punto central. La técnica más común que implementa esta topología es con VPN Site to Site IPsec.

4.1.4.2 Topología de malla completa o parcial.

La topología en malla las organizaciones o empresas que no poseen una estructura jerárquica compleja implementan la topología en malla. En este caso, las sucursales realizan el intercambio de datos entre ellas de manera directa. Las conexiones podrían ser utilizando una topología de malla completa o parcial; todo depende en gran mayoría si las sucursales intercambian información de manera constante entre ellas. La técnica que aplica este tipo de topología es la DMVPN [7].

4.1.5 Protocolos VPN.

Entre algunas de las tecnologías más robustas de tunelización encontramos:

4.1.5.1 Protocolo túnel punto a punto (PPTP).

Es una tecnología de tunelización de capa 2 (Capa de enlace) que corresponde al modelo OSI. Para la creación una conexión ambos extremos del túnel deben de estar de acuerdo y deben negociar las variables de configuración, los datos transferidos mediante esta tecnología son enviados mediante un protocolo basado en datagrama [8].

PPTP es una extensión del protocolo PPP (Protocolo Punto a Punto), cuyos paquetes se encapsulan en otros IP, y que incorpora otros mensajes de control para gestionar el túnel. Este protocolo únicamente se encarga de la creación y gestión del túnel, por lo que, tanto para el cifrado de los datos como para la autenticación de los usuarios, cada fabricante puede emplear los protocolos que considere oportuno, lo cual puede ocasionarnos problemas de compatibilidad [3].

4.1.5.2 Protocolo de túnel de capa 2 (L2PT).

Este protocolo fue creado a partir del protocolo PPTP y del protocolo L2F (Protocolo de reenvió de la capa 2). El objetivo de ambos protocolos es permitir la separación de lo físico hardware de conexión (módems) desde el software de control comunicación a través de las conexiones físicas (es decir, PPP o SLIP) [3]. También es un protocolo de capa de 2 que tiene como principales componentes de seguridad la autenticación y la encriptación de datos.

4.1.5.3 Protocolo de seguridad de Internet (IPsec).

IPsec por sus siglas en ingles IP Security. IPsec es un conjunto de estándares del IETF que proporciona servicios de seguridad a la capa IP y a todos los protocolos de capas superiores basados en IP. IPsec se desarrolla en base a la necesidad creciente de garantizar un nivel de seguridad al protocolo IP. La arquitectura IPsec se describe en el RFC2401.

El propósito de IPsec es proveer de interoperabilidad, integridad, autenticación y cifrado de datos por medio de IPv4 e IPv6 [8]. IPsec no se limita a ningún tipo específico de cifrado, autenticación, algoritmo de seguridad ni tecnología de creación de claves. En realidad, IPsec depende de algoritmos existentes para implementar comunicaciones seguras. También permite que se implementen nuevos y mejores algoritmos sin modificar los estándares existentes de IPsec. Por sus características es considerado como el protocolo estándar para la construcción de redes privadas virtuales.

4.1.5.3.1 Servicios de seguridad de IPsec.

- **Integridad:** Asegurar que el tráfico no ha sido modificado a lo largo de su trayecto utilizando un Hash. Una función hash es método para generar claves o llaves que representen a un documento conjunto de datos y su salida es una huella digital, de tamaño fijo e independiente de la dimensión del documento original. La integridad puede asegurar que la información no ha sido modificada entre el origen de la comunicación hasta el destino. Todas las comunicaciones en una VPN, incluye códigos detectores de errores y que la información no se vea modificada. En caso de ser modificada, automáticamente se descarta el paquete, e incluso se podría ocasionar una caída del túnel VPN por seguridad.

- **Autenticación de los extremos**: Asegurar que el tráfico proviene de un extremo de confianza. La autenticación es uno de los procesos más importantes de una VPN, esta característica permite demostrar a un usuario que es realmente quien dice ser. La forma de demostrarlo es introduciendo una contraseña de paso, hacer uso de un certificado digital, o una combinación de ambas formas de autenticación. Cuando el host recibe un datagrama IPsec de un origen, el host está seguro de que la dirección IP de origen del datagrama es el origen real del mismo, porque se ha autenticado correctamente de forma previa.

- **Confidencialidad:** Asegura que los datos no puedan ser leído por nadie más que las partes a las que está dirigido. Significa que se requiere que la información sea accesible únicamente a las entidades autorizadas, es decir, todas las comunicaciones están cifradas punto a punto, y solamente quien se haya autenticado previamente en el sistema, podrá descifrar toda la información intercambiada. Si alguien es capaz de situarse en el medio de la comunicación y la captura, no será capaz de descifrarla porque estará usando criptografía, ya sea criptografía de clave simétrica o asimétrica.

4.1.5.3.2 Protocolos de seguridad usados por IPsec.

Los protocolos de seguridad protegen la información que se añade a la cabecera de un paquete IP para proporcionar los servicios de seguridad requeridos. Entre los protocolos de seguridad que conforman IPsec tenemos:

Protocolo Encabezado de Autenticación (AH)

El protocolo AH (Authentication Header) proporciona un medio para garantizar la autenticidad e integridad de los datagramas IP [9]. Permite autenticar el origen de

los datos y verificar si dichos datos no han sido alterados en tránsito. Por otra parte, puede autenticar el paquete mediante la suma de comprobación calculada a través de un código de autenticación de mensajes hash (HMAC) mediante una clave secreta y funciones hash MD5 o SHA.

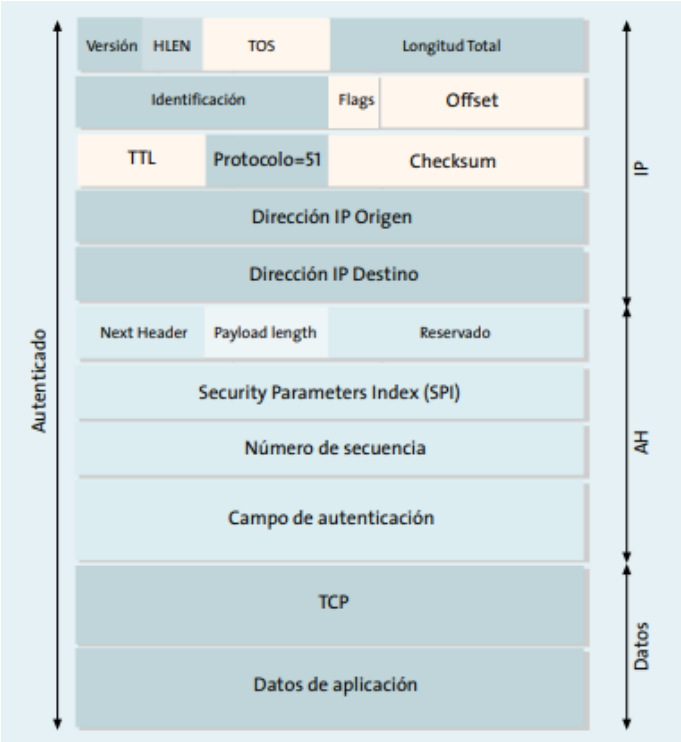

Figura 3. Estructura de un datagrama [9]

Síntesis del mensaje 5 (MD5): un algoritmo que produce un hash de 128 bits (también llamado síntesis de mensajes o firma *digital)* a partir de un mensaje de longitud arbitraria y una clave de 16 bytes. Se utiliza el hash resultante, como una huella dactilar de la entrada, para comprobar el contenido y la autenticidad e integridad del origen.

Algoritmo de hash seguro (SHA): un algoritmo que genera un hash de 160 bits a partir de un mensaje de longitud arbitraria y una clave de 20 bytes. Generalmente se considera más seguro que con MD5 debido al hash de mayor tamaño que produce. Dado que el procesamiento computacional se realiza en los circuitos ASIC, el costo de rendimiento es insignificante.

Protocolo Carga de Autenticación Segura (ESP)

ESP (Encapsulating Security Payload) proporciona un medio para garantizar la privacidad (cifrado) y la autenticación de origen e integridad del contenido (autenticación) [10]. ESP en modo de túnel encapsula todo el paquete IP (encabezado y carga) y, luego, anexa un nuevo encabezado IP al paquete que está ahora cifrado.

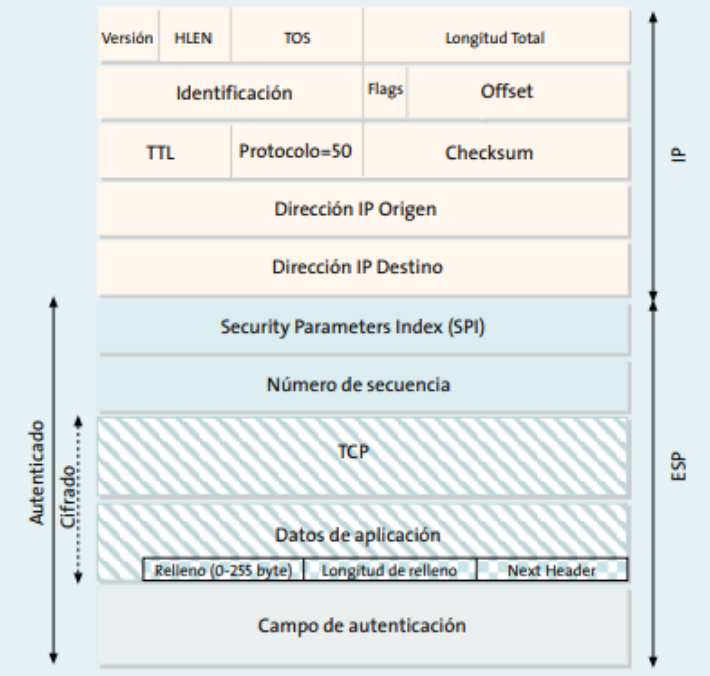

Figura 4. Estructura de datagrama ESP [10]

Este nuevo encabezado de IP contiene la dirección de destino necesaria para enrutar los datos protegidos a través de la red. Con ESP, puede cifrar y autenticar, únicamente cifrar o únicamente autenticar. Para el cifrado, puede elegir uno de los siguientes algoritmos de cifrado:

Estándar de cifrado de datos (DES): un algoritmo de bloque criptográfico con una clave de 56 bits.

Triple DES (3DES): una versión más potente de DES en la que se aplica el algoritmo DES original en tres rondas mediante una clave de 168 bits. DES proporciona ahorros significativos de rendimiento, pero se considera inaceptable para varias transferencias de material clasificadas o sensibles.

Estándar de cifrado avanzado (AES): un estándar de cifrado que ofrece una mayor interoperabilidad con otros dispositivos.

4.1.5.3.3 Protocolo de control Internet Key Exchange – IKE

IKE es un protocolo que permite establecer una SA (Asociación de Seguridad) en el protocolo IPsec [11]. Tanto AH como ESP, hacen uso de asociaciones de seguridad y una función importante de IKE es el establecimiento y mantenimiento de las asociaciones de seguridad. En una asociación de seguridad se definen las direcciones IP origen y destino de la comunicación. En una sola SA se puede proteger un sentido del tráfico; sin embargo, para proteger ambos sentidos, IPsec necesita de dos SA unidireccionales.

Una característica importante de IKE es que su utilidad no se limita a IPsec, sino que es un protocolo estándar de gestión de claves que podría ser útil en otros protocolos, como, por ejemplo, OSPF o RIPv2 [12]. La distribución de claves de forma segura es un requisito esencial para el funcionamiento de ESP y AH. Así mismo es importante que el emisor y el receptor estén de acuerdo en el algoritmo de cifrado y el resto de parámetros comunes a aplicar. Por tal motivo se debe utilizar un gestor de claves que se encargue en negociar y controlar estos parámetros; este gestor es denominado IKE.

IKE es un protocolo híbrido que es resultado de la integración de dos protocolos, ISAKMP y Oakley. ISAKMP define la sintaxis de los mensajes que se utiliza en

IKE, mientras que Oakley especifica la lógica de cómo realizar el intercambio de una clave de forma segura entre dos partes que no se conocen previamente [13].

4.1.5.3.4 Estructura de IPsec.

- **Protocolo del marco de IPsec:** al configurar un gateway IPsec para proporcionar servicios de seguridad, se debe seleccionar un protocolo IPsec. Las opciones son una combinación de ESP y AH. En realidad, las opciones de ESP o ESP+AH casi siempre se seleccionan porque AH en sí mismo no proporciona el cifrado.
- **Confidencialidad (si se implementa IPsec con ESP):** el algoritmo de cifrado elegido se debe ajustar al nivel deseado de seguridad (DES, 3DES o AES). Se recomienda AES, ya que AES-GCM proporciona la mayor seguridad.
- **Integridad:** garantiza que el contenido no se haya alterado en tránsito. Se implementa mediante el uso de algoritmos de hash. Entre las opciones se incluye MD5 y SHA.
- **Autenticación:** representa la forma en que se autentican los dispositivos en cualquiera de los extremos del túnel VPN. Los dos métodos son PSK o RSA.
- **Grupo de algoritmos DH:** representa la forma en que se establece una clave secreta compartida entre los peers. Existen varias opciones, pero DH24 proporciona la mayor seguridad.

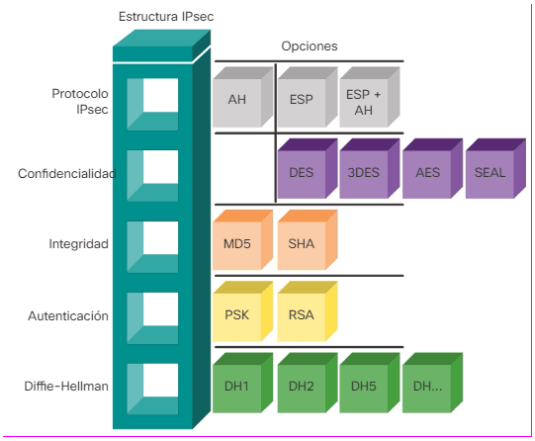

Figura 5. Estructura de marco de trabajo [7]

Modos de funcionamiento IPsec

Las VPN en general no importando el uso de ESP o HA tienen dos modos de protección:

- **Modo transporte**

En modo transporte, sólo los datos que se transfieren, del paquete IP es cifrada y/o autenticada. El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas, ya que eso invalidaría el hash. Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas de ninguna manera [14]. El modo transporte se utiliza para comunicaciones ordenador a ordenador.

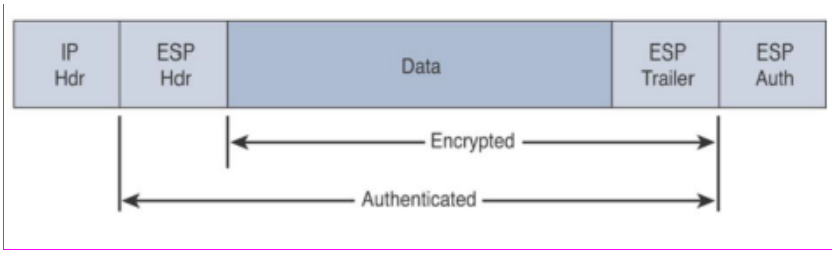

Figura 6. Encabezado IPsec. Modo transporte [7]

- **Modo Túnel**

En el modo túnel, todo el paquete IP es cifrado y/o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El modo túnel se utiliza para comunicaciones red a red o comunicaciones ordenador a red u ordenador a ordenador sobre Internet. El propósito de este modo es establecer una comunicación segura entre dos redes remotas sobre un canal inseguro [14].

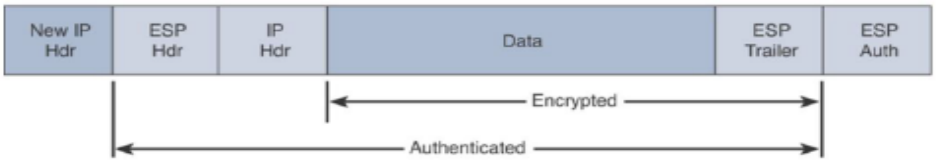

Figura 7. Encabezado IPsec. Modo túnel [8]

4.2 Red Privada Virtual Multipunto (DMVPN).

DMVPN **(**Dynamic Multipoint Virtual Private Network o Red Privada Virtual Multipunto Dinámica**)** es una versión mejorada de VPNs basado en el software de Cisco. Por otra parte, es una tecnología que engloba varios protocolos de comunicación para permitir el establecimiento de túneles privados de manera dinámica sobre redes públicas o privadas [15].

La tecnología DMVPN usa mecanismo de multicast lo que nos permite tener muchas redes VPN. DMVPN proporciona seguridad sobre la red de internet bastantes similares a las que proporciona Frame Relay [16].

Como nueva tecnología esta entra a competir con las tecnologías existentes por lo que las características adicionales y el valor agregado harán la diferencia. Cisco Systems muestra esta tecnología como una solución de seguridad basada en

Software de Cisco IOS para la construcción de VPNs empresariales escalables que soportan aplicaciones distribuidas como voz y video.

DMVPN permite una mejora substancial a gran escala de redes privadas virtuales (VPN), el despliegue de esta tecnología se logra mediante la combinación de túneles de encapsulación de enrutamiento genérico (GRE), cifrado IPsec y el protocolo de resolución de salto próximo (NHRP).

4.2.1 Características de DMVPN.

- **Enrutamiento dinámico a través de VPN:** Soporta protocolos de enrutamiento dinámico como: EIGRP, OSPF y BGP.
- **Reduce la configuración router casa matriz:** DMVPN elimina la necesidad de configurar los mapas criptográficos vinculados a la interfaz física, simplificando drásticamente el número de líneas de configuración requerida para una implementación VPN. Simplifica la configuración de la división de túnel. Centraliza los cambios de configuración en el concentrador de modo que sea ese el que controle el comportamiento de la división del túnel.
- **Túneles sitio a sitio dinámicos:** Los túneles directos entre sucursales eliminan la necesidad de que el tráfico generado entre ellos atraviese por el concentrador. Reduce la latencia para el despliegue de voz sobre IP y mejora el rendimiento efectivo del router principal. Los túneles son creados dinámicamente cuando se requiere y se eliminan cuando se cierra la conexión, permitiendo que el sistema escale de mejor manera.
- **Direccionamiento dinámico para los routers de las sedes remotas:** Los equipos de las sedes remotas pueden usar direcciones IP dinámicas, lo cual es un requisito frecuente para las conexiones a Internet por cable y ADSL.

- **Network Address Translation (NAT):** DMVPN soporta routers de las sedes remotas con NAT o detrás de dispositivos con NAT dinámicos, habilitando mejor seguridad para las subredes de las sucursales.
- **Soporta IP multicast:** DMVPN soporta tráfico IP multicast (entre la sede matriz y la sucursal); el IPsec nativo soporta solamente IP Unicast. Esto proporciona una distribución eficiente y escalable del tráfico punto-multipunto y multipunto-multipunto.
- **Soporta QoS:** Permite la asignación de tráfico en las interfaces del Hub por Spoke o por grupos de Spokes. Permite configurar políticas de QoS en conexiones Hub to Spoke y Spoke to Spoke. Permite configurar políticas de QoS dinámico en el que las plantillas de QoS se unen automáticamente a los túneles que vayan surgiendo.
- **Alta disponibilidad:** Permite el enrutamiento basado en conmutación por error. Enlaces WAN dual y redundancia HUB proporcionan una mayor disponibilidad. DMVPN soporta diseños de doble HUB, donde cada Spoke disponga de dos concentradores, proporcionando failover rápido.
- **Escalabilidad:** DMVPN escala a miles de Spokes que utilizan el equilibrio de carga del servidor (SLB). El cifrado se puede integrar en el dispositivo del SLB o distribuido a los routers VPN cabecera reservados. El rendimiento se puede escalar progresivamente añadiendo HUBs.
- **Soporta el Protocolo Múltiple de Intercambio de Etiquetas (MPLS):** Redes MPLS pueden ser encriptadas sobre túneles DMVPN.

4.2.2 Topología de diseño DMVPN.

Con base en la información presentada por Cisco la tecnología DMVPN puede ser implementada de dos modos o en dos topologías:

4.2.2.1 Modelo de implementación Hub and Spoke.

Se trata de una topología tradicional ya usada por otras tecnologías, esta trabaja de forma que los sitios remotos o spokes son agregados en un dispositivo VPN de cabecera en la sede central (hub). El Tráfico desde cualquier sitio remoto a otros sitios remotos tendría que pasar a través del dispositivo de casa matriz. Cisco DMVPN admite enrutamiento dinámico, QoS y IP multicast al mismo momento que reduce significativamente el esfuerzo de configuración.

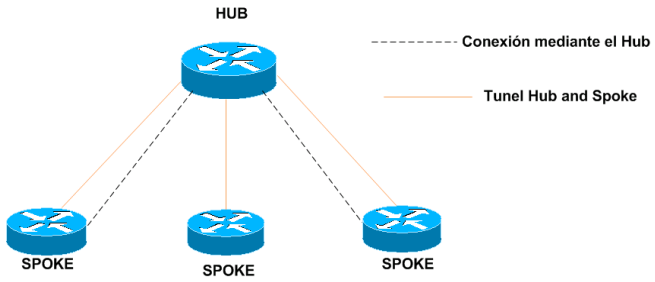

Figura 8. Modelo de Hub-Spoke.

4.2.2.2 Modelo de implementación Spoke-to-Spoke.

Cisco DMVPN permite la creación de una VPN de malla completa, en la cual la conectividad tradicional Hub-and Spoke es suplantada por túneles IPsec creados dinámicamente directamente entre los sitios. Con túneles sitio a sitio directo, el tráfico generado entre los sitios remotos no necesita recorrer el Hub; esto elimina retrasos adicionales y conserva el ancho de banda a nivel WAN.

La capacidad sitio a sitio es soportada en un ambiente de un único concentrador o un ambiente de concentradores múltiples. Las implementaciones en las cuales se usan concentradores múltiples proporcionan mayor escalabilidad de spoke-to-spoke y redundancia [17].

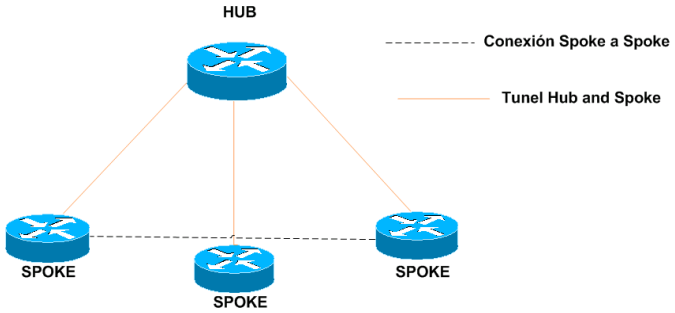

Figura 9. Modelo de Spoke-Spoke.

4.2.3 Arquitectura DMVPN

DMVPN es la combinación de las siguientes técnicas y protocolos:

4.2.3.1 Túnel de encapsulación de enrutamiento genérico (GRE).

Un túnel 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 red IP.

DMPVN usa la encapsulación GRE multipunto (mGRE) y admite protocolos de enrutamiento dinámico, esto elimina mucho de los problemas de soporte asociados con otras tecnologías de VPN. Los túneles 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. El nuevo encabezado 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 [18].

Características de GRE

- GRE se define como un estándar IETF (RFC 1701 y 1702).
- En el encabezado IP externo, en el campo de protocolo se utiliza el número 47 para indicar que lo que sigue es un encabezado GRE.
- La encapsulación de GRE utiliza un campo de “tipo de protocolo” en el encabezado para admitir la encapsulación de cualquier protocolo de capa 3 del modelo OSI. Los tipos de protocolo se definen en RFC 1700 como “EtherTypes”.
- GRE no incluye ningún mecanismo sólido de seguridad para proteger su contenido.
- El encabezado GRE, junto con el encabezado de tunneling IP añade por lo menos 24 bytes a la cabecera de los paquetes que se envían por el túnel.
- GRE permite emplear protocolos de enrutamiento especializados que obtengan el camino óptimo entre los extremos de la comunicación.

4.2.3.2 Protocolo de Resolución del Siguiente Salto (NHRP).

Next Hop Resolution Protocol (NHRP) o Protocolo de Resolución del Siguiente Salto se encuentra definido en la RFC2332. NHRP facilita el establecimiento del túnel dinámico al proveer una resolución de direcciones de túnel a interfaz física. El protocolo además permite la simplificación de la configuración de los equipos; por ejemplo, en DMVPN los equipos que funcionan como hubs no necesitan tener configurada la dirección de ninguno de los spokes y por lo tanto las direcciones de los spokes pueden ser asignados dinámicamente. Únicamente en los spokes es necesario configurar la dirección de uno o todos los hubs de la red.

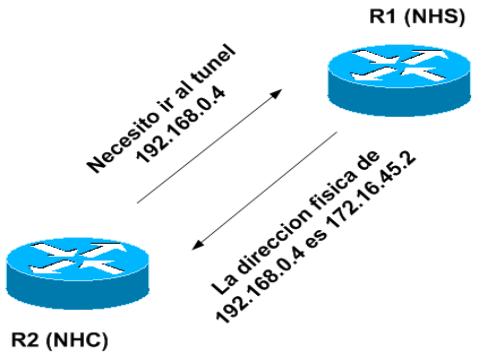

Figura 10. Funcionamiento protocolo NHRP.

Cada spoke de la red debe registrarse en el hub que tenga configurado, estableciendo un túnel permanente entre ambos.el router R1 o hub tiene registradas las rutas de cada spoke. Cuando el router R2, que es uno de los spokes, intenta comunicarse con otro spoke, el router R1 le informa de las rutas aprendidas enviando la dirección física del destino. De esta manera, cuando el spoke necesite comunicarse con otro spoke pueda realizarlo sin problemas y de manera directa, como si se tratara de una red mallada.

4.2.3.2.1 Características de NHRP

NHRP es un protocolo similar a un protocolo de resolución de direcciones (ARP) que mapea dinámicamente una red de acceso múltiple sin difusión (NBMA). Con NHRP, los sistemas conectados a una red NBMA pueden aprender dinámicamente la dirección NBMA (física) de los otros sistemas que forman parte de esa red, permitiendo que estos sistemas se comuniquen directamente.

NHRP es un protocolo de cliente y servidor donde el concentrador es el Next Hop Server (NHS) y los clientes son los Next Hop Clients (NHC). El hub mantiene una base de datos NHRP de las direcciones de interfaz pública de cada spoke. Cada spoke registra su dirección real cuando arranca y consulta la base de datos NHRP

para obtener direcciones reales de los spoke de destino para construir túneles directos.

Cuando NHRP se combina con IPsec, la red NBMA es básicamente una colección de enlaces de túnel lógico punto a punto a través de una red IP física.

NHRP permite dos funciones para ayudar a respaldar estas redes NBMA:

1. Registro de NHRP. NHRP permite que los Next Hop Clients (NHC) se registren dinámicamente con los Next Hop Servers (NHS). Esta función de registro permite que los NHC se unan a la red NBMA sin cambios de configuración en los NHS; especialmente en casos donde el NHC tiene una dirección IP física dinámica o está detrás de un enrutador de traducción de direcciones de red (NAT) que cambia dinámicamente la dirección IP física.

2. Resolución NHRP. Con NHRP, los sistemas conectados a una red NBMA aprenden dinámicamente la dirección NBMA de los otros sistemas que forman parte de esa red, permitiendo que estos sistemas se comuniquen directamente sin requerir que el tráfico use un salto intermedio. Esta función alivia la carga en el salto intermedio (NHS) y puede aumentar el ancho de banda total de la red NBMA para que sea mayor que el ancho de banda del enrutador del concentrador [19].

4.2.3.2.2 Tipos de paquete NHRP

El protocolo NHRP utiliza siete tipos de paquetes que establecen la comunicación e intercambio de información entre los NHS y los NHC a continuación se detallan cada uno de ellos:

- **Registration Request:** petición de registro de un NHC ante un NHS, este registro le permite a los HUBs conocer la información NBMA del spoke.

también el NHC especifica la cantidad de tiempo que el NHS debe mantenerle en registro junto con otros atributos.

- **Registration Reply:** respuesta del NHS al pedido de registro del NHC.
- **Resolution Request:** petición de resolución de una dirección del siguiente salto enviada por el NHC al NHS, estos mensajes son para ubicar y proporcionar la información de resolución de direcciones del Hub de salida hacia el destino.
- **Resolution Reply:** respuesta del NHS al NHC con la dirección solicitada, en esta respuesta se proporciona la dirección IP de túnel y la dirección IP NBMA del spoke remoto
- **Purge Request:** petición de borrado de una entrada de caché enviada por el NHS a un NHC cuando deja de ser válida, estos mensajes notifican a los spokes, la perdida de una ruta de una red que ya no está alcanzable.
- **Purge Reply:** respuesta del NHC al NHS a una petición de borrado.
- **Error indicator:** paquete de error que indica un problema en algún paquete recibido en el equipo que generó el paquete de error.

4.3 Protocolo de enrutamiento.

Los protocolos de enrutamiento, son reglas que utilizan los routers para comunicarse entre la fuente y el destino. Estos no pueden mover o cambiar información en los routers, pero si pueden compartir la tabla de información que contiene cada router.

Por lo general existen 2 principales tipos de enrutamiento:

4.3.1 Enrutamiento estático.

Es un método en el que los administradores de red definen manualmente las rutas que deben seguir los paquetes de datos para llegar a su destino. En este método,

se configuran las rutas en cada uno de los routers de la red y no hay intercambio de información de enrutamiento entre ellos.

4.3.2 Enrutamiento dinámico.

El enrutamiento dinámico, ayuda a los routers ha agregar información de las tablas de contenidos de los demás routers. Estos tipos de protocolos también envían su topología actualizada cada vez que la red cambia la estructura de su topología.

El la figura 11, podemos observar cómo se clasifican los protocolos de enrutamiento, así como también su subclasificación. En este trabajo monográfico solo abarcaremos en protocolo de enrutamiento estado de enlace OSPF.

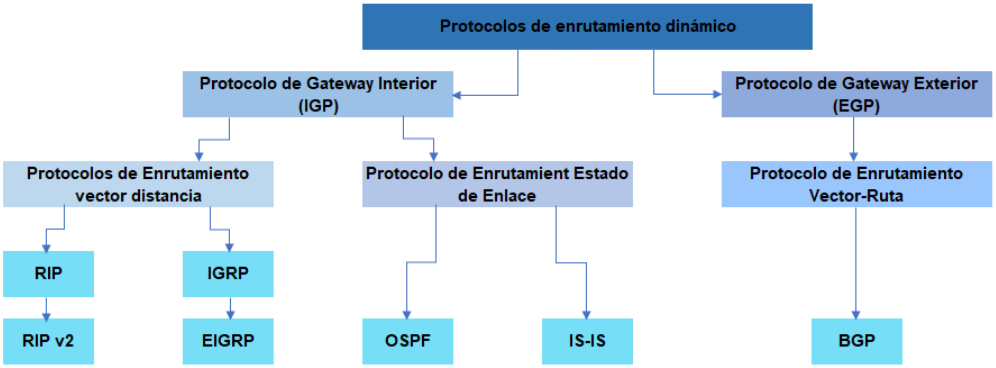

Figura 11. Protocolos de enrutamiento dinámico.

4.3.2.1 Open Shortest Path First (OSPF).

OSPF, es un protocolo de estado de enlace IGP, el cual utiliza el método de escoger la ruta más corta primero. El protocolo OSPF es un protocolo de enrutamiento estándar definido en la RFC 2328 que permite mantener la

información de la database detallada por medio de las redes circundantes. OSPF funciona seleccionando y reenviando el paquete IP a través de la ruta más corta para así llevar el paquete a su destino [20].

OSPF también, usa el algoritmo Dijkstra para recalcular la ruta de red cuando la topología sufre cambios [21]. Este protocolo es seguro y escalable en ambientes grandes, ya que puede autenticar los cambios de protocolo para así poder mantener los datos seguros.

- **Características de OSPF.**

- Enrutamiento de tipo link-state, es decir los routers intercambian información sobre la topología de la red, incluyendo detalles sobre los enlaces y sus estados, para calcular las rutas más cortas.
- OSPF utiliza el algoritmo de cálculo SPF (Shortest Path First) para calcular las rutas más cortas y determinar el mejor camino hacia una red de destino.
- Utiliza una métrica basada en costos para calcular las rutas más cortas. Esto significa que los enlaces más rápidos tendrán un costo menor y serán preferidos en la selección de ruta.
- Tiene la capacidad de converger rápidamente en caso de cambios en la topología de la red. Cada vez que se produce un cambio, OSPF actualiza su base de datos de estado de enlace y recalcula las rutas afectadas de manera eficiente.
- OSPF permite dividir la red en áreas lógicas más pequeñas, lo que ayuda a reducir el tamaño de la base de datos de estado de enlace y a mejorar la escalabilidad del protocolo. Esto permite una administración más eficiente de grandes redes.
- Ofrece opciones de autenticación para asegurar la integridad y confidencialidad de las actualizaciones de estado de enlace, lo que ayuda a proteger la red contra amenazas de seguridad.
- Posee la capacidad de soportar enlaces redundantes y rutas alternativas, lo que aumenta la disponibilidad y la confiabilidad de la red.

- Utiliza las direcciones IP multicast (224.0.0.5 y 224.0.0.6) para la difusión de mensajes de estado de enlace, lo que reduce el consumo de ancho de banda y mejora la eficiencia de la red.
- Permite la definición de políticas de enrutamiento mediante la asignación de diferentes costos a los enlaces o mediante el uso de filtros de ruta, lo que permite una mayor flexibilidad en el diseño y administración de la red.
- Este protocolo de enrutamiento es estándar y ampliamente utilizado, lo que facilita la interoperabilidad entre diferentes fabricantes de equipos de red y la integración con otros protocolos de enrutamiento.

➢ **Ventajas y desventajas.**

Tabla 2. Ventajas vs Desventajas OSPF. [22]

Ventajas	Desventajas
Se adapta al máximo con los protocolos TCP/IP.	Solo soporta el protocolo TCP/IP.
Solicita poco uso de la red.	Requiere una carga de proceso intensiva.
Tiempo de convergencia rápido y consumo de ancho de banda bajo.	Requiere routers más poderosos y más memoria, debido a que sus algoritmos son más complejos.
Puede escalar a interconexiones de redes mayores.	Es complejo y necesita una organización adecuada, lo que genera una administración difícil.
Los cambios en la topología de red son rápidos.	Requiere una amplia memoria ya que mantiene copias de la información de las rutas.

➢ **Tipos de mensaje OSPF.**

OSPF tiene una distancia administrativa (AD) predeterminada de 110, esto determina la confiabilidad o preferencia del origen de la ruta. Los mensajes OSPF

se encapsulan directamente dentro de datagramas IP, con número de protocolo 89 (TCP=6, UDP=17) [23].

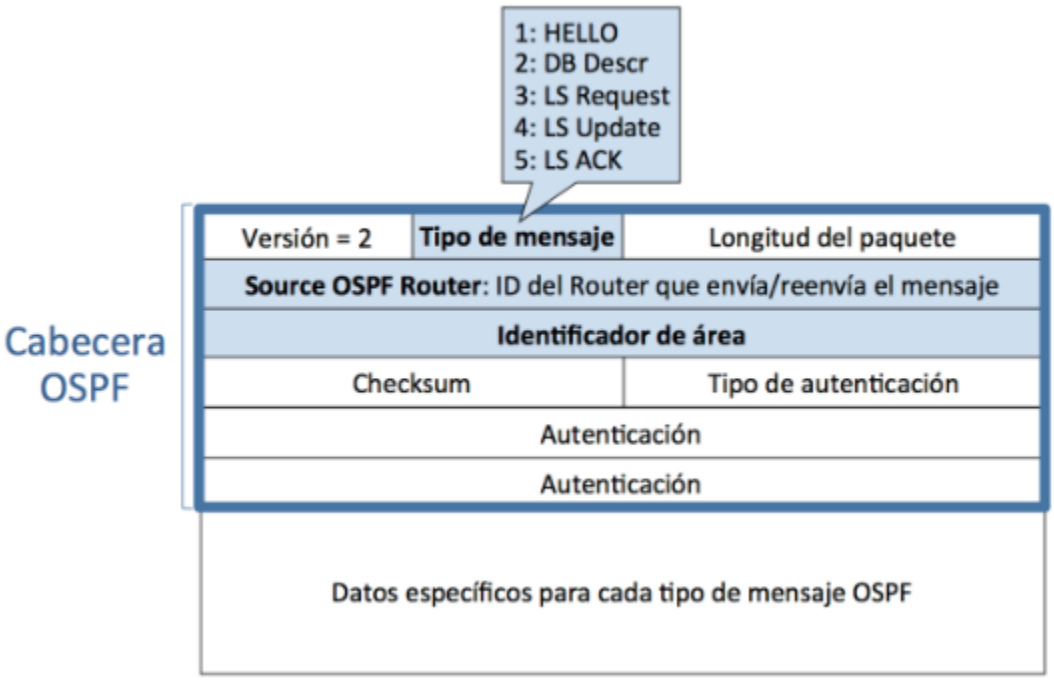

Figura 12. Datagrama OSPF. [23]

- Saludo: Descubrimiento de vecinos mediante mensajes HELLO.
- Descripción de la base de datos (DBD): Intercambio de información de las tablas de ruta.
- Solicitud de estado de enlace (LSR): Solicita datos que un router no tiene en su tabla de rutas.
- Actualización de estado de enlace (LSU): Respuesta a los mensajes de petición del estado de enlace. Informa cambios en la topología de la red.
- Acuse de recibo de estado de enlace (LSAck): Confirma la recepción del estado de enlace [24].

5. Diseño metodológico.

5.1. Metodología.

Este trabajo monográfico está enfocado en brindar una solución de red de alta disponibilidad con la tecnología DMVPN a la empresa Megabyte S.A, con el fin de elaborar plan de implementación detallado para desplegar la tecnología DMVPN. Esta investigación tiene un alcance descriptivo y aplicado. Lo denotamos como descriptivo, ya que, se describirá e interpretará las ventajas que tienen las Redes Privadas Virtuales Dinámicas Multipunto (DMVPN) en busca de la optimización del desempeño de VPN sobre Internet. Y es una investigación aplicada, debido a que se basa en conocimientos o descubrimientos existentes, como lo es la técnica DMVPN, y por otra parte esta investigación es derivada de investigaciones y desarrollos previos.

Descripción del tipo de investigación:

Con la investigación de tipo descriptiva, se busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis [25]. Esto nos permite describir las características y funcionalidades la red DMVPN de la cual realizamos una emulación en el software GNS3.

La investigación aplicada por otra parte, es el tipo de investigación en donde el investigador ya conoce el problema, y el énfasis del estudio está en darle resolución al problema [26]. En este punto planteamos que nuestro tema de investigación monográfico es un proyecto que se desarrollara a futuro en la empresa Megabyte S.A, en la cual ya conocemos las necesidades que tiene la red de la empresa, con el cual brindaremos una solución efectiva a sus problemas de conectividad.

Descripción de las fuentes de información:

Se consideran como fuentes primarias de esta investigación los aportes u opiniones del Gerente General de la empresa acerca de la problemática de conectividad que está presentando actualmente la empresa Megabyte S.A.

Como fuentes secundarias se recopilo información confiable acerca de la tecnología DMVPN, funcionamiento, características e implementación. Esto con el fin de brindar base teórica y práctica al futuro administrador de red la empresa.

6. Análisis de la situación actual.

La Empresa Megabyte S.A, es una empresa de comercio minorista que se dedica a la comercialización de equipos para la solución de gestión de inventario, administración y control de bodegas, rutas de despacho, administración de activos fijos, identificación de personal, redes inalámbricas, entre otros. Esta es una empresa está ubicada en Reparto Bolonia, esquina norte de Canal 2 TV, 1 cuadra hacia el este, en la figura 13 se aprecian las instalaciones de la empresa.

Figura 13. Instalaciones empresa Megabyte S.A.

En la actualidad la empresa está bajo la administración del Ing. James Cantillano, quien tiene 18 colaboradores a su cargo. La empresa se encuentra dividida en 5 (cinco) áreas: Administración, contabilidad, ventas, soporte técnico y bodega. En la figura 14 se muestran el área administrativa de la empresa.

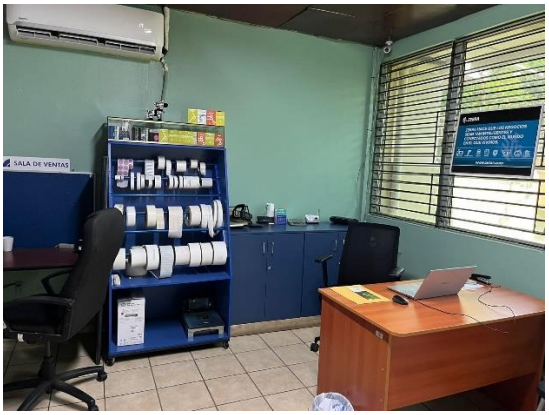

Figura 14. Oficinas empresa Megabyte S.A.

Actualmente la empresa tiene un proyecto de expansión y apertura de nuevas sucursales en los departamentos de Masaya, Matagalpa y Chinandega; Dicho proyecto se estará llevando a cabo a lo largo del año 2024. Debido a esto el administrador de la empresa, el Ing. James Cantillano, buscaba la mejor solución de conectividad WAN, que interconectara la casa matriz con las nuevas sucursales. En la figura 15, se muestra el área de recepción de la empresa.

Figura 15. Recepción empresa Megabyte S.A.

Nosotros como egresados de las carreras Ingeniera Electrónica y Telecomunicaciones, nos encontrábamos en el proceso de investigación de la tecnología basada en túneles DMVPN, ya que percibimos que muchas empresas de nuestro país siguen recurriendo a soluciones VPN sitio a sitio para conectar diferentes sucursales a su casa matriz.

Consideramos que las VPN sitio a sitio no son solución adecuada, debido a que posee una escalabilidad limitada, lo cual genera complejidad de configuración al momento de agregar nuevos sitios a la red, y esto resulta complicado, ya que requiere modificar las configuraciones existentes y una planificación cuidadosa; por otra parte, genera sobrecarga de tráfico de enrutamiento, puesto que todo el tráfico de paquetes de datos pasa a través de la casa matriz.

Otro tipo de tecnología utilizada para conectar distintas sucursales alejadas geográficamente es MPLS; esta tecnología de conmutación mejora la eficiencia y calidad de servicio en redes IP, pero una de sus grandes desventajas es que a medida que aumenta el número de sucursales, aumenta la complejidad y los

costos de implementación. También esta tecnología es muy dependiente del ISP, el cual está encargado de la configuración y el manteniendo de la misma, convirtiéndola en una tecnología no flexible.

Por otra parte, DMVPN mejora algunas de las desventajas planteadas anteriormente, al proporcionar una solución más escalable y eficiente para la conectividad VPN. DMVPN permite crear los túneles de forma dinámica entre los sitios, lo que simplifica la configuración y permite una escalabilidad más fácil. Además, DMVPN utiliza enrutamiento dinámico para optimizar el tráfico y permite conexiones directas entre las sucursales, reduciendo así la sobrecarga de tráfico y mejorando la eficiencia del ancho de banda.

En cuanto a esto, decidimos plantear la solución de conectividad WAN con la tecnología DMVPN a la empresa Megabyte S.A, para la interconexión de sus nuevas sucursales con su casa matriz. En primera instancia realizamos una visita de campo a dicha empresa para conocer su infraestructura de red.

La empresa Megabyte S.A, en su infraestructura de red WAN cuentan con un servicio de perfil domiciliar que tiene como tecnología de última milla un router con tecnología HFC (Hybrid Fiber Coaxial), de la empresa de telecomunicaciones Tigo, este tiene una tasa de transferencia asimétrica de 120 Mb (Download) y 20 Mb (Upload), a como se muestra en la imagen 16.

Figura 16. Router de la empresa Megabyte S.A.

En la parte de su infraestructura LAN, cuentan con un switch Linksys que conecta de forma directa 9 (nueve) CPU distribuidas de la siguiente manera: 2 computadoras en el área administrativa, 3 en ventas, 1 en contabilidad, 2 en soporte técnico y 1 en bodega. La empresa Megabyte S.A no cuenta con área de IT definida, por lo tanto, no se tiene una topología red. Cuando tienen problemas de conectividad cuentan con la ayuda de un colaborador del área de soporte técnico.

Para este proyecto la empresa planteo que se abriría una nueva plaza de Ingeniero IT el cual se encargara de la implementación y la administración de la red y futura expansión de la misma.

7. Diseño de la Red DMVPN.

La implementación de la red DMVPN permite la interconexión entre distintas sedes de una empresa de forma dinámica, rápida, flexible, segura y escalable. En este trabajo monográfico el objetivo principal es desarrollar una red DMVPN de alta disponibilidad, que permita agregar o quitar spokes fácilmente sin tener que configurar túneles punto a punto individuales. DMVPN tiene la capacidad de escalar a medida que las necesidades de la red cambien con el tiempo.

Para la empresa Megabyte S.A se desarrollará un diseño emulado de una conexión DMVPN que conectará 4 (cuatro) sucursales utilizando una topología Hub-Spoke. Teniendo en cuenta una red tolerante a fallas, se emulará un despliegue DMVPN de alta disponibilidad single cloud, en el cual se tendrá redundancia en la casa matriz con 2 (dos) routers, se le asignara el rol de router Hub a los routers ubicados en casa matriz debido a que es donde están alojados los servidores de almacenamiento y herramientas que utilizan los trabajadores. En las sucursales de Masaya, Chinandega y Matagalpa los routers serán configurados como Spokes.

Aparte de diseño y emulación de la red DMVPN también se emulará la red LAN de la empresa, se implementará DHCP (Dynamic Host Configuration Protocol), esto con el fin de reducir la necesidad de asignar direcciones IP manualmente.

El diseño la red DMVPN para la empresa Megabyte S.A, se realizó en los siguientes pasos:

- Infraestructura de la red.
- Evaluación de costo financiero de la implementación de DMVPN.

7.1 Infraestructura de la red.

Este inciso se dividió en 2 (dos) partes:

- **Diseño de la red física:** refiriéndose a la base sobre la cual se construyen las redes de comunicaciones, y es esencial para el correcto funcionamiento de la red.
- **Diseño de la red lógica:** refiriéndose a la forma en que los dispositivos se comunican y comparten información entre sí. La red lógica se enfoca en los protocolos y algoritmos.

7.1.2 Diseño de la red física.

La infraestructura de la red WAN de la empresa Megabyte S.A estará constituida por 2 routers configurados como Hubs, ubicados en la casa matriz en la ciudad de Managua, contará con 3 (tres) sucursales, ubicadas en la cuidad de Masaya, Chinandega y Matagalpa, los routers ubicados en las sucursales estarán configurados como Spokes.

En el diseño de la infraestructura de la red LAN para la cuidad de Managua, la empresa cuenta con 9 computadoras y un switch, en cambio en las 3 (tres) nuevas sucursales contarán con 3 (tres) computadoras y un switch.

En general la red de la empresa Megabyte S.A contará con los siguientes componentes:

Tabla 3. Listados de equipos. [Elaboración propia]

Sucursal	Componentes
Chinandega	Router Cisco 867
	Switch
	3 computadoras
Managua	2 Router Cisco 867
	Switch
	9 computadoras
Masaya	Router Cisco 867
	Switch
	3 computadoras
Matagalpa	Router Cisco 867
	Switch
	3 computadoras

Para el diseño de la topología física, se hicieron propuestas de equipos, tanto routers como switches, ver figuras 17 y 18, y sus tecnologías de última milla a utilizar. Se recomienda al cliente Megabyte S.A utilizar el modelo de router Cisco 867 de la serie 860 y el switch Cisco catalyst 2960 de 24 puertos. Esto se empleará para la casa matriz y sus sucursales, ya que estos equipos cuentan con las características físicas y lógicas para realizar el despliegue de una red de túneles como lo es DMVPN. El router Cisco 867 es ideal para clientes domiciliares y corporativos ya que soporta tecnologías de cobre como ADSL, HFC y de fibra óptica como GPON, siendo una buena opción para administrar pequeñas sucursales.

Figura 17. Router cisco867.

Figura 18. Cisco Catalyst 2960 Series Switches.

En la tabla 4 se detallan las características correspondientes al router Cisco 867 que observamos en la figura 13.

Tabla 4. Características y Beneficios Router Cisco867. [27]

Características	**Beneficios**
Mayor rendimiento	Rendimiento que permite a los usuarios tomar ventaja de las velocidades de la red de banda ancha mientras se ejecutan servicios de seguridad, envió de dato, voz y video.
Seguridad y Calidad de Servicio	● IPsec, VPN con 10 tunnels ● BGP ● Filtrado MAC y seguridad en los puertos ● QoS que incluye LLQ y WFQ ● NBAR y DiffServ
Estado del arte xDSL	● El último standard ADSL2+/VDSL2 ● Mejorar la interoperabilidad frente a varios multiplexores de acceso DSL (DSLAM) implementados en proveedores de servicios en todo el mundo
Diversidad WAN	● GE o DSL multinodo VDSL2 y ADSL 1, 2, and 2+ ● Múltiple opciones WAN que permitir una configuración consistente en diversas implementaciones
Administración de swith en los puertos LAN con GE y FE	● Conexión de múltiples dispositivos dentro del teletrabajo u oficinas pequeñas, con la habilidad de designar puertos como borde de red ● VLANs que permiten la segmentación segura de los recursos de la red
LAN inalámbrica	● 802.11n 2.4 GHz FCC- o ETSI-compliant WiFi ● Cisco IOS® Software Interfaz de línea de comando (CLI) o configuración basada en red con roles basados en accesos Admin/Guest

Puerto CONT/AUX	● Un puerto de doble propósito que provee conexión directa a la consola o a un modem externo para administrar o como punto de acceso de respaldo
Reloj en tiempo real	● Un reloj en tiempo real integrado que mantiene una fecha y hora precisas para las aplicaciones que requieren una marca de tiempo precisa, como registros y certificados digitales

7.1.3 Diseño de la red lógica.

- **Arquitectura, topología y direccionamiento.**

La arquitectura de la red LAN de la empresa será por conexión ethernet, con una topología tipo estrella en la cual todos los nodos de la red se conectan a un nodo central y la comunicación se dirige a través de él. Se escogió este tipo de topología de acuerdo a las necesidades de la empresa ya que es la más adecuada para redes pequeñas, esto con el fin de que su administración y control sea centralizado.

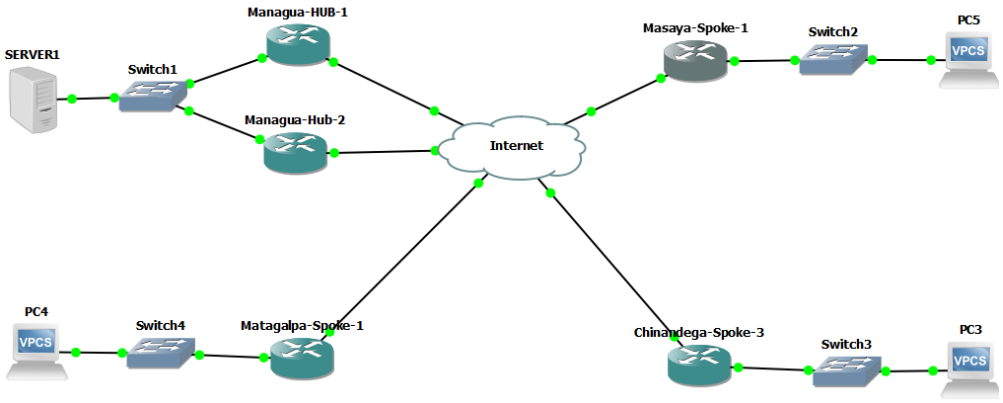

Figura 19. Topología Hub & Spoke empresa Megabyte.

En la tabla 5, se puede observar el direccionamiento IPv4 con los que trabajará la red de la empresa, estos pertenecen a un segmento de red privada, según la RFC 1918.

Tabla 5. Tabla direccionamiento LAN. [Elaboración propia]

Clase	Dirección	Mascara	Prefijo	Función	Cuidad
C	192.168.1.0	255.255.255.0	24	Hub	Managua
C	192.168.2.0	255.255.255.0	24	Spoke	Masaya
C	192.168.3.0	255.255.255.0	24	Spoke	Matagalpa
C	192.168.4.0	255.255.255.0	24	Spoke	Chinandega

Para acceder a la red de internet, la empresa Megabyte S.A cuenta con un contrato con el proveedor de internet Tigo, cabe destacar que con la tecnología DMVPN es posible crear una conexión sobre internet con distintos ISP (Internet Service Provider).

En la tabla 6 se puede observar el listado del direccionamiento IP para cada uno de los ISP. Estas direcciones son utilizadas con fines académicos, por lo cual no están vinculadas con los ISP listados en la tabla.

Tabla 6. Tabla direccionamiento WAN. [Elaboración propia]

Función	Sucursal	IP pública	ISP
Hub 1	Managua	200.10.1.1	Tigo
Hub 2	Managua	200.20.1.1	Claro
Spoke	Masaya	200.1.1.1	Ideay
Spoke	Matagalpa	200.2.2.2	Yota
Spoke	Chinandega	200.3.3.1	Tigo

Se eligieron rangos de direcciones públicas y diferentes ISP con fines demostrativos. A como se puede observar en la siguiente en la figura 20.

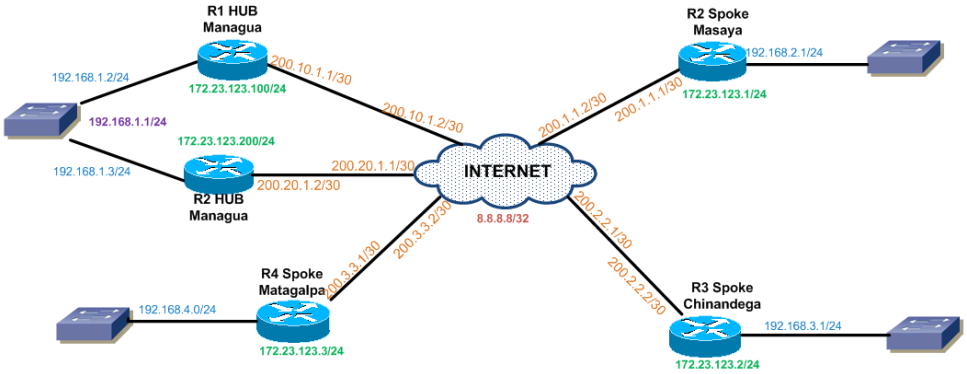

Figura 20. Direcciones IP de la red DMVPN.

Para la implementación de DMVPN se debe considerar un nuevo direccionamiento para los túneles mGRE de cada sitio, las direcciones IP que usamos son las siguientes:

Tabla 7. Tabla direccionamiento mGRE. [Elaboración propia]

Función	Sucursal	Direccionamiento mGRE
Hub 1	Managua	172.23.123.100
Hub 2	Managua	172.23.123.200
Spoke	Masaya	172.23.123.2
Spoke	Matagalpa	172.23.123.3
Spoke	Chinandega	172.23.123.4

7.2. Evaluación de costo financiero de la implementación de DMVPN.

Para evaluar el costo que tendrá el proyecto de la red WAN del cliente Megabyte, se buscó información sobre cotización de presupuestos con uno de los proveedores de internet en nuestro país. Ya que, en primera instancia el ingeniero James Cantillano encargado de la empresa, estaba interesado en el despliegue de su red WAN con el servicio de arrendamiento MPLS, para conectar casa matriz con las distintas sucursales. Se cotizo el precio de despliegue de este servicio dando como resultado de un costo elevado ya que se tendría la instalación de dos

router en casa matriz uno para el servicio de datos MPLS que conectaría con las demás sucursales y otro router de internet centralizado.

En la tabla 8, se muestra el costo de implementación que tendría el despliegue de MPLS en las distintas sucursales.

Tabla 8. Costo implementación MPLS. [Elaboración propia]

Cliente Megabyte						
Servicio MPLS						
Sucursal	**Ancho de banda**	**Distancia cableado fibra óptica (Mts)**	**Router proveído por ISP**	**Plazo de renta / mes**	**Renta mensual**	**Renta total**
Casa Matriz Internet	50 Mb	150 mts	Si	36	$ 350.00	$ 12,600.00
Casa Matriz Datos	50 Mb	150 mts	Si	36	$ 300.00	$ 10,800.00
Sucursal Masaya datos	10 Mb	200 mts	Si	36	$ 95.00	$ 3,420.00
Sucursal Chinandega datos	10 Mb	350 mts	Si	36	$ 95.00	$ 3,420.00
Sucursal Matagalpa datos	10 Mb	400 mts	Si	36	$ 95.00	$ 3,420.00
				Total	**$ 935.00**	**$ 33,660.00**

Podemos concluir que, el servicio de MPLS en la actualidad tiene un costo elevado y que no es ideal para empresas pequeñas que están en proceso de crecimiento. Es por eso que proponemos a la empresa Megabyte hacer uso del despliegue de la tecnología DMVPN ya que basta con tener una conexión a internet en cada una de las sucursales y de esta manera ahorrar costos ya que internet tiene un precio menor comparado con tecnologías de arrendamiento privado como MPLS.

Siguiendo con la evaluación de costos del proyecto, se realizó una nueva cotización con el mismo proveedor de servicios esta para la instalación del servicio de internet corporativo con el arrendamiento de los routers, es decir los routers que se ocuparían en las sucursales serian brindados por el proveedor.

En la tabla 9 se muestra el costo total que tendría la inversión del servicio de internet corporativo incluyendo la renta de los routers:

Tabla 9. Costo servicio de internet más alquiler de dispositivos. [Elaboración propia]

Cliente Megabyte						
Servicio internet con router proveído por ISP						
Sucursal	**Ancho de banda**	**Distancia cableado fibra optica (Mts)**	**Router proveido por ISP**	**Plazo de renta / mes**	**Renta mensual**	**Renta total**
Casa Matriz Internet	50 Mb	150 mts	Si	36	$ 350.00	$ 12,600.00
Sucursal Masaya datos	10 Mb	200 mts	Si	36	$ 95.00	$ 3,420.00
Sucursal Chinandega datos	10 Mb	350 mts	Si	36	$ 95.00	$ 3,420.00
Sucursal Matagalpa datos	10 Mb	400 mts	Si	36	$ 95.00	$ 3,420.00
				Total	**$ 635.00**	**$ 22,860.00**

Analizando este presupuesto podemos concluir que, el costo de la inversión es menor comparado con el despliegue del servicio MPLS, pero sigue siendo demasiado elevado, para una empresa en crecimiento como lo es Megabyte S.A. Por eso propusimos a la empresa realizar la compra de los routers que se ocuparan en cada una de las sucursales.

De esta manera, decidimos realizar una tercera cotización al mismo proveedor de servicios esta para evaluar el costo de solamente el despliegue del servicio de internet, ya que los routers serian propiedad del cliente en este caso la empresa Megabyte.

En la tabla 10 se observan los costos que tendría solamente el arrendamiento del servicio de internet en cada una de las sucursales. Cabe destacar que el ISP genera un contrato por 36 meses, en donde mensualmente se pagara una cuota de $160.00 americanos por la sede de casa matriz y $40.00 por cada una de las otras sucursales.

Tabla 10. Costo de servicio de internet. [Elaboración propia]

Cliente Megabyte				
Servicio internet				
Sucursal	**Ancho de banda**	**Distancia cableado fibra óptica (Mts)**	**Router proveído por ISP**	**Renta mensual**
Casa Matriz Internet	50 Mb	150 mts	No	$ 160.00
Sucursal Masaya datos	10 Mb	200 mts	No	$ 40.00
Sucursal Chinandega datos	10 Mb	350 mts	No	$ 40.00
Sucursal Matagalpa datos	10 Mb	400 mts	No	$ 40.00
			Total	**$ 280.00**

Observamos que, el precio de la inversión por el servicio de internet corporativo tiene un costo mucho menor, cuando el router no es brindado por el proveedor de servicios, siendo la mejor opción adquirir los routers por cuenta propia, los precios de dichos equipos se especifican en la tabla 11, así como también el costo que tendrá la implementación y configuración de los mismos.

Tabla 11. Inversión inicial, implementación DVMP. [Elaboración propia]

Cliente Megabyte						
Inversión Inicial (Equipos e Implementación)						
Sucursal	**Costo router Cisco**	**Costo switch Cisco**	**Horas de trabajo**	**Costo por hora**	**Costo de implementación**	**Costo total por sucursal**
Casa matriz	$ 499.99	$ 200.00	6	$ 40.00	$ 240.00	$ 985.99
Sucursal Masaya	$ 499.99	$ 200.00	6	$ 40.00	$ 240.00	$ 985.99
Sucursal Chinandega	$ 499.99	$ 200.00	6	$ 40.00	$ 240.00	$ 985.99
Sucursal Matagalpa	$ 499.99	$ 200.00	6	$ 40.00	$ 240.00	$ 985.99
					Total	**$ 3,943.96**

Para la compra de los routers, se realizó la comparación de 3 diferentes proveedores reconocidos en la gama de la tecnología de redes, entre los cuales se eligieron Cisco, Huawei y MikroTik, por ser los más utilizados en el país.

Primeramente, se realizó una comparación de las características entre los dispositivos de routing y switching de los diferentes proveedores. Cabe recalcar que cuentan con características similares.

En la tabla 12 se realiza la comparación de características en los routers.

Tabla 12. Características de los routers. [Elaboración propia]

Características	Router Cisco867	Router Huawei AR129	Router MikroTik CCR1009-7G-1C-1S+
Software	Cisco IOS 15.2(2)T	V200R008C20	RouterOS 6
Interfaz WAN	GE o Multimodo VDSL2/ADSL2+ sobre servicios telefonicos	1 x VDSL2 (compatible con ADSL2+ Annex A/M, Annex B/J)	1 x SFP+ ports
Interfaz LAN	2 GE + 3-port 10-/100-Mbps administración de switching	4 x FE (pueden ser cnfiguradas com interfaces WAN)	8 x 10/100/1000 Ethernet ports
WIFI	-	-	-
Puerto USB 2.0	1	1	1
Puert consola	1	1	1
RAM	512 MB	256 MB	2 GB
IPv4 routing	Static route, RIP, and BGP	Static route, RIP, and BGP	Static route, RIP, and BGP
IPv6 routing	Static route, RIPng, ICMPv6	Static route, RIPng, and BGP4+	Static route, RIPng, and BGP4+
Servicios basicos	NAT, DHCP, ACLs, DNS	ARP, PBR, DNS, DHCP, and NAT	NAT, DHCP, ACLs, DNS
Número de usuarios recomendados	10	20	Depende del nivel de licencia que se tengan.

En la tabla 13, se realiza la comparación de características en los switches.

Tabla 13. Características de los switches. [Elaboración propia]

Características	Switch Cisco catalyst 2960	Switch Huawei S5720	CRS326-24G-2S+IN
Interfaz LAN	24 gigabit Ethernet (10/100/1000)	24 gigabit Ethernet (10/100/1000)	24 gigabit Ethernet (10/100/1000)
Puertos SFP	2	4	2
Puerto USB 2.0	2	1	
Puert consola	1	1	1
RAM	256 MB	512MB	512 MB
Cantidad de VLANs	255	4000	4000

Después, se realizó una comparación en los precios de cada uno de los dispositivos, dicha información fue recopilada de las páginas oficiales de cada uno de los proveedores. Ver figura 21.

Presupuesto Implementación DMVPN

Precio por equipo (Cisco)

Router Cisco867	$	499.99
Ingresos adicionales	$	300.00
Total de ingresos mensuales	$	799.99

Precio por equipo (Huawei)

Router AR129	$	491.56
Ingresos adicionales	$	300.00
Total de ingresos mensuales	$	791.56

Precio por equipo (Mikrotik)

Ingreso 1	$	4,000.00
Ingresos adicionales	$	300.00
Total de ingresos mensuales	$	4,300.00

Costo previsto (Equipos Cisco)	$	3,299.95
Costo previsto (Equipos Huawei)	$	3,385.80
Costos previsto (Equipos Mikrotik)	$	3,521.00

Equipos Cisco

	Cantidad prevista	Costo	Costo total
Router Cisco867	5	$ 499.99	$ 2,499.95
Switch Cisco catalyst 2960	4	$ 200.00	$ 800.00
Subtotal			$ 3,299.95

Equipos Huawei

	Cantidad prevista	Costo	Costo total
Router AR129	5	$ 491.56	$ 2,457.80
Switch S5720	4	$ 232.00	$ 928.00
Subtotal			$ 3,385.80

Equipos Mikrotik

	Cantidad prevista	Costo	Diferencia
Router CCR2004-16G-2S+	5	$ 545.00	$ 2,725.00
Switch CRS326-24G-2S+IN	4	$ 199.00	$ 796.00
Subtotal			$ 3,521.00

Figura 21. Presupuesto para la implementación DMVPN.

Podemos concluir que, el costo total del servicio de internet corporativo más el costo de la adquisición de los routers por cuenta propia es la opción ideal para el cliente, así a como de observa en la tabla 14.

Tabla 14. Servicio internet con equipos propios. [Elaboración propia]

Cliente Megabyte						
Servicio internet con equipos propios						
Sucursal	**Ancho de banda**	**Distancia cableado fibra optica (Mts)**	**Router proveido por ISP**	**Plazo de renta**	**Plazo de renta / mes**	**Renta total**
Casa Matriz Internet	50 Mb	150 mts	No	36	$ 160.00	$ 5,760.00
Sucursal Masaya datos	10 Mb	200 mts	No	36	$ 40.00	$ 1,440.00
Sucursal Chinandega datos	10 Mb	350 mts	No	36	$ 40.00	$ 1,440.00
Sucursal Matagalpa datos	10 Mb	400 mts	No	36	$ 40.00	$ 1,440.00
				Total	**$ 280.00**	**$ 10,080.00**

Sin embargo, pare reducir aún más los costos se recomienda al cliente Megabyte adquirir los servicios de internet corporativo solo para los dos enlaces de casa matriz y en las sucursales se recomienda adquirir servicios de internet masivo como HFC y GPON, por lo general estas tecnologías ocupan asignación de direccionamiento WAN de manera dinámica, esto no sería un inconveniente ya que en comparación con otras tecnologías de túnel con el despliegue de DMVPN no es necesario que los spokes tengan configurada una IP publica estática.

8. Guía de implementación de la red DMVPN.

Una vez definido el diseño de la red DMVPN, procedimos con la fase de emulación en el software GNS3 y realizamos una guía de implementación con el paso a paso de las configuraciones.

En esta etapa se realizó la instalación de cada uno de los softwares a utilizar.

8.1 Instalación de software para la emulación.

Para la emulación de la red DMVPN, previamente se instalaron y configuraron los siguientes softwares:

- GNS3 versión 2.2.38.
- VMware Workstation Pro 17.
- Instalación de IOSv cisco en GSN3.
- Wireshark versión 4.0.5.

La instalación de estos softwares se realizó en el sistema operativo Windows, y las especificaciones del ordenador son Procesador: 11th Gen Intel(R) Core (TM) i7-1165G7 @ 2.80GHz 1.69 GHz y RAM instalada 16.0 GB (15.7 GB utilizable).

La emulación y configuración de la red DMVPN se realizó en el software GNS3, en donde, se cargó el IOS de los routers virtuales de la marca Cisco con el sistema operativo IOS 15, cabe mencionar que la emulación se realizó con routers Cisco debido a que la tecnología DMVPN fue desarrollada por la misma marca. Dicha tecnología también puede ser desplegada con diferentes proveedores.

A continuación, se aborda el proceso de la instalación de los softwares que utilizamos para la emulación del proyecto.

- **GNS3 versión 2.2.38.**

Este es un software de emulación, que permite diseñar y probar redes utilizando dispositivos virtuales por medio de las imágenes de dichos dispositivos, tales

como Cisco, Huawei, entre otros. Este software debe de ser ejecutado en una máquina virtual; entre las más utilizadas tenemos: Oracle VM, VirtualBox o VMware Workstation.

Si bien se puedo utilizar el software VIRL (Virtual Internet Routing Lab), que es un producto de la marca Cisco, para la emulación de este proyecto, se decidió utilizar GNS3 ya que este software nos permite personalizar la emulación según las necesidades requeridas de la red. Los requerimientos mínimos para instalar GNS3 en el sistema operativo Windows son los siguientes:

Tabla 15. Requerimientos GNS3. [28]

Ítem	Requerimiento
Sistema operativo	Windows 7 (64 bit)
Procesador	2 o más núcleos lógicos
Virtualización	Se requieren extensiones de virtualización. Es posible que deba habilitar esto a través del BIOS de su computadora.
Memoria	4 GB RAM
Almacenamiento	1 GB de espacio disponible

Para desarrollar la emulación de la red DMVPN, primeramente, se descargó el software gratuito GNS3 en el siguiente link Software | GNS3. Una vez descargado el instalador procedimos a abrir la aplicación de GNS3, para realizar su respectiva instalación de prerrequisitos y softwares opcionales.

- **VMware Workstation Pro 17.**

Este es un software de virtualización que permite ejecutar múltiples sistemas operativos en una sola computadora. Esta VM (Virtual machine) permite configurar y emular redes virtuales para probar y validar configuraciones de red.

Los requisitos generales para su instalación del sistema son:

Tabla 16. Requerimientos VMware Workstation. [29]

Ítem	Requisitos
Sistema Operativo	Windows 7 (32 bit o 64 bit)
Procesador	Velocidad de núcleo de 1,3 GHz o superior
Memoria	4 GB RAM

Se instalo VMware Workstation, para crear una VM segura y aislada, para instalar en ella el software GNS3. Se decidió utilizar la versión pro ya que permite ejecutar múltiples máquinas virtuales al mismo tiempo. El software de VMware Worstation se descargó en el siguiente link: Windows VM | Workstation Pro | VMware. Una vez descargado el software, procedimos a la instalación de la aplicación. El último paso para completar la instalación de GNS3 es la elección de la VM que se utilizará.

Instalación de IOSv cisco en GSN3.

Para la instalación del router virtual de cisco en nuestro GNS3, descargamos los archivos desde el siguiente link de Google drive Software Download - Cisco Systems.

- **Wireshark versión 4.0.5.**

Es un software utilizado para analizar las redes de computadoras, por medio de capturas del tráfico de la red en tiempo real, esto permite identificar y solucionar problemas de rendimiento y seguridad en la red.

Se procedió con la instalación del software Wireshark en su versión 4.0.5, el enlace de descarga del programa es https://www.wireshark.org/download.html. Una vez descargado el software procedimos a la instalación de la aplicación. Al final de la instalación se tendrá reiniciar el ordenador.

En resumen, para ejecutar la máquina virtual del GNS3 se instaló el software Vmware Workstation Pro, para emular la red completa se instaló el software GNS3 y a este se le agregaron las imágenes virtuales del router IOSv15, también se

instaló el software Secure CRT, este para tener acceso a la configuración de los comandos de cada router vía CLI y por último se instaló el software Wireshark para con este analizar el comportamiento del tráfico al hacer uso de los protocolos NHRP y IPSEC.

8.2 Configuración de los equipos.

A continuación, se muestra el paso a paso de la configuración de cada uno de los equipos que forman parte de la red DMVPN de la empresa Megabyte S.A.

A nivel LAN se configuraron los protocolos NAT y DHCP para todas las sucursales y se configuro el protocolo HSRP para tener redundancia de la red LAN en la sucursal de casa matriz. También se realizaron las configuraciones a nivel de túnel de los protocolos mGRE, NHRP, IPsec y de enrutamiento OSPF.

Este proyecto se desarrolló en los siguientes 9 (nueve) pasos, en donde se detallan los comandos utilizados en cada configuración, así como también las validaciones del funcionamiento que tendrá la red una vez que estén implementados cada uno de los protocolos.

- **Paso 1: Configuración interfaces WAN.**

En el primer paso se realizó la configuración de las IP pública **(ver tabla 6)**, en cada una de las interfaces WAN de los routers y también se realizó la configuración de la ruta por defecto con su IP del siguiente salto, ya que a través de estas rutas se alcanzarán las redes que no estén incluida en la tabla de enrutamiento, es decir se alcanzaran redes externas como Internet.

Los segmentos de IP Publicas son proveídos por el ISP, en nuestro trabajo con fin académico se utilizan segmentos IP del rango 200.10.0.0 con máscaras de red /30 o en su expresión decimal 255.255.255.252, con este rango es más que suficiente para realizar la conexión de los routers hacia nuestro proveedor de servicio.

A continuación, de manera ilustrativa se mostrarán las configuraciones en imágenes y en los anexos del documento se podrá obtener la configuración en texto para cada router.

De la figura 22 a la 26 se muestran las configuraciones de las interfaces WAN de cada router involucrado en la red.

- **Configuración Managua_Hub_1**

```
MANAGUA_HUB_1(config)#interface gigabitethernet 0/0
MANAGUA_HUB_1(config-if)#ip address 200.10.1.1 255.255.255.252
MANAGUA_HUB_1(config-if)#no shutdown
MANAGUA_HUB_1(config-if)##
MANAGUA_HUB_1(config-if)#ip route 0.0.0.0 0.0.0.0 200.10.1.2
MANAGUA_HUB_1(config)#
```

Figura 22. Configuración interfaz WAN Managua_Hub_1.

- **Configuración Managua_Hub_2**

```
MANAGUA_HUB_2(config)#int gigabitEthernet 0/0
MANAGUA_HUB_2(config-if)#ip address 200.20.1.2 255.255.255.252
MANAGUA_HUB_2(config-if)#no shutdown
MANAGUA_HUB_2(config-if)##
MANAGUA_HUB_2(config-if)#ip route 0.0.0.0 0.0.0.0 200.20.1.1
MANAGUA_HUB_2(config)#
```

Figura 23. Configuración interfaz WAN Managua_Hub_2.

- **Configuración Masaya_Spoke_1**

```
MASAYA_SPOKE_1(config)#interface ethernet 0/0
MASAYA_SPOKE_1(config-if)#ip address 200.1.1.1 255.255.255.252
MASAYA_SPOKE_1(config-if)#no shutdown
MASAYA_SPOKE_1(config-if)##
MASAYA_SPOKE_1(config-if)#ip route 0.0.0.0 0.0.0.0 200.1.1.2
MASAYA_SPOKE_1(config)#
```

Figura 24. Configuración interfaz WAN Masaya_Spoke_1.

- **Configuración Chinandega_Spoke_2**

```
CHINANDEGA_SPOKE_2(config)#interface Ethernet0/0
CHINANDEGA_SPOKE_2(config-if)#ip address 200.2.2.2 255.255.255.252
CHINANDEGA_SPOKE_2(config-if)#no shutdown
CHINANDEGA_SPOKE_2(config-if)##
CHINANDEGA_SPOKE_2(config-if)#ip route  0.0.0.0 0.0.0.0 200.2.2.1
CHINANDEGA_SPOKE_2(config)#
```

Figura 25. Configuración interfaz WAN Chinandega_Spoke_2.

- **Configuración Matagalpa_Spoke_3**

```
MATAGALPA_SPOKE_3(config)#int ethernet 0/0
MATAGALPA_SPOKE_3(config-if)#ip address 200.3.3.1 255.255.255.252
MATAGALPA_SPOKE_3(config-if)#no shutdown
MATAGALPA_SPOKE_3(config-if)##
MATAGALPA_SPOKE_3(config-if)#ip route 0.0.0.0 0.0.0.0 200.3.3.2
```

Figura 26. Configuración interfaz WAN Matagalpa_Spoke_3.

En la figura 23, encontramos las configuraciones del router “Internet” que simulará la conexión con los distintos proveedores ISP con los cuales tendrá contrato el cliente Megabyte, como se puede observar en cada interface se realizaron las configuraciones de las IP publica con mascara 255.255.255.252 que servirán de gateway o puerta de enlace para cada una de las IP WAN que ya se configuraron en los router de cada sucursal.

También, se realizó la configuración de la interface loopback 5 con la IP Publica 8.8.8.8 con mascará 255.255.255.255, esta IP Publica simulará el acceso a Internet y tendrá más sentido su configuración cuando ya estemos en el paso 4.

- **Configuración router Internet**

```
INTERNET(config)#hostname INTERNET
INTERNET(config)##
INTERNET(config)#interface Ethernet0/0
INTERNET(config-if)#description ISP_MANAGUA_HUB_1
INTERNET(config-if)#ip address 200.10.1.2 255.255.255.252
INTERNET(config-if)#no shutdown
INTERNET(config-if)##
INTERNET(config-if)#interface Ethernet0/1
INTERNET(config-if)#description ISP_MANAGUA_HUB_2
INTERNET(config-if)#ip address 200.20.1.1 255.255.255.252
INTERNET(config-if)#no shutdown
INTERNET(config-if)##
INTERNET(config-if)#interface Ethernet0/2
INTERNET(config-if)#description ISP_MASAYA_SPOKE_1
INTERNET(config-if)#ip address 200.1.1.2 255.255.255.252
INTERNET(config-if)#no shutdown
INTERNET(config-if)##
INTERNET(config-if)#interface Ethernet0/3
INTERNET(config-if)#description ISP_CHINANDEGA_SPOKE_2
INTERNET(config-if)#ip address 200.2.2.1 255.255.255.252
INTERNET(config-if)#no shutdown
INTERNET(config-if)##
INTERNET(config-if)#interface Ethernet1/0
INTERNET(config-if)#description ISP_MATAGALPA_SPOKE_3
INTERNET(config-if)#ip address 200.3.3.2 255.255.255.252
INTERNET(config-if)#no shutdown
INTERNET(config-if)##
INTERNET(config-if)#interface Loopback5
INTERNET(config-if)# ip address 8.8.8.8 255.255.255.255
```

Figura 27. Configuración de las interfaces WAN del ISP.

De la figura 28 a 30, se realizan las validaciones de conectividad para verificar funcionamiento de la red WAN:

- **Prueba de conectividad WAN.**

```
MANAGUA_HUB_1#ping 200.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/13/34 ms
```

Figura 28. Conectividad Hub-Spoke_1.

```
MANAGUA_HUB_1#ping 200.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/9/15 ms
```

Figura 29. Conectividad Hub-Spoke_2.

```
MANAGUA_HUB_1#ping 200.3.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.3.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/9/24 ms
```

Figura 30. Conectividad Hub-Spoke_3.

- **Paso 2: Configuración NAT.**

En el paso 2, se realizaron las configuraciones de las IPs de segmento privado para cada una de las interfaces físicas LAN de los routers **(ver tabla 5),** estas estarán en el segmento IP 192.168.1.0/24 o su expresión en decimal 255.255.255.0, se tendrá este segmento ya que tiene disponible 252 IP para su configuración en cada dispositivo, de esta manera se toma en cuenta el crecimiento que podrá tener en el futuro cada sucursal y así lograr ser una red escalable.

También, en este mismo paso, se procedió con las configuraciones de traslación de redes privadas a publicas utilizando el protocolo NAT, en su forma específica de PAT (Port Address Translation) sobrecargado, ya que en esta versión permite

que múltiples dispositivos en una red privada compartan una única dirección IP pública utilizando diferentes números de puerto.

Primeramente, se realizó la configuración de una lista de accesos numerada para permitir exclusivamente el segmento de IP LAN de cada sucursal, el resto de segmentos será denegado.

Luego, se realizó la configuración de NAT overload donde se toma como origen la lista de acceso que ya fue creada y que contiene el segmento LAN y esta hará un overload o sobrecarga a la interface WAN que contiene el segmento de IP Publica y que tiene salida a internet.

Como último paso, se realizó la configuración de rol NAT que tendrán las interfaces físicas; en la interface LAN se configura el comando **ip nat inside** ya que contiene el segmento IP privado y en la interface WAN, que contiene el segmento IP público, se realizó la configuración de **ip nat outside**.

Entre las figuras número 31 a la 35, se muestra la configuración del paso 2 en cada uno de los routers:

- **Configuración Managua_Hub_1**

```
MANAGUA_HUB_1(config)#  int gi 0/1
MANAGUA_HUB_1(config-if)#ip address 192.168.1.2 255.255.255.0
MANAGUA_HUB_1(config-if)#no shutdown
MANAGUA_HUB_1(config-if)##
MANAGUA_HUB_1(config-if)#access-list 2 permit 192.168.1.0 0.0.0.255
MANAGUA_HUB_1(config)#access-list 2 deny   any
MANAGUA_HUB_1(config)##
MANAGUA_HUB_1(config)#ip nat inside source list 2 interface giga 0/0 overload
MANAGUA_HUB_1(config)##
MANAGUA_HUB_1(config)#interface giga 0/0
MANAGUA_HUB_1(config-if)#ip nat outside
MANAGUA_HUB_1(config-if)##
MANAGUA_HUB_1(config-if)#interface giga 0/1
MANAGUA_HUB_1(config-if)#ip nat inside
MANAGUA_HUB_1(config-if)#
```

Figura 31. Configuración interfaz LAN y NAT Managua_Hub_1.

- **Configuración Managua_Hub_2**

```
MANAGUA_HUB_2(config)#int gi 0/1
MANAGUA_HUB_2(config-if)#ip address 192.168.1.3 255.255.255.0
MANAGUA_HUB_2(config-if)#no shutdown
MANAGUA_HUB_2(config-if)##
MANAGUA_HUB_2(config-if)#access-list 2 permit 192.168.1.0 0.0.0.255
MANAGUA_HUB_2(config)#access-list 2 deny   any
MANAGUA_HUB_2(config)##
MANAGUA_HUB_2(config)#ip nat inside source list 2 interface giga 0/0 overload
MANAGUA_HUB_2(config)##
MANAGUA_HUB_2(config)#interface giga 0/0
MANAGUA_HUB_2(config-if)#ip nat outside
MANAGUA_HUB_2(config-if)##
MANAGUA_HUB_2(config-if)#interface giga 0/1
MANAGUA_HUB_2(config-if)#ip nat inside
```

Figura 32. Configuración interfaz LAN y NAT Managua_Hub_2.

- **Configuración Masaya_Spoke_1**

```
MASAYA_SPOKE_1(config)#int ethernet 0/1
MASAYA_SPOKE_1(config-if)#ip address 192.168.2.1 255.255.255.0
MASAYA_SPOKE_1(config-if)#no shutdown
MASAYA_SPOKE_1(config-if)##
MASAYA_SPOKE_1(config-if)#access-list 2 permit 192.168.2.0 0.0.0.255
MASAYA_SPOKE_1(config)#access-list 2 deny   any
MASAYA_SPOKE_1(config)##
MASAYA_SPOKE_1(config)#$de source list 2 interface ethernet 0/0 overload
MASAYA_SPOKE_1(config)##
MASAYA_SPOKE_1(config)#interface ethernet 0/0
MASAYA_SPOKE_1(config-if)#ip nat outside
MASAYA_SPOKE_1(config-if)##
MASAYA_SPOKE_1(config-if)#interface ethernet 0/1
MASAYA_SPOKE_1(config-if)#ip nat inside
```

Figura 33. Configuración interfaz LAN y NAT Masaya_Spoke_1.

- **Configuración Chinandega_Spoke_2**

```
CHINANDEGA_SPOKE_2(config)#int ethernet 0/1
CHINANDEGA_SPOKE_2(config-if)#ip address 192.168.3.1 255.255.255.0
CHINANDEGA_SPOKE_2(config-if)#no shutdown
CHINANDEGA_SPOKE_2(config-if)##
CHINANDEGA_SPOKE_2(config-if)#access-list 2 permit 192.168.3.0 0.0.0.255
CHINANDEGA_SPOKE_2(config)#access-list 2 deny   any
CHINANDEGA_SPOKE_2(config)##
CHINANDEGA_SPOKE_2(config)#$de source list 2 interface ethernet 0/0 overload
CHINANDEGA_SPOKE_2(config)##
CHINANDEGA_SPOKE_2(config)#interface ethernet 0/0
CHINANDEGA_SPOKE_2(config-if)#ip nat outside
CHINANDEGA_SPOKE_2(config-if)##
CHINANDEGA_SPOKE_2(config-if)#interface ethernet 0/1
CHINANDEGA_SPOKE_2(config-if)#ip nat inside
```

Figura 34. Configuración interfaz LAN y NAT Chinandega_Spoke_2.

- **Configuración Matagalpa_Spoke_3**

```
MATAGALPA_SPOKE_3(config)#int ethernet 0/1
MATAGALPA_SPOKE_3(config-if)#ip address 192.168.4.1 255.255.255.0
MATAGALPA_SPOKE_3(config-if)#no shutdown
MATAGALPA_SPOKE_3(config-if)##
MATAGALPA_SPOKE_3(config-if)#access-list 2 permit 192.168.4.0 0.0.0.255
MATAGALPA_SPOKE_3(config)#access-list 2 deny   any
MATAGALPA_SPOKE_3(config)##
MATAGALPA_SPOKE_3(config)#$de source list 2 interface ethernet 0/0 overload
MATAGALPA_SPOKE_3(config)##
MATAGALPA_SPOKE_3(config)#interface ethernet 0/0
MATAGALPA_SPOKE_3(config-if)#ip nat outside
MATAGALPA_SPOKE_3(config-if)##
MATAGALPA_SPOKE_3(config-if)#interface ethernet 0/1
MATAGALPA_SPOKE_3(config-if)#ip nat inside
```

Figura 35. Configuración interfaz LAN y NAT Matagalpa_Spoke_3.

- **Paso 3: Configuración DHCP.**

En el tercer paso, se procedió con la configuración DHCP (Dynamic Host Configuration Protocol) en los routers de cada sucursal, esto para que la asignación de direcciones IPs, puertas de enlaces, máscaras de red y servidores DNS se realicen de manera automática. En los 2 (dos) routers de casa matriz, los cuales brindan alta disponibilidad, se excluyó 3 (tres) direcciones IP de la asignación automática de DHCP, 2 (dos) pertenecientes a la puerta de enlace física de la red LAN (una por cada router) y 1 (una) que tendrá función de IP virtual. Por otra parte, en las sucursales solamente solo se excluyó 1 (una) dirección IP que representa a la puerta de enlace de cada red LAN.

A partir de la figura 36 hasta la figura 40 se realizan las configuraciones de DHCP en cada router.

- **Configuración Managua_Hub_1**

```
MANAGUA_HUB_1(config)#ip dhcp excluded-address 192.168.1.1
MANAGUA_HUB_1(config)#ip dhcp excluded-address 192.168.1.2
MANAGUA_HUB_1(config)#ip dhcp excluded-address 192.168.1.3
MANAGUA_HUB_1(config)##
MANAGUA_HUB_1(config)#ip dhcp pool DHCP_LAN
MANAGUA_HUB_1(dhcp-config)#network 192.168.1.0 255.255.255.0
MANAGUA_HUB_1(dhcp-config)#default-router 192.168.1.1
MANAGUA_HUB_1(dhcp-config)#lease 0 12 0
MANAGUA_HUB_1(dhcp-config)#dns-server 8.8.8.8
MANAGUA_HUB_1(dhcp-config)#
```

Figura 36. Configuración DHCP Managua_Hub_1.

- **Configuración Managua_Hub_2**

```
MANAGUA_HUB_2(config)#ip dhcp excluded-address 192.168.1.1
MANAGUA_HUB_2(config)#ip dhcp excluded-address 192.168.1.2
MANAGUA_HUB_2(config)#ip dhcp excluded-address 192.168.1.3
MANAGUA_HUB_2(config)##
MANAGUA_HUB_2(config)#ip dhcp pool DHCP_LAN
MANAGUA_HUB_2(dhcp-config)#network 192.168.1.0 255.255.255.0
MANAGUA_HUB_2(dhcp-config)#default-router 192.168.1.1
MANAGUA_HUB_2(dhcp-config)#lease 0 12 0
MANAGUA_HUB_2(dhcp-config)#dns-server 8.8.8.8
```

Figura 37. Configuración DHCP Managua_Hub_2.

- **Configuración Masaya_Spoke_1**

```
MASAYA_SPOKE_1(config)#ip dhcp excluded-address 192.168.2.1
MASAYA_SPOKE_1(config)##
MASAYA_SPOKE_1(config)#ip dhcp pool DHCP_LAN
MASAYA_SPOKE_1(dhcp-config)#network 192.168.2.0 255.255.255.0
MASAYA_SPOKE_1(dhcp-config)#default-router 192.168.2.1
MASAYA_SPOKE_1(dhcp-config)#lease 0 12 0
MASAYA_SPOKE_1(dhcp-config)#dns-server 8.8.8.8
MASAYA_SPOKE_1(dhcp-config)#
MASAYA_SPOKE_1(dhcp-config)#
```

Figura 38. Configuración DHCP Masaya_Spoke_1.

- **Configuración Chinandega_Spoke_2**

```
CHINANDEGA_SPOKE_2(config)#ip dhcp excluded-address 192.168.3.1
CHINANDEGA_SPOKE_2(config)##
CHINANDEGA_SPOKE_2(config)#ip dhcp pool DHCP_LAN
CHINANDEGA_SPOKE_2(dhcp-config)#network 192.168.3.0 255.255.255.0
CHINANDEGA_SPOKE_2(dhcp-config)#default-router 192.168.3.1
CHINANDEGA_SPOKE_2(dhcp-config)#lease 0 12 0
CHINANDEGA_SPOKE_2(dhcp-config)#dns-server 8.8.8.8
```

Figura 39. Configuración DHCP Chinadega_Spoke_2.

- **Configuración Matagalpa_Spoke_3**

```
MATAGALPA_SPOKE_3(config)#ip dhcp excluded-address 192.168.4.1
MATAGALPA_SPOKE_3(config)##
MATAGALPA_SPOKE_3(config)#ip dhcp pool DHCP_LAN
MATAGALPA_SPOKE_3(dhcp-config)#network 192.168.4.0 255.255.255.0
MATAGALPA_SPOKE_3(dhcp-config)#default-router 192.168.4.1
MATAGALPA_SPOKE_3(dhcp-config)#lease 0 12 0
MATAGALPA_SPOKE_3(dhcp-config)#dns-server 8.8.8.8
```

Figura 40. Configuración DHCP Matagalpa_Spoke_3.

- **Paso 4: Configuración HSRP y IP SLA.**

El cuarto paso se basa en la configuración del protocolo HSRP (Hot Standby Router Protocol), con el fin de crear redundancia y brindar una red alta disponibilidad y tolerancia fallas a nivel de LAN y WAN. Este paso solo se configuro en los routers Hubs ubicados en casa matriz, que es donde se implementó una red redúndate para disminuir el tiempo de inactividad cuando se presenten fallas físicas o a nivel de enrutador.

Primeramente, en el Hub_1 que tiene rol de router principal, se realizó la configuración de una IP SLA 1 esto para enviar pings ICMP a la dirección IP 8.8.8.8 (configurada en el router de "Internet" en el paso 1) cada 20 segundos, comenzando de inmediato y ejecutándose de forma continua. Esto permite monitorear la conectividad hacia esa dirección IP específica. Luego se agrupo la IP SLA 1 dentro del objeto track 100.

A continuación, en la figura 41 se muestran las configuraciones de IP SLA realizada en Managua_Hub_1.

- **Configuración Managua_Hub_1**

```
MANAGUA_HUB_1(dhcp-config)#ip sla 1
MANAGUA_HUB_1(config-ip-sla)# icmp-echo 8.8.8.8
MANAGUA_HUB_1(config-ip-sla-echo)# frequency 20
MANAGUA_HUB_1(config-ip-sla-echo)#$dule 1 life forever start-time now
MANAGUA_HUB_1(config)##
MANAGUA_HUB_1(config)#track 100 ip sla 1 reachability
MANAGUA_HUB_1(config-track)##
MANAGUA_HUB_1(config-track)#interface GigabitEthernet0/1
MANAGUA_HUB_1(config-if)# standby version 2
MANAGUA_HUB_1(config-if)# standby 1 ip 192.168.1.1
MANAGUA_HUB_1(config-if)# standby 1 priority 150
MANAGUA_HUB_1(config-if)# standby 1 preempt
MANAGUA_HUB_1(config-if)# standby 1 track 100 decrement 60
```

Figura 41. Configuración IP SLA Managua_Hub_1.

Siguiendo con Managua_Hub_1, se realizó la configuración del protocolo HSRP en su versión 2, esto en la interface física Gi0/1, que tiene el segmento LAN 192.168.1.2 y se crea una segunda IP la cual será virtual 192.168.1.1, que será compartida por ambos routers Hub, luego se le configura una prioridad de HSRP en 150, en HSRP el router que tenga la mayor prioridad tendrá el rol de activo.

También se configuro el comando **standby 1 preempt**, este permite que un router con una prioridad más alta tome el control como router activo si se recupera después de un fallo. En otras palabras, si un router con una prioridad más alta se une a la red, puede tomar el control del grupo HSRP y convertirse en el router activo.

Y finalizamos con la configuración del **standby 1 track 100 decrement 60**, esto hará que, si se pierde la conectividad del track 100 que contiene la IP SLA 1 y que a su vez esta está realizando un ping a la IP 8.8.8.8, este router decrementara su prioridad de HSRP en 60, cuando esto pase la prioridad de 150 pasara a 90 y esto hará que el Managua_HUB_2 asuma el rol de activo, ya que la prioridad por defecto de HSRP es de 100, es decir, esta sería mayor a los 90 que tendría router Managua_Hub_1.

En la imagen 42, se muestra la configuración del protocolo HSRP del router Managua_Hub_1.

```
MANAGUA_HUB_1(config)#interface GigabitEthernet0/1
MANAGUA_HUB_1(config-if)# standby version 2
MANAGUA_HUB_1(config-if)# standby 1 ip 192.168.1.1
MANAGUA_HUB_1(config-if)# standby 1 priority 150
MANAGUA_HUB_1(config-if)# standby 1 preempt
MANAGUA_HUB_1(config-if)# standby 1 track 100 decrement 60
```

Figura 42. Configuración HSRP Managua_Hub_1.

En router Managu_Hub_2, solamente se configura la versión 2 de HSRP, la IP virtual y el preempt, los cuales harán que asuma rol de activo si este llegara a tener una prioridad más alta que el router Managua_Hub_1. A como se puede observar en la figura 43.

- **Configuración Managua_Hub_2**

```
MANAGUA_HUB_2(config)#interface GigabitEthernet0/1
MANAGUA_HUB_2(config-if)# standby version 2
MANAGUA_HUB_2(config-if)# standby 1 ip 192.168.1.1
MANAGUA_HUB_2(config-if)# standby 1 preempt
MANAGUA_HUB_2(config-if)#
```

Figura 43. Configuración HSRP Managua_Hub_2.

Para la validación de alta disponibilidad a nivel de HSRP, se procedió con apagar la interface loopback 5 del router de “Internet”, al hacer esto el ping de la IP SLA de Managua_Hub_1 se pierde y a como se observa en la siguiente figura 44, el router Managua_Hub_1 disminuye el valor de su prioridad pasando a 90, obligándolo a pasar a estado standby.

```
MANAGUA_HUB_1#
*May 31 03:26:59.262: %TRACK-6-STATE: 100 ip sla 1 reachability Up -> Down
MANAGUA_HUB_1#
*May 31 03:26:59.876: %HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 1 state Active -> Speak
MANAGUA_HUB_1#
*May 31 03:27:10.976: %HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 1 state Speak -> Standby
MANAGUA_HUB_1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi0/1       1    90  P Standby 192.168.1.3     local           192.168.1.1
```

Figura 44. Validación alta disponibilidad Hub_1.

En la figura 45, se observa que el router Managua_Hub_2 asume el rol de activo con una prioridad de 100.

```
*May 31 03:27:00.489: %HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 1 state Standby -> Active
MANAGUA_HUB_2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi0/1       1    100 P Active  local           unknown         192.168.1.1
MANAGUA_HUB_2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi0/1       1    100 P Active  local           192.168.1.2     192.168.1.1
```

Figura 45. Validación alta disponibilidad Hub_2.

- **Paso 5: Configuración Tunel mGRE.**

A partir de este quinto paso, se realizan las configuraciones a nivel de túnel y enrutamiento, procedimos con la configuración de los túneles mGRE. Primero se crearon las interfaces túneles, dentro de cada interfaz túnel virtual se tomaron los siguientes parámetros:

- Las IPs deben de estar dentro del mismo segmento de red en nuestro caso decidimos ocupar el segmento 172.23.123.0/24 o en formato decimal 255.255.255.0 **(ver tabla 7).**
- El túnel GRE debe de ser configurado como multipunto
- El túnel source sera la IP publica configurada en cada WAN.

- Se realizan ajustes de los parámetros tcp de 1360 y mtu 1400, debido al incremento de los frames por los 20 bytes adicionales que tiene el tunel mGRE.

A continuación, se muestra las configuraciones realizadas en cada router a partir de la figura 46 a la 50:

- **Configuración Managua_Hub_1**

```
MANAGUA_HUB_1(config)#interface Tunnel100
MANAGUA_HUB_1(config-if)# ip address 172.23.123.100 255.255.255.0
MANAGUA_HUB_1(config-if)# tunnel source 200.10.1.1
MANAGUA_HUB_1(config-if)# tunnel mode gre multipoint
MANAGUA_HUB_1(config-if)# ip tcp adjust-mss 1360
MANAGUA_HUB_1(config-if)# ip mtu 1400
```

Figura 46. Configuración mGRE Managua_Hub_1.

- **Configuración Managua_Hub_2**

```
MANAGUA_HUB_2(config)#interface Tunnel100
MANAGUA_HUB_2(config-if)# ip address 172.23.123.200 255.255.255.0
MANAGUA_HUB_2(config-if)# tunnel source 200.20.1.2
MANAGUA_HUB_2(config-if)# tunnel mode gre multipoint
MANAGUA_HUB_2(config-if)# ip tcp adjust-mss 1360
MANAGUA_HUB_2(config-if)# ip mtu 1400
```

Figura 47. Configuración mGRE Managua_Hub_2.

- **Configuración Masaya_Spoke_1**

```
MASAYA_SPOKE_1(config)#interface Tunnel100
MASAYA_SPOKE_1(config-if)# ip address 172.23.123.1 255.255.255.0
MASAYA_SPOKE_1(config-if)# tunnel source 200.1.1.1
MASAYA_SPOKE_1(config-if)# tunnel mode gre multipoint
MASAYA_SPOKE_1(config-if)# ip tcp adjust-mss 1360
MASAYA_SPOKE_1(config-if)# ip mtu 1400
```

Figura 48. Configuración mGRE Masaya_Spoke_1.

- **Configuración Chinandega_Spoke_2**

```
MATAGALPA_SPOKE_3(config)#interface Tunnel100
MATAGALPA_SPOKE_3(config-if)# ip address 172.23.123.3 255.255.255.0
MATAGALPA_SPOKE_3(config-if)# tunnel source 200.3.3.1
MATAGALPA_SPOKE_3(config-if)# tunnel mode gre multipoint
MATAGALPA_SPOKE_3(config-if)# ip tcp adjust-mss 1360
MATAGALPA_SPOKE_3(config-if)# ip mtu 1400
```

Figura 49. Configuración mGRE Chinandega_Spoke_2.

- **Configuración Matagalpa_Spoke_3**

```
CHINANDEGA_SPOKE_2(config)#interface Tunnel100
CHINANDEGA_SPOKE_2(config-if)# ip address 172.23.123.2 255.255.255.0
CHINANDEGA_SPOKE_2(config-if)# tunnel source 200.2.2.2
CHINANDEGA_SPOKE_2(config-if)# tunnel mode gre multipoint
CHINANDEGA_SPOKE_2(config-if)# ip tcp adjust-mss 1360
CHINANDEGA_SPOKE_2(config-if)# ip mtu 1400
```

Figura 50. Configuración mGRE Matagalpa_Spoke_3.

- **Paso 6: Configuración NHRP Single Cloud.**

En el sexto paso se realiza la configuración del protocolo NHRP, con el fin de conectar los sitios de la empresa a través de una red en común, por medio de túneles de manera dinámica.

Primeramente, se creó un identificador de red, en nuestro caso ocupamos el número 100, con el comando **ip nhrp network-id 100,** este id de red debe de ser el mismo en todos los routers, tanto los designados como servidores a los designados como clientes.

- **Router configurado como servidores**

Se configuro la resolución de nombres NHRP dinámica para paquetes multicast, con el comando **ip nhrp map multicast dynamic**, con el fin que el router resuelva dinámicamente las direcciones de los destinos multicast, en función de los mensajes de solicitud NHRP recibidos, esto permite que el router NHRP aprenda de manera dinámica la dirección multicast de un destino, para luego enrutar el paquete hacia su próximo destino a través del túnel NHRP.

Por último, se configuró el comando **ip nhrp redirect**, que permite que el router servidor actúe como agente de redireccionamiento NHRP, esto con el fin de reenviar paquetes de destinos a nodos que no están conectados directamente al router, por medio de un mensaje NHRP.

A continuación, en la figura 51 se muestran las configuraciones del router servidor Hub_1:

- **Configuración Managua_Hub_1**

```
MANAGUA_HUB_1(config)#interface Tunnel100
MANAGUA_HUB_1(config-if)#ip nhrp network-id 100
MANAGUA_HUB_1(config-if)#ip nhrp redirect
MANAGUA_HUB_1(config-if)# ip nhrp map multicast dynamic
```

Figura 51. Configuración NHRP Managua_Hub_1.

El router servidor Managua_Hub_2, se configura de igual manera que el Managua_Hub_1, con una adicional configuración de mapeo, para indicarle que a pesar que será un router Hub, tiene un router servidor que en este caso son las direcciones IP de túnel y las direcciones IP públicas de Managua_Hub_1.

En la figura 52, se muestra las configuraciones del router servidor Managua_Hub_2.

- **Configuración Managua_Hub_2**

```
MANAGUA_HUB_2(config-if)#interface Tunnel100
MANAGUA_HUB_2(config-if)#ip nhrp network-id 100
MANAGUA_HUB_2(config-if)#ip nhrp redirect
MANAGUA_HUB_2(config-if)# ip nhrp map multicast Dynamic
MANAGUA_HUB_2(config-if)#
MANAGUA_HUB_2(config-if)# ip nhrp nhs 172.23.123.100 nbma 200.10.1.1 multicast
```

Figura 52. Configuración mGRE Managua_Hub_2.

- **Router configurado como cliente**

Por otra parte, los routers clientes se configuraron con el comando **ip nhrp nhs**, para que el router puede identificar las IP de túnel y las IP publica de los dos routers servidores y a través de estas enrutar los paquetes del túnel NHRP.

Adicional, se configura el comando **ip nhrp shortcut**, este permite establecer rutas directas entre router spokes y así mejorar la eficiencia y el rendimiento de la comunicación.

A continuación, entre la figura 53 a la 55, se muestra la configuración en cada uno de los router clientes.

- **Configuración Masaya_Spoke_1**

```
MASAYA_SPOKE_1(config)#interface Tunnel100
MASAYA_SPOKE_1(config-if)#ip nhrp network-id 100
MASAYA_SPOKE_1(config-if)# ip nhrp shortcut
MASAYA_SPOKE_1(config-if)##
MASAYA_SPOKE_1(config-if)# ip nhrp nhs 172.23.123.100
MASAYA_SPOKE_1(config-if)# ip nhrp map multicast 200.10.1.1
MASAYA_SPOKE_1(config-if)# ip nhrp map 172.23.123.100 200.10.1.1
MASAYA_SPOKE_1(config-if)##
MASAYA_SPOKE_1(config-if)#ip nhrp nhs 172.23.123.200
MASAYA_SPOKE_1(config-if)# ip nhrp map multicast 200.20.1.2
MASAYA_SPOKE_1(config-if)# ip nhrp map 172.23.123.200 200.20.1.2
```

Figura 53. Configuración mGRE Masaya_Spoke_1.

- **Configuración Chinandega_Spoke_2**

```
CHINANDEGA_SPOKE_2(config)#interface Tunnel100
CHINANDEGA_SPOKE_2(config-if)#ip nhrp network-id 100
CHINANDEGA_SPOKE_2(config-if)# ip nhrp nhs 172.23.123.100
CHINANDEGA_SPOKE_2(config-if)# ip nhrp map multicast 200.10.1.1
CHINANDEGA_SPOKE_2(config-if)# ip nhrp map 172.23.123.100 200.10.1.1
CHINANDEGA_SPOKE_2(config-if)# ip nhrp shortcut
CHINANDEGA_SPOKE_2(config-if)##
CHINANDEGA_SPOKE_2(config-if)#ip nhrp nhs 172.23.123.200
CHINANDEGA_SPOKE_2(config-if)# ip nhrp map multicast 200.20.1.2
CHINANDEGA_SPOKE_2(config-if)# ip nhrp map 172.23.123.200 200.20.1.2
```

Figura 54. Configuración mGRE Chinandega_Spoke_2.

- **Configuración Matagalpa_Spoke_3**

```
MATAGALPA_SPOKE_3(config)#interface Tunnel100
MATAGALPA_SPOKE_3(config-if)# ip nhrp network-id 100
MATAGALPA_SPOKE_3(config-if)# ip nhrp nhs 172.23.123.100
MATAGALPA_SPOKE_3(config-if)# ip nhrp map multicast 200.10.1.1
MATAGALPA_SPOKE_3(config-if)# ip nhrp map 172.23.123.100 200.10.1.1
MATAGALPA_SPOKE_3(config-if)# ip nhrp shortcut
MATAGALPA_SPOKE_3(config-if)##
MATAGALPA_SPOKE_3(config-if)#ip nhrp nhs 172.23.123.200
MATAGALPA_SPOKE_3(config-if)# ip nhrp map multicast 200.20.1.2
MATAGALPA_SPOKE_3(config-if)# ip nhrp map 172.23.123.200 200.20.1.2
```

Figura 55. Configuración mGRE Matagalpa_Spoke_3.

- **Paso 7: Configuración OSPF.**

En este séptimo paso, procedemos con la configuración del protocolo de enrutamiento dinamico OSPF en la interface tunnel 100, configuramos **ospf**

network point-to-multipoint ya que tendremos conectividad hacia todos los sitios remotos.

En la configuración del **router ospf 1**, se agregaron los segmentos de redes de túnel y las redes LAN de cada sucursal esto permitirá tener conectividad con todas las sucursales de manera dinámica. En las figuras de la 56 a la 60, se muestran las configuraciones de OSPF en cada uno de los routers.

- **Configuración Managua_Hub_1**

```
MANAGUA_HUB_1(config)#interface Tunnel100
MANAGUA_HUB_1(config-if)#ip ospf network point-to-multipoint
MANAGUA_HUB_1(config-if)##
MANAGUA_HUB_1(config-if)#router ospf 1
MANAGUA_HUB_1(config-router)# network 172.23.123.0 0.0.0.255 area 0
MANAGUA_HUB_1(config-router)# network 192.168.1.0 0.0.0.255 area 0
MANAGUA_HUB_1(config-router)# default-information originate
```

Figura 56. Configuración OSPF Managua_Hub_1.

- **Configuración Managua_Hub_2**

```
MANAGUA_HUB_2(config)#interface Tunnel100
MANAGUA_HUB_2(config-if)#ip ospf network point-to-multipoint
MANAGUA_HUB_2(config-if)##
MANAGUA_HUB_2(config-if)#router ospf 1
MANAGUA_HUB_2(config-router)# network 172.23.123.0 0.0.0.255 area 0
MANAGUA_HUB_2(config-router)# network 192.168.1.0 0.0.0.255 area 0
MANAGUA_HUB_2(config-router)# default-information originate
```

Figura 57. Configuración OSPF Managua_Hub_2.

- **Configuración Masaya_Spoke_1**

```
MASAYA_SPOKE_1(config)#interface Tunnel100
MASAYA_SPOKE_1(config-if)#ip ospf network point-to-multipoint
MASAYA_SPOKE_1(config-if)##
MASAYA_SPOKE_1(config-if)#router ospf 1
MASAYA_SPOKE_1(config-router)# network 172.23.123.0 0.0.0.255 area 0
MASAYA_SPOKE_1(config-router)# network 192.168.2.0 0.0.0.255 area 0
MASAYA_SPOKE_1(config-router)# default-information originate
```

Figura 58. Configuración OSPF Masaya_Spoke_1.

- **Configuración Chinandega_Spoke_2**

```
CHINANDEGA_SPOKE_2(config)#interface Tunnel100
CHINANDEGA_SPOKE_2(config-if)#ip ospf network point-to-multipoint
CHINANDEGA_SPOKE_2(config-if)##
CHINANDEGA_SPOKE_2(config-if)#router ospf 1
CHINANDEGA_SPOKE_2(config-router)# network 172.23.123.0 0.0.0.255 area 0
CHINANDEGA_SPOKE_2(config-router)# network 192.168.3.0 0.0.0.255 area 0
CHINANDEGA_SPOKE_2(config-router)# default-information originate
```

Figura 59. Configuración OSPF Chinandega_Spoke_2.

- **Configuración Matagalpa_Spoke_3**

```
MATAGALPA_SPOKE_3(config)#interface Tunnel100
MATAGALPA_SPOKE_3(config-if)#ip ospf network point-to-multipoint
MATAGALPA_SPOKE_3(config-if)##
MATAGALPA_SPOKE_3(config-if)#router ospf 1
MATAGALPA_SPOKE_3(config-router)# network 172.23.123.0 0.0.0.255 area 0
MATAGALPA_SPOKE_3(config-router)# network 192.168.4.0 0.0.0.255 area 0
MATAGALPA_SPOKE_3(config-router)# default-information originate
```

Figura 60. Configuración OSPF Matagalpa_Spoke_3.

➢ **Paso 8: Configuración IPsec.**

En este último paso de las configuraciones, se procedió a habilitar el marco de trabajo IPsec en sus dos fases. Estas configuraciones deberán ser exactamente las mismas en todos los routers.

Fase 1: se procedió con la configuración de las políticas isakmp, se utiliza como método de cifrado AES, como método de integridad de la información Hash, como método de autenticidad se tendrá una clave pre compartida y el grupo 2 de Diffie-Hellman para el intercambio de claves y el establecimiento de claves compartidas.

Para finalizar la configuración de la fase 1, se configura la clave pre compartida que será: “Megabyte” esta clave se utilizará para establecer asociaciones de seguridad con cualquier dirección IP (0.0.0.0).

Fase 2: se configura el transform-set con nombre “Megabyte”, y dentro de este transform-set se configuran los parámetros cifrados de la información. Se utiliza esp-aes 256 y para la integridad y autenticidad se utiliza esp-sha-hmac, el túnel será configurado en modo transporte, ya que tenemos un túnel mGRE ya creado y será este que configuraremos la protección de IPsec.

Luego, creamos un perfil de IPsec donde configuramos el intercambio de claves Perfect Forward Secrecy (PFS) utilizando diffie-hellman de grupo 14. PFS proporciona una clave de sesión única para cada comunicación, lo que mejora la seguridad en caso de que se comprometa una clave. A este perfil se asocia el transform-set ya creado previamente. Como último paso agregamos el perfil de IPsec dentro de la interface de túnel mGRE.

A continuación, en la figura 61 de manera ilustrativa se muestran la configuración del marco de trabajo IPsec para el router Hub_1, a como se señaló previamente esta configuración será la misma en cada uno de los routers de la red DMVPN.

- **Configuración Managua_Hub_1**

```
MANAGUA_HUB_1(config)#crypto isakmp policy 1
MANAGUA_HUB_1(config-isakmp)#encryption aes
MANAGUA_HUB_1(config-isakmp)#hash md5
MANAGUA_HUB_1(config-isakmp)#authentication pre-share
MANAGUA_HUB_1(config-isakmp)#group 2
MANAGUA_HUB_1(config-isakmp)##
MANAGUA_HUB_1(config-isakmp)#crypto isakmp key Megabyte address 0.0.0.0
MANAGUA_HUB_1(config)##
MANAGUA_HUB_1(config)#$c transform-set Megabyte esp-aes 256 esp-sha-hmac
MANAGUA_HUB_1(cfg-crypto-trans)#mode transport
MANAGUA_HUB_1(cfg-crypto-trans)##
MANAGUA_HUB_1(cfg-crypto-trans)#crypto ipsec profile Megabyte
MANAGUA_HUB_1(ipsec-profile)#set pfs group14
MANAGUA_HUB_1(ipsec-profile)#set transform-set Megabyte
MANAGUA_HUB_1(ipsec-profile)##
MANAGUA_HUB_1(ipsec-profile)#interface tunnel 100
MANAGUA_HUB_1(config-if)#tunnel  protection ipsec profile Megabyte
```

Figura 61. Configuración IPsec Managua_Hub_1.

- **Paso 9: Pruebas de funcionabilidad de DMVPN.**

Una vez implementado los protocolos de túnel y enrutamiento mGRE, NHRP, OSPF y el marco de trabajo IPsec, se procedió con la validación del correcto funcionamiento de la red DMVPN.

- **Validaciones túnel mGRE.**

El comando **Show tunnel endpoints tunnel 100**, se ejecuta en el router Managua_Hub_1, para validar que el túnel 100 está en función GRE multipunto, a como se observa en la figura 62.

```
MANAGUA_HUB_1#show tunnel endpoints tunnel 100
 Tunnel100 running in multi-GRE/IP mode

 Endpoint transport 200.1.1.1 Refcount 3 Base 0x1236072C Create Time 02:49:22
   overlay 172.23.123.1 Refcount 2 Parent 0x1236072C Create Time 02:49:22
   Tunnel Subblocks:
      tunnel-nhrp-sb:
         NHRP subblock has 1 entries
 Endpoint transport 200.2.2.2 Refcount 3 Base 0x1236062C Create Time 02:49:22
   overlay 172.23.123.2 Refcount 2 Parent 0x1236062C Create Time 02:49:22
   Tunnel Subblocks:
      tunnel-nhrp-sb:
         NHRP subblock has 1 entries
 Endpoint transport 200.3.3.1 Refcount 3 Base 0x1236052C Create Time 02:49:22
   overlay 172.23.123.3 Refcount 2 Parent 0x1236052C Create Time 02:49:22
   Tunnel Subblocks:
      tunnel-nhrp-sb:
         NHRP subblock has 1 entries
 Endpoint transport 200.20.1.2 Refcount 3 Base 0x1236042C Create Time 02:49:19
   overlay 172.23.123.200 Refcount 2 Parent 0x1236042C Create Time 02:49:19
   Tunnel Subblocks:
      tunnel-nhrp-sb:
         NHRP subblock has 1 entries
```

Figura 62. Tunnel en función GRE multipunto.

Con el comando **Show interface tunnel 100**, validamos el estado del túnel y sus configuraciones como MTU y seguridad del mismo, asi a como se muestra en la figura 63.

```
MANAGUA_HUB_1#show interfaces tunnel 100
*Apr 24 22:40:28.394: %CLEAR-5-COUNTERS: Clear counter on interface Tunnel100 by console
MANAGUA_HUB_1#show interfaces tunnel 100
Tunnel100 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 172.23.123.100/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 200.10.1.1
  Tunnel protocol/transport multi-GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "Megabyte")
  Last input 00:00:00, output never, output hang never
  Last clearing of "show interface" counters 00:00:01
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1 packets input, 116 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

Figura 63. Estado del túnel.

- **Validación NHRP**

Para validar el funcionamiento correcto del protocolo NHRP, utilizamos el comando **show ip nhrp** en router Managua_Hub_1, con este se muestra la tabla completa de los túneles que fueron aprendidos dinámicamente y su IP NBMA que es la IP física con la que se están levantando los túneles, a como se muestra en la figura 64.

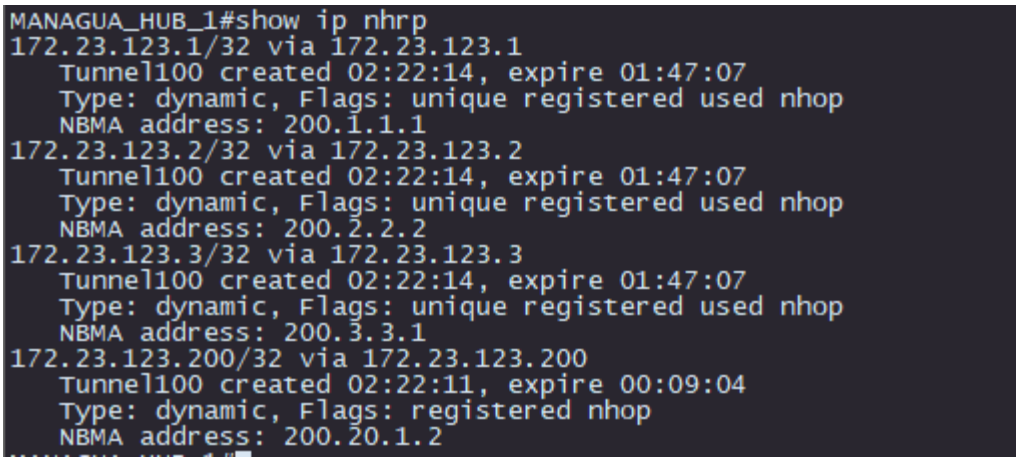

Figura 64. Validación NHRP.

También se valida el funcionamiento de NHRP de spoke a spoke, con el comando **traceroute**, en este caso validamos la conectividad de la LAN del router Masaya_Spoke_1 hacia la LAN del router Matagalpa_Spoke_3, a como se aprecia en la figura 65. Observamos que al ejecutar el comando de **traceroute** por primera vez se tiene dos saltos para llegar a el destino, pero la segunda vez que lo ejecutamos solo se tiene un salto, concluyendo que se realizó la resolución de siguiente salto de NHRP y se estableció la conexión de túnel de Spoke-Spoke, ahora el tráfico que fluya entre ambas sucursales será en un túnel independiente y este no tendrá que atravesar por casa matriz.

```
MASAYA_SPOKE_1#traceroute 192.168.4.1 source 192.168.2.1
Type escape sequence to abort.
Tracing the route to 192.168.4.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.23.123.100 27 msec
    172.23.123.200 22 msec
    172.23.123.100 55 msec
  2 172.23.123.3 74 msec 33 msec 31 msec
MASAYA_SPOKE_1#traceroute 192.168.4.1 source 192.168.2.1
Type escape sequence to abort.
Tracing the route to 192.168.4.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.23.123.3 9 msec 8 msec 7 msec
```

Figura 65. Validación NHRP spoke to spoke.

A nivel de Wireshark validamos este comportamiento observando los paquetes que se intercambian, cuando desde el router de Masaya_Spoke_1 se valida el **traceroute** hacia el router de Matagalpa_Spoke_3.

En la figura 66, que corresponde al enlace WAN de Masaya, se observa que el paquete es de **resolution request** y este es el paquete enviado del router Masaya_Spoke_1 hacia el router Managua_Hub_1, este paquete tiene como destino la IP LAN del spoke de la sucursal de Matagalpa.

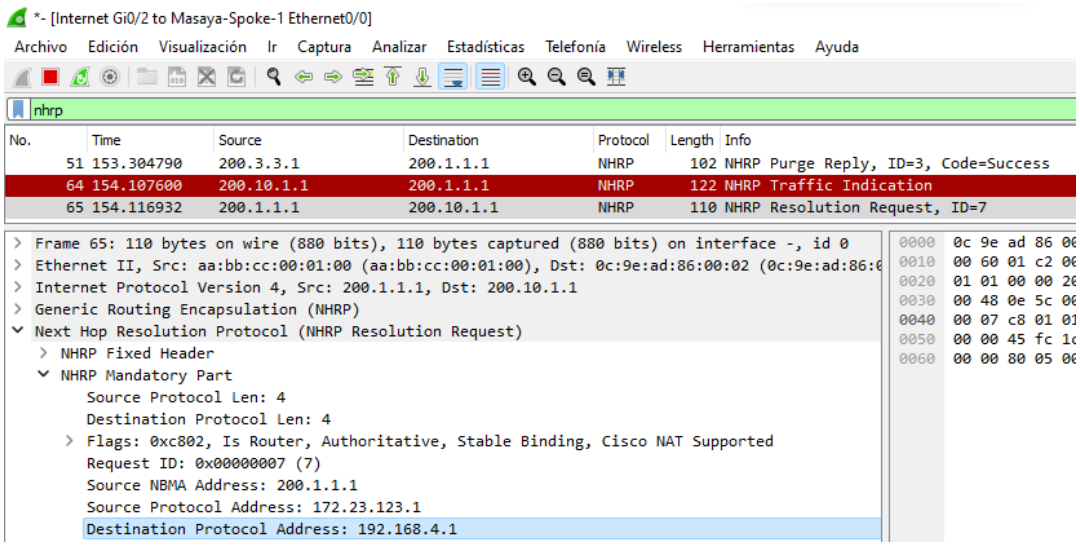

Figura 66. WAN Masaya paquete request.

En la figura 67, que corresponde al enlace WAN del router Managua_Hub_1, se observa que se tiene un mensaje de **resolution request** proveniente del router Masaya_Spoke_1 y que este es reenviado hacia el router Matagalpa_Spoke_3.

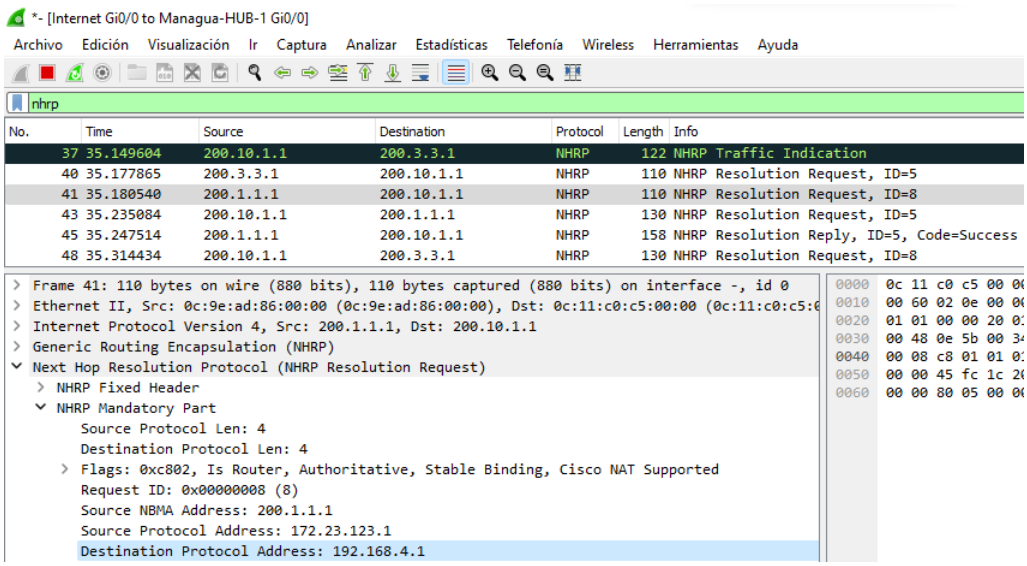

Figura 67. WAN Managua paquete request.

En la figura 68, que corresponde al enlace WAN del router Matagalpa_Hub_3, se observa un mensaje de **resolution reply**, que tiene como destino la IP LAN del router Masaya_Spoke_1.

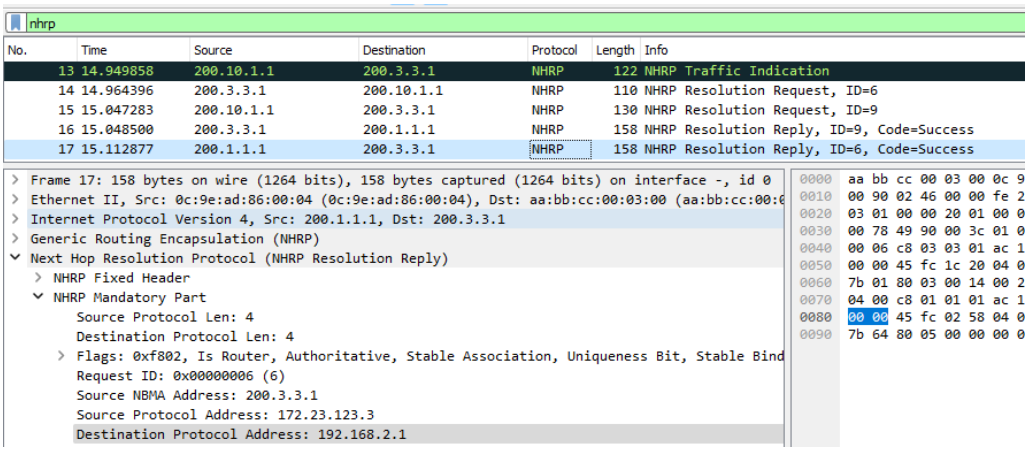

Figura 68. WAN Matagalpa paquete reply,

En la figura 69, correspondiente a la interface WAN del router Masaya_Spoke_1, se observa que se recibe el paquete de **resolution reply** proveniente del router Matagalpa_Spoke_3, y en este se encuentra la IP NBMA del router Matagalpa_Spoke_3 y donde podemos concluir que se levantó el túnel entre ambas sucursales y se realizó la comunicación Spoke-Spoke.

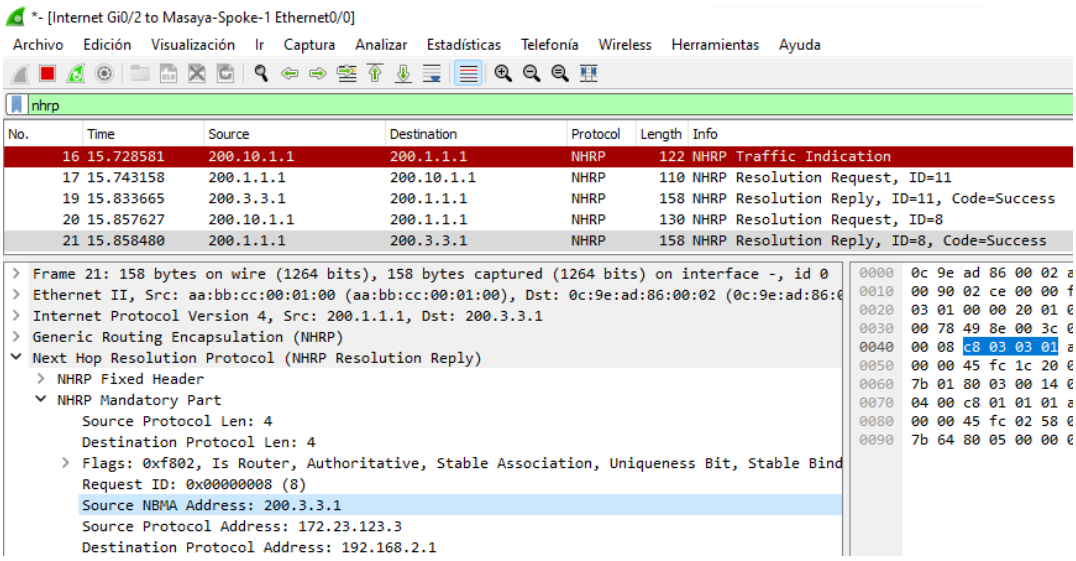

Figura 69. WAN Masaya paquete reply.

- **Validaciones DMVPN.**

Para las validaciones DMVPN, se ejecutó el comando **show dmpvn** en el router Managua_Hub_1, se observa que la creación de los túneles se realizó de manera dinámicamente mediante el prefijo (D) y nos dice que están activos (UP) también nos da la información de las IPs NBMA, de túnel y la cantidad de tiempo que llevan operando los túneles, así a como se aprecia en la figura 70.

```
MANAGUA_HUB_1#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel100, IPv4 NHRP Details
Type:Hub, NHRP Peers:4,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 200.1.1.1          172.23.123.1    UP 01:45:11     D
     1 200.2.2.2          172.23.123.2    UP 01:45:10     D
     1 200.3.3.1          172.23.123.3    UP 01:45:10     D
     1 200.20.1.2       172.23.123.200    UP 01:45:08     D
```

Figura 70. Validación DMVPN.

En los router spokes se ejecutó el mismo comando y se observa que se tienen peer con los router HUB, estos túneles son aprendidos de manera estática. Con fines ilustrativos solo se muestra la imagen 71 del router Masaya_Spoke_1.

```
MASAYA_SPOKE_1#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable
        # 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: Tunnel100, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 200.10.1.1       172.23.123.100    UP 00:07:30     S
     1 200.20.1.2       172.23.123.200    UP 00:07:31     S
```

Figura 71. Validación DMVPN en Spokes.

- **Validación de alta disponibilidad DMVPN single cloud.**

Para la validación de la alta disponibilidad de DMVPN single cloud, se procedió a apagar la interface WAN de Managua_Hub_1.

En la figura 72, se observa que antes de apagar la interface de Managua Hub_1 en el router de Masaya se tiene como primer salto la IP de tunel de Managua_Hub_1, sin embargo, al apagar la interface WAN de Managua_Hub_1, Managua_Hub_2 asume el rol de tunel principal y se observa que el salto se realiza a la IP de tunel de Managua 2.

```
MASAYA_SPOKE_1#traceroute 192.168.3.1
Type escape sequence to abort.
Tracing the route to 192.168.3.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.23.123.100 9 msec
    172.23.123.200 10 msec
    172.23.123.100 16 msec
  2 172.23.123.2 12 msec 10 msec 4 msec
MASAYA_SPOKE_1#traceroute 192.168.3.1
Type escape sequence to abort.
Tracing the route to 192.168.3.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.23.123.2 6 msec 5 msec 3 msec
```

```
MASAYA_SPOKE_1#traceroute 192.168.3.1
Type escape sequence to abort.
Tracing the route to 192.168.3.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.23.123.200 19 msec 10 msec 11 msec
  2 172.23.123.2 13 msec 9 msec 9 msec
MASAYA_SPOKE_1#traceroute 192.168.3.1
Type escape sequence to abort.
Tracing the route to 192.168.3.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.23.123.2 10 msec 5 msec 5 msec
```

Figura 72. Validación DMVPN.

- **Validación OSPF.**

Primeramente, con el comando **show ip protocols** se validó que los protocolos de enrutamiento que están corriendo en nuestro equipo son OSPF y NHRP, así a como se muestra en la figura 73.

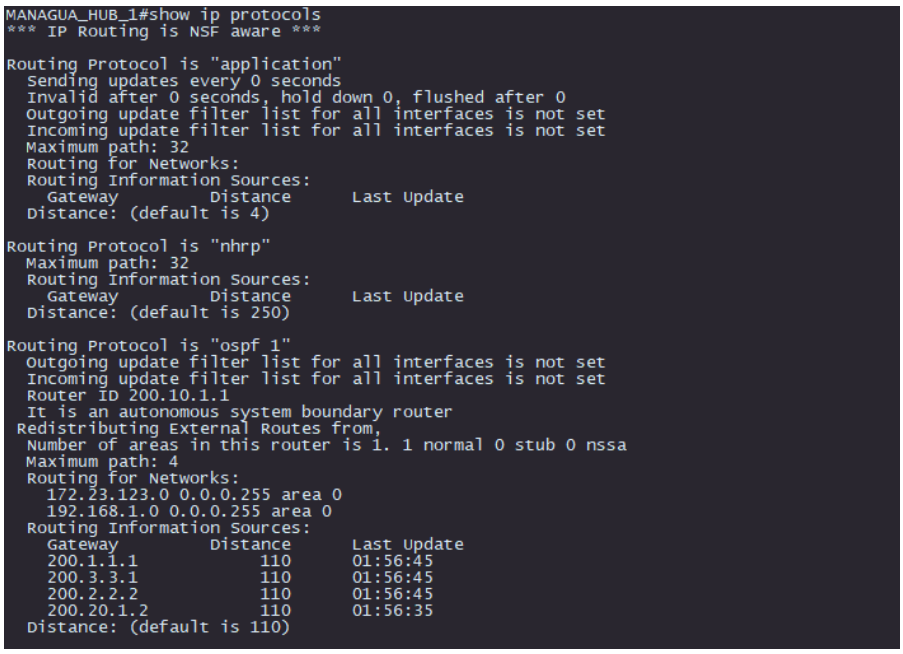

Figura 73. Validación OSPF y NHRP.

Con el comando **Show ip route ospf,** se logra validar la tabla de enrutamiento OSPF, en donde se logra observar que se están enrutando las redes LAN de las sucursales mediante los túneles que fueron creados. Con este comando se puede concluir que, tenemos acceso a las redes LAN de las Sucursales de Masaya, Chinandega y Matagalpa. En la figura 74, se puede apreciar lo antes mencionado.

```
MANAGUA_HUB_1#show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 200.10.1.2 to network 0.0.0.0

      172.23.0.0/16 is variably subnetted, 6 subnets, 2 masks
O        172.23.123.1/32 [110/1000] via 172.23.123.1, 01:50:53, Tunnel100
O        172.23.123.2/32 [110/1000] via 172.23.123.2, 01:50:53, Tunnel100
O        172.23.123.3/32 [110/1000] via 172.23.123.3, 01:50:53, Tunnel100
O        172.23.123.200/32
           [110/1] via 192.168.1.3, 01:50:43, GigabitEthernet0/1
O     192.168.2.0/24 [110/1010] via 172.23.123.1, 01:50:53, Tunnel100
O     192.168.3.0/24 [110/1010] via 172.23.123.2, 01:50:53, Tunnel100
O     192.168.4.0/24 [110/1010] via 172.23.123.3, 01:50:53, Tunnel100
```

Figura 74. Tabla de enrutamiento OSPF.

Con el comando **Show ip ospf neighbor**, se valida que se tiene adyacencia con el router Managua_Hub_2 y con los spokes de las distintas sucursales de la empresa Megabyte, así a como se aprecia en la figura 75.

```
MANAGUA_HUB_1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
200.20.1.2        1   FULL/DR         00:00:29    192.168.1.3     GigabitEthernet0/1
200.20.1.2        0   FULL/  -        00:01:34    172.23.123.200  Tunnel100
200.3.3.1         0   FULL/  -        00:01:48    172.23.123.3    Tunnel100
200.1.1.1         0   FULL/  -        00:01:44    172.23.123.1    Tunnel100
200.2.2.2         0   FULL/  -        00:01:46    172.23.123.2    Tunnel100
```

Figura 75. Validación de adyacencia.

Con el comando **Show ip ospf database**, se valida la tabla de rutas del protocolo OSPF, a como se observa en la figura 76.

```
MANAGUA_HUB_1#show ip ospf database

            OSPF Router with ID (200.10.1.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
200.1.1.1       200.1.1.1       721         0x80000007 0x006242 4
200.2.2.2       200.2.2.2       941         0x80000008 0x00A1F7 4
200.3.3.1       200.3.3.1       900         0x80000007 0x00890B 4
200.10.1.1      200.10.1.1      1504        0x80000009 0x004FE1 6
200.20.1.2      200.20.1.2      1347        0x8000000A 0x004CE1 6

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
192.168.1.3     200.20.1.2      1347        0x80000004 0x006BC9

                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         200.1.1.1       922         0x80000005 0x000FD3 1
0.0.0.0         200.2.2.2       941         0x80000005 0x00F9E5 1
0.0.0.0         200.3.3.1       900         0x80000005 0x00F0ED 1
0.0.0.0         200.10.1.1      1504        0x80000004 0x00C812 1
0.0.0.0         200.20.1.2      1347        0x80000004 0x00725D 1
```

Figura 76. Estado del enlace enrutado.

- **Validaciones IPsec.**

Para las validaciones de IPsec se utilizan los comandos **show crypto engine connections active**, con el que se validan los algoritmos de cifrados de las conexiones activas utilizados por cada fase, a como se puede apreciar en la figura 77.

```
MANAGUA_HUB_1#show crypto engine connections active
Crypto Engine Connections

   ID  Type    Algorithm           Encrypt  Decrypt LastSeqN IP-Address
   37  IPsec   AES256+SHA               0      130      130 200.10.1.1
   38  IPsec   AES256+SHA             136        0        0 200.10.1.1
   39  IPsec   AES256+SHA               0       49       49 200.10.1.1
   40  IPsec   AES256+SHA              42        0        0 200.10.1.1
   41  IPsec   AES256+SHA               0       35       35 200.10.1.1
   42  IPsec   AES256+SHA              30        0        0 200.10.1.1
   43  IPsec   AES256+SHA               0       34       34 200.10.1.1
   44  IPsec   AES256+SHA              30        0        0 200.10.1.1
 1001  IKE     MD5+AES                  0        0        0 200.10.1.1
 1002  IKE     MD5+AES                  0        0        0 200.10.1.1
 1003  IKE     MD5+AES                  0        0        0 200.10.1.1
 1004  IKE     MD5+AES                  0        0        0 200.10.1.1
```

Figura 77. Validación IPsec.

Con el comando **Show crypto isakmp sa**, validamos que hay conexiones activas de la primera fase de IPsec, asi a como se muestra en la figura 78.

```
MANAGUA_HUB_1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
200.10.1.1      200.20.1.2      QM_IDLE           1004 ACTIVE
200.10.1.1      200.2.2.2       QM_IDLE           1002 ACTIVE
200.10.1.1      200.1.1.1       QM_IDLE           1001 ACTIVE
200.10.1.1      200.3.3.1       QM_IDLE           1003 ACTIVE

IPv6 Crypto ISAKMP SA
```

Figura 78. Primera fase IPsec.

Con el comando **Show crypto ipsec sa**, validamos a profundidad el tráfico que ha sido encriptado y desencriptado correspondiente a cada túnel activa el router Managua_Hub_1. En la figura 79, se aprecia dicha información.

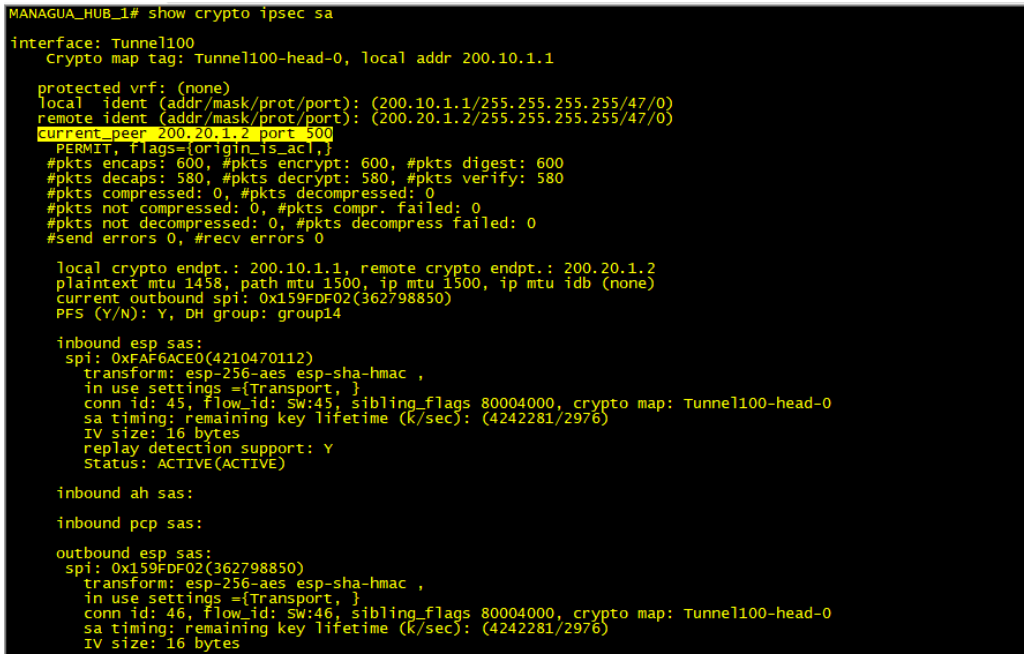

Figura 79. Tráfico por tunnel en Managua_Hub_1.

Con el comando **Show crypto sesión**, validamos la creación de los túneles IPsec y sus estados, a como se observa en la figura 80.

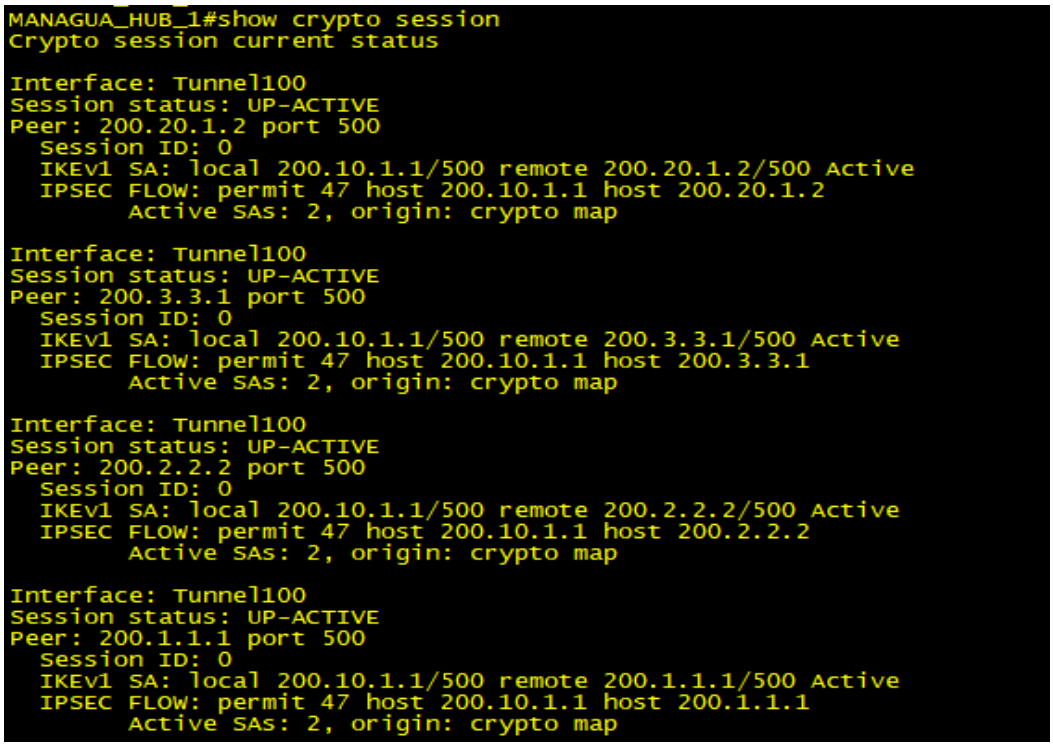

Figura 80. Validación de los estados túneles IPsec.

En la figura 81, observamos que el tráfico en la interface WAN de Managua_Hub_1 se encuentra con el protocolo de IPsec ESP.

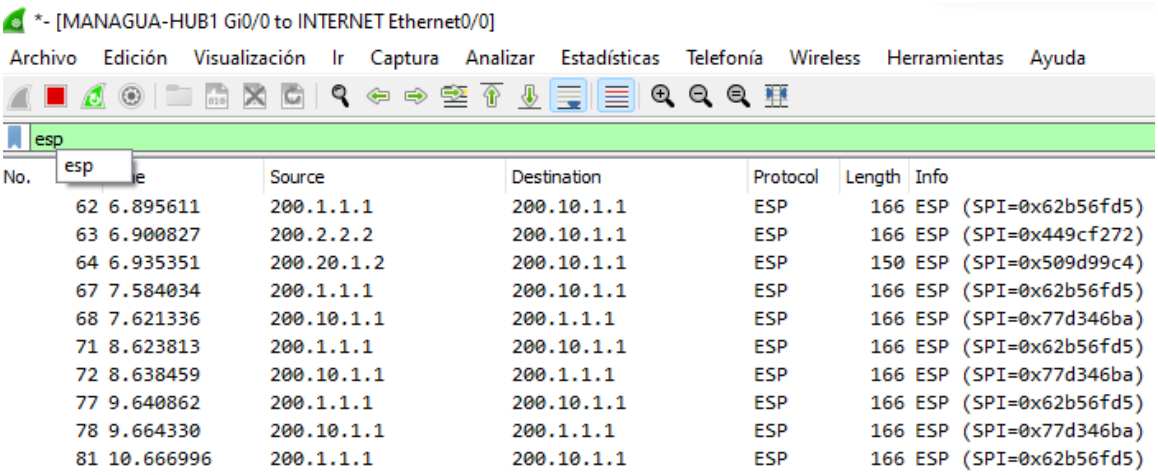

Figura 81. Trafico interfaz WAN Managua_Hub_1.

8.3 Cronograma de trabajo para la implementación de DMVPN.

A como se mencionó en capítulos anteriores, el proyecto de despliegue de la red DMVPN para la empresa Megabyte S.A, se realizará en los primeros 6 (seis) mes del año 2024, según el Ing. Cantillano. Por lo que se tomara el siguiente plan de trabajo, en el cual se levantara una sucursal cada segundo viernes de cada mes, empezando en febrero y concluyendo en mayo.

La implementación de este proyecto se realizará en un día (6 horas de trabajo) por sucursal, abarcando de este modo la configuración de los dispositivos y el montaje del rack, así a como se muestran en las siguientes figuras:

Febrero 2024 9 Proyectos

Proyecto	Estado	Fecha	Observación	Sucursal / Hub
Configuración NAT	En espera	feb. 9, 2024	Configuración / Pruebas	Managua / Hub 1 - 2
Configuración interfaz WAN	En espera	feb. 9, 2024	Configuración / Pruebas	Managua / Hub 1 - 2
Configuración DHCP	En espera	feb. 9, 2024	Configuración / Pruebas	Managua / Hub 1 - 2
Configuración IP SLA	En espera	feb. 9, 2024	Configuración / Pruebas	Managua / Hub 1 - 2
Configuración HSRP	En espera	feb. 9, 2024	Configuración / Pruebas	Managua / Hub 1
Configuración tunel mGRE	En espera	feb. 9, 2024	Configuración / Pruebas	Managua / Hub 1 - 2
Configuración OSPF	En espera	feb. 9, 2024	Configuración / Pruebas	Managua / Hub 1 - 2
Configuración IPsec	En espera	feb. 9, 2024	Configuración / Pruebas	Managua / Hub 1 - 2
Instalación del rack	En espera	feb. 9, 2024		Managua / Hub 1 - 2
+ Agregar Proyecto				

Figura 82. Implementación casa matriz.

Marzo 2024

Proyecto	Estado	Fecha	Observación	Sucursal / Hub
Configuración NAT	En espera	mar. 8, 2024	Configuración / Pruebas	Masaya / Spoke 1
Configuración interfaz WAN	En espera	mar. 8, 2024	Configuración / Pruebas	Masaya / Spoke 1
Configuración DHCP	En espera	mar. 8, 2024	Configuración / Pruebas	Masaya / Spoke 1
Configuración tunel mGRE	En espera	mar. 8, 2024	Configuración / Pruebas	Masaya / Spoke 1
Configuración OSPF	En espera	mar. 8, 2024	Configuración / Pruebas	Masaya / Spoke 1
Configuración IPsec	En espera	mar. 8, 2024	Configuración / Pruebas	Masaya / Spoke 1
Instalación del rack	En espera	mar. 8, 2024		Masaya / Spoke 1
+ Agregar Proyecto				

Figura 83. Implementación Masaya.

Abril 2024

Proyecto	Estado	Fecha	Observación	Sucursal / Hub
Configuración NAT	En espera	abr. 12, 2024	Configuración / Pruebas	Chinandega / Spoke...
Configuración interfaz WAN	En espera	abr. 12, 2024	Configuración / Pruebas	Chinandega / Spoke...
Configuración DHCP	En espera	abr. 12, 2024	Configuración / Pruebas	Chinandega / Spoke...
Configuración tunel mGRE	En espera	abr. 12, 2024	Configuración / Pruebas	Chinandega / Spoke...
Configuración OSPF	En espera	abr. 12, 2024	Configuración / Pruebas	Chinandega / Spoke...
Configuración IPsec	En espera	abr. 12, 2024	Configuración / Pruebas	Chinandega / Spoke...
Instalación del rack	En espera	abr. 12, 2024		Chinandega / Spoke...
+ Agregar Proyecto				

Figura 84. Implementación Chinandega.

Mayo 2024

Proyecto	Estado	Fecha	Observación	Sucursal / Hub
Configuración NAT	En espera	may. 10, 20...	Configuración / Pruebas	Matagalpa / Spoke 3
Configuración interfaz WAN	En espera	may. 10, 20...	Configuración / Pruebas	Matagalpa / Spoke 3
Configuración DHCP	En espera	may. 10, 20...	Configuración / Pruebas	Matagalpa / Spoke 3
Configuración tunel mGRE	En espera	may. 10, 20...	Configuración / Pruebas	Matagalpa / Spoke 3
Configuración OSPF	En espera	may. 10, 20...	Configuración / Pruebas	Matagalpa / Spoke 3
Configuración IPsec	En espera	may. 10, 20...	Configuración / Pruebas	Matagalpa / Spoke 3
Instalación del rack	En espera	may. 10, 20...		Matagalpa / Spoke 3
+ Agregar Proyecto				

Figura 85. Implementación Matagalpa

9. Conclusiones

En el presente trabajo monográfico, se logró diseñar una red privada dinámica multipunto para modernizar la tecnología WAN de la empresa Megabyte S.A en Nicaragua. En primera instancia, se obtuvo un análisis del estado actual de la red de la empresa, logrando obtener información relacionada a los dispositivos conectados a la red, así como también la tecnología WAN y LAN, para así de este modo conocer las limitaciones técnicas y empresariales, a las que se les dio solución con la implementación de la tecnología DMVPN, que proporciona escalabilidad, seguridad y alta disponibilidad.

Posteriormente, se procedió a realizar la evaluación financiera de la implementación de la tecnología basada en túneles, como lo es DMVPN. Se detalló el costo de la adquisición o renta de los equipos de routing y switching, más la mensualidad de la conexión a internet. Por otra parte, se realizó la evaluación de costos entre la tecnología MPLS y DMVPN, estas soluciones fueron evaluadas con los parámetros escalabilidad, seguridad y alta disponibilidad, lo cual nos permitió caracterizar y así poder solventar la problemática de esta empresa.

Subsiguientemente, se procedió a realizar la emulación de la red con softwares especializados, como GNS3, en la cual se realizaron pruebas para verificar funcionalidad y alta disponibilidad del despliegue de la tecnología DMVPN, haciendo uso de protocolos como resolución de siguiente salto NHRP, tunelización mGRE, seguridad IPsec y enrutamiento dinámico OSPF.

Finalmente se elaboró un plan de implementación que detalla el tiempo de despliegue de la red DMVPN que tomara cada sucursal, el costo total del desarrollo del proyecto, así como un plan de soporte para la posible implementación.

10. Recomendaciones

Para darle continuidad al presente proyecto monográfico se plantean las siguientes recomendaciones:

- Realizar un script haciendo uso de lenguajes de programación como Python para realizar la configuración de los equipos de manera automatizada.
- Implementar la tecnología de red DMVPN haciendo uso del protocolo IPv6, ya que este proporciona configuración automática de direcciones, mejoras en seguridad y privacidad, eliminación de la fragmentación de paquetes, soporte nativo para QoS y un espacio de direcciones mucho más amplio en comparación con IPv4.
- Desarrollar el despliegue de la red DMVPN haciendo uso del protocolo de enrutamiento iBGP.
- Realizar el despliegue de la tecnología DMVPN con distintos proveedores de equipos de routing y switching como, por ejemplo: Huawei o Mikrotik.

11. Bibliografía

1] L. M. Casey, «patents.google.com,» 10 Diciembre 2002. [En línea]. Available: https://patents.google.com/patent/US6493349B1/en. [Último acceso: 02 Febrero 2023].

2] CISCO, «www.cisco.com,» 2008. [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html.

3] N. Ardila Castillo, «Seguridad en las VPN´ S,» 2019. [En línea]. Available: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6435/Seguridad%20en%20la%20VPN%c2%b4S-%20Articulo.pdf?sequence=4&isAllowed=y. [Último acceso: 25 03 2023].

4] M. H. J. &. S. R. Finlayson, «VPN Technologies a comparison.,» *Data Connection Limited,* p. 46, 2003.

5] Expressvpn, «Expressvpn.com,» 01 03 2016. [En línea]. Available: https://www.expressvpn.com/es/what-is-vpn. [Último acceso: 04 02 2023].

6] Sapalomera, «www.sapalomera.cat,» 2022. [En línea]. Available: https://www.sapalomera.cat/moodlecf/RS/4/course/module7/7.1.2.1/7.1.2.1.html.

7] O. Gerometta, Bridge CCNA V7.0, 2021.

8] P. V. P. R. &. A. P. Arora, *Comparison of VPN protocols–IPSec, PPTP, and L2TP.,* Department of Electrical and Computer Engineering George Mason University.: Project Report ECE, 646., 2001.

[9] S. K. a. R. ATKINSON, «IP Authentication Header. RFC». BBN Corp Patente RFC 2402, nviembre 1998.

[10] S. K. a. R. ATKINSON, «IP Encapsulating Security Payload (ESP)». Network Working Group BBN Patente RFC 2406, Noviembre 1998.

[11] E. C. Kaufman, «Internet Key Exchange (IKEv2) Protocol». Patente 5282, Diciembre 2005.

[12] D. H. &. D. Carrel, «The Internet Key Exchange (IKE)». Network Working Group Patente RFC 2409, Noviembre 1998.

[13] S. Luz, «www.redeszone.net,» 2022. [En línea]. Available: https://www.redeszone.net/tutoriales/vpn/ipsec-que-es-como-funciona/.

[14] S. Friedl, «laurel.datsi.fi.upm.es,» 8 Octubre 2012. [En línea]. Available: https://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec. [Último acceso: 1 Abril 2023].

[15] R. J. &. I. Jankunaite, «Route creation influence on DMVPN QoS,» IEEE, Cavtat, Croatia, 2009.

[16] K. H. P. W. ,. A. F. &. I. R. J. Siti Ummi Masruroh, «Performance Evaluation DMVPN Using Routing Protocol RIP, OSPF, And EIGRP,» IEEE, Parapat, Indonesia, 2018.

[17] Cisco, «www.cisco.com,» 2017. [En línea]. Available: https://www.cisco.com/c/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/data_sheet_c78-468520.html.

Sapalomera, 2020. [En línea]. Available: https://www.sapalomera.cat/moodlecf/RS/4/course/module7/7.2.1.2/7.2.1.2.html. [18]

A. Jaramillo, «Análisis comparativo entre VPN IPSEC y DMVPN (Dymanic Multipoint Virtual Private Network) para mejorar el desempeño de redes privadas sobre internet,» 2018. [19]

L. Williams, «www.guru99.com,» 04 Mazo 2023. [En línea]. Available: https://www.guru99.com/routing-protocol-types.html. [20]

T. Keary, «www.comparitech.com,» 09 Diciembre 2020. [En línea]. Available: https://www.comparitech.com/net-admin/routing-protocol-types-guide/#Types_of_Routing_Protocol. [Último acceso: Abril 2023]. [21]

E. &. M. R. G. Mier Ruiz, «Repositorio UTB,» 2008. [En línea]. Available: https://repositorio.utb.edu.co/handle/20.500.12585/3208#page=1. [Último acceso: 2023]. [22]

J. Reyes, «www.jossjack.wordpress.com,» 22 Marzo 2017. [En línea]. Available: https://jossjack.wordpress.com/tag/ospf/. [Último acceso: Abril 2023]. [23]

E. M. R. &. G. M. Ruiz, «www.repositorio.utb.edu.co,» 2008. [En línea]. Available: https://repositorio.utb.edu.co/bitstream/handle/20.500.12585/3208/0045016.pdf?sequence=1&isAllowed=y. [Último acceso: Abril 2023]. [24]

R. H. Sampieri, Metodología de la investigación, D.F, México: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V., 2014. [25]

F. Abarza, «Investigación aplicada vs investigación pura (básica),» Junio 2012. [En línea]. Available: [26]

https://abarza.wordpress.com/2012/07/01/investigacion-aplicada-vs-investigacion-pura-basica/. [Último acceso: 2023].

27] Cisco, «Cisco 860VAE Series Integrated Services Routers - Data Sheet,» 23 Octubre 2018. [En línea]. Available: https://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78-693249.html. [Último acceso: 28 Abril 2023].

28] GNS3, «GNS3,» [En línea]. Available: https://www.gns3.com/software/download.

29] VMware Workstation, «VMware Workstation,» [En línea]. Available: https://www.vmware.com/es/products/workstation-pro.html.

30] S. P. Iglesias, «Análisis del protocolo IPSec: el estándar,» Telefónica Investigación y Desarrollo, 2001.

31] J. Fuentes y R. Antonio, «Implementacion de la tecnologia MPLS en el emulador GNS3 con propositos academicos,» 2019.

32] L. Sarmiento, «Diseño y simulación de una red privada virtual multipunto dinámico (DMVPN) en Internet para una empresa de Lima, Perú,» 2018.

12. Anexos

Código de la red DMVPN.

Las configuraciones realizadas en cada dispositivo en los routers y switches de la red DMVPN se especificarán por dispositivo.

- **Hub_Managua_1.**

  Configuración WAN:

  >config terminal
  >hostname MANAGUA_HUB_1
  #
  >interface gigabitethernet 0/0
  >ip address 200.10.1.1 255.255.255.252
  >no shutdown
  #
  >ip route 0.0.0.0 0.0.0.0 200.10.1.2

  Configuración NAT:

  >int gi 0/1
  >ip address 192.168.1.2 255.255.255.0
  >no shutdown
  #
  >access-list 2 permit 192.168.1.0 0.0.0.255
  >access-list 2 deny any
  #
  >ip nat inside source list 2 interface giga 0/0 overload
  #
  >interface giga 0/0
  >ip nat outside

#

>interface giga 0/1

>ip nat inside

Configuración DHCP:

>ip dhcp excluded-address 192.168.1.1

>ip dhcp excluded-address 192.168.1.2

>ip dhcp excluded-address 192.168.1.3

#

>ip dhcp pool DHCP_LAN

>network 192.168.1.0 255.255.255.0

>default-router 192.168.1.1

>lease 0 12 0

>dns-server 8.8.8.8

Configuración HSRP y IP SLA:

>ip sla 1

>icmp-echo 8.8.8.8

>frequency 20

>ip sla schedule 1 life forever start-time now

#

>track 100 ip sla 1 rechability

#

>interface GigabitEthernet0/1

>standby version 2

>standby 1 ip 192.168.1.1

>standby 1 priority 150

>standby 1 preempt

>standby 1 track 100 decrement 60

Configuración Tunnel mGRE:

>interface Tunnel100

>ip address 172.23.123.100 255.255.255.0

>tunnel source 200.10.1.1

>tunnel mode gre multipoint

>ip tcp adjust-mss 1360

>ip mtu 1400

Configuración NHRP:

>interface Tunnel100

#

>ip nhrp network-id 100

>ip nhrp redirect

>ip nhrp map multicast dynamic

#

Configuración OSPF:

>interface Tunnel100

#

>ip ospf network point-to-multipoint

#

>router ospf 1

>network 172.23.123.0 0.0.0.255 area 0

>network 192.168.1.0 0.0.0.255 area 0

>default-information originate

Configuración IPsec:

>crypto isakmp policy 1

>encryption aes

>hash md5

>authentication pre-share

>group 2

#

>crypto isakmp key Megabyte address 0.0.0.0

#

>crypto ipsec transform-set Megabyte esp-aes 256 esp-sha-hmac

>mode transport

#

>crypto ipsec profile Megabyte

>set pfs group14

>set transform-set Megabyte

#

>interface tunnel 100

>tunnel protection ipsec profile Megabyte

- **Hub_Managua_2.**

  Configuración WAN:

  >config terminal

  #

  >hostname MANAGUA_HUB_2

  #

  >int gigabitEthernet 0/0

  >ip address 200.20.1.2 255.255.255.252

  >no shutdown

  #

  >ip route 0.0.0.0 0.0.0.0 200.20.1.1

  Configuración NAT:

>int gi 0/1

>ip address 192.168.1.3 255.255.255.0

>no shutdown

#

>access-list 2 permit 192.168.1.0 0.0.0.255

>access-list 2 deny   any

#

>ip nat inside source list 2 interface giga 0/0 overload

#

>interface giga 0/0

>ip nat outside

#

>interface giga 0/1

>ip nat inside

Configuración DHCP:

>ip dhcp excluded-address 192.168.1.1

>ip dhcp excluded-address 192.168.1.2

>ip dhcp excluded-address 192.168.1.3

#

>ip dhcp pool DHCP_LAN

>network 192.168.1.0 255.255.255.0

>default-router 192.168.1.1

>lease 0 12 0

>dns-server 8.8.8.8

Configuración HSRP y IP SLA:

>interface GigabitEthernet0/1

>standby version 2

>standby 1 ip 192.168.1.1

>standby 1 preempt

Configuración Tunnel mGRE:

>interface Tunnel100

>ip address 172.23.123.200 255.255.255.0

>tunnel source 200.20.1.2

>tunnel mode gre multipoint

>ip tcp adjust-mss 1360

>ip mtu 1400

Configuración NHRP:

>interface Tunnel100

#

>ip nhrp network-id 100

>ip nhrp redirect

>ip nhrp map multicast dynamic

>ip nhrp nhs 172.23.123.100 nbma 200.10.1.1 multicast

Configuración OSPF:

>interface Tunnel100

#

>ip ospf network point-to-multipoint

#

>router ospf 1

>network 172.23.123.0 0.0.0.255 area 0

>network 192.168.1.0 0.0.0.255 area 0

>default-information originate

Configuración IPsec:

>crypto isakmp policy 1

>encryption aes

>hash md5

>authentication pre-share

>group 2

#

>crypto isakmp key Megabyte address 0.0.0.0

#

>crypto ipsec transform-set Megabyte esp-aes 256 esp-sha-hmac

>mode transport

#

>crypto ipsec profile Megabyte

>set pfs group14

>set transform-set Megabyte

#

>interface tunnel 100

>tunnel protection ipsec profile Megabyte

- **Spoke_Masaya_1.**

Configuración WAN:

>config terminal

#

>hostname MASAYA_SPOKE_1

#

>interface ethernet 0/0

>ip address 200.1.1.1 255.255.255.252

>no shutdown

#

>ip route 0.0.0.0 0.0.0.0 200.1.1.2

Configuración NAT:

>int ethernet 0/1

>ip address 192.168.2.1 255.255.255.0

>no shutdown

#

>access-list 2 permit 192.168.2.0 0.0.0.255

>access-list 2 deny   any

#

>ip nat inside source list 2 interface ethernet 0/0 overload

#

>interface ethernet 0/0

>ip nat outside

#

>interface ethernet 0/1

>ip nat inside

Configuración DHCP:

>ip dhcp excluded-address 192.168.2.1

#

>ip dhcp pool DHCP_LAN

>network 192.168.2.0 255.255.255.0

>default-router 192.168.2.1

>lease 0 12 0

>dns-server 8.8.8.8

Configuración Tunnel mGRE:

>interface Tunnel100

>ip address 172.23.123.1 255.255.255.0

>tunnel source 200.1.1.1

>tunnel mode gre multipoint

>ip tcp adjust-mss 1360

>ip mtu 1400

Configuración NHRP:

>interface Tunnel100

#

>ip nhrp network-id 100

>ip nhrp shortcut

#

>ip nhrp nhs 172.23.123.100

>ip nhrp map multicast 200.10.1.1

>ip nhrp map 172.23.123.100 200.10.1.1

#

>ip nhrp nhs 172.23.123.200

>ip nhrp map multicast 200.20.1.2

>ip nhrp map 172.23.123.200 200.20.1.2

Configuración OSPF:

>interface Tunnel100

#

>ip ospf network point-to-multipoint

#

>router ospf 1

>network 172.23.123.0 0.0.0.255 area 0

>network 192.168.2.0 0.0.0.255 area 0

Configuración IPsec:

>crypto isakmp policy 1

>encryption aes

>hash md5

>authentication pre-share

>group 2

#

>crypto isakmp key Megabyte address 0.0.0.0

#

>crypto ipsec transform-set Megabyte esp-aes 256 esp-sha-hmac

>mode transport

#

>crypto ipsec profile Megabyte

>set pfs group14

>set transform-set Megabyte

#

>interface tunnel 100

>tunnel protection ipsec profile Megabyte

- **Spoke_Chinandega_2.**

  Configuración WAN:

  >config terminal

  #

  >hostname CHINANDEGA_SPOKE_2

  #

  >interface Ethernet0/0

  >ip address 200.2.2.2 255.255.255.252

  >no shutdown

  #

  >ip route 0.0.0.0 0.0.0.0 200.2.2.1

  Configuración NAT:

  >int ethernet 0/1

  >ip address 192.168.3.1 255.255.255.0

  >no shutdown

#

>access-list 2 permit 192.168.3.0 0.0.0.255

>access-list 2 deny   any

#

>ip nat inside source list 2 interface ethernet 0/0 overload

#

>interface ethernet 0/0

>ip nat outside

#

>interface ethernet 0/1

>ip nat inside

Configuración DHCP:

>ip dhcp excluded-address 192.168.3.1

#

>ip dhcp pool DHCP_LAN

>network 192.168.3.0 255.255.255.0

>default-router 192.168.3.1

>lease 0 12 0

>dns-server 8.8.8.8

Configuración Tunnel mGRE:

>interface Tunnel100

>ip address 172.23.123.2 255.255.255.0

>tunnel source 200.2.2.2

>tunnel mode gre multipoint

>ip tcp adjust-mss 1360

>ip mtu 1400

Configuración NHRP:

>interface Tunnel100

#

>ip nhrp network-id 100

>ip nhrp shortcut

#

>ip nhrp nhs 172.23.123.100

>ip nhrp map multicast 200.10.1.1

>ip nhrp map 172.23.123.100 200.10.1.1

#

>ip nhrp nhs 172.23.123.200

>ip nhrp map multicast 200.20.1.2

>ip nhrp map 172.23.123.200 200.20.1.2

Configuración OSPF:

>interface Tunnel100

#

>ip ospf network point-to-multipoint

#

>router ospf 1

>network 172.23.123.0 0.0.0.255 area 0

>network 192.168.3.0 0.0.0.255 area 0

Configuración IPsec:

>crypto isakmp policy 1

>encryption aes

>hash md5

>authentication pre-share

>group 2

#

>crypto isakmp key Megabyte address 0.0.0.0

#

>crypto ipsec transform-set Megabyte esp-aes 256 esp-sha-hmac

>mode transport

#

>crypto ipsec profile Megabyte

>set pfs group14

>set transform-set Megabyte

#

>interface tunnel 100

>tunnel protection ipsec profile Megabyte

- **Spoke_Matagalpa_3.**

  Configuración WAN:

  >config terminal

  #

  >hostname MATAGALPA_SPOKE_3

  #

  >int ethernet 0/0

  >ip address 200.3.3.1 255.255.255.252

  >no shutdown

  #

  >ip route 0.0.0.0 0.0.0.0 200.3.3.2

  Configuración NAT:

  >int ethernet 0/1

  >ip address 192.168.4.1 255.255.255.0

  >no shutdown

  #

  >access-list 2 permit 192.168.4.0 0.0.0.255

  >access-list 2 deny any

  #

  >ip nat inside source list 2 interface ethernet 0/0 overload

  #

>interface ethernet 0/0

>ip nat outside

#

>interface ethernet 0/1

>ip nat inside

Configuración DHCP:

>ip dhcp excluded-address 192.168.4.1

#

>ip dhcp pool DHCP_LAN

>network 192.168.4.0 255.255.255.0

>default-router 192.168.4.1

>lease 0 12 0

>dns-server 8.8.8.8

Configuración Tunnel mGRE:

>interface Tunnel100

>ip address 172.23.123.3 255.255.255.0

>tunnel source 200.3.3.1

>tunnel mode gre multipoint

>ip tcp adjust-mss 1360

>ip mtu 1400

Configuración NHRP:

>interface Tunnel100

#

>ip nhrp network-id 100

>ip nhrp shortcut

#

>ip nhrp nhs 172.23.123.100

>ip nhrp map multicast 200.10.1.1

>ip nhrp map 172.23.123.100 200.10.1.1

#

>ip nhrp nhs 172.23.123.200

>ip nhrp map multicast 200.20.1.2

>ip nhrp map 172.23.123.200 200.20.1.2

Configuración OSPF:

>interface Tunnel100

#

>ip ospf network point-to-multipoint

#

>router ospf 1

>network 172.23.123.0 0.0.0.255 area 0

>network 192.168.4.0 0.0.0.255 area 0

Configuración IPsec:

>crypto isakmp policy 1

>encryption aes

>hash md5

>authentication pre-share

>group 2

#

>crypto isakmp key Megabyte address 0.0.0.0

#

>crypto ipsec transform-set Megabyte esp-aes 256 esp-sha-hmac

>mode transport

#

>crypto ipsec profile Megabyte

>set pfs group14

>set transform-set Megabyte

#

>interface tunnel 100

>tunnel protection ipsec profile Megabyte

- **Internet**

  Conexiones WAN:

  >config terminal

  #

  >hostname INTERNET

  #

  >interface Ethernet0/0

  >ip address 200.10.1.2 255.255.255.252

  >no shutdown

  #

  >interface Ethernet0/1

  >ip address 200.20.1.1 255.255.255.252

  >no shutdown

  #

  >interface Ethernet0/2

  >ip address 200.1.1.2 255.255.255.252

  >no shutdown

  #

  >interface Ethernet0/3

  >ip address 200.2.2.1 255.255.255.252

  >no shutdown

  #

  >interface Ethernet1/0

  >ip address 200.3.3.2 255.255.255.252

  >no shutdown

  #

  >interface Loopback5

>ip address 8.8.8.8 255.255.255.255