UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA ELECTRÓNICA

MENCIÓN TELECOMUNICACIONES

MEMORIA LABORAL

"IMPLEMENTACIÓN DE DMVPN PARA LA RED WAN DEL BANCO SOLIDARIO"

POSTULANTE : JUAN CARLOS GONZALES SOLARES

TUTOR : ING. JUAN CARLOS DUCHEN

LA PAZ – BOLIVIA

2019

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE INGENIERIA

LA FACULTAD DE INGENIERIA DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AUTORIZA EL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SI LOS PROPÓSITOS SON ESTRICTAMENTE ACADÉMICOS.

LICENCIA DE USO

El usuario está autorizado a:

a) Visualizar el documento mediante el uso de un ordenador o dispositivo móvil.
b) Copiar, almacenar o imprimir si ha de ser de uso exclusivamente personal y privado.
c) Copiar textualmente parte(s) de su contenido mencionando la fuente y/o haciendo la cita o referencia correspondiente en apego a las normas de redacción e investigación.

El usuario no puede publicar, distribuir o realizar emisión o exhibición alguna de este material, sin la autorización correspondiente.

Dedicatoria

A mis padres Guido y Luisa por su comprensión, dedicación y amor incondicional,
A mis Hermanos Christian (+) y Luis Fernando por su apoyo constante,
A mis hermosos y adorados hijos, ***Demian y Mateo****, la luz de mi vida,*
la fuerza que me impulsa todos los días, son la razón de mi vida,
A todos los docentes y compañeros de la carrera.

AGRADECIMIENTO

En la presente memoria laboral, agradecer a Dios y a la Virgen del Socavón por bendecirme para llegar hasta donde he llegado, porque hicieron realidad este sueño anhelado desde hace mucho tiempo.

A mis padres; Guido y Luisa por su amor y el apoyo incondicional. A mis hermanos Christian (+) y Luis Fernando por todo el apoyo y ejemplos brindados. A mis hijos Demian y Mateo por alegrarme la vida en los momentos difíciles y ser la razón de mi vida, el resultado de todo esto es de ustedes hijitos.

A la Universidad Mayor de San Andres y la carrera Ingeniería Electrónica por permitirme ser parte de tan prestigiosa institución educativa, por proporcionarme una educación gratuita y de alto nivel, por permitirme culminar mis estudios, ser la casa de estudio y cobijo durante todos estos años. A todos mis docentes por su paciencia y por demostrarme que más allá del conocimiento técnico, la humildad y actitud positiva valen más. A mis compañeros de la carrera que siempre alentaron con tanto cariño y desprendimiento.

RESUMEN

El proyecto tiene como objetivo implementar DMVPN (Dynamic Multipoint VPN) en la red WAN del Banco Solidario, como consecuencia, en caso de contingencia en su Sitio Principal de la ciudad de La Paz será posible brindar conectividad de sus regionales hacia su Sitio Alterno de la ciudad de Santa Cruz, de esa manera obtener Alta Disponibilidad en sus servicios ante desastres.

Así mismo, la comunicación entre regionales del Banco Solidario será de forma directa en una topología Full-Mesh sin necesidad de atravesar el Sitio Principal para enrutamiento del tráfico.

Los túneles DMVPN utilizarán cifrado IPSEC punto a punto para proteger la información en la red de los proveedores MPLS para de esa manera cumplir con normativas de Seguridad de Información locales.

El proyecto tiene un alcance de aplicación para el Sitio Principal de La Paz, Sitio Alterno de Santa Cruz y Regionales: Cochabamba, Sucre, Tarija, Potosi, Oruro, Trinidad, Cobija.

TABLA DE CONTENIDO

TABLA DE CONTENIDO

INDICE DE CUADROS

INDICE DE FIGURAS

1. INTRODUCCIÓN.

Resumen de la actividad laboral

Dentro del historial laboral que se pudo obtener, 14 años aproximadamente, se puede destacar la oportunidad de trabajar en la Administradora de Tarjetas de Crédito S.A. Red Enlace, esta empresa con más de 25 años de vigencia es la pionera en medios de pagos electrónicos, cajeros automáticos (ATMs) y puntos de venta (POS). Se tuvo la oportunidad de trabajar 11 años en áreas de Redes y Comunicaciones, Seguridad de la Información, Riesgos y Certificación de Sistemas Transaccionales, dadas las características operativas se pudo interactuar con el sector financiero más importante del mercado nacional (Banco Mercantil Santa Cruz, Banco Nacional, Banco Bisa, Banco de Crédito) e internacional (Visa, MasterCard).

Por otro lado, también se puede destacar la experiencia laboral en la empresa Datec Ltda., que, siendo una empresa de servicios tecnológicos, abarca una amplia gama de clientes potenciales dentro del sector financiero, sector petrolero, minero y entidades públicas. En alrededor de dos años, se desarrollaron proyectos varios de Seguridad de Redes Cisco, Redes WAN, HSMs y soporte especializado en telecomunicaciones y redes de datos especialmente en el sector financiero a nivel nacional, tales como, Banco Unión, Banco Sol, Banco Mercantil Santa Cruz, entre otros.

1.1. Administradora de Tarjetas de Crédito S.A.

1.1.1 Organización.

Administradora de Tarjetas de Crédito S.A. – Red Enlace, empresa de servicios financieros complementarios pionera y líder en servicios financieros, que administra la red de pagos electrónicos más grande en Bolivia. Ofrece una amplia variedad de productos y servicios, los mismos que, son utilizados por las Entidades Financieras para ofrecer a sus propios clientes, programas de crédito y débito; y por los Establecimientos Comerciales, como una alternativa diferente al pago con dinero en efectivo. La red de procesamiento provee servicios de valor agregado que incluyen la administración de riesgo y fraude, resolución de controversias, servicios de lealtad/fidelización y otras aplicaciones avanzadas de negocios. En conjunto, estos elementos brindan seguridad, conveniencia y opciones confiables para realizar

transacciones con tarjetas de crédito y débito en más de 4.000 comercios y 564 cajeros automáticos en Bolivia, y más de 24 millones de comercios y 1 millón de cajeros automáticos en todo el mundo.

Como Bancos miembros cuenta con Banco Nacional de Bolivia, Banco Mercantil Santa Cruz, Banco de Crédito, Banco Bisa.

También tiene interconectividad con Banco Solidario, Banco FIE, Banco Fortaleza, La Primera EFV, Banco PYME Ecofuturo, Banco Prodem, Banco PYME de la Comunidad, La Promotora EFV, Cooperativa Jesús Nazareno, Credifondo, Fortaleza SAFI, Bisa SAFI, Mercantil Santa Cruz SAFI.

1.1.2 Posiciones.

Analista de Comunicaciones.

El cargo inicial con el que se ingresó a ATC S.A. en el año 2003 durante 5 años, la dependencia en ese momento era directa de Gerencia de Sistemas.

Jefe de Seguridad de Información

A partir del año 2009 hasta el año 2012, cargo promovido por la experiencia adquirida en Seguridad de Redes e Información y procesos transaccionales con criptografía. La dependencia fue directa con el Gerente de Riesgos y Seguridad.

Supervisor de Pruebas y Certificación

A partir del año 2012 hasta el año 2013, cargo promovido por la experiencia en Redes de Datos y Transaccionales con mensajería ISO8583. La dependencia fue directa con el Gerente de Riesgos y Seguridad. Se contaba con dos dependientes, dos analistas de pruebas y certificación.

Especialista de Infraestructura y Redes A.

A partir del año 2013 hasta el año 2015, cargo asumido como especialista Senior en Redes de Datos y Seguridad, para encarar la certificación PCI-DSS. La dependencia fue con el Supervisor de Infraestructura y Redes y la Subgerencia de Seguridad de Información para PCI-DSS.

1.1.3 Dependencia

Durante la permanencia en ATC S.A., sólo en el cargo asumido como Supervisor de Pruebas y Certificación se contaba con dependientes, dos Analistas de Pruebas y Certificación.

La dependencia superior en función al área de trabajo fue la siguiente:

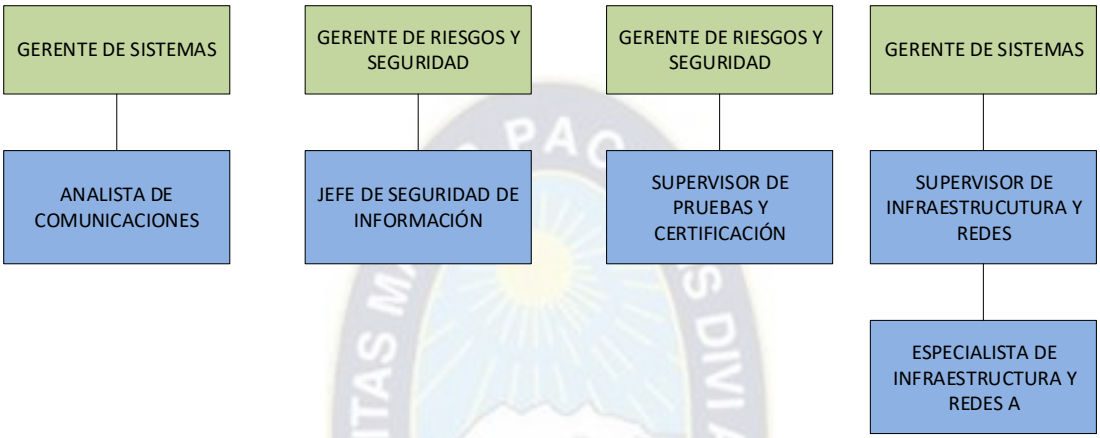


Figura 1 Dependencia, organigrama laboral ATC S.A.

Fuente: Elaboración Propia

1.1.4 Actividad.

Las actividades más destacadas durante aproximadamente 12 años de permanencia en ATC S.A. fueron:

- ✓ Administración de la red de cajeros automáticos ATMs y POS.
- ✓ Implementación de red de POS GPRS.
- ✓ Administración del sistema de telefonía AVAYA.
- ✓ Ejecución de Hardening sobre la red para cumplimiento PCI DSS.
- ✓ Implementación de POS con comunicación SSL.
- ✓ Implementación de ATMs con comunicación SSL.
- ✓ Implementación de IntelliNAC para POS.

- ✓ Certificación y puesta en producción del módulo EMV Emisor de ITM Euronet con las EIFs/Bancos.
- ✓ Certificación y puesta en producción del módulo Host to Host con las EIFs/Bancos.
- ✓ Certificación de mensajería IS8583 y NDC.
- ✓ Implementación, administración de Zonas y Llaves criptográficas (ATM, POS, VISA, MASTERCARD)
- ✓ Administración y operación de HSMs.
- ✓ Administración de Bases de Datos Oracle – DBA del sistema SIRED.

1.1.5 Resultados

Los resultados más destacados obtenidos durante toda la experiencia de trabajar en tan prestigiosa institución se detallan a continuación:

- ✓ Conocimientos en redes de comunicaciones de ATMs.
- ✓ Conocimientos en redes de comunicaciones de POS.
- ✓ Conocimientos en criptografía avanzada con HSMs.
- ✓ Conocimientos en Switch transaccional ITM Euronet.
- ✓ Conocimientos en mensajería ISO8583 (Transacciones financieras)
- ✓ Conocimientos en EMV tarjetas chip.

1.2. Datec Ltda.

1.2.1. Organización.

Datec Ltda. es una empresa boliviana, que está en el mercado hace 18 años trabajando en el rubro de tecnología, convertida hoy en la empresa líder del mercado tecnológico en Bolivia.

Actualmente es socio de negocios de las marcas más importantes del rubro, ofreciendo a sus clientes productos y servicios de calidad para satisfacer sus necesidades de tecnología de información. Las principales marcas que representamos en Bolivia son: IBM, Lenovo, Motorola, HP, Elo Technology, ViewSonic, Rejiband, HellermannTyton, Siemon, Allied

Telesis, Cisco, Riverbed, Juniper, Zebra, NetApp, TrippLite, Targus, Motorola, VMWare, Lexmark, Wincor - Nixdorf, Vision Solutions, LG.

Actualmente, DATEC cuenta con un plantel de recursos humanos de más de 200 personas, prestando sus habilidades, conocimientos y formación profesional, aportando a un mayor fortalecimiento y crecimiento juntamente con las exigencias del mercado boliviano.

1.2.2. Posiciones.

Especialista en Servicios de Redes y Comunicaciones.

Cargo asumido desde el año 2015 hasta junio 2017, la dependencia fue con el Coordinador de Servicios de Redes y Comunicaciones.

1.2.3. Dependencia.

Durante la permanencia en Datec Ltda., no se tuvo dependientes en el cargo asumido.

La dependencia superior en función al área fue la siguiente:

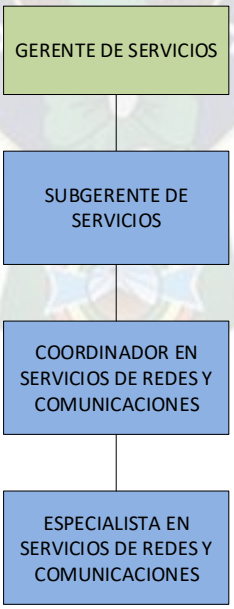


Figura 2 Dependencia, organigrama laboral DATEC LTDA.

Fuente: Elaboración Propia

1.2.4. Actividad

Las actividades más destacadas durante aproximadamente 2 años de permanencia en Datec Ltda. fueron:

- ✓ Diseño e implementación de proyectos en redes WAN, LAN, DATACENTER, SEGURIDAD DE REDES.

1.2.5. Resultados

Los resultados más destacados obtenidos durante la experiencia de trabajar en la empresa de servicios más importante del país se detallan a continuación:

- ✓ Topologías nuevas en WAN, DMVPN, IWAN.
- ✓ Nuevos sistemas de Seguridad, Firepower de Cisco.
- ✓ Certificaciones Cisco, CCNA Routing and Switching, CCNA Security, CCNP Security,
- ✓ Certificaciones Cisco, Advanced Security Architecture Field Engineer, Express Security NGFW Engineer, IPS Express Security Engineer.

2. CASO DE ESTUDIO

Como caso de estudio se seleccionó el proyecto realizado dentro mi permanencia en la empresa de servicios Datec Ltda. Su cliente Banco Solidario requirió el proyecto para la **IMPLEMENTACIÓN DE DMVPN PARA LA RED WAN,** mismo que se me asignó como especialista y se desarrolló de acuerdo con las necesidades del banco y se explica en detalle en el presente documento.

El grado de participación que tuve en el proyecto fue de Ejecución Técnica del mismo, contemplando fases de: levantamiento de información, ajustes en el diseño, implementación y pruebas de funcionalidad de la arquitectura implementada.

2.1. Antecedentes.

Las empresas financieras del país requieren interconectar varias sucursales, agencias o regionales con sus sitios de procesamientos de datos, a fin de proporcionar el servicio financiero a toda su cobertura de clientes finales. Así mismo, las empresas financieras requieren cumplir regulaciones de ASFI en relación con la disponibilidad de sus servicios.

Las comunicaciones WAN (redes de área amplia) han evolucionado, son más flexibles, dinámicas y redujeron los costos de aplicación y arrendamiento de enlaces dedicados.

La red de comunicaciones del Banco contaba con enlaces MPLS entre sus regionales y el sitio principal La Paz, enlaces que no se encontraban cifrados y dependían del enrutamiento del proveedor MPLS.

El Banco Solidario (BancoSol) ha requerido realizar un análisis e implementación de tecnologías, como DMVPN (Redes Privadas Virtuales Multipunto Dinámicas), que permitan mejorar y asegurar sus comunicaciones, por otro lado, activar su Sitio Alterno en la ciudad de Santa Cruz y que éste pueda brindar los servicios financieros con la Disponibilidad esperada a sus clientes finales.

2.1.1. Objetivos.

Objetivo Principal.

El objetivo principal del proyecto fue la implementación de la tecnología DMVPN en la red WAN del BancoSol para proporcionar Alta Disponibilidad en la red de servicios a sus clientes a nivel nacional.

Objetivos Secundarios.

Se realizó el levantamiento de información con la cual se preparó el diseño final, así mismo, a partir de ello se depuraron datos innecesarios en la red del Banco.

Se aplicó cifrado IPSEC en las comunicaciones WAN del Banco para evitar intercepción de tráfico en las redes públicas de los proveedores (TELCOs).

Se optimizó el consumo de ancho de banda entre el sitio principal La Paz y las regionales aplicando una topología enmallada (Full-Mesh).

Se realizaron pruebas funcionales del caso de contingencia para validar la alta disponibilidad de enlaces y DMVPN.

2.1.2. Justificación.

El proyecto DMVPN en el Banco iba a beneficiar las comunicaciones a nivel nacional, permitiendo la conexión cifrada entre todos sus dispositivos WAN (red de área amplia).

El uso de los enlaces MPLS existentes colaboraría en la reducción de costos referentes al arrendamiento de enlaces de comunicación.

DMVPN podía aplicarse en los equipos de comunicación que contaba el banco, solamente fue necesario la adquisición de equipos para el sitio alterno, lo cual benefició en el aspecto económico por la cantidad mínima de adquisición de equipos.

El Banco se beneficiaría con la selección de enlaces de comunicación para su tráfico crítico de forma dinámica a través de los protocolos a implementar.

2.1.3. Alcances y límites.

Alcances.

El proyecto DMVPN se aplicó al sitio principal (La Paz), sitio alterno (Santa Cruz) y las regionales del Banco (Cochabamba, Sucre, Tarija, Oruro, Potosí, Trinidad, Cobija).

Se estableció aplicar cifrado IPSEC en todos los túneles a nivel nacional para proteger la información en redes públicas o dedicadas y evitar la intercepción de datos confidenciales.

Se realizaron pruebas de funcionalidad de DMVPN, llegando a cubrir la convergencia de conectividad al sitio alterno y el retorno al sitio principal.

Límites.

La implementación del proyecto se aplicó a routers Cisco con los que contaba el Banco y a los routers que se adquirieron dentro del proyecto.

Las comunicaciones con agencias rurales iba a realizarlas el Banco en base al modelo a implementarse con la regionales.

2.1.4. Marco Referencial.

Para la implementación del proyecto se han requerido conocimientos sobre protocolos de encapsulamiento, protocolos de enrutamiento, cifrado de enlaces de datos, redes privadas virtuales.

A continuación, se especificarán los fundamentos teóricos que se emplearon durante el desarrollo del proyecto.

2.1.4.1 Definición de VPN.

Una VPN es una conexión virtual entre dos dispositivos que permite el envío de información de manera segura a través de un medio inseguro como lo es Internet. Con una VPN podemos desarrollar toda una infraestructura de red WAN (Wide Area Network) de forma más rápida y económica en comparación con la contratación del servicio de línea de fijas Frame Relay, ATM u otro tipo de tecnologías.

Por ejemplo, una configuración de VPN Site to Site es realizada utilizando el protocolo IPSec (Internet Protocol Security) brindando las siguientes ventajas:

- Confidencialidad
- Integridad de la información
- Autenticación

Confidencialidad, significa que la información enviada a través del VPN no podrá ser leída por un usuario o dispositivo tercero que no participe en la comunicación. En otras palabras, la información enviada por la VPN no podrá se accedida por ninguna entidad no autorizada. La confidencialidad se logra en la práctica a través de la implementación de técnicas de cifrado de datos. Para los no entendidos en la materia, el cifrado de información logra convertir un texto original en un formato no entendible (texto cifrado) para todo aquel que no conozca: (1) el algoritmo de cifrado y (2) la llave secreta. En IPSec podemos implementar cifrado de datos utilizando algoritmos simétricos tales como 3DES y AES.

Integridad de la información, significa que la información enviada entre dos dispositivos en una VPN debe de llegar tal cual fue enviada por el dispositivo emisor. En otras palabras, IPSec garantiza que la información, mientras esté en tránsito, no será modificada ni alterada. La integridad de la información en la práctica se logra a través de la implementación de técnicas de Hashing. Un Hash es una función matemática que no tiene inversa, por lo tanto, va a partir del resultado no es posible —matemáticamente hablando— conseguir la información original.

En IPSec podemos implementar Hashing utilizando algoritmos tales como MD5, SHA-1 y SHA-2.

Autenticación, consiste en establecer mecanismos de seguridad para validar la identidad de los dispositivos envueltos en la transmisión de información a través de una VPN. En IPSec tenemos la opción utilizar diferentes mecanismos de autenticación como son: (1) Pre-share Key y (2) Digital Signature.

Una VPN IPSec requiere del establecimiento de dos túneles. El primero llamado IKE Phase 1 (Internet Key Exchange Fase 1) que es utilizado para que los routers se comuniquen directamente entre ellos. Este túnel no es utilizado para el envío de paquetes IP de los usuarios, sino más bien, para el intercambio información de control. Para que el túnel IKE Phase 1 pueda establecerse con éxito, ambos routers o peers deben de estar de acuerdo en las siguientes variables:

- Hash algorithm (Algoritmo Hash)
- Encryption algorithm (Algoritmo de Encriptación)
- Diffie-Hellman DH group (Grupo DH)
- Authentication method (Método de Autenticación)
- Lifetime (Tiempo de Vida)

Después que ambos routers o peers agotan con éxito la primera fase del IPSec — IKE Phase 1 —, sí y solo sí se establece la segunda fase — IKE Phase 2 — donde se establece el túnel por donde viaja la información de los usuarios de manera encriptada.

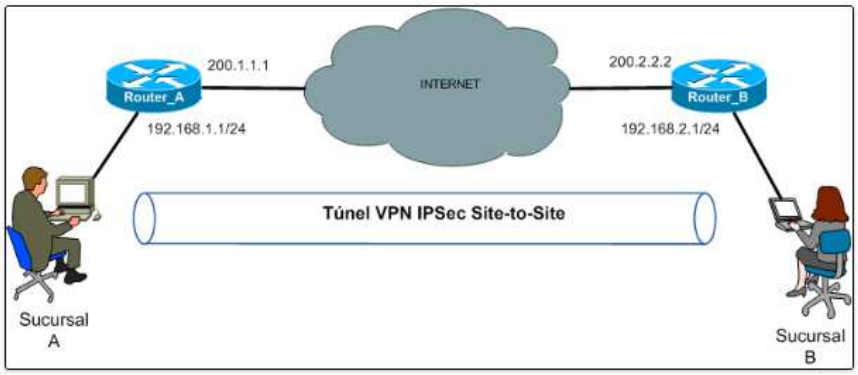


Figura 3 VPN Site-to-Site con IPSEC

Fuente: Internet

https://datagramsite.wordpress.com/2016/07/17/transmitiendo-datos-de-forma-segura/

2.1.4.2 Multipunto GRE.

El protocolo GRE es definido por la RFC 1701 y 2784, y es un protocolo de túnel propietario por Cisco. Es importante que entendamos lo que significa "efecto túnel", es la creación de un "túnel" en una red de datos. Un túnel en una red de datos no es más que la encapsulación de un protocolo a otro, es decir, tomamos el protocolo que se desea enviar a través de túnel e incluso añade a la cabecera del protocolo de túnel (como GRE). El GRE solo es capaz de crear túneles, pero no cifra los datos que pasan por estos túneles. (RFC 1701, 1994).

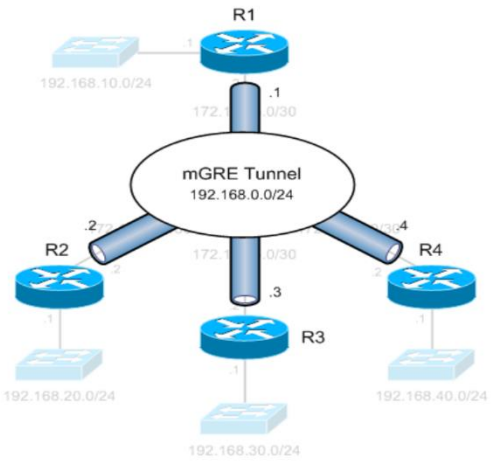


Figura 4 Túnel Multipunto GRE

Fuente: Internet

https://ccnabolivia.blogspot.com/2015/10/conociendo-dynamic-multipoint-vpn-dmvpn.html

2.1.4.3 Protocolo NHRP

El protocolo NHRP permite la simplificación de la configuración de los equipos, tanto de spokes como de hubs. Los equipos que actúan como hubs no necesitan tener configurada la dirección de ninguno de los spokes de la red y por tanto las direcciones de los spokes pueden haber sido asignadas dinámicamente. Solo los spokes necesitan tener configurada la dirección de uno o varios hubs.

Cuando un equipo remoto (Spoke) que es parte de la red DMVPN, entabla el túnel IPsec automáticamente hacia el equipo de la sede principal (Hub), automáticamente arranca el protocolo NHRP, informando a otros concentradores su IP física actual en uso.

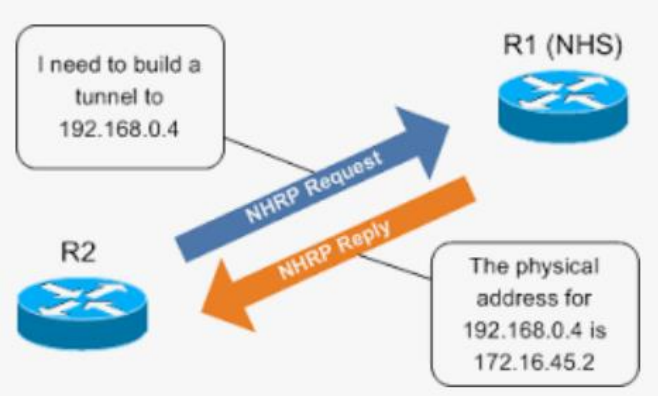


Figura 5 Intercambio Protocolo NHRP

Fuente: Internet

https://community.cisco.com/t5/blogs-routing-y-switching/conociendo-dynamic-multipoint-vpn-dmvpn/ba-p/3101118

Cada uno de los Spoke está encargado de registrarse en el Hub que tenga ya configurado, estableciendo de esta forma el túnel permanente entre ambos. Todos y cada uno de los Spoke tiene configurada una dirección de multicast a la que envían e informan de las rutas aprendidas por algún protocolo de ruteo dinámico, de esta forma el concentrador es informado de las rutas de los Spoke.

Una vez que los Spoke establecen los túneles con el Hub, este último registra las rutas de cada uno de ellos y crea una entrada multicast igual para cada uno, al mismo tiempo

informa de las rutas aprendidas a los Spoke de forma que, de tener alguna solicitud de conexión entre Spoke, esta se realice sin problemas como si se tratara de una red completamente enmallada, sin complicar la configuración de las estaciones remotas.

En el protocolo NHRP existen siete tipos de paquete posibles que viajan entre los NHC's (Next Hop Client) y los NHS's (Next Hop Servers):

1. Registration Request: petición de registro del NHC en el NHS.
2. Registration Reply: respuesta del NHS al NHC a una petición de registro.
3. Resolution Request: petición de resolución de una dirección de siguiente salto que envía el NHC al NHS.
4. Resolution Reply: respuesta del NHS al NHC con la dirección de siguiente salto solicitada.
5. Purge Request: petición de borrado de una entrada de cache que envía el NHS al NHC cuando la información de dicha entrada deja de ser válida.
6. Purge Reply: respuesta del NHC al NHS a una petición de borrado de una entrada de cache.
7. Indication de Error: paquete de error que indica algún problema en alguno de los paquetes recibidos en el equipo que genera el paquete de error.

2.1.4.4 Protocolo IPSEC

IPSec (Internet Protocol Security). Inicialmente se desarrolló para usarse con el estándar IPv6 y posteriormente se adaptó a IPv4. Es una extensión al protocolo IP. Añade los servicios de autenticación y cifrado. IPSec actúa dentro del modelo OSI en la capa 3 (capa de red). No está ligado a ningún algoritmo de encriptación o autenticación, tecnología de claves o algoritmos de seguridad específico. De hecho, es un estándar que permite que cualquier algoritmo nuevo se pueda introducir. Por sus características es considerado como el protocolo estándar para la construcción de redes privadas virtuales.

La especificación del protocolo se encuentra en la RFC 2401. IPSec cuenta con dos protocolos diferentes, de forma que se empleará uno u otro en función de lo que nos interese proteger y el modo en que realicemos las comunicaciones.

Cabecera de Autenticación (Authentication Header, AH). Se trata de una nueva cabecera que obtenemos de la básica IP y que se añade a los resúmenes criptográficos ("hash") de los datos e información de identificación.

Encapsulado de Seguridad (Encapsulating Security Payload, ESP). Permite reescribir los datos en modo cifrado. No considera los campos de la cabecera IP por lo que sólo garantiza la integridad de los datos.

Ambos protocolos controlan el acceso y distribuyen las claves criptográficas. No pueden ser aplicados los dos a la vez. Lo que sí se permite es aplicarlos uno después de otro, es decir, a un datagrama IP aplicarle un protocolo y al paquete resultante aplicarle otro. Si se hace esto el orden de aplicación es: ESP-AH Cada uno de estos protocolos pueden funcionar en dos modos distintos:

- Modo transporte.
- Modo túnel.

El modo transporte es el que usa un anfitrión que genera los paquetes. En modo transporte, las cabeceras de seguridad se añaden antes que las cabeceras de la capa de transporte (TCP, UDP), antes de que la cabecera IP sea añadida al paquete.

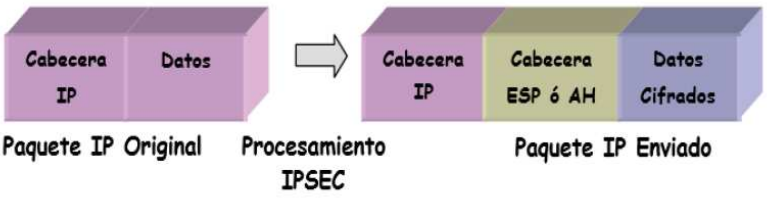


Figura 6 Paquetes IP en modo transporte IPSEC

Fuente: Internet

http://www.it.uc3m.es/~teldat/TeldatC/castellano/protocolos/Dm739v10_10_IPSec.PDF

El modo Túnel se usa cuando la cabecera IP extremo-a-extremo ya ha sido adjuntada al paquete, y uno de los extremos de la conexión segura es solamente una pasarela.

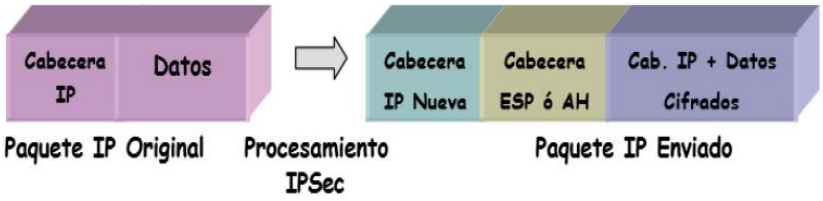


Figura 7 Paquetes IP en modo túnel IPSEC

Fuente: Internet

http://www.it.uc3m.es/~teldat/TeldatC/castellano/protocolos/Dm739v10_10_IPSec.PDF

2.1.4.5 Protocolo EIGRP

DMVPN utiliza EIGRP como el protocolo de enrutamiento primario, ya que es fácil de configurar, no requiere una gran cantidad de planificación, tiene una flexible sumarización y filtrado, y puede escalar hasta grandes redes. A medida que las redes crecen, el número de prefijos IP o rutas en las tablas de enrutamiento crece también. Con EIGRP se puede reducir la cantidad de ancho de banda, el procesador y la memoria necesaria para portar las tablas de enrutamiento grandes, así como reducir el tiempo de convergencia asociada con un fallo de enlace.

A continuación, en la siguiente figura se muestra la escalabilidad de los protocolos de enrutamiento dinámico y se observa que EIGRP es óptima para un reducido número de oficinas remotas como para un largo número de estas.

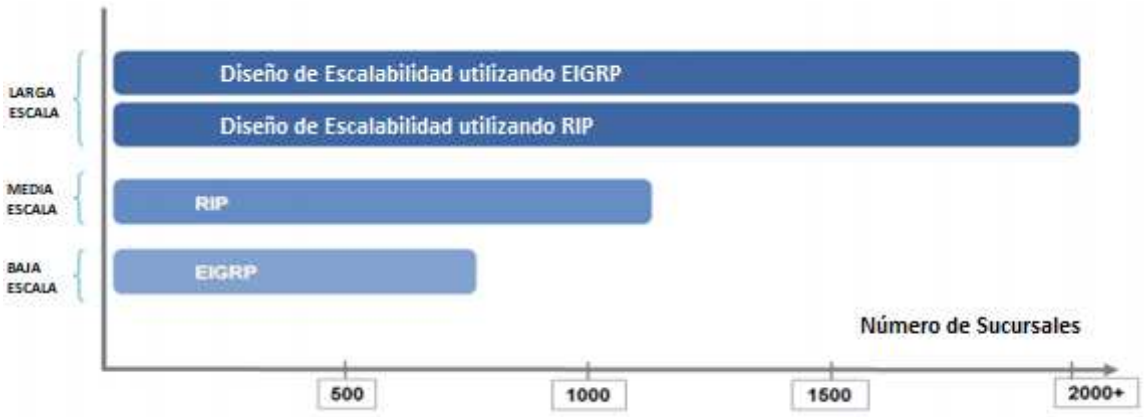


Figura 8 Escalabilidad de protocolos de enrutamiento dinámico

Fuente: Internet

https://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/dmvpn_design_guide.pdf

En la siguiente figura se muestra el desempeño de los protocolos de enrutamiento dinámico:

	Tipo de Red	Control de Ruta	Convergencia	CPU	Escalabilidad	Notas
EIGRP	Hub-Spoke Spoke-Spoke	Bueno	Más Rápido	Alto	Más Baja	
OSPF	Hub-Spoke Spoke-Spoke	Razonable	Más Rápido	Alto	Más Baja	Área Simple
BGP	Hub-Spoke Spoke-Spoke	Bueno	Más Lento	Medio	Media	Vecindad Estática
RIPv2	Hub-Spoke	Pobre	Más Lento	Bajo	Alta	Modo Pasivo necesita IP SLA
ODR	Hub-Spoke	Ninguno	Más Lento	Bajo	Alta	Sólo Ruta Por Defecto

Figura 9 Protocolos de enrutamiento vs. Desempeño

Fuente: Internet – Cisco Systems

https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2017/pdf/BRKSEC-4054.pdf

2.1.4.6 Definición de DMVPN

Dynamic Multipoint VPN (Red privada virtual multipunto dinámica) es una solución de seguridad basada en el software Cisco IOS® para crear VPN empresariales escalables que admitan aplicaciones distribuidas como voz y video.

Una DMVPN es una iteración evolucionada de los túneles "Hub and Spoke" (DMVPN por sí misma no es un protocolo, más bien un concepto de diseño).

En una topología genérica "Hub and Spoke" se implementan túneles estáticos (usando típicamente GRE o IPSEC) entre un router "hub" ubicado en el centro y sus "Spokes" o satélites, los cuales generalmente conectan oficinas sucursales a la sede central.

Para industrias como las entidades bancarias, empresas petroleras, compañías de seguros, entre muchas otras, que cuentan con un gran número de localidades (*Sites*) remotas que requieren estar conectadas con la oficina principal (*Headquarter*), la tecnología *Dynamic Multipoint VPN (DMVPN)* les proporciona la capacidad de establecer estas conexiones a través de Internet creando una red de túneles VPN entre las oficinas remotas y la sede principal, así como también, creando túneles VPN de manera dinámica cuando se requiera que dos o más localidades remotas se comuniquen de manera directa.

Esta tecnología permite también establecer enlaces de respaldo (*backup*) a través de Internet para las comunicaciones WAN de empresas que cuentan con infraestructura propia (ATM, Fibra óptica, etc.) para comunicar su sede principal y sus sedes remotas.

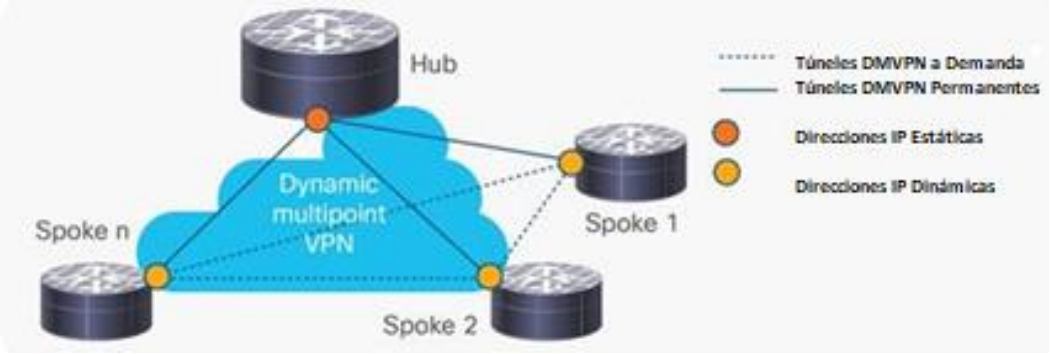


Figura 10 VPNs Dinámicas Multipunto (DMVPN)

Fuente: Internet – Cisco
https://www.cisco.com/c/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/data_sheet_c78-468520.html

2.1.4.7 Ventajas de DMVPN

Algunas de las principales ventajas que ofrece el uso de DMVPN son:

- Elimina los costos asociados a los enlaces WAN rentados a Proveedores de Servicio (ISP) entre los que encontrábamos muy comúnmente enlaces Frame Relay.
- Reduce la complejidad de la configuración: Pensemos en una entidad bancaria que cuenta con 50 sucursales en todo el país que deben conectarse con la oficina principal. Haciendo uso de otras tecnologías de túnel point-to-point deberíamos crear 50 interfaces en el Router principal (Hub) donde cada interfaz requiere al menos siete líneas de código para configurarla; estaríamos hablando de al menos 350 líneas de código solo en este Router Hub para esta configuración. Cada vez que exista el requerimiento de anexar una nueva oficina remota tendríamos que crear una nueva interfaz túnel en el Router Hub. Con DMVPN solo se configuraría una interfaz túnel con unas 15 líneas de código, la cual no cambia en caso de tener que adicionar una nueva oficina remota en la topología.
- Permite el uso de protocolos de enrutamiento (EIGRP, OSFP, BGP)
- Permite el uso de QoS y IP Multicast.
- Permite configurar IPSec para proporcionar cifrado y confidencialidad de los datos.
- Permite diseñar una solución robusta y confiable adicionando un segundo Router (Hub) en la topología (Dual-Hub).
- Reduce la latencia y el consumo de ancho de banda al permitir conexiones directas entre las localidades remotas sin pasar necesariamente por la sede principal.
- Permite anexar localidades remotas (sitios) sin realizar ningún tipo de cambio en la configuración del Router Hub.

2.1.4.8 Modelos y topologías DMVPN

Cisco define modelos y topologías que pueden aplicarse a los diferentes requerimientos o necesidades, básicamente pueden implementarse dos modos y sobre ellos las variaciones que permiten.

2.1.4.9 Modelo HUB y SPOKE

En una topología genérica "Hub and Spoke" se implementan túneles estáticos (usando típicamente GRE o IPSEC) entre un router "hub" ubicado en el centro y sus "Spokes" o satélites, los cuales generalmente conectan oficinas sucursales a la sede central.

Cada nuevo "Spoke" requiere que se haga una configuración adicional en el router "Hub" y el tráfico entre los "Spokes" debe ser desviado a través del "HUB" para que salga de un túnel y luego ingrese en otro. Mientras que esta podría ser una solución aceptable a pequeña escala, se vuelve difícil de manejar cuando los "Spokes" van multiplicándose y creciendo en número.

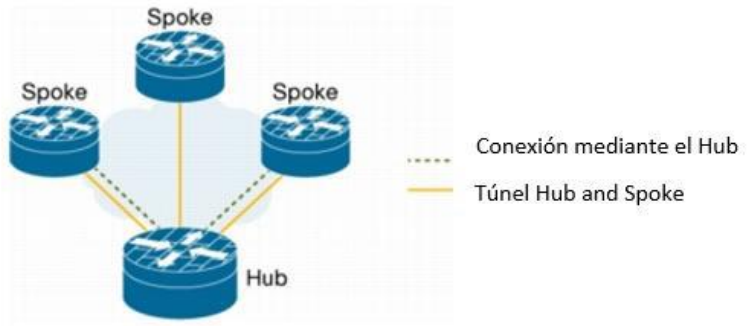


Figura 11 DMVPN Modelo Hub y Spoke

Fuente: Internet – Cisco

https://www.cisco.com/c/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/data_sheet_c78-468520.html

2.1.4.10 Modelo SPOKE a SPOKE

Se permite la creación de una VPN de malla completa, en la cual la conectividad tradicional Hub-and Spoke es suplementada 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.

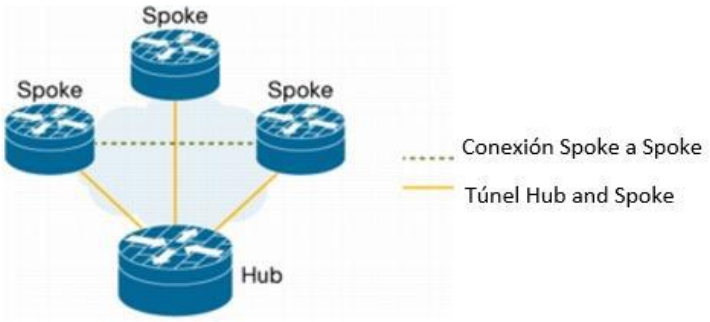


Figura 12 DMVPN Modelo Spoke y Spoke

Fuente: Internet – Cisco
https://www.cisco.com/c/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/data_sheet_c78-468520.html

2.1.4.11 Protocolo L2TPv3.

L2TP (Layer 2 Tunneling Protocol) es un protocolo utilizado por redes privadas virtuales que fue diseñado por un grupo de trabajo de IETF como el heredero aparente de los protocolos PPTP y L2F, creado para corregir las deficiencias de estos protocolos y establecerse como un estándar aprobado por el IETF (RFC 2661).

Empresas y operadores buscan formas de maximizar la eficiencia y el coste de sus redes, así como de simplificar su gestión, transportando múltiples servicios de Nivel 2 por una misma troncal IP. A diferencia de las VPN IP, las VPN de Nivel 2 basadas en L2TPv3 permiten el transporte de tráfico tanto IP como no IP a través de una infraestructura común.

Originalmente, L2TPv3 era un protocolo propietario de Cisco Systems para troncales IP nativas que añadía la tecnología Universal Transport Interface (UTI) de la

compañía al estándar L2TP. UTI permite a dos routers conectados vía una red IP proporcionar conectividad de Nivel 2 entre dos interfaces para la construcción de Layer 2 VPN. Se trata, en definitiva, de una extensión del conocido L2TP de naturaleza “apátrida” (stateless, como dicen en inglés) que carece de mecanismos propios de señalización y “keep-alive”.

Tunneling dinámico L2TP, definido en RFC 2661, fue diseñado para proporcionar tunneling dinámico a múltiples circuitos de Nivel 2 a través de redes de paquetes de datos. Describe un método estándar de tunneling que permite a las conexiones de tipo circuito entre una o más redes de Nivel 3 aparecer como enlaces punto a punto o punto a multipunto entre los emplazamientos del cliente. Consta de un protocolo de control para la creación, mantenimiento y terminación, de forma dinámica, de sesiones L2TP; y de encapsulación de datos para multiplexar y demultiplexar tráfico de Nivel 2 entre nodos enlazados por IP.

Con L2TPv3, la interfaz física que se conecta a la red del cliente se convierte en la interfaz de entrada/salida del túnel. Por lo tanto, el tráfico no necesita ser enrutado en el túnel por el proveedor de servicios. Según llegan los paquetes a la interfaz, se encapsulan y envían directamente hacia el punto extremo del túnel. Una vez recibido, el paquete original puede ser enviado fuera por la interfaz de salida si el identificador de túnel es reconocido por el router; en caso contrario, se descarta todo tipo de tráfico.

Cómo funciona L2TPv3:

1- Los paquetes ATM, Frame Relay o Ethernet entran en el router de extremo.
2- El router de extremo encapsula el paquete con la cabecera L2TPv3 que contiene Session ID (utilizado para identificar el túnel) y cookie (para validación).
3- El router de extremo lee la cabecera L2TPv3 desencapsula el paquete y lo envía a su destino.

La cabecera que se crea cuando usamos L2TPv3 es la siguiente:

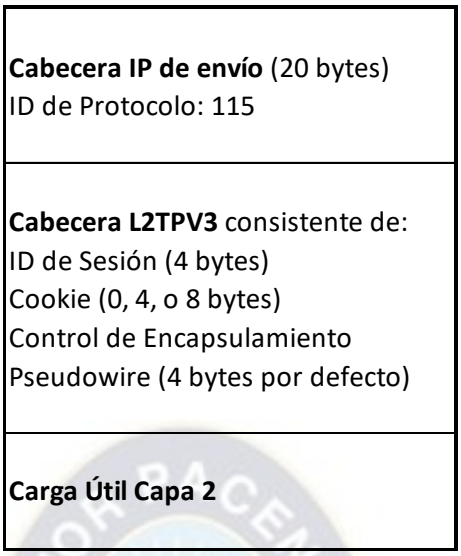


Figura 13 Formato de cabecera L2TPv3

Fuente: Internet

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/wan_lserv/configuration/xe-3s/wan-lserv-xe-3s-book/wan-l2-tun-pro-v3-xe.pdf

ID de Sesión: Identifica la sesión. Valor del 0 al 23, aunque el 0 está reservado para el protocolo. Debe ser un identificador único.

Session Cookie: Es un canal de control. Los valores pueden ser 0, 4 y 8.

Control de Encapsulamiento Pseudowire: Es el control de la secuencia de los paquetes L2TP.

Las sesiones de L2TPv3 pueden ser estáticas o dinámicas. También podemos hacer un "local switching" que es configurar el túnel con dos interfaces del mismo router.

Para evitar fragmentación de paquetes y mayor consumo de procesamiento debemos configurar la MTU del CE más pequeña que la asignada para el Pseudowire.

En la siguiente figura se puede observar un esquema lógico de conexión L2TPv3 a través de una red IP L3:

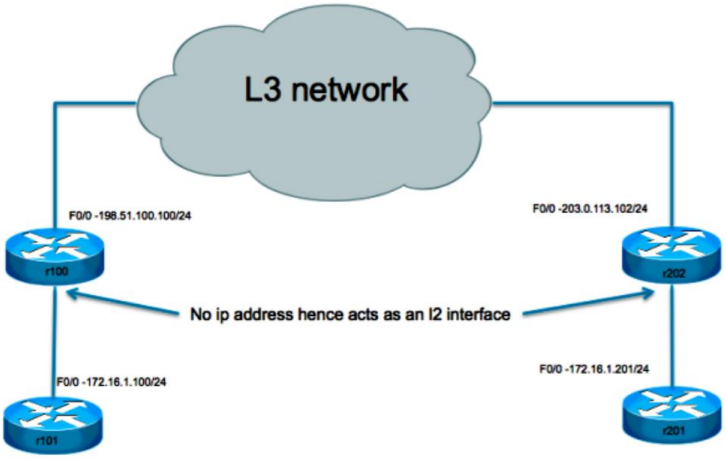


Figura 14 Esquema lógico L2TPv3

Fuente: Internet – Cisco Systems

https://www.cisco.com/c/en/us/support/docs/ip/layer-two-tunnel-protocol-l2tp/116266-configure-l2-00.html

2.2. Desarrollo.

Debido a la característica de una institución financiera, en este caso Banco Sol, los servicios al cliente interno y externo deben permanecer el mayor tiempo disponible, por esta razón, las modificaciones en la arquitectura de la red de comunicaciones que el proyecto involucró tuvieron que realizarse en fases controladas y coordinadas con el área técnica de la entidad.

Se establecieron cuatro fases para el desarrollo del preste proyecto, fase de levantamiento de información, fase de diseño, fase de implementación y la fase de pruebas de funcionalidad de la arquitectura implementada.

2.2.1 Fase de Levantamiento de Información

El levantamiento de información fue realizado revisando la configuración de equipos de comunicación y la topología de red en general. A continuación, se detallan los puntos de interés que se encontraron para el proyecto:

- La comunicación WAN entre las regionales y la oficina central de La Paz utilizaba enlaces MPLS, en la gran mayoría de regionales se contaba con dos enlaces MPLS, por contingencia, cada uno de diferente proveedor (Entel y Tigo).

- El enrutamiento IP sobre la red WAN MPLS la realizaban los proveedores (Entel y Tigo).
- El enrutamiento IP en la red nacional se realizaba de forma estática, se aplicaba PBR (Policy-Based Routing) para seleccionar el enlace MPLS de preferencia para el tráfico que el banco definía como crítico.
- La comunicación sobre la WAN y enlaces MPLS no se encontraba cifrada.
- A continuación, se detalla la relación de ancho de banda que utilizaban las regionales en la red WAN:

Departamento	Ciudad	Tipo de Oficina:	Nombre Oficina:	Proveedor Tel	Tecnologia	Velocidad Kbps
LA PAZ	LA PAZ	Oficina Central	Oficina Nacional	ENTEL	MPLS	20480
LA PAZ	LA PAZ	Oficina Central	Oficina Nacional	TIGO	MPLS	20992
BENI	TRINIDAD	Sucursal	Regional Beni	ENTEL	MPLS	1024
BENI	TRINIDAD	Sucursal	Regional Beni	TIGO	MPLS	1024
CHUQUISACA	SUCRE	Sucursal	Regional Sucre	ENTEL	MPLS	3072
CHUQUISACA	SUCRE	Sucursal	Regional Sucre	TIGO	MPLS	2048
COCHABAMBA	COCHABAMBA	Sucursal	Regional Cochabamba	ENTEL	MPLS	7168
COCHABAMBA	COCHABAMBA	Sucursal	Regional Cochabamba	TIGO	MPLS	4096
ORURO	ORURO	Sucursal	Regional Oruro	ENTEL	MPLS	3072
ORURO	ORURO	Sucursal	Regional Oruro	TIGO	MPLS	2048
POTOSI	POTOSI	Sucursal	Regional Potosí	ENTEL	MPLS	3072
POTOSI	POTOSI	Sucursal	Regional Potosí	TIGO	MPLS	2048
SANTA CRUZ	SANTA CRUZ	Sucursal	Regional Santa Cruz	ENTEL	MPLS	7168
SANTA CRUZ	SANTA CRUZ	Sucursal	Regional Santa Cruz	TIGO	MPLS	4096
TARIJA	TARIJA	Sucursal	Regional Tarija	ENTEL	MPLS	3072
TARIJA	TARIJA	Sucursal	Regional Tarija	TIGO	MPLS	2048
PANDO	COBIJA	Sucursal	Regional Pando	ENTEL	MPLS	1024
PANDO	COBIJA	Sucursal	Regional Pando	TIGO	MPLS	1024

Tabla 1 Ancho de Banda MPLS Regionales

Fuente: Elaboración Propia

- El acceso de los usuarios a Internet a nivel nacional era a través de la oficina central de La Paz.

- El acceso a los servidores principales se realizaba a través del Switch Core Cisco 6500 el cuál se encontraba en modo VSS.
- En base a la información revisada y analizada, se obtuvo el siguiente esquema de red general antes de los cambios:

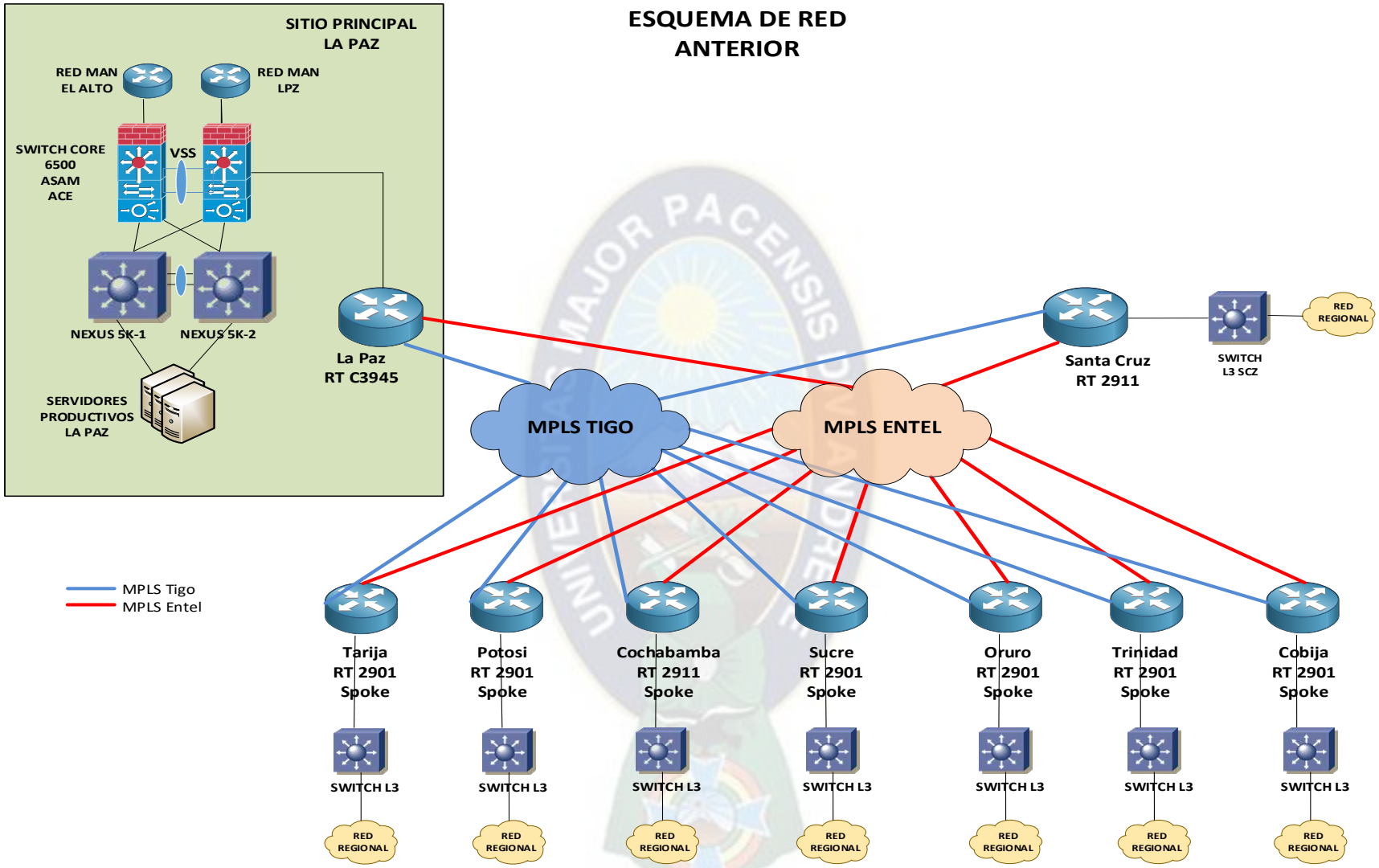


Figura 15 Esquema General de Red Anterior

Fuente: Elaboración Propia

2.2.2 Fase de Diseño

Para alcanzar los objetivos planteados y en base a la información obtenida en la fase anterior, se definieron las siguientes características de la nueva arquitectura de red en coordinación con el Encargado de Redes del Banco Sol (Ing. Hugo Durán) y mi persona como encargado de la Ejecución del Proyecto.

2.2.2.1 Topología DMVPN

Para cubrir las necesidades del Banco Sol, se seleccionó la topología mixta "Hub y Spoke" y "Spoke y Spoke", generando dos DMVPNs en un esquema "**Dual DMVPN/ Dual HUB"**, mismo que fue factible porque se contaban con dos (2) proveedores (Entel y Tigo), ambos proporcionaban enlaces MPLS en las Regionales del Banco donde se debía aplicar la topología.

Con la tecnología DMVPN se logró realizar comunicación cifrada (IPSEC) entre los Routers WAN de las regionales (Spokes) y los Routers WAN del Sitio Principal (Hub1) y Sito Alterno (Hub2), así mismo, la comunicación entre las regionales (spoke-spoke) se estableció directamente por los canales MPLS a través de un túnel cifrado IPSEC.

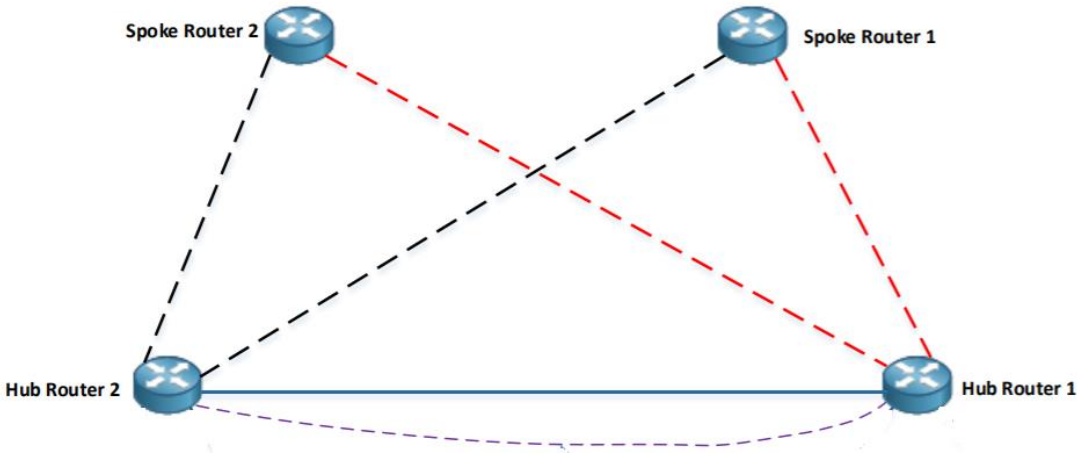


Figura 16 Topología Dual Hub/Dual DMVPN

Fuente: Elaboración Propia

2.2.2.2 Enrutamiento Dinámico EIGRP

Debido a la cantidad de sucursales, la escalabilidad necesaria y las recomendaciones de las guías de implementación de Cisco, se decidió aplicar enrutamiento dinámico EIGRP sobre la topología DMVPN.

El protocolo EIGRP colaboró con los criterios para seleccionar los túneles con mejor rendimiento para el tráfico crítico del Banco.

2.2.2.3 Extensión de Capa 2 con L2TPv3

Se requería realizar réplica de Datos, datos en relación con la plataforma virtual de Servidores. La réplica de datos debía realizarse entre el Sitio Principal (La Paz) y el Sitio Alterno (Santa Cruz).

La funcionalidad de réplica de la plataforma de servidores virtuales requería contar con la conectividad sobre los mismos segmentos de red (mismas VLANs), es decir, por ejemplo, si la Vlan 100 era utilizada por los servidores “A” en el Sitio Principal la misma Vlan 100 debía existir en el Sitio Alterno para los servidores “B" y estar funcionalmente activa para el constante tráfico de datos de réplica.

Se determinó utilizar el protocolo L2TPv3 para extender Vlans en capa 2 entre el Sitio Principal (La Paz) y el Sitio Alterno (Santa Cruz) a través de una red MPLS dedicada para ese fin.

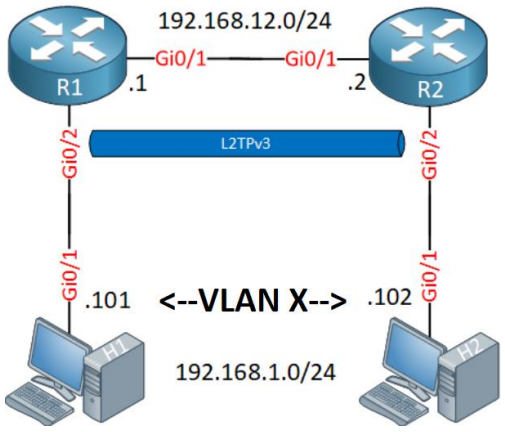


Figura 17 Extensión de Vlan a través de L2TPv3

Fuente: Internet

https://networklessons.com/cisco/ccie-routing-switching-written/l2tpv3-layer-2-tunnel-protocol-version-3

2.2.2.4 Equipos seleccionados

Los equipos de comunicación seleccionados para la implementación del presente proyecto se muestran en la tabla de abajo, donde los equipos Vigentes fueron equipos con los que ya contaba el Banco y sólo se realizaron adecuaciones en configuración.

Los equipos Nuevos fueron necesarios adquirirlos para cumplir con los objetivos del Banco.

Equipo	Tipo de Equipo	Ciudad	Funcionalidad	Observación
CISCO C3945	Router Activo	La Paz	Conexión WAN DMVPN	Equipo Vigente
CISCO ISR4431	Router	Santa Cruz	Conexión WAN DMVPN	Equipo Nuevo
CISCO ISR4321	Router	La Paz	Conexión L2TPv3	Equipo Nuevo
CISCO ISR4321	Router	Santa Cruz	Conexión L2TPv3	Equipo Nuevo
CISCO2911	Router	Cochabamba	Conexión WAN DMVPN	Equipo Vigente
CISCO2901	Router	Oruro	Conexión WAN DMVPN	Equipo Vigente
CISCO2901	Router	Potosi	Conexión WAN DMVPN	Equipo Vigente
CISCO2901	Router	Sucre	Conexión WAN DMVPN	Equipo Vigente
CISCO2901	Router	Tarija	Conexión WAN DMVPN	Equipo Vigente
CISCO2901	Router	Trinidad	Conexión WAN DMVPN	Equipo Vigente
CISCO2901	Router	Cobija	Conexión WAN DMVPN	Equipo Vigente

Tabla 2 Equipos Routers seleccionados para DMVPN

Fuente: Elaboración Propia

Equipo	Características Técnicas y Funcionales
CISCO C3945 	**Algoritmos de seguridad soportados:** IPSEC,SSL/TLS. **Estándares de red:** IEEE 802.1Q,IEEE 802.1ag,IEEE 802.3,IEEE 802.3ah **Protocolo de routing:** BGP,EIGRP,IGRP,IS-IS,OSPF **Protocolos de red compatibles:** IPSec **Protocolos soportados:** IPv4, IPv6, OSPF, EIGRP, BGP, IS-IS, IGMPv3, PIM SM, SSM, DVMRP, IPv4-to-IPv6 Multicast, MPLS, VPN, IPSec, L2TPv3, BFD, IEEE802.1ag, and IEEE802.3ah **Seguridad:** UL 60950-1, CAN/CSA C22.2 No. 60950-1, EN 60950-1, AS/NZS 60950-1, IEC 60950-1

Equipo	Características Técnicas y Funcionales
CISCO ISR 4431  	**Algoritmos de seguridad soportados:** 128-bit AES,256-bit AES,DES **Estándares de red:** IEEE 802.1Q,IEEE 802.1ag,IEEE 802.3,IEEE 802.3ah **Protocolo de routing**: BGP,EIGRP,IS-IS,OSPF Protocolos de red compatibles: IPv4, IPv6, RIP, RIPv2, IGMPv3 **Seguridad:** UL 60950-1, CAN/CSA C22.2 No. 60950-1, EN 60950-1, AS/NZS 60950-1, IEC 60950-1 **Seguridad con cortafuegos:** IPSec VPN, EZVPN, DMVPN, FlexVPN
CISCO ISR 4321  	
CISCO 2911  	**Estándares de red:** IEEE 802.1Q,IEEE 802.1ag,IEEE 802.3,IEEE 802.3ab,IEEE 802.3af,IEEE 802.3ah,IEEE 802.3u **Protocolo de routing:** BGP,EIGRP,OSPF **Protocolos soportados:** IPv4, IPv6, IS-IS, IGMPv3, PIM SM, SSM, DVMRP, IPSec, GRE, BVD, MPLS, L2TPv3, PPP, MLPPP, MLFR, HDLC, RS-232, RS-449, X.21, V.35, EIA-530, PPPoE, ATM **Seguridad:** UL 60950-1, CAN/CSA C22.2 No. 60950-1, EN 60950-1, AS/NZS 60950-1, IEC 60950-1 **Seguridad con cortafuegos:** IOS

Equipo	Características Técnicas y Funcionales
CISCO 2901 	**Estándares de red**: IEEE 802.1Q,IEEE 802.1ag,IEEE 802.3,IEEE 802.3ab,IEEE 802.3af,IEEE 802.3ah **Protocolo de routing**: BGP,EIGRP,OSPF **Protocolos soportados:** IPv4, IPv6, IS-IS, IGMPv3, PIM SM, SSM, DVMRP, IPSec, GRE, BVD, MPLS, L2TPv3, PPP, MLPPP, MLFR, HDLC, RS-232, RS-449, X.21, V.35, EIA-530, PPPoE, ATM **Seguridad:** UL 60950-1, CAN/CSA C22.2 No. 60950-1, EN 60950-1, AS/NZS 60950-1, IEC 60950-1 **Seguridad con cortafuegos:** IOS

Tabla 3 Especificaciones Técnicas de los equipos seleccionados

Fuente: Internet Cisco Systems
https://www.cisco.com/

2.2.2.5 Costos de Equipamiento e Implementación

A continuación, se indican los costos aproximados del equipamiento adquirido y los servicios de implementación:

ITEM	Número de Parte / Servicio	Descripción	Duración de SNTC (Meses)	Precio Unitario USD	Cantidad	Precio SubTotal USD	Precio SubTotal Bolivianos
1.0	**ISR4431-AX/K9**	Cisco ISR 4431 AX Bundle with APP and SEC license	---	19.500,00	1	19.500,00	135.720,00
1.1	CON-SNTP-ISR4431A	SNTC-24X7X4 Cisco ISR 4431 AX Bundle with APP and SEC li	36	11.100,00	1	11.100,00	77.256,00
1.2	SL-44-IPB-K9	IP Base License for Cisco ISR 4400 Series	---	0,00	1	0,00	0,00
1.3	MEM-4400-4GU8G	4G to 8G DRAM Upgrade (4G+4G) for Cisco ISR 4400	---	1.500,00	1	1.500,00	10.440,00
1.4	MEM-FLSH-8U16G	8G to 16G eUSB Flash Memory Upgrade for Cisco ISR 4430	---	1.500,00	1	1.500,00	10.440,00
1.5	NIM-2GE-CU-SFP	2-port GE WAN NIM, dual-mode RJ45 & SFP	---	1.800,00	2	3.600,00	25.056,00
1.6	PWR-4430-AC	AC Power Supply for Cisco ISR 4430	---	0,00	1	0,00	0,00
1.7	PWR-4430-AC/2	AC Power Supply (Secondary PS) for Cisco ISR 4430	---	800,00	1	800,00	5.568,00
1.8	CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	---	0,00	2	0,00	0,00
1.9	ISRWAAS-RTU-1300	ISRWAAS RTU for 1300 connections	---	0,00	1	0,00	0,00
1.10	CON-ECMU-IW1300	SWSS UPGRADES ISRWAAS RTU for 1300 connections	36	0,00	1	0,00	0,00
1.11	MEM-4400-DP-2G	2G DRAM (1 DIMM) for Cisco ISR 4400 Data Plane	---	0,00	1	0,00	0,00

ITEM	Número de Parte / Servicio	Descripción	Duración de SNTC (Meses)	Precio Unitario USD	Cantidad	Precio SubTotal USD	Precio SubTotal Bolivianos
1.12	SL-44-APP-K9	AppX License for Cisco ISR 4400 Series	---	0,00	1	0,00	0,00
1.13	NIM-BLANK	Blank faceplate for NIM slot on Cisco ISR 4400	---	0,00	1	0,00	0,00
1.14	SL-44-SEC-K9	Security License for Cisco ISR 4400 Series	---	0,00	1	0,00	0,00
1.15	SISR4400UK9-166	Cisco ISR 4400 Series IOS XE Universal	---	0,00	1	0,00	0,00
2.0	**ISR4321-SEC/K9**	Cisco ISR 4321 Sec bundle w/SEC license	---	3.400,00	2	6.800,00	47.328,00
2.1	CON-SSSNP-ISR4321S	Cisco ISR 4321 Sec bundle w SEC license	36	3.250,00	2	6.500,00	45.240,00
2.2	SL-4320-IPB-K9	IP Base License for Cisco ISR 4320 Series	---	0,00	2	0,00	0,00
2.3	MEM-4320-4GU8G	4G to 8G DRAM Upgrade (Fixed 4G + additional 4G) for ISR4320	---	800,00	2	1.600,00	11.136,00
2.4	MEM-FLSH-4U8G	4G to 8G eUSB Flash Memory Upgrade for Cisco ISR 4300	---	1.000,00	2	2.000,00	13.920,00
2.5	NIM-2GE-CU-SFP	2-port GE WAN NIM, dual-mode RJ45 & SFP	---	1.800,00	2	3.600,00	25.056,00
2.6	PWR-4320-AC	AC Power Supply for Cisco ISR 4320	---	0,00	2	0,00	0,00
2.7	CAB-AC-C5	AC Power Cord, Type C5, US, Canada	---	0,00	2	0,00	0,00
2.8	SL-4320-SEC-K9	Security License for Cisco ISR 4320 Series	---	0,00	2	0,00	0,00
2.9	SISR4300UK9-166	Cisco ISR 4300 Series IOS XE Universal	---	0,00	2	0,00	0,00
					Sub Total USD	**58.500,00**	
						Sub Total Bolivianos	**407.160,00**
3.0	**Servicios Profesionales**	Servicios Profesionales para la Implementación		3.000,00	1	3.000,00	20.880,00
					Total USD	**61.500,00**	
						Total Bolivianos	**428.040,00**

Tabla 4 Costos de equipamiento e implementación

Fuente: Elaboración Propia

2.2.2.6 Esquema de Red Nuevo

Como parte del diseño, se armó el Esquema de Red Nuevo, el cual refleja la arquitectura DMVPN seleccionada **Dual DMVPN/ Dual Hub,** la conectividad entre Regionales, Sitio Principal y Sitio Alterno. A continuación, se muestra el esquema generado:

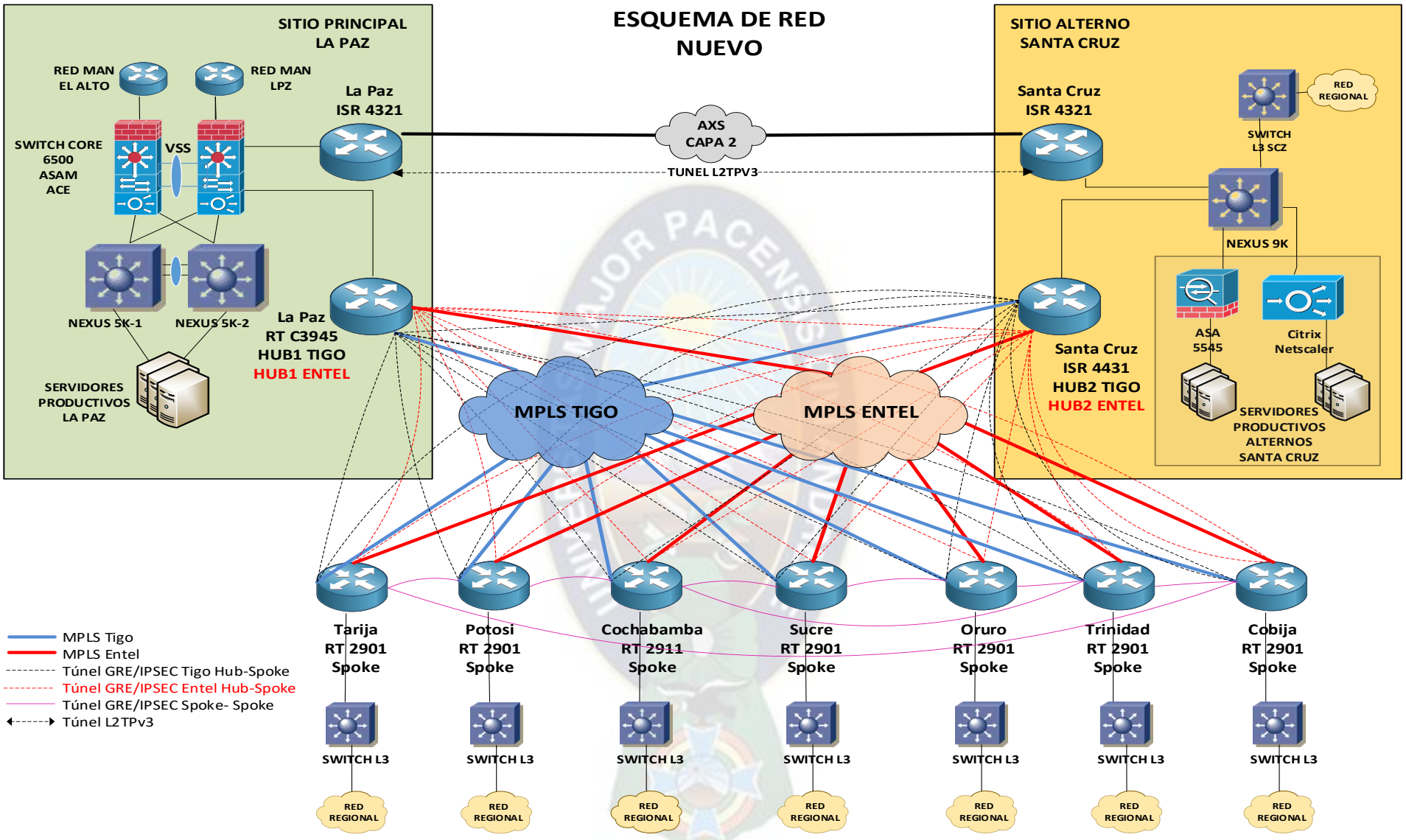


Figura 18 Esquema de Red Nuevo DMVPN

Fuente: Elaboración Propia

2.2.2.7 Direccionamiento IP DMVPN

En coordinación con el Banco, se definieron las direcciones IP a ser utilizadas en la implementación de los túneles con las distintas regionales y agencias.

A continuación, se muestra la relación de IPs utilizadas en la topología DMVPN:

DMVPN TIGO					
ROL DMVPN	CIUDAD	SOURCE INTERFACE	IP SOURCE	IP TUNNEL 21	IP LOOPBACK
HUB 1 Primario	LPZ	g0/1	172.21.65.58/29	172.21.254.10	10.100.100.10
HUB 2 Alterno-Spoke	SCZ	g0/2	172.21.13.18/29	172.21.254.11	10.100.100.11
Spoke	CBB	g0/2	172.21.132.2/29	172.21.254.12	10.100.100.12
Spoke	SCR	g0/1	172.21.224.66/29	172.21.254.13	10.100.100.13
Spoke	TRJ	g0/1	172.21.176.50/29	172.21.254.14	10.100.100.14
Spoke	TRN	f0/3/0	172.21.248.74 /29	172.21.254.15	10.100.100.15
Spoke	ORU	g0/1	172.21.192.50/29	172.21.254.16	10.100.100.16
Spoke	PTS	g0/1	172.21.225.50/29	172.21.254.17	10.100.100.17
Spoke	CBJ	g0/0	172.20.249.50/29	172.21.254.18	10.100.100.18
DMVPN ENTEL					
ROL DMVPN	CIUDAD	SOURCE INTERFACE	IP SOURCE	IP TUNNEL31	IP LOOPBACK
HUB 1 Primario	LPZ	f0/2/0	172.31.65.58/29	172.31.254.10	10.100.100.10
HUB 2 Alterno-Spoke	SCZ	g0/1	172.31.13.18/29	172.31.254.11	10.100.100.11
Spoke	CBB	g0/1	172.31.132.2/29	172.31.254.12	10.100.100.12
Spoke	SCR	f0/2/0	172.31.224.66/29	172.31.254.13	10.100.100.13
Spoke	TRJ	f0/3/0	172.31.176.50/29	172.31.254.14	10.100.100.14
Spoke	TRN	g0/1	172.31.226.50/29	172.31.254.15	10.100.100.15
Spoke	ORU	f0/2/0	172.31.192.50/29	172.31.254.16	10.100.100.16
Spoke	PTS	f0/2/0	172.31.225.50/29	172.31.254.17	10.100.100.17
Spoke	CBJ	f0/3/0	172.31.227.50/29	172.31.254.18	10.100.100.18

Tabla 5 Direccionamiento IP DMVPN

Fuente: Elaboración Propia

2.2.2.8 Conectividad en las Redes MPLS

Como requisito para establecer los túneles en la topología DMVPN seleccionada, se debió solicitar las gestiones del Banco con los proveedores MPLS Entel y Tigo para que exista conectividad entre las direcciones IP proporcionadas por los proveedores:

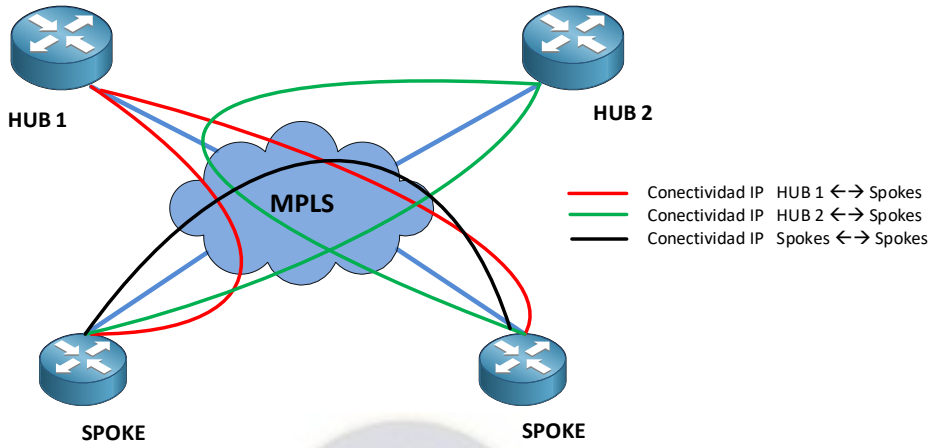


Figura 19 Conectividad IP necesaria sobre MPLS

Fuente: Elaboración Propia

2.2.2.9 Configuración y comandos por utilizar

De acuerdo con las necesidades del Banco y guías de Cisco para establecer DMVPN con enrutamiento EIGRP, se planteó las siguientes configuraciones modelo para el escenario y topología seleccionados.

CONFIGURACIÓN O COMANDO	PROPOSITO
Crypto isakmp policy numero Ejemplo: Router(config)# crypto isakmp policy 1	Se crea las pollticas de seguridad isakmp (Internet Security Association and Key Management Protocol) escogiendo un numero para todos los routers
Authentication pre-share Ejemplo: Router(config-isakmp)# authetication pre-share	Es una clave secreta compartida con anterioridad entre las dos partes usando algun canal seguro antes de que se utilice
Encryption aes numero Ejemplo: Router(config-isakmp)# encryption aes 192	Se utiliza un algoritmo de cifrado y el numero es la cantidad de bits para el cifrado
Hash sha Ejemplo: Router(config-isakmp)# hash sha	hash es metodo para generar claves o llaves.
Group 5 Ejemplo: Router(config-isakmp)# group 5	Permite que dos dispositivos puedan establecer un llave compartido por una red no segura.
Crypto isakmp policy numero {contrasena}[Direccion de red] Ejemplo: Router(config)# crypto isakmp key 6 cisco address 192.168.1.0 255.255.255.128	Configura una clave de autenticacion previamente compartida. Contrasena se debe escoger una contrasena para la autenticacion de todos los Routers que participan en la Red Y finalmente escoger las redes que son confiables para poner tener una conexión
crypto ipsec profile nombre Example: Router(config)# crypto ipsec profile vpnprof	Define los parametros de IPSec que deben ser utilizados para la encripcion de IPSec entre "spoke y concentrador" y el Routers del "spoke y del spoke". Este comando ingresa al modo de configuracion de la correspondencia de criptografia. • nombre El argumento especifica el nombre del perfil de ipsec.

Tabla 6 Configuración de Seguridad ISAKMP/IPSEC

Fuente: Internet – Cisco Systems

CONFIGURACIÓN O COMANDO	PROPOSITO
enable Ejemplo: Router> enable	Habilita el nivel privilegiado, como el modo EXEC privilegiado. Ingrese su contrasena si se le pide que lo haga.
Configure Terminal Ejemplo: Router#configure terminal	Ingresa en el modo de configuracion global.
Interface tunnel numero Ejemplo: Router(config)# interface tunnel 5	Configura una interfaz del tunel e ingresa al modo de configuracion de la interfaz del tunel. El argumento especifica el numero de la interfaz del tunel que usted quiere crear o configurar. El rango de la numero del tunel puede ir de <0 - 2147483647>
ip address {direccion de IP y mascara} Ejemplo: Router(config-if)# ip Address 10.0.0.1 255.255.255.0	Establece una direccion IP primaria o secundaria para la interfaz de tunel. Observe todo el Hubs y el spokes que esta en la misma red DMVPN se debe dirigir en la misma subred.
tunnel source {direccion IP o Interface} Ejemplo: Router(config-if)# tunnel source Ethernet0	Fija a la direccion de origen para una interfaz del tunel.
tunnel mode gre multipoint Example: Router(config-if)# tunnel mode gre multipoint	Establece el modo de encapsulacion en mGRE de la interfaz de tunel.

Tabla 7 Configuración mGRE

Fuente: Internet Cisco Systems

https://www.cisco.com/

CONFIGURACIÓN O COMANDO	PROPOSITO
Interface tunnel numero Ejemplo: Router(config)# interface tunnel 5	Ingresar a la interface del tunel ya creado en el anterior paso
ip nhrp network-id numero Ejemplo: Router(config-if)# ip nhrp network-id 99	Habilita NHRP en una interfaz. Numero es el argumento especifica el identificador de red de 32 bits unico a global de una red del acceso multiple sin broadcast (NBMA). El rango es a partir la 1 a 4294967295
ip nhrp authentication cadena Ejemplo: Router(config-if)# ip nhrp authentication donttell	Configura la cadena de la autenticacion de una interfaz usando NHRP. Observe que la autenticacion nhrp es una cadena que debe ser fijado al mismo valor tanto en el Hubs y spokes que esten en la misma red DMVPN.
ip nhrp holdtime segundos Ejemplo: Router(config-if)# ip nhrp holdtime 450	Cambia el numero de segundos que se anuncian las direcciones NHRP NBMA como validas en las respuestas NHRP autorizadas. Segundos El argumento especifica el tiempo en los segundos de que los direccionamientos NBMA se hacen publicidad como validos en las respuestas autoritarias positivas NHRP. El valor recomendado se situa entre 60 y 600 segundos.
ip nhrp map {direccion IP del tunel y IP publica del HUB} Ejemplo: Router(config-if)# ip nhrp map 172.16.1.3 10.10.10.2	Hace un mapeo de la direccion del tunel hacia la direccion IP que es publica. Se apunta a la direccion del HUB
ip nhrp nhs {direccion del Tunel Hub} Ejemplo: Router(config-if)#ip nhrp nhs 172.16.1.3	Es para indicar donde esta el servidor NHRP
ip nhrp map multicast {direccion de ip publica hub} Ejemplo: Router(config-if)#ip nhrp map multicast 10.10.10.2	Sirve para encapsular el trafico multicast con la direccion publica del Hub

Tabla 8 Configuración NHRP

Fuente: Internet - Cisco Systems

https://www.cisco.com/

CONFIGURACIÓN O COMANDO	PROPOSITO
Interface tunnel numero Ejemplo: Router(config)# interface tunnel 5	Ingresar a la interface del tunel ya creado en el anterior paso
ip mtu bytes Ejemplo: Router(config-if)# ip mtu 1400	Fija la talla del MTU, en los bytes, de los paquetes IP enviados en una interfaz.
ip tcp adjust-mss maxsegment- size Ejemplo: Router(config-if)# ip tcp adjust-mss 1360	Ajusta el valor del Tamano de segmento maximo (MSS) de los paquetes TCP que pasan por un router. max-segment-size El argumento especifica el Maximum Segment Size, en los bytes. El rango es a partir el 500 a 1460. El valor de la cantidad recomendada es 1360 cuando el numero de bytes IP MTU se fija a 1400. Con esta configuracion recomendada, las sesiones TCP se vuelven a escalar rapidamente a paquetes IP de 1400 bytes para que estos "quepan" en el tunel.

Tabla 9 Control de MTU

Fuente: Internet Cisco Systems
https://www.cisco.com/

CONFIGURACIÓN O COMANDO	PROPOSITO
enable Ejemplo: Router> enable	Habilita el nivel privilegiado, como el modo EXEC privilegiado. Ingrese su contrasena si se le pide que lo haga.
Configure Terminal Ejemplo: Router#configure terminal	Ingresa en el modo de configuracion global.
Router eigrp numero Ejemplo: Router(config)# router eigrp 1	Se activa el enrutamiento eigrp con el comando y se debe escoger un numero de sistema autonomo que va desde <1-65535> que debe ser igual en todos los routers
network {direccion de IP y mascara} Ejemplo: Router(config-if)# network 10.0.0.0 0.0.0.255	Se establece todas las redes que van a participar en el enrutamiento
Router eigrp numero Ejemplo: Router(config)# router eigrp 1	Se activa el enrutamiento eigrp con el comando y se debe escoger un numero de sistema autonomo que va desde <1-65535> que debe ser igual en todos los routers
No autosumary Ejemplo: Router(config-router)#no autosumary	A1 ingresar este comando le decimos al router que NO sumarize las rutas que tiene. Es de gran utilidad cuando no tenemos redes contiguas.
passive-interface [Nombre de interfaz] ejemplo: Router(config-router)# passive-interface fastethernet 0/0/0	Es un comando de mucha utilidad a la hora de ahorrar ancho de banda, porque nos permite decirle al router que por la interfaz [Nombre de interfaz] no envie actualizaciones de su tabla de enrutamiento.

Tabla 10 Aplicación de EIGRP

Fuente: Internet - Cisco Systems
https://www.cisco.com/

CONFIGURACIÓN O COMANDO	PROPOSITO
Configure un L2TP-class (opcional) **l2tp-class test** **hostname stanford password** **7 082E5C4B071F091805**	Esta clase se utiliza para definir una cierta autenticación y los parámetros de control para el L2TP hacen un túnel. Si se utiliza, los dos extremos deben duplicarse.
pseudowire-class test **encapsulation l2tpv3** **ip local interface Loopback0** **ip pmtu**	Mientras que el nombre sugiere, esta sección se utiliza para configurar el túnel o el "pseudowire real" entre los dos puntos finales. Defina una plantilla que contenga la encapsulación del pseudowire, un punto final, y el protocolo del canal de control.
Utilice Xconnect para proporcionar el destino del túnel **interface GigabitEthernet** **encapsulation dot1Q XX** **no cdp enable** **xconnect zzz.zzz.zzz.zzz encapsulation l2tpv3 pw-class l2tpv3-tunnel**	El pseudowire L2TP al circuito de la conexión (interfaz hacia el lado local L2) y defina su destino • El circuito en sí mismo de la conexión no tiene ninguna dirección IP configurada. • El origen de túnel configurado con la interfaz local IP está en la sección de la pseudowireclase. • El destino del túnel se define con el comando del xconnect.

Tabla 11 Configuración de L2TPv3

Fuente: Internet - Cisco Systems
https://www.cisco.com/

2.2.3 Fase de Implementación

La fase de implementación se realizó de forma controlada en coordinación con el Banco, debido a que la implementación se realizó con equipos de comunicación y tráfico productivo, se contempló el siguiente procedimiento y plan de migración hacia la nueva topología:

a. Se realizó una copia de respaldo de toda la configuración de los equipos de comunicación involucrados.

b. En una primera instancia, no se afectaron los túneles GRE punto a punto existentes (entre Oficinas Regionales y Oficina Central) sobre las interfaces MPLS, su enrutamiento era estático y no se contaba con cifrado en el túnel.

c. Se configuraron nuevos túneles GRE utilizando nuevo direccionamiento IP de acuerdo a la Tabla 4, sobre las mismas interfaces asociadas al enlace MPLS, se aplicó cifrado IPSEC y la topología DMVPN seleccionada. Se aplicó direccionamiento dinámico EIGRP inicialmente sólo con las redes de los túneles nuevos, el proceso fue gradual empezando por La Paz como HUB principal, Santa Cruz como HUB

secundario y regionales con poco tráfico. No se afectó el tráfico productivo que se trasportaba por los túneles antiguos.

d. Se aplicó la configuración inicial de los nuevos túneles a cada regional involucrada en un tiempo de 2 días.

e. Para migrar el tráfico de una regional a los nuevos túneles, se adicionaron las redes locales de las regionales al enrutamiento EIGRP de su router regional, como también las redes locales en el lado del router HUB principal en La Paz. Se depuraron registros necesarios de rutas estáticas para que tome efecto el enrutamiento dinámico.

f. Se aplicaron las configuraciones del punto f) a todas las regionales en un tiempo aproximado a tres (3) días tomando en cuenta ventanas de tiempo autorizadas por el Banco para estas tareas.

g. Las verificaciones y pruebas que se realizaron a la configuración inicial de los nuevos túneles y migración del tráfico fueron:

VERIFICACIONES Y PRUEBAS A CONFIGURACIONES INICIALES	
COMANDO UTILIZADO	**PROPÓSITO**
#show dmvpn	*Verificar la creación de los túneles DMVPN*
#show ip route	*Verificar la tabla de enrutamiento con la creación de EIGRP.*
#show cryptomap isakmp sa	*Verificar que el túnel esté cifrado con IPSEC.*
#ping (IP del túnel nuevo)	*Verificar conectividad y estabilidad de los túneles nuevos.*

Tabla 12 Verificación de Configuraciones Iniciales

h. Se depuraron los túneles GRE antiguos.

i. La configuración del túnel L2TPv3 fue nueva y no afectó a producción, se realizó inicialmente con Vlas de prueba y posteriormente se adicionaron vlans productivas para extenderlas hacia el sitio alterno.

j. Hasta este punto, ya se contaba con toda la configuración necesaria aplicada para probar la convergencia del sitio principal al sitio alterno, lo cual se explica más adelante con mayor detalle.

2.2.3.1 Configuración aplicada en los Routers HUBs

En esta parte se muestra la configuración aplicada en los routers que tienen el rol de HUBs. A continuación, se representa un diagrama de flujo de los procesos de configuración:

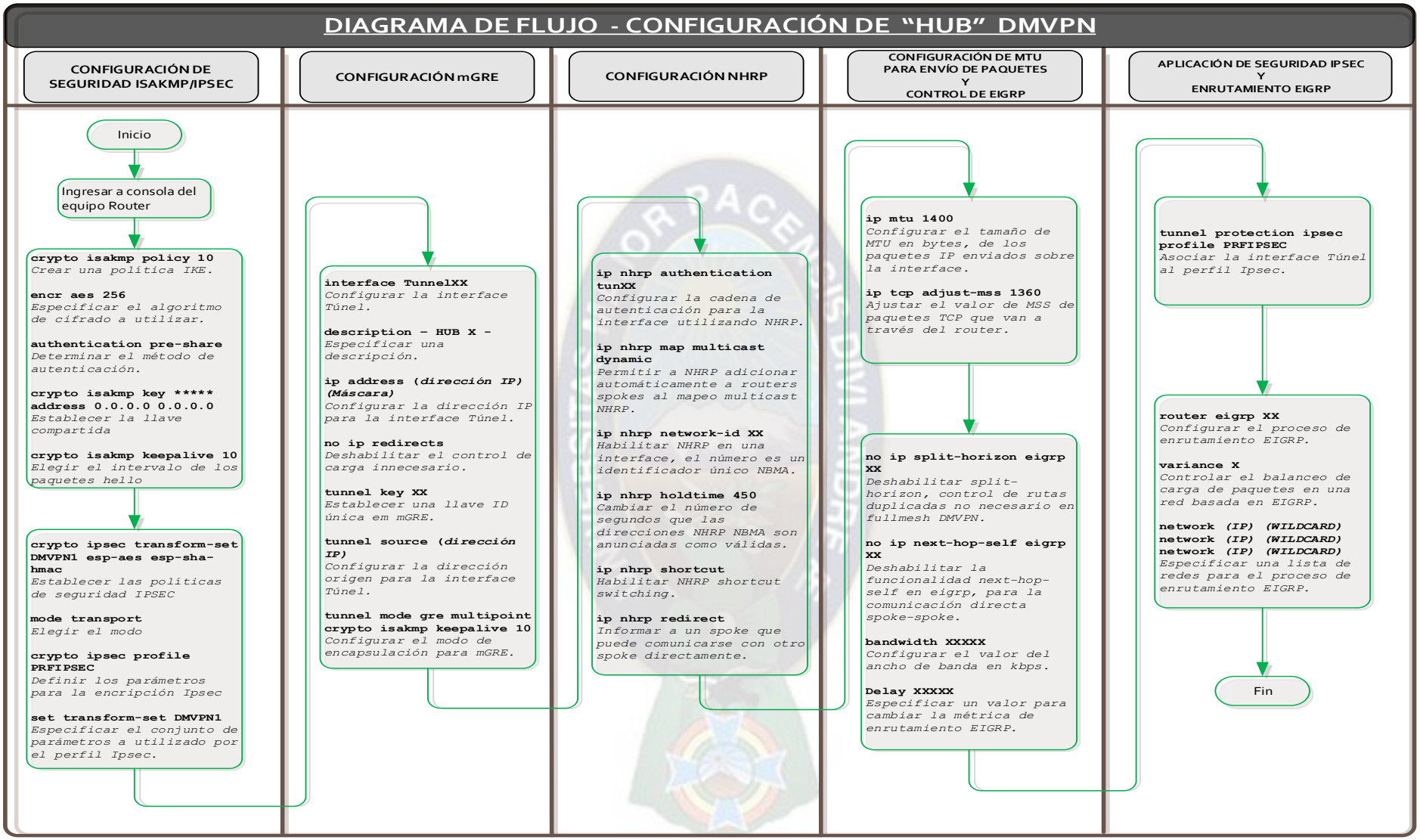


Figura 20 Diagrama de Flujo - Configuración HUB DMVPN

Fuente: Elaboración Propia

2.2.3.2 Hub 1 La Paz (Sitio Principal)

CONFIGURACIÓN DE SEGURIDAD ISAKMP/IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
crypto isakmp policy 10	*Crear una política IKE. Cada política se identifica por su número de prioridad (de 1 a 10.000; 1 la prioridad más alta)*
encr aes 256	*Especificar el algoritmo de cifrado a utilizar. AES soporta 128,192,256 bits.*
authentication pre-share	*Determinar el método de autenticación. (Llaves compartidas)*
crypto isakmp key *** address 0.0.0.0 0.0.0.0**	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
crypto isakmp keepalive 10	*Elegir el intervalo de los paquetes hello (por defecto 10 segundos)*
crypto ipsec transform-set DMVPN1 esp-aes esp-sha-hmac	*Establece las políticas de seguridad IPSEC que se usarán en las comunicaciones.*
mode transport	*Elegir el modo*
crypto ipsec profile PRFIPSEC	*Define los parámetros que serán utilizados para la encriptación Ipsec entre routers "hub y spoke" y "spoke y spoke".*
set transform-set DMVPN1	*Especificar cual conjunto de parámetros puede ser utilizado por el perfil Ipsec.*

HUB 1 DMVPN TIGO

CONFIGURACIÓN mGRE	
COMANDO IMPLEMENTADO	**PROPÓSITO**
interface Tunnel21	*Configurar la interface Túnel, con el número asignado.*
description --- HUB 1 DMVPN TIGO ---	*Especificar una descripción para la interface Túnel creada.*
ip address 172.21.254.10 255.255.255.0	*Configurar la dirección IP para la interface Túnel dentro de la misma subred IP de la DMVPN.*
no ip redirects	*Deshabilitar el control de carga innecesario.*
tunnel key 21	*Establecer una llave ID única que deberá ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
tunnel source 172.21.65.58	*Configurar la dirección origen para la interface Túnel.*
tunnel mode gre multipoint	*Configurar el modo de encapsulación para mGRE para la interface Túnel.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp authentication tun21	*Configurar la cadena de autenticación para una interface utilizando NHRP, la cadena debe ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
ip nhrp map multicast dynamic	*Permitir a NHRP adicionar automáticamente a routers spokes al mapeo multicast NHRP.*
ip nhrp network-id 21	*Habilitar NHRP en una interface, el número es un identificador único NBMA.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp holdtime 450	*Cambiar el número de segundos que las direcciones NHRP NBMA son anunciadas como válidas.*
ip nhrp shortcut	*Habilitar NHRP shortcut switching.*
ip nhrp redirect	*Informar a un spoke que puede comunicarse con otro spoke directamente.*

CONFIGURACIÓN DE MTU PARA ENVÍO DE PAQUETES	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip mtu 1400	*Configurar el tamaño de MTU en bytes, de los paquetes IP enviados sobre la interface.*
ip tcp adjust-mss 1360	*Ajustar el valor de MSS de paquetes TCP que van a través del router.*

CONTROL DE PROTOCOLO DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
no ip split-horizon eigrp 60	*Deshabilitar split-horizon, control de rutas duplicadas no necesario en fullmesh DMVPN.*
no ip next-hop-self eigrp 60	*Deshabilitar la funcionalidad next-hop-self en eigrp, para la comunicación directa spoke-spoke.*
bandwidth 20000	*Configurar el valor del ancho de banda en kbps.*
delay 2400	*Especificar un valor para cambiar la métrica de enrutamiento EIGRP.*

APLICACIÓN DE SEGURIDAD IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
tunnel protection ipsec profile PRFIPSEC	*Asociar la interface Túnel al perfil Ipsec.*

HUB 1 DMVPN ENTEL

CONFIGURACIÓN mGRE	
COMANDO IMPLEMENTADO	**PROPÓSITO**
interface Tunnel31	*Configurar la interface Túnel, con el número asignado.*
description --- HUB 1 DMVPN ENTEL ---	*Especificar una descripción para la interface Túnel creada.*
ip address 172.31.254.10 255.255.255.0	*Configurar la dirección IP para la interface Túnel dentro de la misma subred IP de la DMVPN.*
no ip redirects	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
tunnel key 31	*Establecer una llave ID única que deberá ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*

CONFIGURACIÓN mGRE	
COMANDO IMPLEMENTADO	**PROPÓSITO**
tunnel source 172.31.65.58	*Configurar la dirección origen para la interface Túnel.*
tunnel mode gre multipoint	*Configurar el modo de encapsulación para mGRE para la interface Túnel.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp authentication tun31	*Configurar la cadena de autenticación para una interface utilizando NHRP, la cadena debe ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
ip nhrp map multicast dynamic	*Permitir a NHRP adicionar automáticamente a routers spokes al mapeo multicast NHRP.*
ip nhrp network-id 31	*Habilitar NHRP en una interface, el número es un identificador único NBMA.*
ip nhrp holdtime 450	*Cambiar el número de segundos que las direcciones NHRP NBMA son anunciadas como válidas.*
ip nhrp shortcut	*Habilitar NHRP shortcut switching.*
ip nhrp redirect	*Informar a un spoke que puede comunicarse con otro spoke directamente.*

CONFIGURACIÓN DE MTU PARA ENVÍO DE PAQUETES	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip mtu 1400	*Configurar el tamaño de MTU en bytes, de los paquetes IP enviados sobre la interface.*
ip tcp adjust-mss 1360	*Ajustar el valor de MSS de paquetes TCP que van a través del router.*

CONTROL DE PROTOCOLO DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
no ip next-hop-self eigrp 60	*Deshabilitar split-horizon, control de rutas duplicadas no necesario en fullmesh DMVPN.*
no ip split-horizon eigrp 60	*Deshabilitar la funcionalidad next-hop-self en eigrp, para la comunicación directa spoke-spoke.*
bandwidth 20000	*Configurar el valor del ancho de banda en kbps.*
delay 1000	*Especificar un valor para cambiar la métrica de enrutamiento EIGRP.*

APLICACIÓN DE SEGURIDAD IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
tunnel protection ipsec profile PRFIPSEC	*Asociar la interface Túnel al perfil Ipsec.*

Aplicando el protocolo de enrutamiento EIGRP, se realizó el balanceo de tráfico, induciendo que se utilice con mayor preferencia el enlace del proveedor ENTEL en una relación 2 a 1 con el proveedor TIGO.

APLICACIÓN DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
router eigrp 60	*Configurar el proceso de enrutamiento EIGRP.*
variance 2	*Controlar el balanceo de carga de paquetes en una red basada en EIGRP.*
network 10.100.100.10 0.0.0.0 **network 172.21.254.0 0.0.0.255** **network 172.31.254.0 0.0.0.255** **network 192.168.127.48 0.0.0.15**	*Especificar una lista de redes para el proceso de enrutamiento EIGRP.*

2.2.3.3 Hub 2 – Spoke Santa Cruz (Sitio Alterno)

La regional de Santa Cruz cumple el rol de Spoke cuando el sitio principal La Paz está activo. Cuando el sitio principal La Paz no se encuentra activo, el sitio alterno Santa Cruz actúa como Hub2.

CONFIGURACIÓN DE SEGURIDAD ISAKMP/IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
crypto isakmp policy 10	*Crear una política IKE. Cada política se identifica por su número de prioridad (de 1 a 10.000; 1 la prioridad más alta)*
encr aes 256	*Especificar el algoritmo de cifrado a utilizar. AES soporta 128,192,256 bits.*
authentication pre-share	*Determinar el método de autenticación. (Llaves compartidas)*
crypto isakmp key *** address 0.0.0.0 0.0.0.0**	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
crypto isakmp keepalive 10	*Elegir el intervalo de los paquetes hello (por defecto 10 segundos)*
crypto ipsec transform-set DMVPN1 esp-aes esp-sha-hmac	*Establece las políticas de seguridad IPSEC que se usarán en las comunicaciones.*
mode transport	*Elegir el modo*
crypto ipsec profile PRFIPSEC	*Define los parámetros que serán utilizados para la encriptación Ipsec entre routers "hub y spoke" y "spoke y spoke".*
set transform-set DMVPN1	*Especificar cual conjunto de parámetros puede ser utilizado por el perfil Ipsec.*

HUB 2 - SPOKE DMVPN TIGO

CONFIGURACIÓN mGRE	
COMANDO IMPLEMENTADO	**PROPÓSITO**
interface Tunnel21	*Configurar la interface Túnel, con el número asignado.*
description --- HUB2 SANTA CRUZ DMVPN TIGO ---	*Especificar una descripción para la interface Túnel creada.*
ip address 172.21.254.11 255.255.255.0	*Configurar la dirección IP para la interface Túnel dentro de la misma subred IP de la DMVPN.*
no ip redirects	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
tunnel key 21	*Establecer una llave ID única que deberá ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
tunnel source 172.21.13.18	*Configurar la dirección origen para la interface Túnel.*
tunnel mode gre multipoint	*Configurar el modo de encapsulación para mGRE para la interface Túnel.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp authentication tun21	*Configurar la cadena de autenticación para una interface utilizando NHRP, la cadena debe ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
ip nhrp map multicast dynamic	*Permitir a NHRP adicionar automáticamente a routers spokes al mapeo multicast NHRP.*
ip nhrp network-id 21	*Habilitar NHRP en una interface, el número es un identificador único NBMA.*
ip nhrp holdtime 450	*Cambiar el número de segundos que las direcciones NHRP NBMA son anunciadas como válidas.*
ip nhrp map multicast 172.21.65.58	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.*
ip nhrp map 172.21.254.10 172.21.65.58	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.*
ip nhrp nhs 172.21.254.10	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.*
ip nhrp shortcut	*Habilitar NHRP shortcut switching.*
ip nhrp redirect	*Informar a un spoke que puede comunicarse con otro spoke directamente.*

CONFIGURACIÓN DE MTU PARA ENVÍO DE PAQUETES	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip mtu 1400	*Configurar el tamaño de MTU en bytes, de los paquetes IP enviados sobre la interface.*
ip tcp adjust-mss 1360	*Ajustar el valor de MSS de paquetes TCP que van a través del router.*

CONTROL DE PROTOCOLO DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
no ip split-horizon eigrp 60	*Deshabilitar split-horizon, control de rutas duplicadas no necesario en fullmesh DMVPN.*
no ip next-hop-self eigrp 60	*Deshabilitar la funcionalidad next-hop-self en eigrp, para la comunicación directa spoke-spoke.*
bandwidth 4000	*Configurar el valor del ancho de banda en kbps.*
delay 3000	*Especificar un valor para cambiar la métrica de enrutamiento EIGRP.*

APLICACIÓN DE SEGURIDAD IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
tunnel protection ipsec profile PRFIPSEC	*Asociar la interface Túnel al perfil Ipsec.*

HUB 2 - SPOKE DMVPN ENTEL

CONFIGURACIÓN mGRE	
COMANDO IMPLEMENTADO	**PROPÓSITO**
interface Tunnel31	*Configurar la interface Túnel, con el número asignado.*
description --- HUB 2 SANTA CRUZ DMVPN ENTEL ---	*Especificar una descripción para la interface Túnel creada.*
ip address 172.31.254.11 255.255.255.0	*Configurar la dirección IP para la interface Túnel dentro de la misma subred IP de la DMVPN.*
no ip redirects	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
tunnel key 31	*Establecer una llave ID única que deberá ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
tunnel source 172.31.13.18	*Configurar la dirección origen para la interface Túnel.*
tunnel mode gre multipoint	*Configurar el modo de encapsulación para mGRE para la interface Túnel.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp authentication tun31	*Configurar la cadena de autenticación para una interface utilizando NHRP, la cadena debe ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
ip nhrp map multicast dynamic	*Permitir a NHRP adicionar automáticamente a routers spokes al mapeo multicast NHRP.*
ip nhrp network-id 31	*Habilitar NHRP en una interface, el número es un identificador único NBMA.*
ip nhrp holdtime 450	*Cambiar el número de segundos que las direcciones NHRP NBMA son anunciadas como válidas.*
ip nhrp map multicast 172.31.65.58	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp map 172.31.254.10 172.31.65.58	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.*
ip nhrp nhs 172.31.254.10	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.*
ip nhrp shortcut	*Habilitar NHRP shortcut switching.*
ip nhrp redirect	*Informar a un spoke que puede comunicarse con otro spoke directamente.*

CONFIGURACIÓN DE MTU PARA ENVÍO DE PAQUETES	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip mtu 1400	*Configurar el tamaño de MTU en bytes, de los paquetes IP enviados sobre la interface.*
ip tcp adjust-mss 1360	*Ajustar el valor de MSS de paquetes TCP que van a través del router.*

CONTROL DE PROTOCOLO DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
no ip split-horizon eigrp 60	*Deshabilitar split-horizon, control de rutas duplicadas no necesario en fullmesh DMVPN.*
no ip next-hop-self eigrp 60	*Deshabilitar la funcionalidad next-hop-self en eigrp, para la comunicación directa spoke-spoke.*
bandwidth 7100	*Configurar el valor del ancho de banda en kbps.*
delay 1400	*Especificar un valor para cambiar la métrica de enrutamiento EIGRP.*

APLICACIÓN DE SEGURIDAD IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
tunnel protection ipsec profile PRFIPSEC	*Asociar la interface Túnel al perfil Ipsec.*

Aplicando el protocolo de enrutamiento EIGRP, listas de acceso y offset, se indujo que se utilice el enlace del proveedor TIGO para la conexión de la regional con las redes críticas declaradas en la ACL PRIMARIO. El resto de tráfico fue balanceado e inducido para utilizar el enlace de ENTEL en una relación 2 a 1 con respecto al enlace de TIGO.

APLICACIÓN DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip access-list standard PRIMARIO	*Crear lista de acceso a utilizarse para el criterio de uso en el offset (compensación)*
permit 10.7.0.0 0.0.0.255 **permit 10.10.0.0 0.0.0.255**	*Definir las redes para el criterio del offset.*
router eigrp 60	*Configurar el proceso de enrutamiento EIGRP.*
variance 2	*Controlar el balanceo de carga de paquetes en una red basada en EIGRP.*
network 1.64.200.200 0.0.0.7 **network 10.100.100.11 0.0.0.0** **network 172.21.254.0 0.0.0.255** **network 172.31.254.0 0.0.0.255** **network 192.168.128.48 0.0.0.15**	*Especificar una lista de redes para el proceso de enrutamiento EIGRP.*
offset-list PRIMARIO in 3000000 Tunnel31	*Configurar el valor offset que se adicionará a la métrica de enrutamiento aplicada a métricas entrantes.*

2.2.3.4 Configuración aplicada en las Regionales (Spokes)

En esta parte se muestra la configuración aplicada en los routers de regionales que tienen el rol de Spokes. A continuación, se representa un diagrama de flujo de los procesos de configuración:

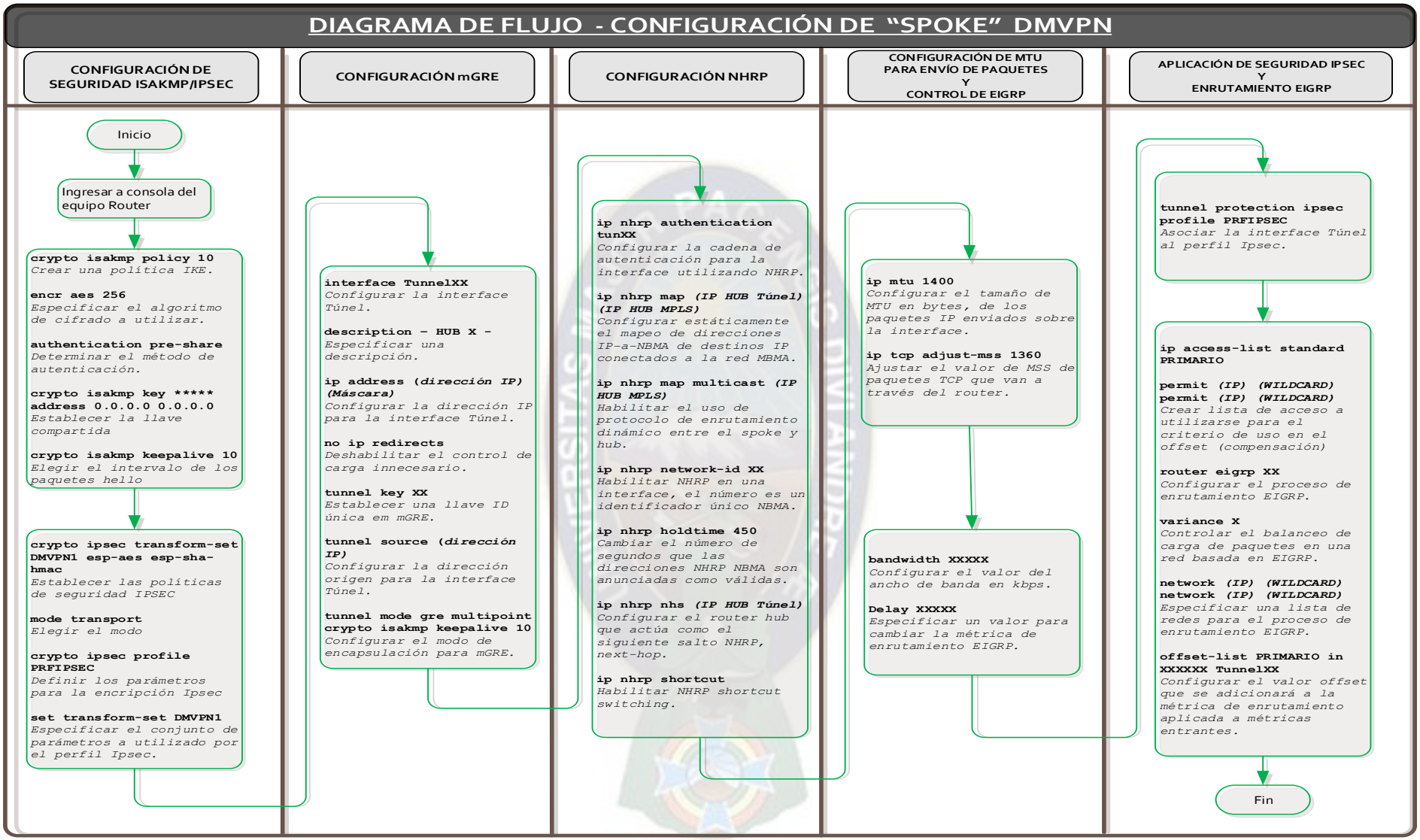


Figura 21 Diagrama de Flujo - Configuración SPOKE DMVPN

Fuente: Elaboración Propia

2.2.3.5 Spoke Cochabamba

CONFIGURACIÓN DE SEGURIDAD ISAKMP/IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
crypto isakmp policy 10	*Crear una política IKE. Cada política se identifica por su número de prioridad (de 1 a 10.000; 1 la prioridad más alta)*
encr aes 256	*Especificar el algoritmo de cifrado a utilizar. AES soporta 128,192,256 bits.*
authentication pre-share	*Determinar el método de autenticación. (Llaves compartidas)*
crypto isakmp key *** address 0.0.0.0 0.0.0.0**	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
crypto isakmp keepalive 10	*Elegir el intervalo de los paquetes hello (por defecto 10 segundos)*
crypto ipsec transform-set DMVPN1 esp-aes esp-sha-hmac	*Establece las políticas de seguridad IPSEC que se usarán en las comunicaciones.*
mode transport	*Elegir el modo*
crypto ipsec profile PRFIPSEC	*Define los parámetros que serán utilizados para la encriptación Ipsec entre routers "hub y spoke" y "spoke y spoke".*
set transform-set DMVPN1	*Especificar cual conjunto de parámetros puede ser utilizado por el perfil Ipsec.*

SPOKE DMVPN TIGO

CONFIGURACIÓN mGRE	
COMANDO IMPLEMENTADO	**PROPÓSITO**
interface Tunnel21	*Configurar la interface Túnel, con el número asignado.*
description --- COCHABAMBA DMVPN TIGO ---	*Especificar una descripción para la interface Túnel creada.*
ip address 172.21.254.12 255.255.255.0	*Configurar la dirección IP para la interface Túnel dentro de la misma subred IP de la DMVPN.*
no ip redirects	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
tunnel key 21	*Establecer una llave ID única que deberá ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
tunnel source 172.21.132.2	*Configurar la dirección origen para la interface Túnel.*
tunnel mode gre multipoint	*Configurar el modo de encapsulación para mGRE para la interface Túnel.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp authentication tun21	*Configurar la cadena de autenticación para una interface utilizando NHRP, la cadena debe ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
ip nhrp map 172.21.254.10 172.21.65.58	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB LPZ TIGO)***
ip nhrp map multicast 172.21.65.58	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB LPZ TIGO)***
ip nhrp map 172.21.254.11 172.21.13.18	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB SCZ TIGO)***
ip nhrp map multicast 172.21.13.18	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB SCZ TIGO)***
ip nhrp network-id 21	*Habilitar NHRP en una interface, el número es un identificador único NBMA.*
ip nhrp holdtime 450	*Cambiar el número de segundos que las direcciones NHRP NBMA son anunciadas como válidas.*
ip nhrp nhs 172.21.254.10	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB LPZ TIGO)***
ip nhrp nhs 172.21.254.11	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB SCZ TIGO)***
ip nhrp shortcut	*Habilitar NHRP shortcut switching.*

CONFIGURACIÓN DE MTU PARA ENVÍO DE PAQUETES	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip mtu 1400	*Configurar el tamaño de MTU en bytes, de los paquetes IP enviados sobre la interface.*
ip tcp adjust-mss 1360	*Ajustar el valor de MSS de paquetes TCP que van a través del router.*

CONTROL DE PROTOCOLO DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
bandwidth 4000	*Configurar el valor del ancho de banda en kbps.*
delay 1600	*Especificar un valor para cambiar la métrica de enrutamiento EIGRP.*

APLICACIÓN DE SEGURIDAD IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
tunnel protection ipsec profile PRFIPSEC	*Asociar la interface Túnel al perfil Ipsec.*

SPOKE DMVPN ENTEL

CONFIGURACIÓN mGRE	
COMANDO IMPLEMENTADO	**PROPÓSITO**
interface Tunnel31	*Configurar la interface Túnel, con el número asignado.*
description --- COCHABAMBA DMVPN ENTEL ---	*Especificar una descripción para la interface Túnel creada.*
ip address 172.31.254.12 255.255.255.0	*Configurar la dirección IP para la interface Túnel dentro de la misma subred IP de la DMVPN.*
no ip redirects	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
tunnel key 31	*Establecer una llave ID única que deberá ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
tunnel source 172.31.132.2	*Configurar la dirección origen para la interface Túnel.*
tunnel mode gre multipoint	*Configurar el modo de encapsulación para mGRE para la interface Túnel.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp authentication tun31	*Configurar la cadena de autenticación para una interface utilizando NHRP, la cadena debe ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
ip nhrp map 172.31.254.10 172.31.65.58	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB LPZ ENTEL)***
ip nhrp map multicast 172.31.65.58	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB LPZ ENTEL)***
ip nhrp map 172.31.254.11 172.31.13.18	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB SCZ ENTEL)***
ip nhrp map multicast 172.31.13.18	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB SCZ ENTEL)***
ip nhrp network-id 31	*Habilitar NHRP en una interface, el número es un identificador único NBMA.*
ip nhrp holdtime 450	*Cambiar el número de segundos que las direcciones NHRP NBMA son anunciadas como válidas.*
ip nhrp nhs 172.31.254.10	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB LPZ ENTEL)***
ip nhrp nhs 172.31.254.11	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB SCZ ENTEL)***
ip nhrp shortcut	*Habilitar NHRP shortcut switching.*

CONFIGURACIÓN DE MTU PARA ENVÍO DE PAQUETES	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip mtu 1400	*Configurar el tamaño de MTU en bytes, de los paquetes IP enviados sobre la interface.*
ip tcp adjust-mss 1360	*Ajustar el valor de MSS de paquetes TCP que van a través del router.*

CONTROL DE PROTOCOLO DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
bandwidth 7100	*Configurar el valor del ancho de banda en kbps.*
delay 800	*Especificar un valor para cambiar la métrica de enrutamiento EIGRP.*

APLICACIÓN DE SEGURIDAD IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
tunnel protection ipsec profile PRFIPSEC	*Asociar la interface Túnel al perfil Ipsec.*

Aplicando el protocolo de enrutamiento EIGRP y listas de acceso, se indujo que se utilice el enlace del proveedor TIGO para la conexión de la regional con las redes críticas declaradas en la ACL PRIMARIO. El resto de tráfico fue balanceado e inducido para utilizar el enlace de ENTEL en una relación 2 a 1 con respecto al enlace de TIGO.

APLICACIÓN DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip access-list standard PRIMARIO	*Crear lista de acceso a utilizarse para el criterio de uso en el offset (compensación)*
permit 10.7.0.0 0.0.0.255 **permit 10.10.0.0 0.0.0.255**	*Definir las redes para el criterio del offset.*
router eigrp 60	*Configurar el proceso de enrutamiento EIGRP.*
variance 2	*Controlar el balanceo de carga de paquetes en una red basada en EIGRP.*
network 1.80.200.200 0.0.0.3 **network 10.100.100.12 0.0.0.0** **network 172.21.254.0 0.0.0.255** **network 172.31.254.0 0.0.0.255**	*Especificar una lista de redes para el proceso de enrutamiento EIGRP.*
offset-list PRIMARIO in 3000000 Tunnel31	*Configurar el valor offset que se adicionará a la métrica de enrutamiento aplicada a métricas entrantes.*

2.2.3.6 Spoke Sucre

CONFIGURACIÓN DE SEGURIDAD ISAKMP/IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
crypto isakmp policy 10	*Crear una política IKE. Cada política se identifica por su número de prioridad (de 1 a 10.000; 1 la prioridad más alta)*
encr aes 256	*Especificar el algoritmo de cifrado a utilizar. AES soporta 128,192,256 bits.*
authentication pre-share	*Determinar el método de autenticación. (Llaves compartidas)*
crypto isakmp key *** address 0.0.0.0 0.0.0.0**	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
crypto isakmp keepalive 10	*Elegir el intervalo de los paquetes hello (por defecto 10 segundos)*
crypto ipsec transform-set DMVPN1 esp-aes esp-sha-hmac	*Establece las políticas de seguridad IPSEC que se usarán en las comunicaciones.*
mode transport	*Elegir el modo*
crypto ipsec profile PRFIPSEC	*Define los parámetros que serán utilizados para la encriptación Ipsec entre routers "hub y spoke" y "spoke y spoke".*
set transform-set DMVPN1	*Especificar cual conjunto de parámetros puede ser utilizado por el perfil Ipsec.*

SPOKE DMVPN TIGO

CONFIGURACIÓN mGRE	
COMANDO IMPLEMENTADO	**PROPÓSITO**
interface Tunnel21	*Configurar la interface Túnel, con el número asignado.*
description --- SUCRE DMVPN TIGO ---	*Especificar una descripción para la interface Túnel creada.*
ip address 172.21.254.13 255.255.255.0	*Configurar la dirección IP para la interface Túnel dentro de la misma subred IP de la DMVPN.*
no ip redirects	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
tunnel key 21	*Establecer una llave ID única que deberá ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
tunnel source 172.21.224.66	*Configurar la dirección origen para la interface Túnel.*
tunnel mode gre multipoint	*Configurar el modo de encapsulación para mGRE para la interface Túnel.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp authentication tun21	*Configurar la cadena de autenticación para una interface utilizando NHRP, la cadena debe ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
ip nhrp map 172.21.254.10 172.21.65.58	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB LPZ TIGO)***
ip nhrp map multicast 172.21.65.58	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB LPZ TIGO)***
ip nhrp map 172.21.254.11 172.21.13.18	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB SCZ TIGO)***
ip nhrp map multicast 172.21.13.18	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB SCZ TIGO)***
ip nhrp network-id 21	*Habilitar NHRP en una interface, el número es un identificador único NBMA.*
ip nhrp holdtime 450	*Cambiar el número de segundos que las direcciones NHRP NBMA son anunciadas como válidas.*
ip nhrp nhs 172.21.254.10	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB LPZ TIGO)***
ip nhrp nhs 172.21.254.11	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB SCZ TIGO)***
ip nhrp shortcut	*Habilitar NHRP shortcut switching.*

CONFIGURACIÓN DE MTU PARA ENVÍO DE PAQUETES	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip mtu 1400	*Configurar el tamaño de MTU en bytes, de los paquetes IP enviados sobre la interface.*
ip tcp adjust-mss 1360	*Ajustar el valor de MSS de paquetes TCP que van a través del router.*

CONTROL DE PROTOCOLO DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
bandwidth 2000	*Configurar el valor del ancho de banda en kbps.*
delay 1000	*Especificar un valor para cambiar la métrica de enrutamiento EIGRP.*

APLICACIÓN DE SEGURIDAD IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
tunnel protection ipsec profile PRFIPSEC	*Asociar la interface Túnel al perfil Ipsec.*

SPOKE DMVPN ENTEL

CONFIGURACIÓN mGRE	
COMANDO IMPLEMENTADO	**PROPÓSITO**
interface Tunnel31	*Configurar la interface Túnel, con el número asignado.*
description --- SUCRE DMVPN ENTEL ---	*Especificar una descripción para la interface Túnel creada.*
ip address 172.31.254.13 255.255.255.0	*Configurar la dirección IP para la interface Túnel dentro de la misma subred IP de la DMVPN.*
no ip redirects	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
tunnel key 31	*Establecer una llave ID única que deberá ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
tunnel source 172.31.224.66	*Configurar la dirección origen para la interface Túnel.*
tunnel mode gre multipoint	*Configurar el modo de encapsulación para mGRE para la interface Túnel.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp authentication tun31	*Configurar la cadena de autenticación para una interface utilizando NHRP, la cadena debe ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
ip nhrp map 172.31.254.10 172.31.65.58	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB LPZ ENTEL)***
ip nhrp map multicast 172.31.65.58	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB LPZ ENTEL)***
ip nhrp map 172.31.254.11 172.31.13.18	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB SCZ ENTEL)***
ip nhrp map multicast 172.31.13.18	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB SCZ ENTEL)***
ip nhrp network-id 31	*Habilitar NHRP en una interface, el número es un identificador único NBMA.*
ip nhrp holdtime 450	*Cambiar el número de segundos que las direcciones NHRP NBMA son anunciadas como válidas.*
ip nhrp nhs 172.31.254.10	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB LPZ ENTEL)***
ip nhrp nhs 172.31.254.11	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB SCZ ENTEL)***
ip nhrp shortcut	*Habilitar NHRP shortcut switching.*

CONFIGURACIÓN DE MTU PARA ENVÍO DE PAQUETES	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip mtu 1400	*Configurar el tamaño de MTU en bytes, de los paquetes IP enviados sobre la interface.*
ip tcp adjust-mss 1360	*Ajustar el valor de MSS de paquetes TCP que van a través del router.*

CONTROL DE PROTOCOLO DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
bandwidth 3000	*Configurar el valor del ancho de banda en kbps.*
delay 50	*Especificar un valor para cambiar la métrica de enrutamiento EIGRP.*

APLICACIÓN DE SEGURIDAD IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
tunnel protection ipsec profile PRFIPSEC	*Asociar la interface Túnel al perfil Ipsec.*

Aplicando el protocolo de enrutamiento EIGRP y listas de acceso, se indujo que se utilice el enlace del proveedor TIGO para la conexión de la regional con las redes críticas declaradas en la ACL PRIMARIO. El resto de tráfico fue balanceado e inducido para utilizar el enlace de ENTEL en una relación 2 a 1 con respecto al enlace de TIGO.

APLICACIÓN DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip access-list standard PRIMARIO	*Crear lista de acceso a utilizarse para el criterio de uso en el offset (compensación)*
permit 10.7.0.0 0.0.0.255 **permit 10.10.0.0 0.0.0.255**	*Definir las redes para el criterio del offset.*
router eigrp 60	*Configurar el proceso de enrutamiento EIGRP.*
variance 2	*Controlar el balanceo de carga de paquetes en una red basada en EIGRP.*
network 1.112.200.200 0.0.0.3 **network 10.100.100.13 0.0.0.0** **network 172.21.254.0 0.0.0.255** **network 172.31.254.0 0.0.0.255**	*Especificar una lista de redes para el proceso de enrutamiento EIGRP.*
offset-list PRIMARIO in 3000000 Tunnel31	*Configurar el valor offset que se adicionará a la métrica de enrutamiento aplicada a métricas entrantes.*

2.2.3.7 Spoke Tarija

CONFIGURACIÓN DE SEGURIDAD ISAKMP/IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
crypto isakmp policy 10	*Crear una política IKE. Cada política se identifica por su número de prioridad (de 1 a 10.000; 1 la prioridad más alta)*
encr aes 256	*Especificar el algoritmo de cifrado a utilizar. AES soporta 128,192,256 bits.*
authentication pre-share	*Determinar el método de autenticación. (Llaves compartidas)*
crypto isakmp key *** address 0.0.0.0 0.0.0.0**	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
crypto isakmp keepalive 10	*Elegir el intervalo de los paquetes hello (por defecto 10 segundos)*
crypto ipsec transform-set DMVPN1 esp-aes esp-sha-hmac	*Establece las políticas de seguridad IPSEC que se usarán en las comunicaciones.*
mode transport	*Elegir el modo*
crypto ipsec profile PRFIPSEC	*Define los parámetros que serán utilizados para la encriptación Ipsec entre routers "hub y spoke" y "spoke y spoke".*
set transform-set DMVPN1	*Especificar cual conjunto de parámetros puede ser utilizado por el perfil Ipsec.*

SPOKE DMVPN TIGO

CONFIGURACIÓN mGRE	
COMANDO IMPLEMENTADO	**PROPÓSITO**
interface Tunnel21	*Configurar la interface Túnel, con el número asignado.*
description --- TARIJA DMVPN TIGO ---	*Especificar una descripción para la interface Túnel creada.*
ip address 172.21.254.14 255.255.255.0	*Configurar la dirección IP para la interface Túnel dentro de la misma subred IP de la DMVPN.*
no ip redirects	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
tunnel key 21	*Establecer una llave ID única que deberá ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
tunnel source 172.21.176.50	*Configurar la dirección origen para la interface Túnel.*
tunnel mode gre multipoint	*Configurar el modo de encapsulación para mGRE para la interface Túnel.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp authentication tun21	*Configurar la cadena de autenticación para una interface utilizando NHRP, la cadena debe ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
ip nhrp map 172.21.254.10 172.21.65.58	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB LPZ TIGO)***
ip nhrp map multicast 172.21.65.58	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB LPZ TIGO)***
ip nhrp map 172.21.254.11 172.21.13.18	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB SCZ TIGO)***
ip nhrp map multicast 172.21.13.18	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB SCZ TIGO)***
ip nhrp network-id 21	*Habilitar NHRP en una interface, el número es un identificador único NBMA.*
ip nhrp holdtime 450	*Cambiar el número de segundos que las direcciones NHRP NBMA son anunciadas como válidas.*
ip nhrp nhs 172.21.254.10	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB LPZ TIGO)***
ip nhrp nhs 172.21.254.11	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB SCZ TIGO)***
ip nhrp shortcut	*Habilitar NHRP shortcut switching.*

CONFIGURACIÓN DE MTU PARA ENVÍO DE PAQUETES	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip mtu 1400	*Configurar el tamaño de MTU en bytes, de los paquetes IP enviados sobre la interface.*
ip tcp adjust-mss 1360	*Ajustar el valor de MSS de paquetes TCP que van a través del router.*

CONTROL DE PROTOCOLO DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
bandwidth 2000	*Configurar el valor del ancho de banda en kbps.*
delay 1000	*Especificar un valor para cambiar la métrica de enrutamiento EIGRP.*

APLICACIÓN DE SEGURIDAD IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
tunnel protection ipsec profile PRFIPSEC	*Asociar la interface Túnel al perfil Ipsec.*

SPOKE DMVPN ENTEL

CONFIGURACIÓN mGRE	
COMANDO IMPLEMENTADO	**PROPÓSITO**
interface Tunnel31	*Configurar la interface Túnel, con el número asignado.*
description --- TARIJA DMVPN ENTEL ---	*Especificar una descripción para la interface Túnel creada.*
ip address 172.31.254.14 255.255.255.0	*Configurar la dirección IP para la interface Túnel dentro de la misma subred IP de la DMVPN.*
no ip redirects	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
tunnel key 31	*Establecer una llave ID única que deberá ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
tunnel source 172.31.176.50	*Configurar la dirección origen para la interface Túnel.*
tunnel mode gre multipoint	*Configurar el modo de encapsulación para mGRE para la interface Túnel.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp authentication tun31	*Configurar la cadena de autenticación para una interface utilizando NHRP, la cadena debe ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
ip nhrp map 172.31.254.10 172.31.65.58	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB LPZ ENTEL)***
ip nhrp map multicast 172.31.65.58	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB LPZ ENTEL)***
ip nhrp map 172.31.254.11 172.31.13.18	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB SCZ ENTEL)***
ip nhrp map multicast 172.31.13.18	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB SCZ ENTEL)***
ip nhrp network-id 31	*Habilitar NHRP en una interface, el número es un identificador único NBMA.*
ip nhrp holdtime 450	*Cambiar el número de segundos que las direcciones NHRP NBMA son anunciadas como válidas.*
ip nhrp nhs 172.31.254.10	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB LPZ ENTEL)***
ip nhrp nhs 172.31.254.11	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB SCZ ENTEL)***
ip nhrp shortcut	*Habilitar NHRP shortcut switching.*

CONFIGURACIÓN DE MTU PARA ENVÍO DE PAQUETES	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip mtu 1400	*Configurar el tamaño de MTU en bytes, de los paquetes IP enviados sobre la interface.*
ip tcp adjust-mss 1360	*Ajustar el valor de MSS de paquetes TCP que van a través del router.*

CONTROL DE PROTOCOLO DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
bandwidth 3000	*Configurar el valor del ancho de banda en kbps.*
delay 80	*Especificar un valor para cambiar la métrica de enrutamiento EIGRP.*

APLICACIÓN DE SEGURIDAD IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
tunnel protection ipsec profile PRFIPSEC	*Asociar la interface Túnel al perfil Ipsec.*

Aplicando el protocolo de enrutamiento EIGRP y listas de acceso, se indujo que se utilice el enlace del proveedor TIGO para la conexión de la regional con las redes críticas declaradas en la ACL PRIMARIO. El resto de tráfico fue balanceado e inducido para utilizar el enlace de ENTEL en una relación 2 a 1 con respecto al enlace de TIGO.

APLICACIÓN DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip access-list standard PRIMARIO	*Crear lista de acceso a utilizarse para el criterio de uso en el offset (compensación)*
permit 10.7.0.0 0.0.0.255 **permit 10.10.0.0 0.0.0.255**	*Definir las redes para el criterio del offset.*
router eigrp 60	*Configurar el proceso de enrutamiento EIGRP.*
variance 2	*Controlar el balanceo de carga de paquetes en una red basada en EIGRP.*
network 1.48.200.200 0.0.0.7 **network 10.100.100.14 0.0.0.0** **network 172.21.254.0 0.0.0.255** **network 172.31.254.0 0.0.0.255**	*Especificar una lista de redes para el proceso de enrutamiento EIGRP.*
offset-list PRIMARIO in 3000000 Tunnel31	*Configurar el valor offset que se adicionará a la métrica de enrutamiento aplicada a métricas entrantes.*

2.2.3.8 Spoke Trinidad

CONFIGURACIÓN DE SEGURIDAD ISAKMP/IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
crypto isakmp policy 10	*Crear una política IKE. Cada política se identifica por su número de prioridad (de 1 a 10.000; 1 la prioridad más alta)*
encr aes 256	*Especificar el algoritmo de cifrado a utilizar. AES soporta 128,192,256 bits.*
authentication pre-share	*Determinar el método de autenticación. (Llaves compartidas)*
crypto isakmp key *** address 0.0.0.0 0.0.0.0**	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
crypto isakmp keepalive 10	*Elegir el intervalo de los paquetes hello (por defecto 10 segundos)*
crypto ipsec transform-set DMVPN1 esp-aes esp-sha-hmac	*Establece las políticas de seguridad IPSEC que se usarán en las comunicaciones.*
mode transport	*Elegir el modo*
crypto ipsec profile PRFIPSEC	*Define los parámetros que serán utilizados para la encriptación Ipsec entre routers "hub y spoke" y "spoke y spoke".*
set transform-set DMVPN1	*Especificar cual conjunto de parámetros puede ser utilizado por el perfil Ipsec.*

SPOKE DMVPN TIGO

CONFIGURACIÓN mGRE	
COMANDO IMPLEMENTADO	**PROPÓSITO**
interface Tunnel21	*Configurar la interface Túnel, con el número asignado.*
description --- TRINIDAD DMVPN TIGO ---	*Especificar una descripción para la interface Túnel creada.*
ip address 172.21.254.15 255.255.255.0	*Configurar la dirección IP para la interface Túnel dentro de la misma subred IP de la DMVPN.*
no ip redirects	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
tunnel key 21	*Establecer una llave ID única que deberá ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
tunnel source 172.21.248.74	*Configurar la dirección origen para la interface Túnel.*
tunnel mode gre multipoint	*Configurar el modo de encapsulación para mGRE para la interface Túnel.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp authentication tun21	*Configurar la cadena de autenticación para una interface utilizando NHRP, la cadena debe ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
ip nhrp map 172.21.254.10 172.21.65.58	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB LPZ TIGO)***
ip nhrp map multicast 172.21.65.58	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB LPZ TIGO)***
ip nhrp map 172.21.254.11 172.21.13.18	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB SCZ TIGO)***
ip nhrp map multicast 172.21.13.18	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB SCZ TIGO)***
ip nhrp network-id 21	*Habilitar NHRP en una interface, el número es un identificador único NBMA.*
ip nhrp holdtime 450	*Cambiar el número de segundos que las direcciones NHRP NBMA son anunciadas como válidas.*
ip nhrp nhs 172.21.254.10	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB LPZ TIGO)***
ip nhrp nhs 172.21.254.11	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB SCZ TIGO)***
ip nhrp shortcut	*Habilitar NHRP shortcut switching.*

CONFIGURACIÓN DE MTU PARA ENVÍO DE PAQUETES	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip mtu 1400	*Configurar el tamaño de MTU en bytes, de los paquetes IP enviados sobre la interface.*
ip tcp adjust-mss 1360	*Ajustar el valor de MSS de paquetes TCP que van a través del router.*

CONTROL DE PROTOCOLO DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
bandwidth 1000	*Configurar el valor del ancho de banda en kbps.*
delay 1000	*Especificar un valor para cambiar la métrica de enrutamiento EIGRP.*

APLICACIÓN DE SEGURIDAD IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
tunnel protection ipsec profile PRFIPSEC	*Asociar la interface Túnel al perfil Ipsec.*

SPOKE DMVPN ENTEL

CONFIGURACIÓN mGRE	
COMANDO IMPLEMENTADO	**PROPÓSITO**
interface Tunnel31	*Configurar la interface Túnel, con el número asignado.*
description --- TRINIDAD DMVPN ENTEL ---	*Especificar una descripción para la interface Túnel creada.*
ip address 172.31.254.15 255.255.255.0	*Configurar la dirección IP para la interface Túnel dentro de la misma subred IP de la DMVPN.*
no ip redirects	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
tunnel key 31	*Establecer una llave ID única que deberá ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
tunnel source 172.31.226.50	*Configurar la dirección origen para la interface Túnel.*
tunnel mode gre multipoint	*Configurar el modo de encapsulación para mGRE para la interface Túnel.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp authentication tun31	*Configurar la cadena de autenticación para una interface utilizando NHRP, la cadena debe ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
ip nhrp map 172.31.254.10 172.31.65.58	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB LPZ ENTEL)***
ip nhrp map multicast 172.31.65.58	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB LPZ ENTEL)***
ip nhrp map 172.31.254.11 172.31.13.18	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB SCZ ENTEL)***
ip nhrp map multicast 172.31.13.18	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB SCZ ENTEL)***
ip nhrp network-id 31	*Habilitar NHRP en una interface, el número es un identificador único NBMA.*
ip nhrp holdtime 450	*Cambiar el número de segundos que las direcciones NHRP NBMA son anunciadas como válidas.*
ip nhrp nhs 172.31.254.10	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB LPZ ENTEL)***
ip nhrp nhs 172.31.254.11	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB SCZ ENTEL)***
ip nhrp shortcut	*Habilitar NHRP shortcut switching.*

CONFIGURACIÓN DE MTU PARA ENVÍO DE PAQUETES	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip mtu 1400	*Configurar el tamaño de MTU en bytes, de los paquetes IP enviados sobre la interface.*
ip tcp adjust-mss 1360	*Ajustar el valor de MSS de paquetes TCP que van a través del router.*

CONTROL DE PROTOCOLO DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
bandwidth 1000	*Configurar el valor del ancho de banda en kbps.*
delay 1000	*Especificar un valor para cambiar la métrica de enrutamiento EIGRP.*

APLICACIÓN DE SEGURIDAD IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
tunnel protection ipsec profile PRFIPSEC	*Asociar la interface Túnel al perfil Ipsec.*

Aplicando el protocolo de enrutamiento EIGRP y listas de acceso, se indujo que se utilice el enlace del proveedor TIGO para la conexión de la regional con las redes críticas declaradas en la ACL PRIMARIO. El resto de tráfico fue balanceado e inducido para utilizar el enlace de ENTEL en una relación 2 a 1 con respecto al enlace de TIGO.

APLICACIÓN DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip access-list standard PRIMARIO	*Crear lista de acceso a utilizarse para el criterio de uso en el offset (compensación)*
permit 10.7.0.0 0.0.0.255 **permit 10.10.0.0 0.0.0.255**	*Definir las redes para el criterio del offset.*
router eigrp 60	*Configurar el proceso de enrutamiento EIGRP.*
variance 2	*Controlar el balanceo de carga de paquetes en una red basada en EIGRP.*
network 1.144.0.0 0.0.1.255 **network 1.144.50.8 0.0.0.7** **network 10.100.100.15 0.0.0.0** **network 172.21.254.0 0.0.0.255** **network 172.31.254.0 0.0.0.255**	*Especificar una lista de redes para el proceso de enrutamiento EIGRP.*
offset-list PRIMARIO in 2000 Tunnel31	*Configurar el valor offset que se adicionará a la métrica de enrutamiento aplicada a métricas entrantes.*

2.2.3.9 Spoke Oruro

CONFIGURACIÓN DE SEGURIDAD ISAKMP/IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
crypto isakmp policy 10	*Crear una política IKE. Cada política se identifica por su número de prioridad (de 1 a 10.000; 1 la prioridad más alta)*
encr aes 256	*Especificar el algoritmo de cifrado a utilizar. AES soporta 128,192,256 bits.*
authentication pre-share	*Determinar el método de autenticación. (Llaves compartidas)*
crypto isakmp key *** address 0.0.0.0 0.0.0.0**	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
crypto isakmp keepalive 10	*Elegir el intervalo de los paquetes hello (por defecto 10 segundos)*
crypto ipsec transform-set DMVPN1 esp-aes esp-sha-hmac	*Establece las políticas de seguridad IPSEC que se usarán en las comunicaciones.*
mode transport	*Elegir el modo*
crypto ipsec profile PRFIPSEC	*Define los parámetros que serán utilizados para la encriptación Ipsec entre routers "hub y spoke" y "spoke y spoke".*
set transform-set DMVPN1	*Especificar cual conjunto de parámetros puede ser utilizado por el perfil Ipsec.*

SPOKE DMVPN TIGO

CONFIGURACIÓN mGRE	
COMANDO IMPLEMENTADO	**PROPÓSITO**
interface Tunnel21	*Configurar la interface Túnel, con el número asignado.*
description --- ORURO DMVPN TIGO ---	*Especificar una descripción para la interface Túnel creada.*
ip address 172.21.254.16 255.255.255.0	*Configurar la dirección IP para la interface Túnel dentro de la misma subred IP de la DMVPN.*
no ip redirects	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
tunnel key 21	*Establecer una llave ID única que deberá ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
tunnel source 172.21.192.50	*Configurar la dirección origen para la interface Túnel.*
tunnel mode gre multipoint	*Configurar el modo de encapsulación para mGRE para la interface Túnel.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp authentication tun21	*Configurar la cadena de autenticación para una interface utilizando NHRP, la cadena debe ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
ip nhrp map 172.21.254.10 172.21.65.58	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB LPZ TIGO)***
ip nhrp map multicast 172.21.65.58	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB LPZ TIGO)***
ip nhrp map 172.21.254.11 172.21.13.18	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB SCZ TIGO)***
ip nhrp map multicast 172.21.13.18	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB SCZ TIGO)***
ip nhrp network-id 21	*Habilitar NHRP en una interface, el número es un identificador único NBMA.*
ip nhrp holdtime 450	*Cambiar el número de segundos que las direcciones NHRP NBMA son anunciadas como válidas.*
ip nhrp nhs 172.21.254.10	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB LPZ TIGO)***
ip nhrp nhs 172.21.254.11	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB SCZ TIGO)***
ip nhrp shortcut	*Habilitar NHRP shortcut switching.*

CONFIGURACIÓN DE MTU PARA ENVÍO DE PAQUETES	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip mtu 1400	*Configurar el tamaño de MTU en bytes, de los paquetes IP enviados sobre la interface.*
ip tcp adjust-mss 1360	*Ajustar el valor de MSS de paquetes TCP que van a través del router.*

CONTROL DE PROTOCOLO DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
bandwidth 2000	*Configurar el valor del ancho de banda en kbps.*
delay 1000	*Especificar un valor para cambiar la métrica de enrutamiento EIGRP.*

APLICACIÓN DE SEGURIDAD IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
tunnel protection ipsec profile PRFIPSEC	*Asociar la interface Túnel al perfil Ipsec.*

SPOKE DMVPN ENTEL

CONFIGURACIÓN mGRE	
COMANDO IMPLEMENTADO	**PROPÓSITO**
interface Tunnel31	*Configurar la interface Túnel, con el número asignado.*
description --- ORURO DMVPN ENTEL ---	*Especificar una descripción para la interface Túnel creada.*
ip address 172.31.254.16 255.255.255.0	*Configurar la dirección IP para la interface Túnel dentro de la misma subred IP de la DMVPN.*
no ip redirects	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
tunnel key 31	*Establecer una llave ID única que deberá ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
tunnel source 172.31.192.50	*Configurar la dirección origen para la interface Túnel.*
tunnel mode gre multipoint	*Configurar el modo de encapsulación para mGRE para la interface Túnel.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp authentication tun31	*Configurar la cadena de autenticación para una interface utilizando NHRP, la cadena debe ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
ip nhrp map 172.31.254.10 172.31.65.58	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB LPZ ENTEL)***
ip nhrp map multicast 172.31.65.58	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB LPZ ENTEL)***
ip nhrp map 172.31.254.11 172.31.13.18	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB SCZ ENTEL)***
ip nhrp map multicast 172.31.13.18	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB SCZ ENTEL)***
ip nhrp network-id 31	*Habilitar NHRP en una interface, el número es un identificador único NBMA.*
ip nhrp holdtime 450	*Cambiar el número de segundos que las direcciones NHRP NBMA son anunciadas como válidas.*
ip nhrp nhs 172.31.254.10	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB LPZ ENTEL)***
ip nhrp nhs 172.31.254.11	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB SCZ ENTEL)***
ip nhrp shortcut	*Habilitar NHRP shortcut switching.*

CONFIGURACIÓN DE MTU PARA ENVÍO DE PAQUETES	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip mtu 1400	*Configurar el tamaño de MTU en bytes, de los paquetes IP enviados sobre la interface.*
ip tcp adjust-mss 1360	*Ajustar el valor de MSS de paquetes TCP que van a través del router.*

CONTROL DE PROTOCOLO DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
bandwidth 3000	*Configurar el valor del ancho de banda en kbps.*
delay 50	*Especificar un valor para cambiar la métrica de enrutamiento EIGRP.*

APLICACIÓN DE SEGURIDAD IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
tunnel protection ipsec profile PRFIPSEC	*Asociar la interface Túnel al perfil Ipsec.*

Aplicando el protocolo de enrutamiento EIGRP y listas de acceso, se indujo que se utilice el enlace del proveedor TIGO para la conexión de la regional con las redes críticas declaradas en la ACL PRIMARIO. El resto de tráfico fue balanceado e inducido para utilizar el enlace de ENTEL en una relación 2 a 1 con respecto al enlace de TIGO.

APLICACIÓN DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip access-list standard PRIMARIO	*Crear lista de acceso a utilizarse para el criterio de uso en el offset (compensación)*
permit 10.7.0.0 0.0.0.255 **permit 10.10.0.0 0.0.0.255**	*Definir las redes para el criterio del offset.*
router eigrp 60	*Configurar el proceso de enrutamiento EIGRP.*
variance 2	*Controlar el balanceo de carga de paquetes en una red basada en EIGRP.*
network 1.96.0.0 0.0.1.255 **network 1.96.4.0 0.0.1.255** **network 1.96.6.0 0.0.1.255** **network 1.96.50.8 0.0.0.7** **network 1.96.50.16 0.0.0.7** **network 1.96.50.24 0.0.0.7** **network 1.96.54.8 0.0.0.7** **network 1.96.54.16 0.0.0.7** **network 1.96.122.0 0.0.1.255** **network 1.96.200.4 0.0.0.3** **network 1.96.200.204 0.0.0.3** **network 1.96.200.208 0.0.0.7** **network 1.96.250.0 0.0.0.31** **network 1.96.250.32 0.0.0.15**	*Especificar una lista de redes para el proceso de enrutamiento EIGRP.*

APLICACIÓN DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
network 10.100.100.16 0.0.0.0 **network 172.21.254.0 0.0.0.255** **network 172.31.254.0 0.0.0.255**	
offset-list PRIMARIO in 3000000 Tunnel31	*Configurar el valor offset que se adicionará a la métrica de enrutamiento aplicada a métricas entrantes.*

2.2.3.10 Spoke Potosi

CONFIGURACIÓN DE SEGURIDAD ISAKMP/IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
crypto isakmp policy 10	*Crear una política IKE. Cada política se identifica por su número de prioridad (de 1 a 10.000; 1 la prioridad más alta)*
encr aes 256	*Especificar el algoritmo de cifrado a utilizar. AES soporta 128,192,256 bits.*
authentication pre-share	*Determinar el método de autenticación. (Llaves compartidas)*
crypto isakmp key *** **address 0.0.0.0 0.0.0.0**	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
crypto isakmp keepalive 10	*Elegir el intervalo de los paquetes hello (por defecto 10 segundos)*
crypto ipsec transform-set DMVPN1 **esp-aes esp-sha-hmac**	*Establece las políticas de seguridad IPSEC que se usarán en las comunicaciones.*
mode transport	*Elegir el modo*
crypto ipsec profile PRFIPSEC	*Define los parámetros que serán utilizados para la encriptación Ipsec entre routers "hub y spoke" y "spoke y spoke".*
set transform-set DMVPN1	*Especificar cual conjunto de parámetros puede ser utilizado por el perfil Ipsec.*

SPOKE DMVPN TIGO

CONFIGURACIÓN mGRE	
COMANDO IMPLEMENTADO	**PROPÓSITO**
interface Tunnel21	*Configurar la interface Túnel, con el número asignado.*
description --- POTOSI DMVPN TIGO ---	*Especificar una descripción para la interface Túnel creada.*
ip address 172.21.254.17 255.255.255.0	*Configurar la dirección IP para la interface Túnel dentro de la misma subred IP de la DMVPN.*
no ip redirects	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
tunnel key 21	*Establecer una llave ID única que deberá ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
tunnel source 172.21.225.50	*Configurar la dirección origen para la interface Túnel.*
tunnel mode gre multipoint	*Configurar el modo de encapsulación para mGRE para la interface Túnel.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp authentication tun21	*Configurar la cadena de autenticación para una interface utilizando NHRP, la cadena debe ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
ip nhrp map 172.21.254.10 172.21.65.58	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB LPZ TIGO)***
ip nhrp map multicast 172.21.65.58	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB LPZ TIGO)***
ip nhrp map 172.21.254.11 172.21.13.18	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB SCZ TIGO)***
ip nhrp map multicast 172.21.13.18	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB SCZ TIGO)***
ip nhrp network-id 21	*Habilitar NHRP en una interface, el número es un identificador único NBMA.*
ip nhrp holdtime 450	*Cambiar el número de segundos que las direcciones NHRP NBMA son anunciadas como válidas.*
ip nhrp nhs 172.21.254.10	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB LPZ TIGO)***
ip nhrp nhs 172.21.254.11	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB SCZ TIGO)***
ip nhrp shortcut	*Habilitar NHRP shortcut switching.*

CONFIGURACIÓN DE MTU PARA ENVÍO DE PAQUETES	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip mtu 1400	*Configurar el tamaño de MTU en bytes, de los paquetes IP enviados sobre la interface.*
ip tcp adjust-mss 1360	*Ajustar el valor de MSS de paquetes TCP que van a través del router.*

CONTROL DE PROTOCOLO DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
bandwidth 2000	*Configurar el valor del ancho de banda en kbps.*
delay 1000	*Especificar un valor para cambiar la métrica de enrutamiento EIGRP.*

APLICACIÓN DE SEGURIDAD IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
tunnel protection ipsec profile PRFIPSEC	*Asociar la interface Túnel al perfil Ipsec.*

SPOKE DMVPN ENTEL

CONFIGURACIÓN mGRE	
COMANDO IMPLEMENTADO	**PROPÓSITO**
interface Tunnel31	*Configurar la interface Túnel, con el número asignado.*
description --- POTOSI DMVPN ENTEL ---	*Especificar una descripción para la interface Túnel creada.*
ip address 172.31.254.17 255.255.255.0	*Configurar la dirección IP para la interface Túnel dentro de la misma subred IP de la DMVPN.*
no ip redirects	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
tunnel key 31	*Establecer una llave ID única que deberá ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
tunnel source 172.31.225.50	*Configurar la dirección origen para la interface Túnel.*
tunnel mode gre multipoint	*Configurar el modo de encapsulación para mGRE para la interface Túnel.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp authentication tun31	*Configurar la cadena de autenticación para una interface utilizando NHRP, la cadena debe ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
ip nhrp map 172.31.254.10 172.31.65.58	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB LPZ ENTEL)***
ip nhrp map multicast 172.31.65.58	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB LPZ ENTEL)***
ip nhrp map 172.31.254.11 172.31.13.18	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB SCZ ENTEL)***
ip nhrp map multicast 172.31.13.18	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB SCZ ENTEL)***
ip nhrp network-id 31	*Habilitar NHRP en una interface, el número es un identificador único NBMA.*
ip nhrp holdtime 450	*Cambiar el número de segundos que las direcciones NHRP NBMA son anunciadas como válidas.*
ip nhrp nhs 172.31.254.10	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB LPZ ENTEL)***
ip nhrp nhs 172.31.254.11	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB SCZ ENTEL)***
ip nhrp shortcut	*Habilitar NHRP shortcut switching.*

CONFIGURACIÓN DE MTU PARA ENVÍO DE PAQUETES	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip mtu 1400	*Configurar el tamaño de MTU en bytes, de los paquetes IP enviados sobre la interface.*
ip tcp adjust-mss 1360	*Ajustar el valor de MSS de paquetes TCP que van a través del router.*

CONTROL DE PROTOCOLO DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
bandwidth 3000	*Configurar el valor del ancho de banda en kbps.*
delay 80	*Especificar un valor para cambiar la métrica de enrutamiento EIGRP.*

APLICACIÓN DE SEGURIDAD IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
tunnel protection ipsec profile PRFIPSEC	*Asociar la interface Túnel al perfil Ipsec.*

Aplicando el protocolo de enrutamiento EIGRP y listas de acceso, se indujo que se utilice el enlace del proveedor TIGO para la conexión de la regional con las redes críticas declaradas en la ACL PRIMARIO. El resto de tráfico fue balanceado e inducido para utilizar el enlace de ENTEL en una relación 2 a 1 con respecto al enlace de TIGO.

APLICACIÓN DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip access-list standard PRIMARIO	*Crear lista de acceso a utilizarse para el criterio de uso en el offset (compensación)*
permit 10.7.0.0 0.0.0.255 **permit 10.10.0.0 0.0.0.255**	*Definir las redes para el criterio del offset.*
router eigrp 60	*Configurar el proceso de enrutamiento EIGRP.*
variance 2	*Controlar el balanceo de carga de paquetes en una red basada en EIGRP.*
network 1.128.0.0 0.0.1.255 **network 1.128.50.8 0.0.0.3** **network 1.128.50.16 0.0.0.3** **network 1.128.54.8 0.0.0.3** **network 1.128.200.4 0.0.0.3** **network 1.128.200.208 0.0.0.3** **network 10.100.100.17 0.0.0.0** **network 172.21.254.0 0.0.0.255** **network 172.31.254.0 0.0.0.255**	*Especificar una lista de redes para el proceso de enrutamiento EIGRP.*
offset-list PRIMARIO in 2000 Tunnel31	*Configurar el valor offset que se adicionará a la métrica de enrutamiento aplicada a métricas entrantes.*

2.2.3.11 Spoke Cobija

CONFIGURACIÓN DE SEGURIDAD ISAKMP/IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
crypto isakmp policy 10	*Crear una política IKE. Cada política se identifica por su número de prioridad (de 1 a 10.000; 1 la prioridad más alta)*
encr aes 256	*Especificar el algoritmo de cifrado a utilizar. AES soporta 128,192,256 bits.*
authentication pre-share	*Determinar el método de autenticación. (Llaves compartidas)*
crypto isakmp key *** address 0.0.0.0 0.0.0.0**	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
crypto isakmp keepalive 10	*Elegir el intervalo de los paquetes hello (por defecto 10 segundos)*
crypto ipsec transform-set DMVPN1 esp-aes esp-sha-hmac	*Establece las políticas de seguridad IPSEC que se usarán en las comunicaciones.*
mode transport	*Elegir el modo*
crypto ipsec profile PRFIPSEC	*Define los parámetros que serán utilizados para la encriptación Ipsec entre routers "hub y spoke" y "spoke y spoke".*
set transform-set DMVPN1	*Especificar cual conjunto de parámetros puede ser utilizado por el perfil Ipsec.*

SPOKE DMVPN TIGO

CONFIGURACIÓN mGRE	
COMANDO IMPLEMENTADO	**PROPÓSITO**
interface Tunnel21	*Configurar la interface Túnel, con el número asignado.*
description --- COBIJA DMVPN TIGO ---	*Especificar una descripción para la interface Túnel creada.*
ip address 172.21.254.18 255.255.255.0	*Configurar la dirección IP para la interface Túnel dentro de la misma subred IP de la DMVPN.*
no ip redirects	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
tunnel key 21	*Establecer una llave ID única que deberá ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
tunnel source 172.20.249.50	*Configurar la dirección origen para la interface Túnel.*
tunnel mode gre multipoint	*Configurar el modo de encapsulación para mGRE para la interface Túnel.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp authentication tun21	*Configurar la cadena de autenticación para una interface utilizando NHRP, la cadena debe ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
ip nhrp map 172.21.254.10 172.21.65.58	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB LPZ TIGO)***
ip nhrp map multicast 172.21.65.58	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB LPZ TIGO)***
ip nhrp map 172.21.254.11 172.21.13.18	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB SCZ TIGO)***
ip nhrp map multicast 172.21.13.18	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB SCZ TIGO)***
ip nhrp network-id 21	*Habilitar NHRP en una interface, el número es un identificador único NBMA.*
ip nhrp holdtime 450	*Cambiar el número de segundos que las direcciones NHRP NBMA son anunciadas como válidas.*
ip nhrp nhs 172.21.254.10	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB LPZ TIGO)***
ip nhrp nhs 172.21.254.11	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB SCZ TIGO)***
ip nhrp shortcut	*Habilitar NHRP shortcut switching.*

CONFIGURACIÓN DE MTU PARA ENVÍO DE PAQUETES	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip mtu 1400	*Configurar el tamaño de MTU en bytes, de los paquetes IP enviados sobre la interface.*
ip tcp adjust-mss 1360	*Ajustar el valor de MSS de paquetes TCP que van a través del router.*

CONTROL DE PROTOCOLO DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
bandwidth 1000	*Configurar el valor del ancho de banda en kbps.*
delay 1000	*Especificar un valor para cambiar la métrica de enrutamiento EIGRP.*

APLICACIÓN DE SEGURIDAD IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
tunnel protection ipsec profile PRFIPSEC	*Asociar la interface Túnel al perfil Ipsec.*

SPOKE DMVPN ENTEL

CONFIGURACIÓN mGRE	
COMANDO IMPLEMENTADO	**PROPÓSITO**
interface Tunnel31	*Configurar la interface Túnel, con el número asignado.*
description --- COBIJA DMVPN ENTEL ---	*Especificar una descripción para la interface Túnel creada.*
ip address 172.31.254.18 255.255.255.0	*Configurar la dirección IP para la interface Túnel dentro de la misma subred IP de la DMVPN.*
no ip redirects	*En la oficina central: establecer la llave compartida que se usará con cualquier router remoto*
tunnel key 31	*Establecer una llave ID única que deberá ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
tunnel source 172.31.227.50	*Configurar la dirección origen para la interface Túnel.*
tunnel mode gre multipoint	*Configurar el modo de encapsulación para mGRE para la interface Túnel.*

CONFIGURACIÓN NHRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip nhrp authentication tun31	*Configurar la cadena de autenticación para una interface utilizando NHRP, la cadena debe ser la misma en todos los hubs y spokes dentro de la misma red DMVPN.*
ip nhrp map 172.31.254.10 172.31.65.58	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB LPZ ENTEL)***
ip nhrp map multicast 172.31.65.58	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB LPZ ENTEL)***
ip nhrp map 172.31.254.11 172.31.13.18	*Configurar estáticamente el mapeo de direcciones IP-a-NBMA de destinos IP conectados a la red MBMA. Se define el servidor NHRP hacia el hub, el cual es permanentemente mapeado a la dirección IP publica estática del hub.* ***(HUB SCZ ENTEL)***
ip nhrp map multicast 172.31.13.18	*Habilitar el uso de protocolo de enrutamiento dinámico entre el spoke y hub, y el envío de paquetes multicast al router hub.* ***(HUB SCZ ENTEL)***
ip nhrp network-id 31	*Habilitar NHRP en una interface, el número es un identificador único NBMA.*
ip nhrp holdtime 450	*Cambiar el número de segundos que las direcciones NHRP NBMA son anunciadas como válidas.*
ip nhrp nhs 172.31.254.10	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB LPZ ENTEL)***
ip nhrp nhs 172.31.254.11	*Configurar el router hub que actúa como el siguiente salto NHRP, next-hop.* ***(HUB SCZ ENTEL)***
ip nhrp shortcut	*Habilitar NHRP shortcut switching.*

CONFIGURACIÓN DE MTU PARA ENVÍO DE PAQUETES	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip mtu 1400	*Configurar el tamaño de MTU en bytes, de los paquetes IP enviados sobre la interface.*
ip tcp adjust-mss 1360	*Ajustar el valor de MSS de paquetes TCP que van a través del router.*

CONTROL DE PROTOCOLO DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
bandwidth 1000	*Configurar el valor del ancho de banda en kbps.*
delay 1000	*Especificar un valor para cambiar la métrica de enrutamiento EIGRP.*

APLICACIÓN DE SEGURIDAD IPSEC	
COMANDO IMPLEMENTADO	**PROPÓSITO**
tunnel protection ipsec profile PRFIPSEC	*Asociar la interface Túnel al perfil Ipsec.*

Aplicando el protocolo de enrutamiento EIGRP y listas de acceso, se indujo que se utilice el enlace del proveedor TIGO para la conexión de la regional con las redes críticas declaradas en la ACL PRIMARIO. El resto de tráfico fue balanceado e inducido para utilizar el enlace de ENTEL en una relación 2 a 1 con respecto al enlace de TIGO.

APLICACIÓN DE ENRUTAMIENTO EIGRP	
COMANDO IMPLEMENTADO	**PROPÓSITO**
ip access-list standard PRIMARIO	*Crear lista de acceso a utilizarse para el criterio de uso en el offset (compensación)*
permit 10.7.0.0 0.0.0.255 **permit 10.10.0.0 0.0.0.255**	*Definir las redes para el criterio del offset.*
router eigrp 60	*Configurar el proceso de enrutamiento EIGRP.*
variance 2	*Controlar el balanceo de carga de paquetes en una red basada en EIGRP.*
network 1.98.0.0 0.0.1.255 **network 1.98.2.0 0.0.1.255** **network 1.98.4.0 0.0.1.255** **network 10.100.100.18 0.0.0.0** **network 172.21.254.0 0.0.0.255** **network 172.31.254.0 0.0.0.255**	*Especificar una lista de redes para el proceso de enrutamiento EIGRP.*
offset-list PRIMARIO in 2000 Tunnel31	*Configurar el valor offset que se adicionará a la métrica de enrutamiento aplicada a métricas entrantes.*

2.2.3.12 Configuración del Túnel L2 L2TPv3 (La Paz – Santa Cruz)

Se utilizó la funcionalidad del túnel L2tpv3 aplicada a los routers ISR 4321, para replicar y extender las VLANs 15 y 30 entre el sitio principal - La Paz y el sitio Alterno – Santa Cruz, a fin de que ambos sitios se encuentren sincronizados en los datos de servidores cuando exista contingencia o migración entre sitios. A continuación, se representa un diagrama de flujo de los procesos de configuración:

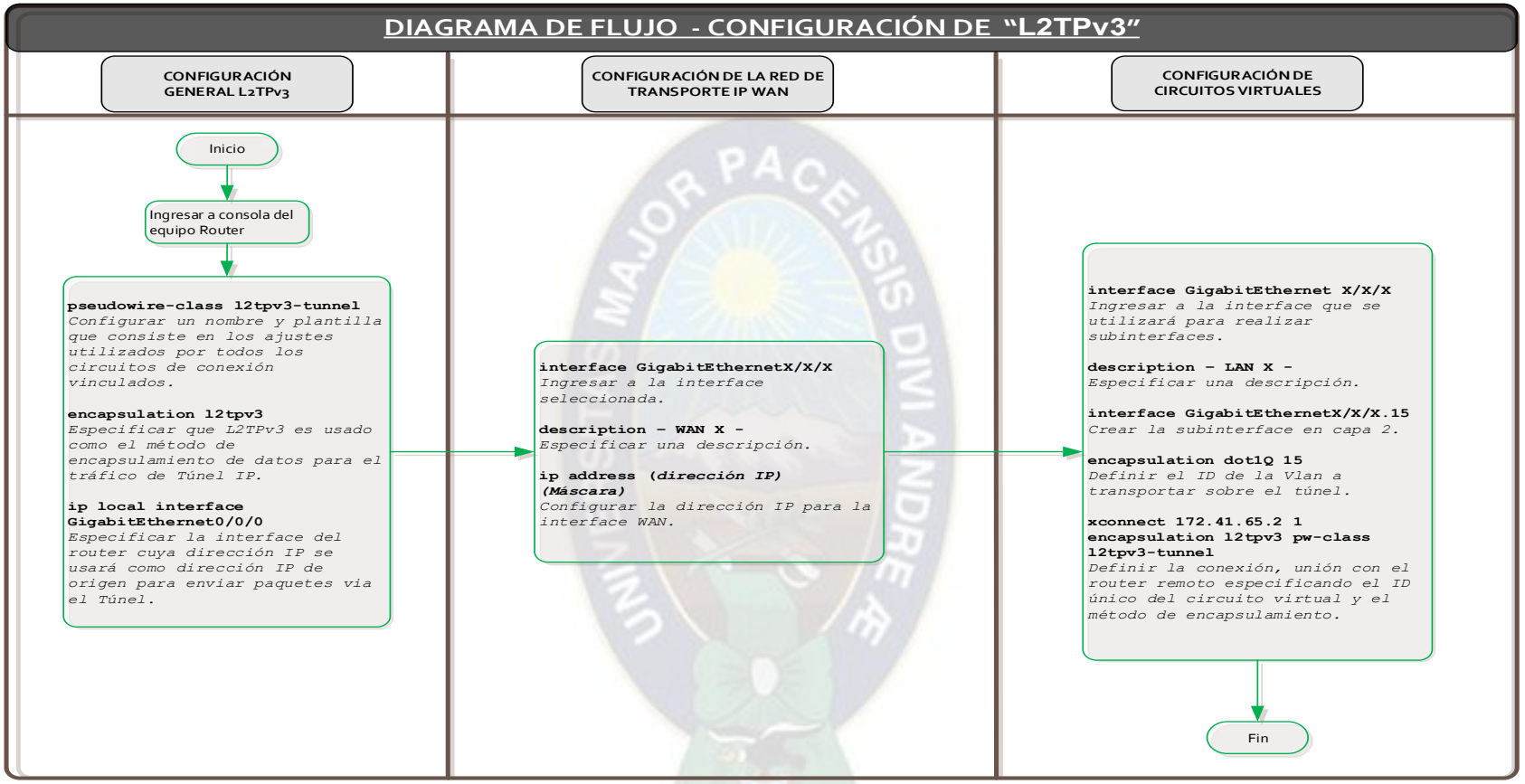


Figura 22 Diagrama de Flujo - Configuración L2TPv3

Fuente: Elaboración Propia

2.2.3.13 Router 4321 La Paz

CONFIGURACIÓN DE TÚNEL L2 L2TPv3 – LA PAZ	
COMANDO IMPLEMENTADO	**PROPÓSITO**
pseudowire-class l2tpv3-tunnel	*Configurar un nombre y plantilla que consiste en los ajustes utilizados por todos los circuitos de conexión vinculados.*
encapsulation l2tpv3	*Especificar que L2TPv3 es usado como el método de encapsulamiento de datos para el tráfico de Túnel IP.*
ip local interface GigabitEthernet0/0/0	*Especificar la interface del router cuya dirección IP se usará como dirección IP de origen para enviar paquetes via el Túnel.*
interface GigabitEthernet0/0/0	*Ingresar a la interface seleccionada.*
description --- WAN LA PAZ A SANTA CRUZ ---	*Definir una descripción para la interface.*
ip address 172.41.65.1 255.255.255.248	*Configurar la dirección IP para la interface.*
interface GigabitEthernet0/1/0	*Ingresar a la interface que se utilizará para realizar subinterfaces.*
description --- LAN 1 ---	*Definir una descripción para la interface.*
interface GigabitEthernet0/1/0.15	*Crear la subinterface en capa 2.*
encapsulation dot1Q 15	*Definir el ID de la Vlan a transportar sobre el túnel.*
xconnect 172.41.65.2 1 encapsulation l2tpv3 pw-class l2tpv3-tunnel	*Definir la conexión, unión con el router remoto especificando el ID único del circuito virtual y el método de encapsulamiento.*
interface GigabitEthernet0/1/0.30	*Crear la subinterface en capa 2.*
encapsulation dot1Q 30	*Definir el ID de la Vlan a transportar sobre el túnel.*
xconnect 172.41.65.2 2 encapsulation l2tpv3 pw-class l2tpv3-tunnel	*Definir la conexión, unión con el router remoto especificando el ID único del circuito virtual y el método de encapsulamiento.*

2.2.3.14 Router 4321 Santa Cruz

CONFIGURACIÓN DE TÚNEL L2 L2TPv3 - SANTA CRUZ	
COMANDO IMPLEMENTADO	**PROPÓSITO**
pseudowire-class l2tpv3-tunnel	*Configurar un nombre y plantilla que consiste en los ajustes utilizados por todos los circuitos de conexión vinculados.*
encapsulation l2tpv3	*Especificar que L2TPv3 es usado como el método de encapsulamiento de datos para el tráfico de Túnel IP.*
ip local interface GigabitEthernet0/0/0	*Especificar la interface del router cuya dirección IP se usará como dirección IP de origen para enviar paquetes via el Túnel.*
interface GigabitEthernet0/0/0	*Ingresar a la interface seleccionada.*
description --- WAN SANTA CRUZ A LA PAZ ---	*Definir una descripción para la interface.*
ip address 172.41.65.2 255.255.255.248	*Configurar la dirección IP para la interface.*

CONFIGURACIÓN DE TÚNEL L2 L2TPv3 - SANTA CRUZ	
COMANDO IMPLEMENTADO	**PROPÓSITO**
interface GigabitEthernet0/1/0	*Ingresar a la interface que se utilizará para realizar subinterfaces.*
description --- LAN 1 ---	*Definir una descripción para la interface.*
interface GigabitEthernet0/1/0.15	*Crear la subinterface en capa 2.*
encapsulation dot1Q 15	*Definir el ID de la Vlan a transportar sobre el túnel.*
xconnect 172.41.65.1 1 encapsulation l2tpv3 pw-class l2tpv3-tunnel	*Definir la conexión, unión con el router remoto especificando el ID único del circuito virtual y el método de encapsulamiento.*
interface GigabitEthernet0/1/0.30	*Crear la subinterface en capa 2.*
encapsulation dot1Q 30	*Definir el ID de la Vlan a transportar sobre el túnel.*
xconnect 172.41.65.1 2 encapsulation l2tpv3 pw-class l2tpv3-tunnel	*Definir la conexión, unión con el router remoto especificando el ID único del circuito virtual y el método de encapsulamiento.*

2.2.4. Pruebas de la funcionalidad

Las pruebas de funcionalidad que se realizaron evaluaron la topología aplicada y configuraciones realizadas en los equipos de comunicación en relación con la comunicación DMVPN para que el Sitio Alterno Santa Cruz pueda proporcionar acceso a los servicios productivos en caso de contingencia con el Sitio Principal de La Paz.

Estas pruebas fueron coordinadas con el Banco y realizadas en horarios controlados debido a ser tráfico productivo.

A continuación, se detallan el esquema y diagrama de flujo del escenario de prueba:

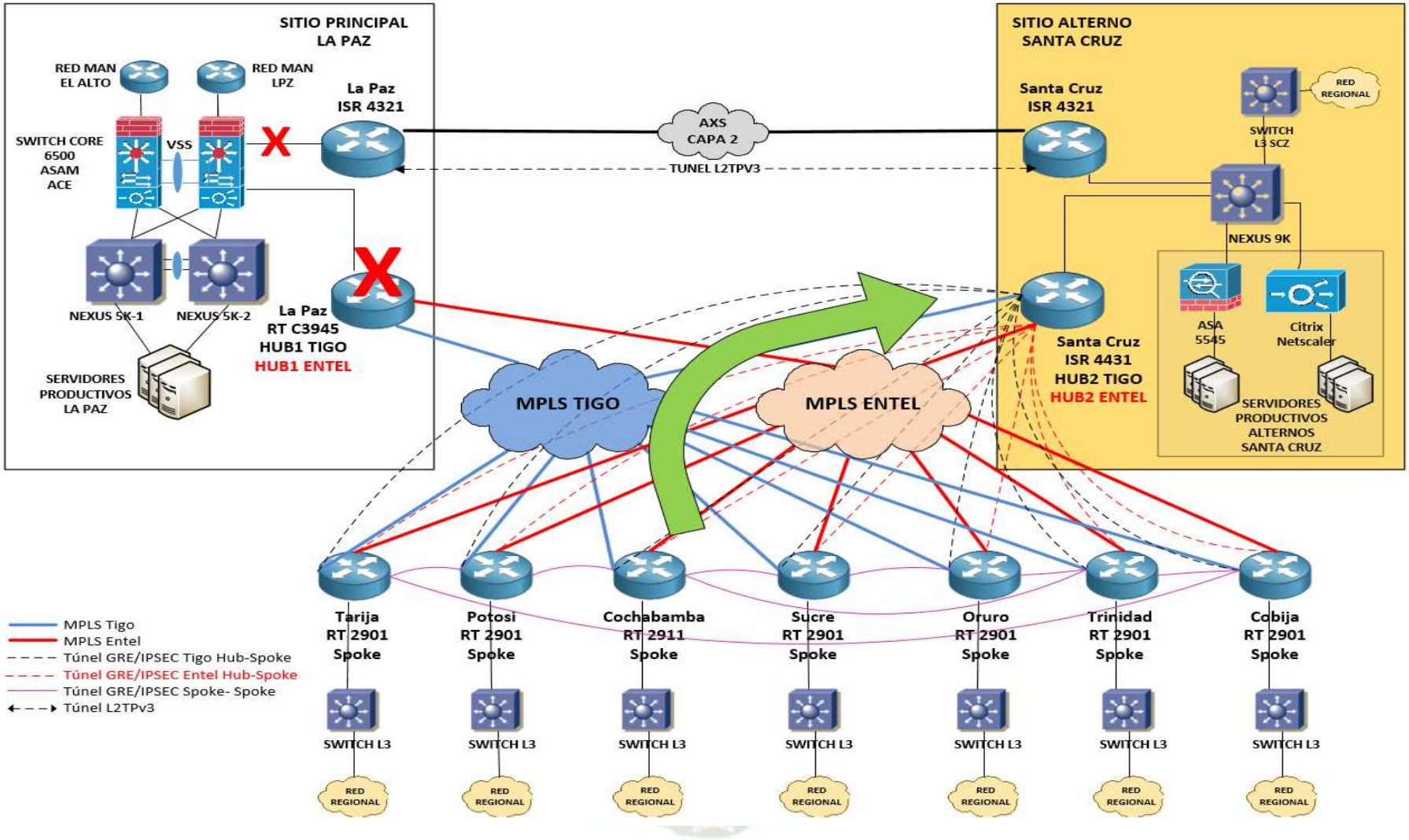


Figura 23 Esquema de prueba de funcionamiento DMVPN en contingencia

Fuente: Elaboración Propia

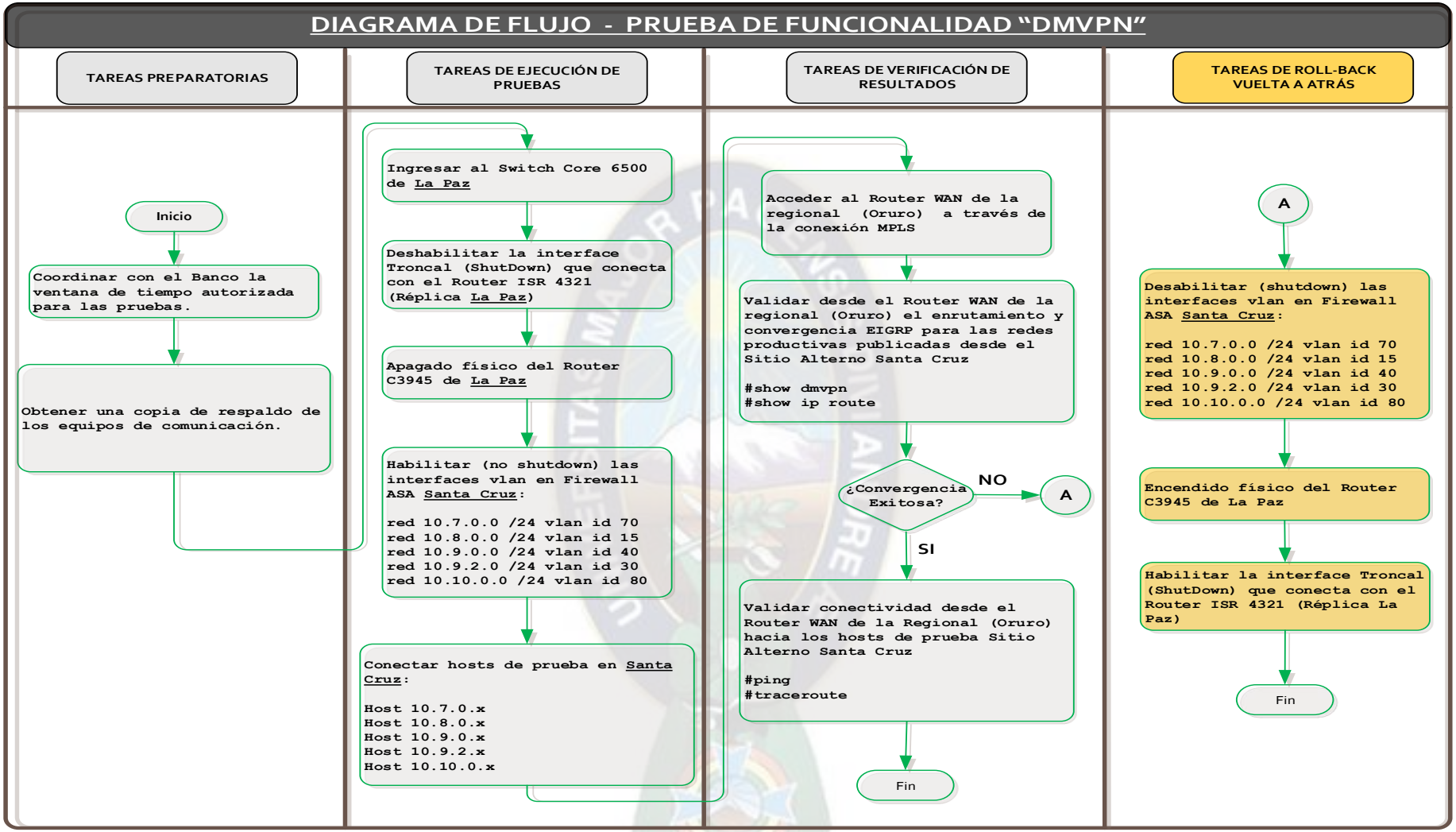


Figura 24 Diagrama de Flujo – Prueba de Funcionalidad DMVPN

Fuente: Elaboración Propia

Se evaluó el caso que no se cuente con conectividad al sitio principal La Paz, las regionales (para la prueba Oruro) converjan su comunicación a través de EIGRP al sitio alterno Santa Cruz (Hub 2) sobre la comunicación DMVPN establecida. En el sitio alterno Santa Cruz se contaba con PCs de prueba en redes productivas. Por otro lado, se validó la conectividad en la extensión de VLANs mediante el enlace L2TPv3.

Se ejecutó la siguiente matriz de pruebas para el escenario planteado:

FECHA/HORA	TIEMPO	ACTIVIDADES	RESPONSABLE	ESTADO	OBSERVACIONES
Domingo 17 Enero 2016 - 07:00	2 min	Bajar troncal (shutdown) del core 6500 LPZ que conecta al ISR 4321 LPZ	BSOL	**OK**	Se desconectó la comunicación de las Regionales hacia La Paz (Routers WAN LPZ apagados). Se habilitaron las Vlan's Productivas en el Sitio Alterno SCZ (vlan 15, 30, 40, 70, 80). Se validó que el enrutamiento dinámico dirigió el tráfico de las Regionales hacia el Sitio Alterno de SCZ (DMVPN HUB2 SCZ), abajo se muestra imagen de ejemplo.
	2 min	Apagado de router WAN LPZ	BSOL		
	2 min	Subir (no shutdown) las interfaces vlan en ASA SCZ: red 10.7.0.0 /24 vlan id 70 red 10.8.0.0 /24 vlan id 15 red 10.9.0.0 /24 vlan id 40 red 10.9.2.0 /24 vlan id 30 red 10.10.0.0 /24 vlan id 80	DATEC - BSOL		
	5 min	Conectar hosts de prueba: Host 10.7.0.x Host 10.8.0.x Host 10.9.0.x Host 10.9.2.x Host 10.10.0.x	DATEC – BSOL		
	5 min	Acceder a los Router WAN de las regionales (Oruro) a través de la conexión MPLS	DATEC – BSOL		
	5 min	Validar desde los Router WAN de las Regionales (Oruro) el enrutamiento y convergencia EIGRP para las redes productivas publicadas desde el Sitio Alterno	DATEC – BSOL		
	15 min	Validar conectividad desde los Router WAN de las Regionales (Oruro) hacia los hosts de prueba-Sitio Alterno	DATEC – BSOL		

Tabla 13 Matriz de pruebas DMVPN: HUB 1 en contingencia

Fuente: Elaboración Propia

2.2.4.1 Resultado de las Pruebas

En la siguiente figura se muestra el estado de las DMVPNs desde el router de la regional de Oruro, se puede observar que el sitio principal La Paz Hub 1 está fuera de servicio en sus dos enlaces (Tigo y Entel) y que el sitio alterno Santa Cruz Hub 2 se encuentra operativo:

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

Interface: Tunnel21, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1    172.21.65.58   172.21.254.10   IKE 00:13:16     S <-- Hub1 LPZ TIGO - Down
     1    172.21.13.18   172.21.254.11    UP     2w4d     S <-- Hub2 SCZ TIGO - Up

Interface: Tunnel31, IPv4 NHRP Details
Type:Spoke, NHRP Peers:9,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1    172.31.65.58   172.31.254.10   IKE 00:13:17     S <-- Hub1 LPZ ENTEL - Down
     1    172.31.13.18   172.31.254.11    UP    5d10h     S <-- Hub2 SCZ ENTEL -Up
     1    172.31.132.2   172.31.254.12    UP     1w3d     D
     1   172.31.224.66   172.31.254.13    UP     1w0d     D
     1   172.31.176.50   172.31.254.14    UP 14:06:39     D
     1   172.31.226.50   172.31.254.15    UP 00:05:39     D
```

Figura 25 Estado de las DMVPNs en contingencia del Hub 1 La Paz

Fuente: Elaboración Propia

En la siguiente figura se observa la convergencia del enrutamiento EIGRP hacia el sitio alterno Santa Cruz Hub 2, las regionales cuentan con conectividad a las redes productivas en el sitio alterno, en sus dos enlaces (Tigo y Entel):

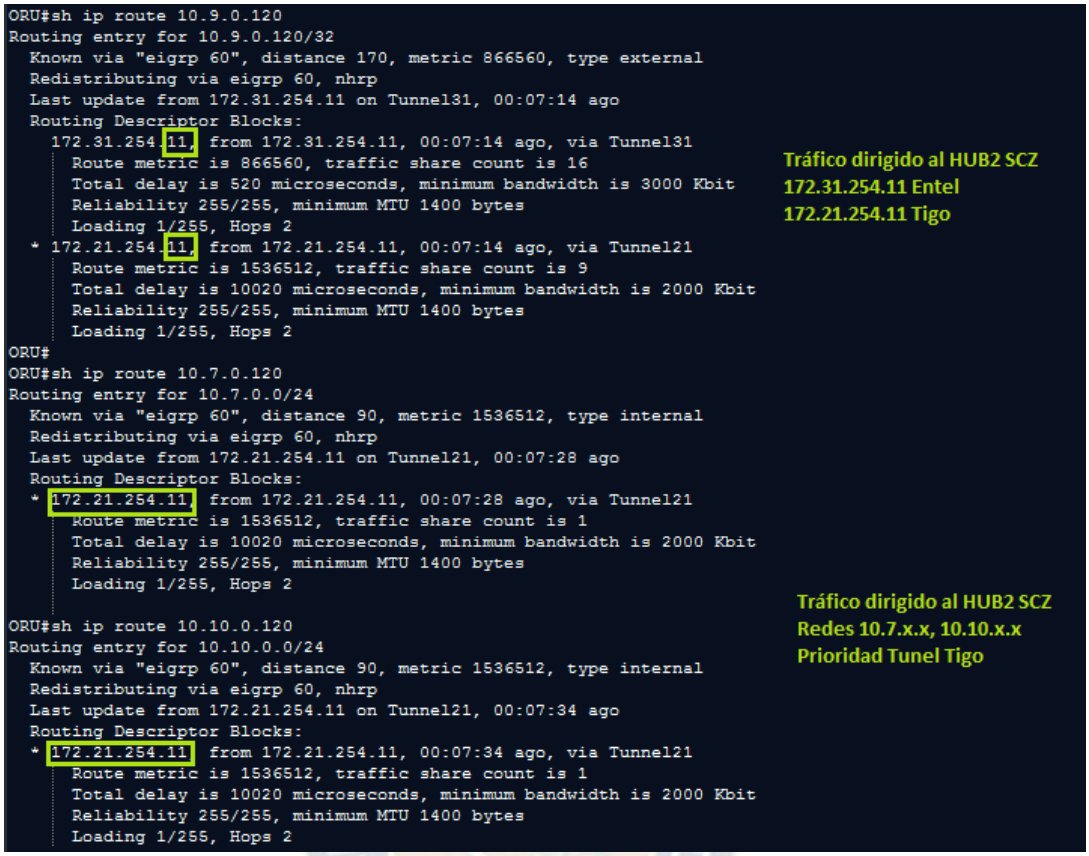


Figura 26 Estado de las DMVPNs en contingencia con el Hub 1 La Paz

Fuente: Elaboración Propia

2.3. Conclusiones y Recomendaciones.

2.3.1. Resultados principales.

La solución DMVPN aplicada ha logrado satisfacer al BancoSol por la continuidad de sus servicios financieros en un sitio alterno, obteniendo tiempos de convergencia mínimos en la red en un escenario de contingencia de su sitio principal.

Fue posible aplicar selección de mejor ruta para el tráfico crítico del Banco a través del protocolo EIGRP y DMVPN.

Así mismo, se aplicó balanceo de tráfico en los dos enlaces para el tráfico menos crítico, con convergencia automática en caso de falla de uno de los enlaces.

Las pruebas satisfactorias realizadas en producción confirmaron la funcionalidad esperada. Al ser coordinadas con el banco y coordinadas en horarios menos disruptivos no afectaron el servicio al cliente final.

Se logró proteger y cifrar el tráfico del Banco para evitar la intercepción en las redes MPLS.

2.3.2. Recomendaciones.

Se recomienda adicionar un segundo router en cada sitio para separar los enlaces de comunicación MPLS.

En función a las exigencias y demanda de ancho de banda de las aplicaciones del Banco, se recomienda aplicar políticas de Calidad de Servicio en los mismos routers u otras soluciones independientes que sean compatibles con la solución DMVPN aplicada.

En función al crecimiento de regionales, evaluar a mediano plazo la escalabilidad al protocolo de enrutamiento dinámico OSPF.

3. ANALISIS DE LA ACTIVIDAD.

3.1. Desempeño Laboral.

De acuerdo con lo expuesto en la primera parte del presente documento, a partir de mi egreso de la carrera de Ingeniería Electrónica se tuvo la oportunidad de trabajar en una empresa privada, ATC S.A. Red Enlace en el área de redes y comunicaciones, empresa del rubro financiero pionera en el servicio de medios de pago electrónicos y con cobertura nacional de comunicaciones.

En la empresa ATC S.A. Red Enlace estuve 11 años en diferentes cargos con orientación técnica, demostrando en cada uno de ellos la solvencia en el análisis de problemas y sus soluciones, implementación de nuevas tecnologías en comunicaciones para ATMs (cajeros automáticos) y POS (puntos de venta), comunicaciones con entidades financieras nacionales (Bancos) e internacionales (Visa, MasterCard).

Por la capacidad demostrada, la empresa ATC S.A. me encargó realizar procesos de implementación y certificación a sistemas de comunicación y sistemas transaccionales,

mismos que son de criticidad Alta para las entidades financieras, certificaciones realizadas con éxito para su salida a Producción, por ejemplo, POS GPRS con SSL, Transacciones con Tarjetas Chip EMV entre otros.

En otra empresa donde también se tuvo la oportunidad de demostrar la experiencia en el manejo de redes y telecomunicaciones fue en la empresa Datec Ltda., empresa de servicios tecnológicos en la cual realicé proyectos de implementación de redes WAN, Seguridad en redes con Firepower Cisco entre otros, para el sector financiero, justamente se me asignó el proyecto del presente documento en la empresa Datec Ltda.

Adicionalmente, destacar que gracias al contenido curricular de la carrera se pudo complementar con el aprendizaje de tecnologías Cisco y obtener certificaciones como ser, CCNA Routing and Switching, CCNA Security y CCNP Security, lo cual coadyuvó el desarrollo de varios proyectos sobre esta tecnología.

En este sentido, se está seguro de que la experiencia obtenida durante la etapa laboral aplicando los conocimientos obtenidos en la carrera colaboraron en la toma de decisiones en diseños e implementación de proyectos en telecomunicaciones, así como la resolución de problemas y análisis de otras tecnologías como ser el área transaccional y mensajería ISO8583.

3.2. Formación Recibida en la UMSA.

Se valora toda la formación recibida en la Universidad Mayor de San Andrés, ha sido de gran beneficio para encarar cargos como Analista de Redes, Supervisor de Infraestructura, Supervisor de Certificación, Especialista de Servicios en Redes y Comunicaciones.

Las materias base en la carrera son de vital importancia en el análisis y la metodología de estudio para aplicar en las áreas de ingeniería.

Las materias de especialidad en la carrera han sido fundamentales para encarar el mundo real, donde se puede observar un sin fin de tecnologías, sin embargo, todas en base a estándares que sin su estudio previo se haría difícil su aplicación y utilización.

Las materias de Redes de Datos (ETN 935) y Tecnología de Telecomunicaciones (ETN 1038) han sido importantes en la coyuntura de mi egreso, debido a que las empresas del rubro

financiero donde empecé a trabajar se encontraban en proceso de migración de tecnologías como ser X.25, SDLC a tecnología TCP/IP.

Considero que es importante la inclusión de materias donde se estudien tecnologías emergentes, para que el estudiante pueda estar alineado a la evolución tecnológica del entorno real. Especializaciones como Cisco colaboran en reafirmar los conocimientos que nos brinda la carrera.

Se puede indicar que en la Facultad de Ingeniería y carrera de Electrónica se nos transmite un alto nivel de conocimiento teórico, lo cual representa un sólido cimiento para la carrera profesional. Por las empresas donde se pudo trabajar o relacionar, se pudo comprobar que los profesionales de la carrera son muy valorados por su capacidad y formación.

GLOSARIO.

DMVPN: Dynamic Multipoint VPN (VPN Dinámica Multipunto), es un protocolo de CISCO para crear VPN securizadas.

VPN: Virtual Private Network (Red Privada Virtual), es una tecnología de red de computadoras que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet.

WAN: Wide Area Network (Red de Área Amplia), es una red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física.

FULL MESH: Enmallado completo, es una topología de red en la que cada nodo está conectado a todos los nodos.

IPSEC: Internet Protocol Security, es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

MPLS: Multiprotocol Label Switching (Conmutación de Etiquetas Multiprotocolo) es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI.

HSM: Hardware Security Module (Módulo de Seguridad Hardware), Un HSM es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y suele aportar aceleración hardware para operaciones criptográficas.

ATM: Automated Teller Machine, es decir, cajero automático. Es una computadora especializada que le permite manejar su dinero de forma conveniente.

POS: Point Of Sale (Punto de Venta), es un dispositivo que, en un establecimiento comercial, permite gestionar tareas relacionadas con la venta, tales como el cobro por tarjeta de crédito o débito.

ASFI: Autoridad de Supervisión del Sistema Financiero, es una institución de derecho público y de duración indefinida, con personalidad jurídica, patrimonio propio y autonomía de gestión administrativa, financiera, legal y técnica, con jurisdicción, competencia y estructura de alcance nacional, bajo tuición del Ministerio de Economía y Finanzas Públicas y sujeta a control social.

TELCO: es un nombre genérico utilizado para designar a una gran empresa de telecomunicaciones, que necesita unas aplicaciones enormes para poder dar servicios a millones de clientes.

SITE TO SITE: Sitio a Sitio, término utilizado en Redes cuando se refiere a la comunicación de un sitio con otro sitio de forma directa o mediante VPN.

HASHING: Las funciones hash criptográficas son aquellas que cifran una entrada y actúan de forma parecida a las funciones hash, ya que comprimen la entrada a una salida de menor longitud y son fáciles de calcular.

PRE-SHARE KEY: En criptografía, una clave previamente compartida, clave pre compartida o PSK (en inglés pre-shared key) es una clave secreta compartida con anterioridad entre las dos partes usando algún canal seguro antes de que se utilice.

IKE: Internet key exchange (IKE) es un protocolo usado para establecer una Asociación de Seguridad (SA) en el protocolo IPsec. IKE emplea un intercambio secreto de claves de tipo Diffie-Hellman para establecer el secreto compartido de la sesión.

ROUTER: Un router —también conocido como enrutador, o rúter— Se trata de un producto de hardware que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer qué ruta se destinará a cada paquete de datos dentro de una red informática.

GRE: El GRE (Generic Routing Encapsulation) es un protocolo para el establecimiento de túneles a través de Internet.

NHRP: El Protocolo de resolución de próximo salto es una extensión del mecanismo de enrutamiento que a veces se usa para mejorar la eficiencia del enrutamiento del tráfico de la red de computadoras a través de redes de acceso múltiple sin difusión.

MULTICAST: La multidifusión o difusión múltiple es el envío de la información en múltiples redes a múltiples destinos simultáneamente.

IPv4: El Protocolo de Internet versión 4 en inglés, Internet Protocol version 4 (IPv4), es la cuarta versión del Internet Protocol (IP), un protocolo de interconexión de redes basados en Internet, y fue la primera versión implementada para la producción de ARPANET, en 1983. Definida en el RFC 791.

IPv6: El Protocolo de Internet versión 6, en inglés: Internet Protocol version 6 (IPv6), es una versión del Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol version 4 (IPv4) RFC 791, que a 2016 se está implementando en la gran mayoría de dispositivos que acceden a Internet.

TCP: (Transmission Control Protocol) Protocolo de Control de Transmisión.: Este protocolo se encarga de crear “conexiones” entre sí para que se cree un flujo de datos. Este proceso garantiza que los datos sean entregados en destino sin errores y en el mismo orden en el que salieron.

UDP: El protocolo de datagramas de usuario es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

ESP: lo denominado carga de seguridad encapsulada, ESP ofrece autenticación, integridad y confidencialidad de los datos transmitidos a través de IPsec. Para conseguir estas características de seguridad, se hace un intercambio de llaves públicas.

EIGRP: (Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado en español) es un protocolo de encaminamiento de vector distancia, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancia.

HUB: En DMVPN, router central que se encarga de la gestión de túneles e informar a los routers Spokes.

SPOKE: En DMVPN, router remote que se comunica con el router Hub para establecer un túnel. También puede comunicarse con otro router Spoke para establecer un túnel directo.

BACKUP: Se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.

ISP: Son las siglas de Internet Service Provider Proveedor de Servicios de Internet, una compañía que proporciona acceso a Internet.

FRAME RELAY: Se utiliza para un servicio de transmisión de voz y datos a alta velocidad que permite la interconexión de redes de área local separadas geográficamente a un coste menor.

L2TPv3: Layer 2 Tunneling Protocol Version 3 es un estándar IETF relacionado con L2TP que se puede usar como un protocolo alternativo al Multiprotocol Label Switching para la encapsulación del tráfico de comunicaciones multiprotocolo Layer 2 a través de redes IP.

Keep-Alive: Un keepalive es un mensaje enviado por un dispositivo a otro para verificar que el enlace entre los dos está funcionando, o para evitar que se rompa el enlace.

MULTIPLEXAR: En telecomunicación, la multiplexación es la técnica de combinar dos o más señales, y transmitirlas por un solo medio de transmisión.

PSEUDOWIRE: En redes de computadoras y telecomunicaciones, un pseudowire es una emulación de una conexión punto a punto a través de una red de conmutación de paquetes. El pseudowire emula el funcionamiento de un "cable transparente" que lleva el servicio, pero se da cuenta de que esta emulación rara vez será perfecta.

MTU: La unidad máxima de transferencia (Maximum Transmission Unit - MTU) es un término de redes de computadoras que expresa el tamaño en bytes de la unidad de datos más grande que puede enviarse usando un protocolo de comunicaciones. Ejemplos de MTU para distintos protocolos usados en Internet: Ethernet: 1500 bytes.

L3: La capa de red del modelo OSI proporciona el enrutamiento de mensajes y determina si el destino de estos es la capa 4 (Transporte) o la capa 2 (Enlace de Datos).

PBR: Enrutamiento basado en políticas. El comportamiento habitual de un enrutador o router cuando recibe un paquete es la de reenviarlo en función de la dirección IP destino incluida en el paquete, que utiliza para comparar con su tabla de enrutamiento.

VSS: es el acrónimo de Virtual Switching System, y cuando hablamos de VSS hablamos de un cluster, no de un stack. VSS permite la combinación de dos switches para conseguir una única entidad lógica de red desde las perpectivas de plano de control y gestión.

SWITCH: Un switch o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

VLAN: Acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.

SPLIT-HORIZON: En redes de computadoras, el protocolo de vector de distancias emplea la regla de horizonte dividido que prohíbe a un router publicar una ruta por la misma interfaz por la que se aprendió en primer lugar.

ISAKMP: Internet Security Association and Key Management Protocol es un protocolo criptográfico que constituye la base del protocolo de intercambio de claves IKE. Está definido en el RFC 2408.

BANDWIDTH: En computación de redes, ancho de banda digital, ancho de banda de red o simplemente ancho de banda es la medida de datos y recursos de comunicación disponible o consumida expresados en bit/s o múltiplos de él como serían los Kbit/s, Mbit/s y Gigabit/s.

DELAY: Retardo de red, también retraso de red, en ciencias de la computación, es un parámetro importante en el diseño y caracterización de una red de telecomunicaciones. El retardo de red especifica cuánto tiempo tarda un bit de datos para viajar a través de la red desde un nodo origen a uno final.

VARIANCE: configura el equilibrio de carga de coste desigual definiendo la diferencia entre la métrica óptima y la peor métrica aceptable.

OFFSET-LIST: Una lista de compensación es el mecanismo para aumentar las métricas entrantes y salientes a las rutas aprendidas a través de EIGRP o Protocolo de información de enrutamiento (RIP).

BIBLIOGRAFÍA.

Academia de Networking de Cisco Systems: Guía del primer año, Segunda Edición.

(ISBN: 84-205-3297-7)

Academia de Networking de Cisco Systems: Guía del segundo año, Segunda Edición.

(ISBN: 84-205-3297-5)

PEARSON EDUCACIÓN, S.A.

Nuñez de Balboa, 120

28006 Madrid

Designing Cisco Network Service Architectures (ARCH) Foundation Learning Guide: (CCDP ARCH 642-874), 3rd Edition

John Tiso, CCIE No. 5162, CCDP

Copyright 2012

(ISBN-10: 1-58714-288-0)

CCIE Routing and Switching v5.0 Official Cert Guide, Volume 2, 5th Edition

Narbik Kocharians CCIE No. 12410, Terry Vinson CCIE No. 35347

Copyright 2015

(ISBN-10: 1-58714-491-3)

DMVPN

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book.pdf

http://ccnp-jncis-en-espanol.blogspot.com/2015/12/dmvpn-dynamic-multipoint-vpn.html

https://community.cisco.com/t5/blogs-routing-y-switching/conociendo-dynamic-multipoint-vpn-dmvpn/ba-p/3101118

L2TPv3

https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/l2tpv325.html#wp1051371

https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-1/lxvpn/configuration/guide/vc41crs/vc41tpv3.pdf

NHRP

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nhrp/configuration/xe-3s/nhrp-xe-3s-book/nhrp-switch-enhancemts-dmvpn.html

IPSEC

https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-2/security/command/reference/b_syssec_cr42crs/b_syssec_cr41crs_chapter_010.pdf

COMANDOS EIGRP

https://www.cisco.com/c/en/us/td/docs/ios/12_2/iproute/command/reference/fiprrp_r/1rfeigrp.html

ANEXOS.

A. CONFIRMACIÓN DE LAS PRUEBAS EXITOSAS

De: Juan Carlos Gonzales [mailto:JGonzales@datec.com.bo]
Enviado el: lunes, 18 de enero de 2016 11:55
Para: Hugo Duran
CC: Franklin Arraya; Armando Medrano; Boris Barrenechea; Carlos Laura; Francisco Guzman; Borys Espada
Asunto: RE: RV: Sitio Alterno SCZ

Estimado Hugo,

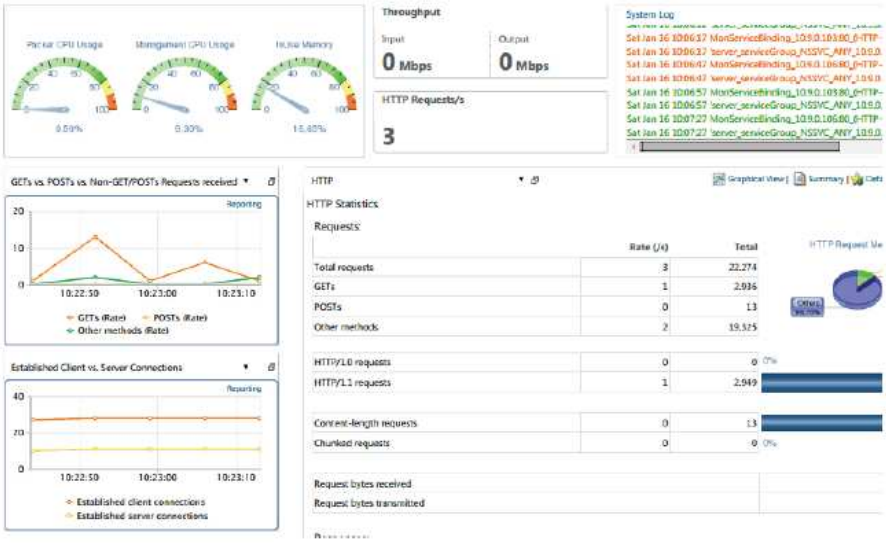
Se realizaron las pruebas programadas con resultados satisfactorios:

- Viernes 15/ 9:00 AM - Prueba aislada del balanceo Web Citrix Cisco.

Se configuró el Citrix Netscaler con vlan's de prueba y 2 hosts web.
El balanceo fue efectivo consumiendo el sitio http://10.60.0.170 desde LPZ.

- Sábado 16/ 7:00 AM - Prueba controlada del balanceo Web Citrix Cisco con Servidores productivos de La Paz.
-

Se utilizó el Citrix Netscaler de SCZ para balancear servidores productivos LPZ WEB (BANTOTAL).
La funcionalidad de balanceo fue efectiva, abajo se muestra imagen del estado de Citrix en el momento de las pruebas. Adjunto logs y reportes adicionales.
En algunas ocasiones se registró error de permisos de usuario (código 5) en el aplicativo web, esto debe ser validado por el Banco para describir el código de error.
Se debe considerar que este escenario de prueba no se presentará en el entorno productivo donde el Citrix balanceará en contingencia servicios Web locales de SCZ y no servicios Web extendidos de LPZ.



- Domingo 17/ 7:00 AM - Prueba controlada del HUB DMVPN Secundario SCZ y conectividad hacia el Sitio Alterno.

Se desconectó la comunicación de las Regionales hacia La Paz (Routers WAN LPZ apagados).
Se habilitaron las Vlan's Productivas en el Sitio Alterno SCZ (vlan 15, 32, 40, 70, 80).
Se validó que el enrutamiento dinámico dirigió el tráfico de las Regionales hacia el Sitio Alterno de SCZ (DMVPN HUB2 SCZ), abajo se muestra imagen de ejemplo, adjunto respaldo desde todas las regionales.

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

Interface: Tunnel21, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1    172.21.65.58    172.21.254.10   IKE 00:13:16     S <-- Hub1 LPZ TIGO - Down
     1    172.21.13.18    172.21.254.11    UP     2w4d     S <-- Hub2 SCZ TIGO - Up

Interface: Tunnel31, IPv4 NHRP Details
Type:Spoke, NHRP Peers:9,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1    172.31.65.58    172.31.254.10   IKE 00:13:17     S <-- Hub1 LPZ ENTEL - Down
     1    172.31.13.18    172.31.254.11    UP    5d10h     S <-- Hub2 SCZ ENTEL -Up
     1    172.31.132.2    172.31.254.12    UP     1w3d     D
     1   172.31.224.66    172.31.254.13    UP     1w0d     D
     1   172.31.176.50    172.31.254.14    UP 14:06:39     D
     1   172.31.226.50    172.31.254.15    UP 00:05:39     D
```

```
ORU#sh ip route 10.9.0.120
Routing entry for 10.9.0.120/32
  Known via "eigrp 60", distance 170, metric 866560, type external
  Redistributing via eigrp 60, nhrp
  Last update from 172.31.254.11 on Tunnel31, 00:07:14 ago
  Routing Descriptor Blocks:
    172.31.254.11, from 172.31.254.11, 00:07:14 ago, via Tunnel31
      Route metric is 866560, traffic share count is 16
      Total delay is 620 microseconds, minimum bandwidth is 3000 Kbit
      Reliability 255/255, minimum MTU 1400 bytes
      Loading 1/255, Hops 2
  * 172.21.254.11, from 172.21.254.11, 00:07:14 ago, via Tunnel21
      Route metric is 1536512, traffic share count is 5
      Total delay is 10020 microseconds, minimum bandwidth is 2000 Kbit
      Reliability 255/255, minimum MTU 1400 bytes
      Loading 1/255, Hops 2
ORU#
ORU#sh ip route 10.7.0.120
Routing entry for 10.7.0.0/24
  Known via "eigrp 60", distance 90, metric 1536512, type internal
  Redistributing via eigrp 60, nhrp
  Last update from 172.21.254.11 on Tunnel21, 00:07:28 ago
  Routing Descriptor Blocks:
  * 172.21.254.11, from 172.21.254.11, 00:07:28 ago, via Tunnel21
      Route metric is 1536512, traffic share count is 1
      Total delay is 10020 microseconds, minimum bandwidth is 2000 Kbit
      Reliability 255/255, minimum MTU 1400 bytes
      Loading 1/255, Hops 2

ORU#sh ip route 10.10.0.120
Routing entry for 10.10.0.0/24
  Known via "eigrp 60", distance 90, metric 1536512, type internal
  Redistributing via eigrp 60, nhrp
  Last update from 172.21.254.11 on Tunnel21, 00:07:34 ago
  Routing Descriptor Blocks:
  * 172.21.254.11, from 172.21.254.11, 00:07:34 ago, via Tunnel21
      Route metric is 1536512, traffic share count is 1
      Total delay is 10020 microseconds, minimum bandwidth is 2000 Kbit
      Reliability 255/255, minimum MTU 1400 bytes
      Loading 1/255, Hops 2
```

Tráfico dirigido al HUB2 SCZ
172.31.254.11 Entel
172.21.254.11 Tigo

Tráfico dirigido al HUB2 SCZ
Redes 10.7.x.x, 10.10.x.x
Prioridad Tunel Tigo

Para el rollback, se deshabilitaron las Vlan's Productivas en el Sitio Alterno SCZ (vlan 15, 32, 40, 70, 80).
Se encendieron los Routers WAN de LPZ.
Se validó que las regionales retomaron comunicación con la Central LPZ.

En conclusión, las pruebas de comunicación resultaron exitosas y la plataforma estaría lista.

Saludos.

Juan Carlos Gonzales.
Representante de Servicios Networking
Teléfono: (591-2) 211-1920 Int. - Cel. 766-60800

Calle Rosendo Gutiérrez # 727 | La Paz- Bolivia Telf. Fax Server: (591-2) 211-1920 Int. 2298

From: Juan Carlos Gonzales/DATEC
To: Hugo Duran <hduran@bancosol.com.bo>
Cc: Franklin Arraya <Farraya@bancosol.com.bo>, "Armando Medrano" <amedrano@bancosol.com.bo>, Boris Barrenechea <bbarrenechea@datec.com.bo>, Carlos Laura <CLaura@datec.com.bo>, Francisco Guzman <FGuzman@datec.com.bo>, Borys Espada/DATEC@DOMINO
Date: 14/01/2015 09:06 a. m.
Subject: RE: RV: Sitio Alterno SCZ

Estimado Hugo,

Adjunto documento con las actividades a realizar en las pruebas de comunicaciones, favor tu revisión. Según tu requerimiento se realizarían 3 pruebas estos días:

- Viernes 15/ 9:00 AM - Prueba aislada del balanceo Web Citrix Cisco.
- Sábado 16/ 7:00 AM - Prueba controlada del balanceo Web Citrix Cisco con Servidores productivos de La Paz.
- Domingo 17/ 7:00 AM - Prueba controlada del HUB DMVPN Secundario SCZ y conectividad hacia el Sitio Alterno.

Las personas que estarán presentes por Datec son:

LPZ: Juan Carlos Gonzales Solares - CI: 4759882 L.P.
SCZ: Francisco Guzmán - CI: 4741654 L.P.

[anexo Sitio Alterno BancoSol - Pruebas de Comunicaciones.pdf eliminado por Juan Carlos Gonzales/DATEC]

Saludos,

Juan Carlos Gonzales.
Representante de Servicios Networking
Teléfono: (591-2) 211-1920 Int. - Cel. 765-60800

Calle Rosendo Gutiérrez # 727 | La Paz- Bolivia Telf. Fax Server: (591-2) 211-1920 Int. 2298