FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

DESARROLLO DE UN MODELO DE IMPLEMENTACIÓN DE REDES PRIVADAS VIRTUALES MULTIPUNTO DINÁMICAS (DMVPN) PARA PEQUEÑAS Y MEDIANAS EMPRESAS (PYMES).

"Trabajo de titulación presentado en conformidad a los requisitos establecidos para obtener el título de Ingeniero en Redes y Telecomunicaciones"

Profeso Guía

Ing. Jorge Narvaez

Autor

Edison Santiago Tituaña Quilumba

Año

2015

DECLARACIÓN DEL PROFESOR GUIA

“Declaro haber dirigido este trabajo a través de las reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulen los trabajos de titulación”

……

Jorge Narvaez
Ingeniero en Electrónica y Redes de la Información
Master en Tecnologías de la Información y Comunicación aplicadas a la Educación
C.I. 1714566849

DECLARACIÓN DEL ESTUDIANTE

“Declaro que este trabajo es original y de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

……

Edison Santiago Tituaña Quilumba

CI: 1721104931

AGRADECIMIENTOS

A Dios que me ha regalado una vocación que me gusta y por poner a las personas adecuadas en mi camino para llegar a este logro.

A mis padres María Quilumba y Pedro Tituaña que con su impulso y sus ánimos me han ayudado a seguir adelante.

A mis hermanos, a mi novia y amigos que siempre me animaron y han sido un gran soporte en mi vida.

A mi profesor guía de tesis que con su experiencia y sabiduría me ha ayudado a la realización de este proyecto.

DEDICATORIA

A Dios por su apoyo incondicional durante mi vida y a nivel profesional.
A mis padres por ser unas personas ejemplares y guías en mi camino.

Aquellas personas que contribuyeron de forma especial durante este proceso de formación, maestros, tutor, amigos, compañeros y mi novia, que me brindaron sus conocimientos para alcanzar mi meta propuesta.

RESUMEN

Propuesta de Diseño de una red segura para envío y recepción de información orientada a empresas PYMES, empleando la tecnología DMVPN a través de una infraestructura de un proveedor de servicio de Internet (ISP).

ABSTRACT

Proposed design of a secure network for sending and receiving of information oriented to the Pymes, employing the DMVPN technology through an infrastructure of a provider of Internet (ISP).

INDICE

Introducción

Descripción de la Realidad del problema

El mundo de la tecnología, por así decirlo, se ha tornado tan importante que cada usuario sin importar su ubicación geográfica necesita estar conectado a la red, bien sea esta privada o pública, en el último caso tenemos como ejemplo el despliegue de nuevas tecnologías que han sido promovidos por la Corporación Nacional de Telecomunicaciones, CNT, para dar servicios 4G con el fin de proporcionar conectividad no sólo telefónica, sino también de datos e Internet de alta velocidad. “Doris González, Gerente de Ingeniería e Implementación en la CNT, dió a conocer que la empresa de telecomunicaciones se ha preocupado en realizar grandes inversiones para implementar la red 3G HSPA+, que permite llegar a velocidades de hasta 21 Mbps” (teleamazonas.com, 2012).

Todo converge a tener administración y control sobre los dispositivos electrónicos y mantener contacto con cualquier parte del mundo sin tener que movilizarse. En unos inicios el escritorio remoto fue la gran solución que prometía quedarse, sin embargo fueron apareciendo más soluciones que hacían lo mismo e integraban mayor número de características, este es el caso de las VPNs utilizadas en la actualidad, con esta propuesta innovadora es posible conectarse sin tener que desplazarse al lugar de trabajo, a otra ciudad o sector, este es el método utilizado por excelencia.

Sin embargo cuando el número de usuarios aumenta e incluso la necesidad sea de unir dos redes LAN o más entre sí, las VPNs tradicionales presentan dificultad, esto no quiere decir que no se pueda realizar, al contrario se lo podría realizar pero sería una solución costosa y si se trata de una empresa mediana esto no es factible, incluyendo la difícil tarea de administración y complejidad al momento de habilitar una nueva conexión.

Por estas razones la necesidad de utilizar una solución diferente de VPN, que plantee realizar conexiones seguras entre las redes LAN, fáciles de administrar y sobre todo seguras y escalables.

El presente proyecto tiene como finalidad presentar una solución diferente a las VPNs tradicionales, que presentan problemas al momento de agregar más conexiones a la red creada, empleando tecnologías más seguras y fiables que permitarán una comunicación efectiva.

Formulación de Problema.

El problema radica en que el servicio de interconexión de dos oficinas o más ubicadas en lugares geográficamente distintos requiere mayor inversión tanto en recursos humanos, infraestructura y financiamiento, por ejemplo, en un escenario propuesto para conectar dos oficinas localizadas en la ciudad de Quito, una al norte de la ciudad y la otra al sur respectivamente, se debe desplegar medios físicos que permitan esta conexión, puede ser una solución que se utilice Fibra Óptica como medio de transmisión, no obstante este resultaría una inversión elevada a largo plazo, puesto que, tendríamos que adquirir la fibra óptica que además de ser cara no existe una fábrica en Ecuador y el proveedor debería importarla de países productores, sin mencionar que se debe instalar en la postería de la ciudad lo que implica permisos, además involucra desplegar personal que realice la actividad, y entre otras cosas que serían necesarias. Otra alternativa sería implementar un enlace de última milla Radial que comparado a la Fibra Óptica oferta precios más atractivos, pero este tipo de tecnología requiere que se tenga línea de vista entre ambos puntos lo que es sumamente complicado por la variedad de alturas que se presentan en todo el país, además de las distancias que serían considerablemente extensas, como se conoce toda empresa se proyecta a expandirse regionalmente y algo fundamental, los PYMES en el país apuntan a Empresas que aún carecen de solidez económicas por ello las tecnologías ya

mencionadas, no resultan ser tan favorables y se opta por soluciones más viables.

Se plantea el uso de los proveedores de Internet (ISP) o carriers que ya constan con una red desplegada y disponen de las tecnologías de acceso al medio dependiendo de donde se requiera, ahora bien, los ISP o carriers dan una solución más rápida al usar su red lo que se conoce como enlaces dedicados, y por aquello obtienen su comisión que resulta igual de elevado.

Como solución alternativa aparecen las VPNs que permiten entablar conexiones utilizando la red pública o Internet, en relación a los enlaces dedicados tiene un costo menor. Las redes privadas virtuales (VPN) permiten tener una extensión de la red LAN, he incluso usuarios remotos, es decir, lógicamente se tiene una sola red que utiliza como medio de transmisión la red de Internet.

Las VPNs presentan las siguientes limitaciones:

- Requiere una comprensión detallada de conceptos de seguridad de redes de información y minuciosa instalación y configuración.
- Problema de compatibilidad.
- IPSec es un protocolo complejo, debido a que tiene muchas características y opciones, lo que implica una configuración complicada.
- Para acceder a una VPN IPsec, se requiere de la instalación de un software cliente, que quizá no sea soportado o compatible por el sistema operativo de los equipos remotos.

Las redes privadas virtuales multipunto dinámicas (DMVPNs) presentadas en el presente proyecto de titulación son una versión más completa de las VPNs tradicionales, resolviendo las vulnerabilidades que estas últimas mantienen y añaden características importantes a la hora de decidir la forma de transmitir información en una red.

Entre las principales características de DMVPN tenemos:

- Reducción de la configuración del enrutador HUB.

- Iniciación automática de encriptación de IPsec.
- Creación dinámica de los túneles spoke a spoke.
- DMVPN integra reenvío de enrutamiento virtual (VRF).
- Soporte para los routers Spokes dinámicamente dirigidos.

Prognosis.

Si no se realiza el presente proyecto de titulación no se dispondría de información sobre el correcto funcionamiento de la tecnología DMVPN para PYMES en Ecuador, adicionalmente, este proyecto puede servir como referencia para cualquier empresa sea esta pequeña, mediana he incluso grande que requiera este tipo de solución y tenga la base para la implementación de esta tecnología en su infraestructura.

Objetivo General.

- Desarrollar un modelo de implementación de redes privadas virtuales multipunto dinámicas para pequeñas y medianas empresas.

Objetivos específicos.

- Definir los requerimientos y procedimientos necesarios para implementar DMVPN.
- Verificar el correcto funcionamiento de la tecnología implementada como solución.
- Implementar el modelo en un ambiente de laboratorio.

Justificación de la Investigación.

Se promueve el desarrollo del presente proyecto de titulación debido al aumento del sector empresarial en el país, por esta razón es necesario buscar soluciones alternativas para interconectar todas estas empresas, ayudando de esta forma al crecimiento económico del Ecuador. La elaboración de este proyecto confirmará el correcto y eficiente funcionamiento de esta tecnología que en comparación a otras soluciones tiene mayores beneficios. Dmvpn va a interconectar los diferentes puntos de las empresas entre sí, resultando de esta conexión una red completamente mallada, permitirá enviar información utilizando la red pública de una forma segura, de modo que los datos enviados sean resguardados de cualquier tipo de ataque que se pueda propiciar en la red de Internet.

Alcance.

Este proyecto se enfocará en realizar el estudio sobre las redes privadas del sector empresarial y sus sucursales en sitios remotos y de la conexión utilizando la tecnología DMVPN mediante una topología Hub-and-spoke basada en el protocolo IPsec y TCP-IP, se analizará la situación actual de esta tecnología y se realizará un modelo de implementación teórico con el fin comprobarla y que sirva de guía para futuras implementaciones.

Se implementará además el modelo en un escenario de pruebas con cuatro routers; los resultados obtenidos se usarán para determinar los requerimientos y procesos necesarios para interconectar los sitios remotos de las empresas con esta tecnología.

Limitaciones del Estudio.

El presente estudio y desarrollo de modelo se enfocará en la tecnología DMVPN. Se utiliza el protocolo de resolución del siguiente salto NHRP, el protocolo IPsec y el protocolo mGRE. El modelo estará basado en enrutadores Cisco, las pruebas a realizarse consisten en el levantamiento de interconexiones entre los distintos puntos, que serán simulados por enrutadores y la nube de Internet que está configurada y de igual forma usará enrutadores Cisco.

No se realizará pruebas de paso de información de alguna aplicación en común, solo se verificará que las conexiones entre los distintos sitios se entablen y el proceso de convergencia de la red DMVPN funcione correctamente.

Viabilidad del proyecto.

El proyecto es viable en recursos humanos y recursos económicos, se realizará el estudio en el tiempo esperado debido a que se dispone de todo lo necesario para implementar y demostrar el correcto funcionamiento del mismo, para lo antes mencionado se cuenta con apoyo de la Universidad de Las Américas que va a facilitar el uso de los equipos de comunicaciones que actualmente tiene en sus laboratorios.

La metodología utilizada en el proyecto es inductiva pues se extrae conclusiones generales, resultado de la acumulación de datos particulares y apoyada de la metodología experimental puesto que se experimentará (emulación de una red DMVPN), y se obtendrá el nivel de factibilidad dando así las respuestas correspondientes a los objetivos del proyecto.

Cabe mencionar que se adquirieron los conocimientos previos y necesarios en todos estos años de Universidad, para elaborar correctamente las

configuraciones e investigaciones necesarias para el proyecto conforme a lo estipulado en el presente reglamento.

1. Marco Teórico.

1.1. Antecedentes.

Para la implementación del proyecto de Grado **Desarrollo de un modelo de implementación de redes privadas virtuales multipunto dinámicas (DMVPN) para pequeñas y medianas empresas (PYMES)** se requiere de conocimientos del Modelo OSI, Protocolos de Enrutamiento, Encriptación y Autenticación para establecer la seguridad en la información, así como las PYMES.

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

1.1.1. Definición de las PYMES.

Las PYMES son llamadas al conjunto de pequeñas y medianas empresas que de acuerdo a su número de ventas, importe de capital, número de empleados y su nivel de producción o activos reflejan características oportunas de este tipo de entidades económicas.

La real academia española define a las Pymes como “Empresa mercantil, industrial, etc., compuesta por un número reducido de trabajadores, y con un moderado volumen de facturación” (Real academia Española, 2014).

1.1.1.1. Las Pymes en el Ecuador y su Distribución Sectorial.

Basándonos en el estudio Ranking PYMES realizado por Ekos Negocios (2013, pp. 28), en Octubre del 2013, indica que Ecuador cuenta con más de 16 000 Pymes.

A continuación las estadísticas realizadas según el estudio.

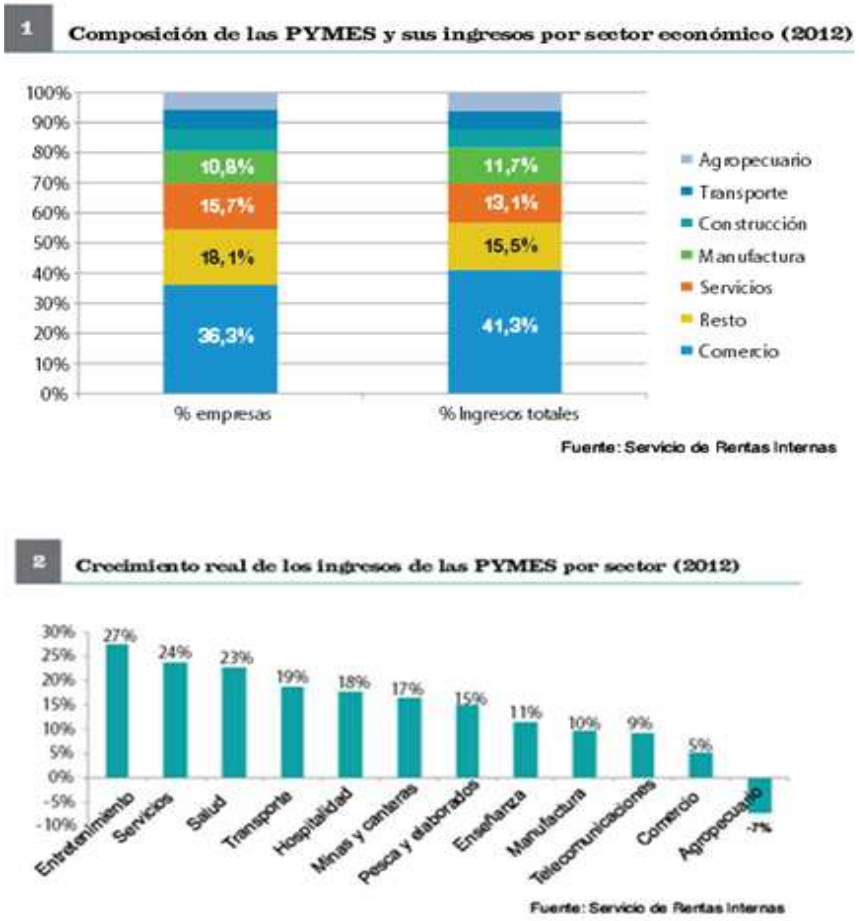


Figura 1. Composición y Crecimiento real de ingresos de las PYMES por el sector

Tomado de Ekonegocios, 2013, p. 30.

Según las estadísticas de EkosNegocios realizada a las Pymes, estas “tuvieron un año 2012 favorable en lo que a nivel de ingresos se refiere y existe una importante concentración en el comercio, servicios y manufactura. El desempeño de la economía en su conjunto incide de manera directa en los

resultados de estas empresas, no obstante los desafíos de las Pymes siguen siendo muy importantes y también afectan los ingresos. De esta manera, la necesidad de inversión y acceso al crédito siguen siendo fundamentales" (EkosNegocios, 2013, p. 33). Las estadísticas son claras y mencionan que aún es una falencia la parte de inversión en tecnología en el país, debido a ello se debe aprovechar al máximo los recursos que estén implementadas en las PYMES.

"Las Pymes deben dirigir sus operaciones hacia actividades que les permita capitalizarse a través del cambio tecnológico y la asociatividad" (EkosNegocios, 2013, p.34).

1.1.2. Fundamentos Teóricos

1.1.2.1. ¿Qué es un Protocolo?

El usuario de un dispositivo que procesa de información (computadora, portátil, celulares), automáticamente se convierte en un cliente al intentar tener acceso a un Web Site (Sitio de Internet) así como, a través de una línea telefónica, podría requerir información sobre un servicio o un producto a un proveedor, a quien se le denomina como un servidor. Al método de ponerse de acuerdo en cuanto al modo de envío y recepción de un artículo o servicio adquirido telefónicamente, se le denomina protocolo.

Así, en términos técnicos y orientados a las Telecomunicaciones, un protocolo es un "conjunto de normas y procedimientos útiles para la transmisión de datos, conocido por el emisor y el receptor" (wordreference, s.f).

1.1.2.1.1. Protocolos de Internet

El Internet es el resultado de miles de redes con tecnologías distintas, en apariencia esta tecnología es uniforme, pues ese fue el trato entre la gran

variedad de redes que conforman el Internet, que para poder transmitir información sea utilizado el lenguaje común denominado protocolo TCP/IP (Transmisión Control Protocol/Internet Protocol).

1.1.2.1.1.1. Protocolo TCP/IP

> "Los protocolos IP (Protocolo de Internet) y TCP (Protocolo de Control de Transmisión) se originaron a principios de 1980 y fueron adoptados por la red ARPANET en 1983, que estaba integrada por cientos de computadoras de universidades, centros de investigación militar y algunas empresas.
>
> El e-mail (electronic mail) fue el servicio más comúnmente utilizado entonces, mientras que el sistema operativo más empleado era UNIX, en su versión BSD UNIX, desarrollada por la Universidad de California. Fue a mediados de los ochenta cuando fue creado el protocolo TCP/IP con la finalidad de contar con un lenguaje común a todas las computadoras conectadas a Internet, ya con la unión de las redes ARPANET, CSNET y MILNET" (Estrada, 2004, p.4).

Se podría definir que el protocolo TCP/IP son las reglas que hacen posible la conexión de computadoras de marcas y tecnologías diferentes.

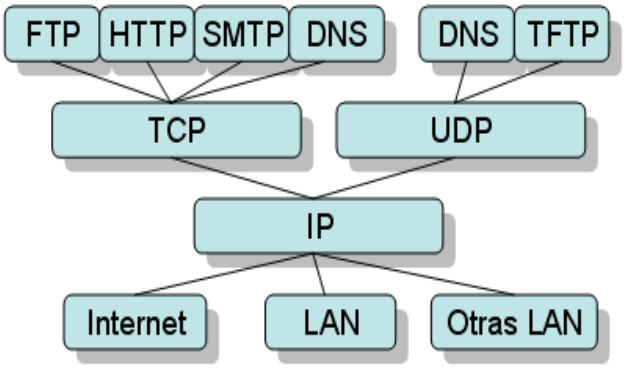


Figura 2. Protocolos de Internet
Tomado de Garcia, 2012, p.11.

TCP e IP son los protocolos más trascendentales e importantes en la transmisión de datos. Se trata de un conjunto de protocolos que conforman la arquitectura de cinco niveles o capas:

1. **Aplicación.**

   “Están contenidos los protocolos SMTP, para el correo electrónico; FTP, para las transferencia de archivos; TELNET, para la conexión remota, y HTTP, Hypertext Transfer Protocol” (Estrada, 2004, p. 4).

2. **Transporte**

   Esta parte de la estructura comprende a los protocolos TCP y UDP, y su función es el manejo y el transporte de los datos o paquetes.

3. **Internet**

   Este tiene como tarea el envio de paquetes de información y se ubica en el nivel de red.

4. **Físico**

   Este es el encargado de los bits (1 y 0) y de la transmisión del mismo, como referencia se podría decir que es análogo al nivel físico del modelo OSI.

   .

5. **Red**

   Este último corresponde a la interfaz de red.

A continuación se muestra la arquitectura del protocolo:

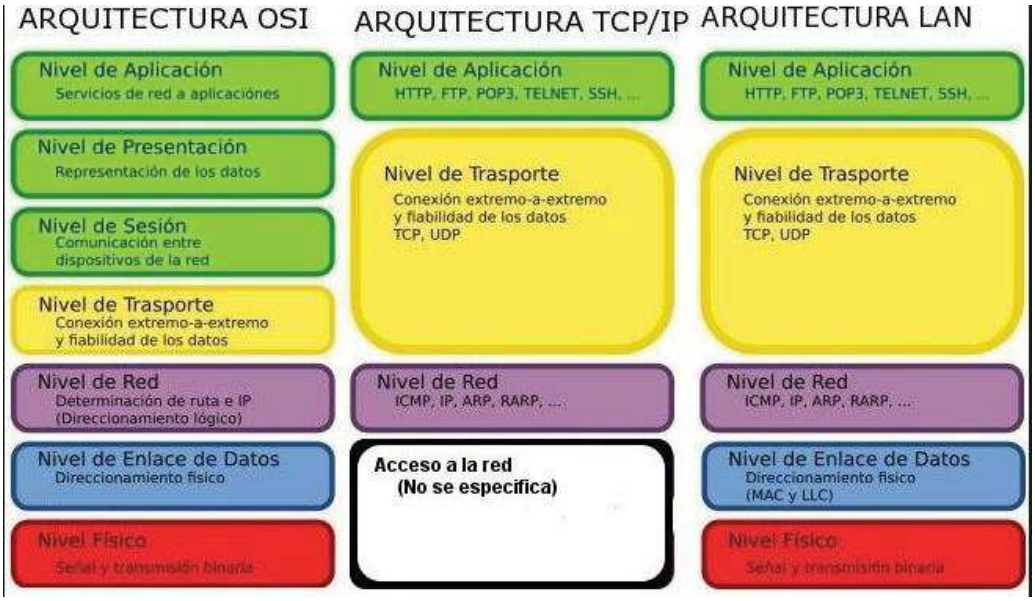


Figura 3. Diseño de Arquitectura Modelo OSI, Arquitectura TCP/IP, Arquitectura LAN.
Tomado de (bitacoraderedes.wordpress, s.f.)
https://bitacoraderedes.files.wordpress.com/2013/04/un.jpg

1.1.2.2 Definición de VPN

Se denomina a una VPN como una extensión más de una red LAN, que opera sobre una infraestructura de red de transmisión pública (Internet), mediante la creación de túneles privados que brindan seguridad de la información.

Explicado de una mejor manera una VPN es una conexión entre dos o más puntos utilizando como medio de transmisión el Internet, sin embargo, las VPNs se las puede utilizar en enlaces arrendados como, enlaces ATM, Frame Relay o redes digitales de servicios integrados ISDN, líneas digitales de abonados (xDSL), los diferentes ISPs utilizan las VPNs con otro tipo de enlaces como sobre la tecnología MPLs.

Cuando se utiliza las VPNs como tecnología para interconectar sitios geográficamente diferentes se puede obtener beneficios extras como lo es el

poder utilizar una red netamente pública para transportar datos internos, como es de conocimiento la nube llamada Internet tiene en sus entrañas diferentes tecnologías de transportes y así mismo dicha nube se la puede reemplazar por una nube ATM FR o MPLS (Multiprotocol Label Switching), sin embargo esta última sería tomada como una red interna por un proveedor de servicio pero para el cliente seguirá siendo una conexión publica.

1.1.2.2.1. Impacto de las VPNs en el sector Empresarial.

En la última década, el impacto de la tecnología, Internet y las telecomunicaciones ha generado que las empresas, tomando como referencia las PYMES, siendo en este proyecto nuestro escenario, modifiquen su forma de trabajar en el sector empresarial. La prioridad de las empresas es expandir su mercado, ello conlleva a nuevas sucursales, departamentos, ciudades pero a la vez inicia la búsqueda de un medio confiable, seguro, eficaz todo ello sobre un indicador importante como es el costo.

Los efectos que una VPN logre tener sobre una organización son dramáticos.

Las ventas pueden aumentarse al igual que el desarrollo y comercialización de productos, muchas estrategias de negocios son fortalecidas en una forma nunca antes posible.

Antes de la aparición de las soluciones basadas en VPN, la opción para crear este tipo de comunicaciones fueron costosas líneas dedicadas o circuitos Frame-Relay.

Al usar VPN’s el acceso a Internet es, por lo común, local y aún más económico que las conexiones dedicadas a Servidores de Acceso Remoto (Remote Access Ser-ver). El proyecto ha implementarse tiene como prioridad ejecutar una tecnología basada en la seguridad, confidencialidad y autenticidad de los usuarios locales como remotos al momento de transmitir y receptar información, tratando de optimizar al máximo sus recursos humanos, tecnológicos y económicos.

1.1.2.2.1.1. Desafío de las Empresas con las VPNS.

Según los estudios y diseño de redes virtuales privadas se enumeran cuatro los desafíos al implementar una solución de VPNS, y que las empresas deben tomar en consideración (Tejada, León y Astudillo, 2001, p.59).

- Seguridad de la informacion.
- Rendimiento de la Red.
- Posibilidad de escalabilidad.
- Administración Empresarial.

1.1.2.2.2. Arquitectura de las VPNS

Existen dos tipos Arquitectura de las VPNS, se detalla a continuación:

1.1.2.2.2.1 Acceso remoto.

Es la forma en que se puede acceder a los recursos de una determinada red privada y poder utilizar sus recursos como si estuviera en el interior de ella. La interacción que se logra entre sitios remotos conforme se usa el acceso remoto, aplicado a conceptos como teletrabajo, tele enseñanza, telemedicina o tele banca. Una VPN de acceso remoto se implementa entre los usuarios móviles, usuarios en casa, agencias remotas y la matriz o concentadores como se les denomina.

Durante los últimos años las soluciones disponibles para esta problemática han variado considerablemente. Un largo recorrido ha tenido que pasar para llegar a disponer de las soluciones que hoy en día se tiene, sin embargo, antes de poner en marcha una solución se debe tomar en cuenta aspectos como la red de comunicaciones que será utilizada, tipo de conectividad, velocidad de transmisión, el costo que involucra cada solución, seguridad, etc.

1.1.2.2.2.2. De Sitio a Sitio

1.1.2.2.2.2.1. Segmento interno

Este segmento de red es más reducido que el externo, como su nombre lo indica se trata de la parte interna de una red, esto también quiere decir que los protocolos que se encuentren corriendo dentro de este segmento de red dependerán de la administración del mismo, sin embargo también hablan el protocolo IP que es el mismo que hablan las redes del segmento externo aunque con otra mascara de subred.

1.1.2.2.2.2.2. Segmento externo (Internet)

Se trata del conjunto de sistemas autónomos (SA), cada uno de ellos administrador o con una autoridad propia y diferente entre ellas. Como base todos los SA utilizan el protocolo IP para realizar la comunicación entre los distintos sitios o hacia los distintos sitios, esto no significa que los SA tengan los mismos protocolos de red corriendo en su infraestructura, sin embargo, se usan protocolos comunes o estándares para permitir la comunicación entre ellos y hacer posible la comunicación hacia cualquier lugar en el mundo.

1.1.2.2.3. Requisitos una VPN.

Las soluciones de VPN se presentan tanto en software como en hardware con complementos adicionales que garanticen que el envío de información se realice de forma segura. Para lograr la funcionalidad de las redes privadas y seguras se deben cumplir la disponibilidad, compatibilidad, seguridad, interoperabilidad, confiabilidad y escalabilidad.

1.1.2.2.4. Seguridad en las VPN

Para la implementación de VPN’s sobre el Internet, debemos tener claros dos conceptos fundamentales a tomar en consideración: seguridad y rendimiento.

El Protocolo de Control de Transmisión y Protocolo de Internet (TCP/IP) y el Internet no fueron creados desde un inicio con estas consideraciones porque el número de usuarios y las aplicaciones iniciales no requerían fuertes y extremas medidas de seguridad o un rendimiento garantizado como lo es en la actualidad.

La vulnerabilidad es muy elevada cuando un paquete es enviado hacia su destino en una red interna y aumenta más en una red pública. El tráfico para que sea apreciado como seguro al momento de ser transportado por una red pública como Internet, este debe cumplir con principios básicos como:

1.1.2.2.4.1. Autenticación y autorización.

Cada operación que se realice debe ser controlada y conocer quién esté haciendo dicha operación sea quién dice ser mediante su autenticación, y de este modo también controlar mejor las acciones que se realicen mediante la autorización que se otorgue a cada usuario.

1.1.2.2.4.2. No repudio.

En cuánto un usuario es autenticado y cuenta con las autorizaciones respectivas, realizará tareas y estas deben poder ser garantizadas de modo que no exista repudio.

1.1.2.2.4.3. Integridad.

Los datos enviados y recibidos por ningún motivo deberán ser alterados durante el trayecto en que son transportados hasta llegar a su destino, ya sea por otras personas o por fallas que pueden existir en la red.

1.1.2.2.4.4. Confidencialidad.

La información en el camino no debe ser retenida o accedida por personal no autorizado, para ello se usan métodos de encriptación para evitar que en el paso por una red como el Internet los datos sean interceptados, y de ocurrir esto último los datos no sean legibles.

1.1.2.2.5. Criptografía.

Un número grande de personas tiene acceso a las redes que son recursos compartidos, y mediante los diferentes aplicativos que existen se extrae toda la información deseada. Todas estas personas tienen diferentes propósitos para la información que adquieren, sin embargo no toda la información que transita por las redes debe ser pública, siempre existirán casos en que la información es confidencial y muy delicada, de modo que estos datos requieren que se los proteja por algún medio.

Una red se puede llamar segura si el nivel de protección de la información que por esta transita es alto, esto se logra con combinaciones complejas de protocolos y algoritmos, de esto nace la criptografía.

La criptografía pretende mediante el procedimiento de cifrado que el contenido de un determinado mensaje el cual se requiere ocultar sea transcrito en números, letras o símbolos de acorde con una clave.

1.1.2.3. La DMVPN

La creación de DMVPN se sustenta en permitir la interconexión entre las distintas sedes de una empresa o compañía, manteniendo el concepto de una red completamente mallada. Es decir que exista conectividad no solo entre las sucursales y la matriz sino también entre estas sucursales, además como un agregado el tráfico no necesariamente transita por la matriz. Como nueva tecnología esta entra a competir con las tecnologías existentes por lo que las características adicionales y el valor agregado harán la diferencia. Cisco Systems (2009, p.3) muestra esta tecnología como una solución de seguridad basada en Software de Cisco IOS para la construcción de VPNs empresariales escalables que soportan aplicaciones distribuidas como voz y video.

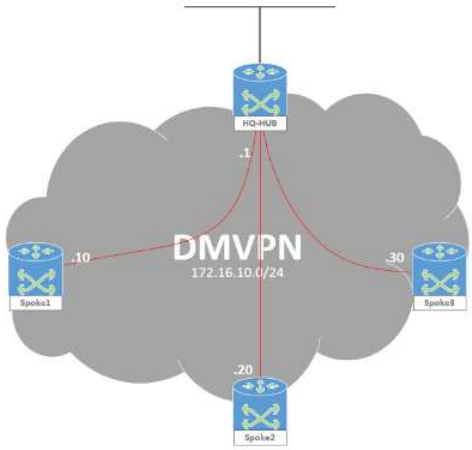


Figura 4. Diseño de una red DMVPN
Tomado de (Networkknerd.blogspot.com, 2014.)
http://networkknerd.blogspot.com/search?q=dmvpn

Cisco DMVPN es ampliamente utilizado para interconectar sucursales empresariales, tele trabajadores, y conectividad extranet.

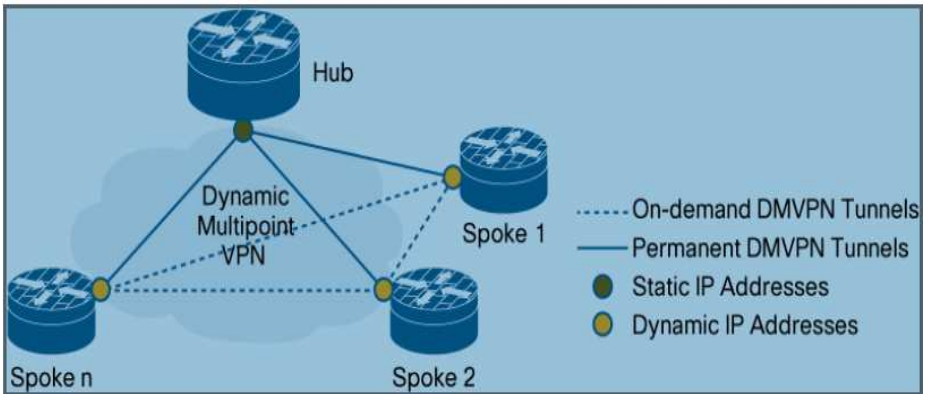


Figura 5. Conexiones DMVPN con IPs estáticas y dinámicas con túneles bajo de manda y permanentes.
Tomado de Cisco System, 2013, p.3.

Cisco DMVPN puede implementarse en conjunto con Cisco IOS Firewall y Cisco IOS IPS, así como con calidad de servicio (QoS), IP Multicast, split

tunneling y enrutamiento basado en mecanismos de failover. A gran escala, son posibles despliegues Cisco DMVPN de alta disponibilidad mediante el equilibrio de carga entre varios concentradores Cisco DMVPN.

1.1.2.3.1. Componentes de diseño.

Como Cisco (2008, p.11) lo indica, las VPNs dan una alternativa a las tecnologías WAN tradicionales como las líneas arrendadas, Frame Relay, y ATM. La tecnología VPN permite que las WANs privadas existan en una red de transporte público tal como lo es el Internet. Las VPNs LAN a LAN son implementadas principalmente para conectar las locaciones de las oficinas con la central (o entre sitios) de una empresa.

Los clientes empresariales requieren servicios tradicionales de WAN privadas, como soportar multiprotocolos, alta disponibilidad, escalabilidad, y seguridad. Estos últimos no están alejados de las redres privadas virtuales y son también requerimientos para las mismas.

Las VPNs pueden en su mayoría cumplir con estos requerimientos más ventajosamente y con mayor flexibilidad que los servicios WAN privados.

Los siguientes son componentes clave de este diseño DMVPN:

- Router Cisco de gama alta que actúan como dispositivos de terminación de cabecera VPN en la central (dispositivo de cabecera).

- Router Cisco de acceso VPN que actúan como dispositivos terminales VPN en las localidades de oficinas remotas (dispositivos remotos).

- DMVPN cliente servidor para realizar interconexiones sucursal – central.

- DMVPN cliente – cliente para realizar la interconexión entre sucursales.

- Servicio de Internet (ISP) que sirve como medio de interconexión WAN.

Los routers Cisco VPN son una buena opción para implementaciones VPN, ya que pueden ofrecer cualquier requerimiento tradicional que provee una red de línea privada. Estos requerimientos incluyen que se soporte multicast, tráfico sensible a latencia y protocolos de ruteo (Cisco System, 2007, p. 19).

“Una nube DMVPN es un grupo de routers que se configura con una interface multipunto GRE (mGRE) o interfaces GRE punto a punto (P2P) (o la combinación de ambos) que comparten el mismo direccionamiento IP. Proporcionan alta disponibilidad con el uso adicional de un segundo concentrador, que puede estar en la misma subred DMVPN del primer router concentrador. Esto se conoce comúnmente como una sola topología de nube DMVPN. El segundo router concentrador solamente puede dar servicio en su propia subred DMVPN” (Cisco System, 2008, pp. 11-13).

1.1.2.3.2. Topología de Diseño.

En un diseño DMVPN, se pueden implementar las siguientes topologías:

- Nube DMVPN doble con concentrador doble.

- Nube DMVPN doble con un concentrador.

Nota: no hay limitación en el uso de HUBs en ninguna de las dos topologías mencionadas.

En ambas topologías al menos dos concentradores o terminales de cabecera son recomendados para redundancia.

1.1.2.3.3. Ventajas de Dynamic Multipoint VPN (DMVPN).

Según el artículo emitido por Cisco (2009, p. 3), Dmvpn nos presenta las ventajas.
A continuación se detalla:

- Reducción de la configuración del router de eje de conexión

- “Para cada router Spoke hay un bloque separado de las líneas de configuración en el router HUB de conexión que definen las características de la correspondencia de criptografía, y la lista de acceso de cifrado, a la interfaz de túnel GRE. Esta característica permite que los usuarios configuren una sola interfaz de túnel MGRE, un solo perfil de ipsec, y ninguna Lista de acceso crypto adicional en el router HUB de conexión para manejar todos los routeres remotos. Así, los tamaños de la configuración en el router de eje de conexión siguen siendo constantes incluso si agregan mas enrutadores Spoke a la red” (Cisco, 2009, p .4).

.

La arquitectura DMVPN puede agrupar mucho spokes en una sola interfaz de múltiples puntos GRE, quitando la necesidad de una comprobación distinta o la interfaz lógica para cada spoke en una instalación nativa del IPSec.

- Iniciación automática de encripción de IPsec.

  “El GRE tiene las direcciones de origen y de destino del par configuradas o resueltas con el NHRP. Así, esta característica permite que el IPSec sea accionado inmediatamente para la tunelización GRE de punto a punto o cuando resuelven a la dirección de peer GRE vía el NHRP para el túnel GRE de múltiples puntos.” (Cisco, 2009, p .5).

- Soporte para los routeres radiales dinámicamente dirigidos

  “Al usar las redes VPN del Punto a punto GRE y del hub-and-spoke del IPSec, la dirección IP de la interfaz física de los routeres radiales debe ser sabida al configurar el router de eje de conexión porque la dirección IP se debe configurar como la dirección destino del túnel GRE. Esta característica permite que los routeres radiales tengan IP Addresses dinámicos de la interfaz física (comunes para el cable y las conexiones DSL). Cuando viene el router radial en línea, enviará los paquetes de inscripción al router de eje de conexión: dentro de estos paquetes de

inscripción, es la dirección IP actual de la interfaz física de este spoke." (Cisco, 2009, pp .4-5).

- Creación dinámica para los túneles del spoke al spoke

- "Esta característica elimina la necesidad de la configuración del spoke al spoke para los túneles directos. Cuando un router radial quiere transmitir un paquete a otro router radial, puede ahora utilizar el NHRP para determinar dinámicamente el direccionamiento de destino requerido del router radial de la blanco. (El router de eje de conexión actúa como el servidor NHRP, manejando el pedido el router radial de la fuente.) Los dos routeres radiales crean dinámicamente un túnel IPsec entre ellos así que los datos pueden ser transferidos directamente." (Cisco, 2009, p .4).

1.1.2.3.4. Campos de Aplicación de la Tecnología DMVPN.

Cisco DMVPN es la solución preferida para organizaciones que requieren conectividad WAN cifrada entre sitios remotos. Los factores incluyen el uso de Internet para reemplazar o proporcionar respaldo de líneas alquiladas privadas y enlaces Frame Relay y presiones reglamentarias que requieren encriptación de enlaces privados WAN basada en el costo.

1.1.2.3.4.1 Empresas grandes y medianas en la tecnología DMVPN.

En el sector empresarial como Finanza, seguros, ventas al por menor, numerosos sitios suelen estar conectados a la matriz de la corporación. Cisco DMVPN permite que estos sitios se conecten utilizando una red pública como lo es el Internet, brindando privacidad e integridad a los datos transmitidos mientras mantiene los requerimientos de desempeño que demandan las aplicaciones críticas de de los negocios. Aplicaciones críticas como cajeros de bancos ATM y máquinas de puntos de ventas (POS) envían su tráfico sobre estas conexiones.

1.1.2.3.4.2. Oficinas empresariales pequeñas o de hogar (Enterprise small office/home office (SOHO)) en la tecnología DMVPN:

Cisco DMVPN puede soportar tanto tráfico de voz como de datos gracias a que puede utilizar QoS perfecto para empleados que requieran acceder a la red desde un ambiente SOHO.

1.1.2.3.4.3. Extranet empresarial con las DMVPN

Con frecuencia las grandes empresas requieren conectividad hacia la mayoría de sus socios de negocios. DMVPN puede ser usado para conectar empresas y varios sitios de socios y transportar tráfico seguro

1.1.2.3.4.4. Enlaces WAN de respaldo con la tecnología DMVPN.

DMVPN puede ser usado como una solución para en enlace backup para redes WAN privadas, permitiendo que las sedes remotas se conecten de forma segura a la matriz utilizando enlaces de Internet.

1.1.2.3.5. Proveedor de servicio VPN.

Cisco DMVPN permite a los proveedores de servicio ofrecer servicios VPN gestionados. El Tráfico de múltiples clientes puede ser agregado en un router de borde de un único proveedor, y mantenerlos aislados usando características como el reenvió de enrutamiento virtual (Virtual Routing Forward).

1.1.2.3.6. Características DMVPN

Enseguida se detalla las características de la tecnología DMPVN:

Tabla 1. Caracteristicas y Benefecios de DMVPN.

Feature	Descripción y beneficio
Enrutamiento dinámico a través de VPN	● Permite que tablas de enrutamiento IP sean distribuidas de forma segura entre el sitio remoto y la sede central corporativa sobre túneles encriptados. Permite mayor accesibilidad sin necesidad de definir manualmente las rutas permitidas ● Soporta protocolos de enrutamiento como: Protocolo de enrutamiento de puerta de enlace interior mejorado (EIGRP), Protocolo del primer camino más corto abierto (OSPF), Protoclo de puerta de enlace de borde (BGP).
Reduce la configuración de la cabecera (Overhead)	● DMVPN elimina la necesidad de configurar los mapas criptográficos vinculados a la interfaz física, simplificando drásticamente el número de líneas de configuración requerida para una implementación de VPN (por ejemplo, para una implementación de 1000 sitios, DMVPN reduce el esfuerzo de configuración en el hub de 3900 líneas a 13 líneas). ● Añadir nuevos sitios remotos o conexiones no requiere de cambios en el concentrador. ● Simplifica la configuración de la división de túnel. Centraliza los cambios de configuración en el concentrador de modo que sea este el que controle el comportamiento de la división del túnel. Lo que no pasa en el IPsec tradicional que todos los remotos necesitan ser modificados.
Implementación sin interacción (Zero-Touch Deployment)	● Cisco DMVPN puede desplegarse en modelos de implementación sin interacción mediante el fácil despliegue de dispositivos seguros para el aprovisionamiento de dispositivos de seguridad basados en PKI. Los dispositivos pueden ser arrancados remotamente, evitando la necesidad de extensas operaciones para la puesta en marcha.
Túneles sitio a sitio dinámicos (Dynamic Spoke-to-Spoke Tunnels)	● Los túneles directos entre sedes eliminan la necesidad que el trafico generado entre ellos atraviese por el concentrador o matriz. ● Reduce la latencia para despliegues de voz sobre IP (VoIP) sobre DMVPN y mejora el rendimiento efectivo del router principal. ● Los túneles son creados dinámicamente cuando

	se requiere y finalizada la conexión son eliminados, permitiendo que el sistema escale de mejor manera (Es decir que las sedes más pequeñas pueden participar en la malla completa virtual).
Direccionamiento dinámico para los Routers de las sedes remotas.	● los equipos de las sedes remotas pueden usar direcciones IP dinámicas , un requisito frecuente para las conexiones a Internet por cable y el DSL
Network Address Translation (NAT) Traversal	● DMVPN soporta routers de las sedes remotas con NAT o detrás de dispositivos NAT dinámicos, Habilitando mejor seguridad para las subredes de la sucursal.
Soporta IP Multicast	● DMVPN soporta trafico IPMulticast (entre la sede matriz y la sucursal); el IPsec nativo soporta solamente IP Unicast. Esto proporciona una distribución eficiente y escalable del tráfico punto a multipunto y multipunto -multipunto.
Soporta QoS	DMVPN de Cisco es compatible con los siguientes mecanismos avanzados de QoS. ● Asignacion de trafico en las interfaces del Hub por Spoke o por grupo de Spokes. ● Politicas de Qos en conexiones Hub-to-spoke and spoke-to-spoke. ● Políticas de QoS dinámico en el que las plantillas de QoS se unen automáticamente a los túneles que vayan surgiendo. ● Politicas de Qos por Spoke, permite diferenciar a cada Spoke, y protejer la red de ser invadido de ancho de banda de Spokes hambrientos.
Alta disponibilidad	● Cisco DMVPN permitel enrutamiento basado en conmutación por error. ● Enlaces WAN dual y redundancia hub proporcionan una mayor disponibilidad. DMVPN soporta diseños de doble HUB, donde cada Spoke disponga de dos concentradores, proporcionando failover rápido. ● Topologías de concentrador mulitiple permiten ininterrumpida comunicación Spoke a Apoke en el caso de cualquier fallo sobre el Hub principal.
Escalabilidad	● DMVPN escala a miles de Spokes que utilizan el equilibrio de carga del servidor (SLB). El cifrado se puede integrar en el dispositivo del SLB o distribuido a los routers VPN cabecera reservados. Los túneles equilibran la carga sobre los HUB

	disponibles. ● El rendimiento se puede escalar progresivamente añadiendo HUBs. . ● Despliegues de hubs jerarquicos permiten una escalabilidad mejorada.
Manejabilidad	● Soporta manejabilidad, se proporciona a través de IPsec (incluyendo VRF-consciente IPsec) MIB, PNDH MIB, y la interfaz de línea de comandos (CLI).
VRF Awareness	● DMVPN VRF desplegado en los HUB de borde del proveedor permite la segregación de tráfico de clientes. .
Soporta el protocolo multiple de intercambio de etiquetas (MPLS).	● Redes MPLS pueden ser encriptaas sobre tuneles DMVPN

Tomado de Cisco System, 2009, p. 4.

1.1.2.3.7. Topologías de Diseño DMVPN

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

1.1.2.3.7.1. Modelo de implementación Hub-and-spoke:

Se trata de una topología tradicional ya usada por otras tecnologías, esta trabaja de forma que los sitios remotos o spokes son agregados en un dispositivo VPN de cabecera en la sede central (hub).

El Tráfico desde cualquier sitio remoto a otros sitios remotos tendría que pasar a través del dispositivo de cabecera. Cisco DMVPN admite enrutamiento dinámico, QoS y IP multicast al mismo momento que reduce significativamente el esfuerzo de configuración.

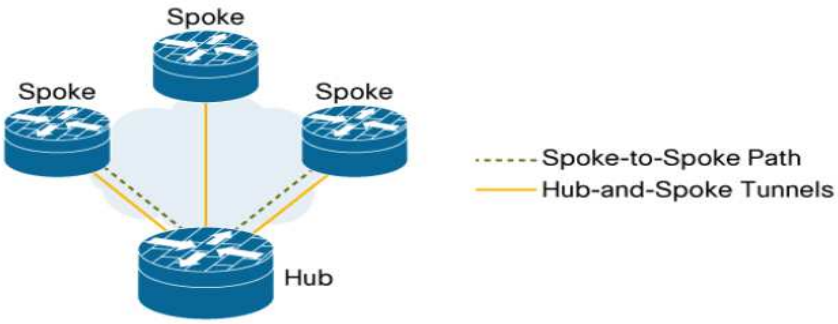


Figura 6. Diseño Modelo Hub-and-Spoke
Tomado de Cisco System Troubleshoot Guide, 2010, p.4.

1.1.2.3.7.2 Modelo de implementación Spoke-to-Spoke:

Cisco DMVPN permite la creación de una VPN de malla completa, en la cual la conectividad tradicional Hub-and Spoke es 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 resilencia spoke-to-spoke y redundancia.

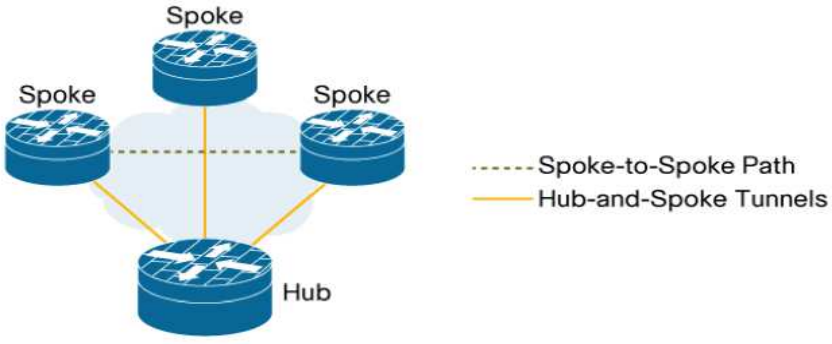


Figura 7. Modelo de implementación Cisco DMVPN Spoke-to-Spoke.
Tomado de Cisco System Troubleshoot Guide, 2010, p. 5.

Las Implementaciones de VPN Spoke-to-Spoke de tamaño mediano o a gran escala requieren apoyo para servicios de red IP avanzada como:

1.1.2.3.7.2.1 . IP Multicast.

Requerido para comunicaciones escalables y eficientes en conexiones uno a varios (es decir difusión de Internet) y de varios a varios (por ejemplo conferencias) y comúnmente necesario para voz, video y para ciertas aplicaciones de datos.

1.1.2.3.7.2.2 Protocolos de ruteo dinámico.

Por lo general se requiere en todos pero los despliegues más pequeños o donde el enrutamiento estático no es manejable u óptimo.

1.1.2.3.7.2.3 QoS.

Obligatorio para garantizar el rendimiento y la calidad de la voz, video y las aplicaciones de datos en tiempo real.

1.1.2.3.8 Arquitectura

Tradicionalmente, soportar estos servicios requiere túneles IPsec dentro de protocolos como Generic Route Encapsulation (GRE), que introducen una red superpuesta, lo que resulta complejo de configurar y administrar, y limita la escalabilidad de la solución. De hecho, el IPsec tradicional sólo es compatible con IP de unidifusión (Unicast), haciéndolo ineficiente para desplegar aplicaciones que involucren a comunicaciones de uno a varios y varios a varios.

Cisco DMVPN combina túneles GRE y cifrado IPsec, con enrutamiento del protocolo de resolución del siguiente salto (NHRP), de manera que cumpla con estos requisitos mientras que reduce la carga administrativa.

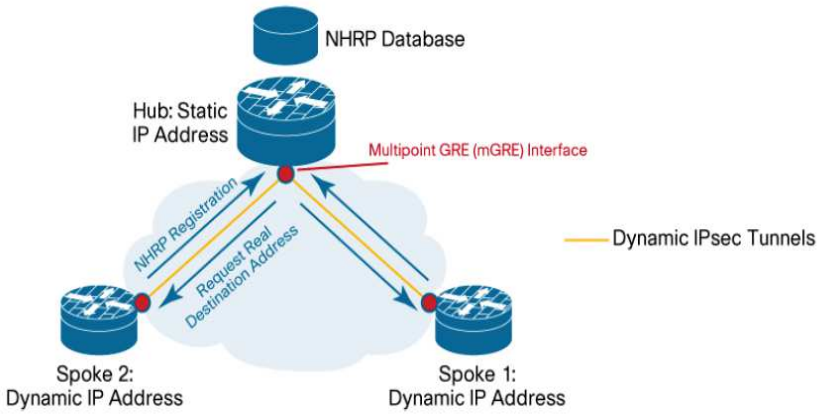


Figura 8. Arquitectura de la tecnología DMVPN de Cisco.
Tomado de Cisco Data Sheet, 2009, p.3.

En base a la Figura 7 arriba mostrada se enumeran algunos de los componentes clave que incluyen:

1.1.2.3.8.1 Interfaz de túnel GRE multipunto (Multipoint GRE [mGRE] tunnel interface).

Permite a una única interfaz GRE soportar múltiples túneles IPsec, simplificando el tamaño y la complejidad de la configuración.

1.1.2.3.8.2. Detección Dinámica de los puntos finales del túnel IPsec y los perfiles de cifrado.

Elimina la necesidad de configurar mapas de cifrado estáticos que definen a cada par de compañeros IPsec, lo que simplifica aún más la configuración.

1.1.2.3.8.3. NHRP.

Este protocolo permite que los sitios remotos sean desplegados con direcciones IP públicas asignadas dinámicamente (es decir detrás de un enrutador de un ISP). El concentrador mantiene una base de datos NHRP de las direcciones de la interfaz pública de cada remoto. Cada sucursal registra su dirección real cuando arranca; cuando una sucursal requiere construir túneles directo con otras sucursales, consulta la base de datos NHRP para hallar las direcciones reales de los sitios destino.

Los protocolos arriba descritos se verán de una forma más explícita más adelante.

1.1.2.3.9. Requerimientos de Software y Hardware para DMVPN.

1.1.2.3.9.1 Plataformas de Hardware cisco que soportan Cisco DMVPN

Se detalla en la siguiente tabla el equipamiento que opera con DMVPN:

Tabla 2.- Plataformas de Hardware Cisco, que la tecnología DMPVN.

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

Tomado de Cisco data sheet, 2009, p. 5.

1.1.2.3.9.2 Requerimientos de Software para la tecnología DMVPN de Cisco.

A continuación se detalla el IOS, cargado en los equipos Cisco:

Tabla 3. IOS de los Equipos que implementan DMPVN.

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

Tomado de Cisco data sheet, 2009, p. 6.

1.1.2.4. Protocolos.

1.1.2.4.1. El 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. Sólo los spokes necesitan tener configurada la dirección de uno o varios hubs.

1.1.2.4.1.1 Funcionamiento del protocolo NHRP

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.

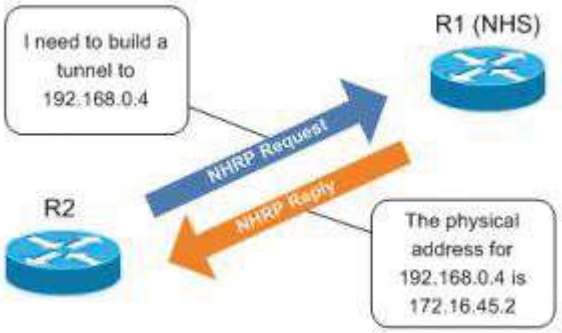


Figura 9. Negociación del protocolo NHRP
Tomado de (packetlife, s.f.) http://packetlife.net/blog/2008/jul/23/dynamic-multipoint-vpn-dmvpn/

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 mallada, sin complicar la configuración de las estaciones remotas.

1.1.2.4.1.2 Tipos de paquete NHRP

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 caché 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 caché.

7. Indicación de Error: paquete de error que indica algún problema en alguno de los paquetes recibidos en el equipo que genera el paquete de error.

1.1.2.4.2 El protocolo IPSEC

El presente proyecto investigativo, tiene como objetivo fundamental la seguridad, he de ahí la necesidad de implementar protocolos encriptados y confiables, se define, Qué es IPSEC? "Es un protocolo que está sobre la capa del protocolo de Internet (IP). Este, permite a dos o más equipos comunicarse de forma segura (de ahí viene el nombre). La "pila de red" IPsec incluye soporte para las dos familias de protocolos, IPv4 e IPv6" (Clayton y Pandya, s.f).

"IPsec (abreviatura de 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" (Posada, 2013).

El Protocolo IPSec, se encuentra diseñado en un modelo de seguridad de extremo a extremo, con el propósito de la protección de los paquetes. Cada equipo controla la seguridad por sí mismo en su extremo, bajo la hipótesis de que el medio por el que se establece la comunicación no es seguro.

1.1.2.4.2.1. Modos de Funcionamiento

Dependiendo del nivel sobre el que se actúe, podemos establecer dos modos básicos de operación de IPsec: modo transporte y modo túnel.

1.1.2.4.2.1.1. En modo túnel el datagrama.

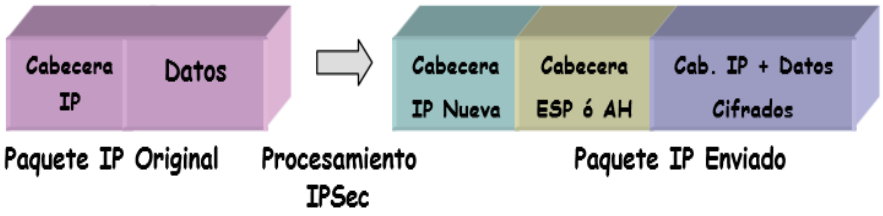


Figura 10. Modo de Funcionamiento Túnel
Tomado de Teldat, 2003, p.15.

> "En el modo túnel, todo el paquete IP (datos más cabeceras del mensaje) es cifrado o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El modo túnel se utiliza para comunicaciones red a red (túneles seguros entre routers, p.e. para VPNs) o comunicaciones ordenador a ordenador". (Teldat, 2003.P.5).

1.1.2.4.2.1.2 En modo transporte IPsec

Figura 11.- Modo de Transporte IPSEC
Tomado de Teldat, 2003, p.15.

> "En modo transporte, sólo la carga útil (los datos que se transfieren) del paquete IP es cifrada o autenticada. El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas, ya que eso invalidaría el hash. Las capas de transporte y aplicación están siempre aseguras por un hash, de forma que no pueden ser modificadas de ninguna manera (por ejemplo traduciendo los números de puerto TCP y UDP). El modo transporte se utiliza para comunicaciones ordenador a ordenador" (Teldat,2003.P.4).

1.1.2.4.2.2 Los protocolos IPsec.

En el siguiente proyecto se estudiará los protocolos IPsec, ellos son: el AH (Authentication Header - Cabecera de autenticación) y el ESP (Encapsulated Security Payload - Carga de seguridad encapsulada). Ambos son protocolos IP independientes. AH es el protocolo IP 51 y ESP el protocolo IP 50.

A continuación se detalla el funcionamiento de los mismos:

1.1.2.4.2.2.1. AH - Cabecera de autenticación

"Esta cabecera proporciona autenticación e integridad a los datos transmitidos, para proporcionar esta característica IPsec hace uso de las huellas digitales HMAC, calculará funciones HASH al contenido del paquete IP, como SHA-1 o MD5 y una clave secreta compartida.

Esta cabecera no proporciona confidencialidad porque no está cifrada.

Esta cabecera se integra entre la cabecera IP y la carga útil, se puede transmitir mediante TCP o UDP" (De Luz, 2011).

La estructura de la cabecera es la siguiente:

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Next header	Payload length	RESERVED	
Security parameters index (SPI)			
Sequence number			
Hash Message Authentication Code (variable)			

Figura 12.- Cabecera Protocolo AH

Tomado de (edeszone.net, 2011)
http://www.redeszone.net/2011/08/30/ipsec-volumen-ii-ah-cabecera-de-autenticacion/.

El siguiente gráfico demuestra el funcionamiento del protocolo AH y los elementos que lo integran:

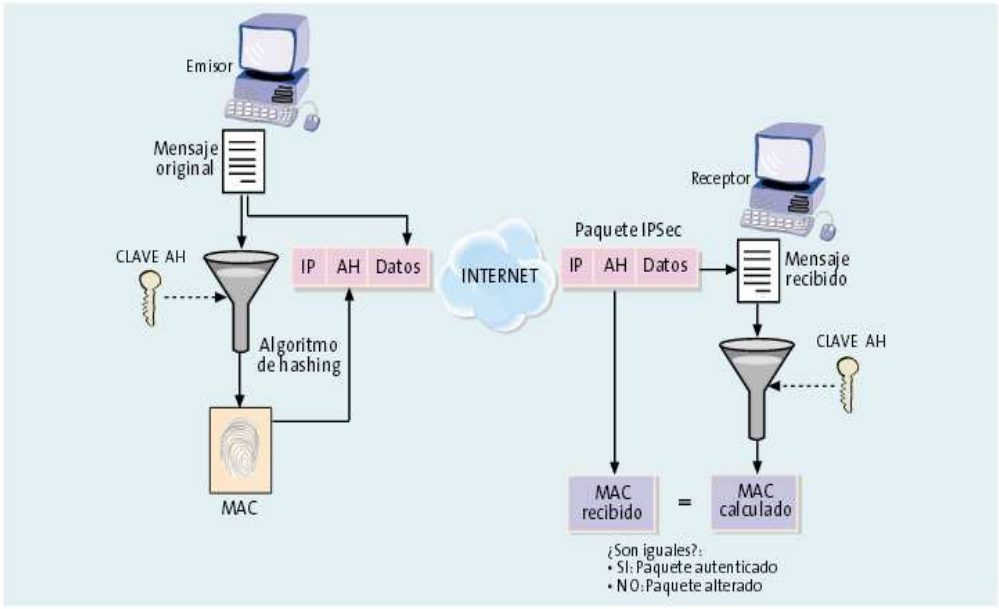


Figura 13. Funcionamiento del Protocolo AH

Tomado de Pérez, 2001, p.7.

> "Primero el emisor calcula la función hash a partir del mensaje a transmitir. Se copiará a la cabecera AH en el campo "Datos de Autenticación. Se transmiten los datos vía Internet. Cuando el paquete llega al receptor, aplicará la función hash y la comparará con la que ya tenía (ambos tienen la misma clave secreta compartida)" (De Luz, 2011).

1.1.2.4.2.2.2 ESP (Carga de seguridad encapsulada)

El segundo protocolo es ESP, según Serguio de Luz de edeszone.net (2011).

> "Ofrece autenticación, integridad y confidencialidad de los datos transmitidos a través de IPsec. Para conseguir éstas características de seguridad, se hace un intercambio de llaves públicas (Algoritmos de cifrado asimétrico).

La función principal del protocolo ESP es proporcionar confidencialidad a los datos, para poder hacerlo, ESP define el cifrado y la forma en la que se ubicarán los datos en un nuevo datagrama IP. Para proporcionar autenticación e integridad, ESP usa mecanismos parecidos a AH.

La estructura de ESP es más complejo que AH ya que aporta más funciones. Los datos se pueden transmitir vía TCP, UDP o un datagrama IP completo (lo mismo ocurría con AH). La cabecera del paquete IP no está protegida por ESP (si utilizamos el modo túnel, la protección será a todo el paquete IP interno)" (De Luz, 2011).

La estructura de un paquete ESP es la siguiente:

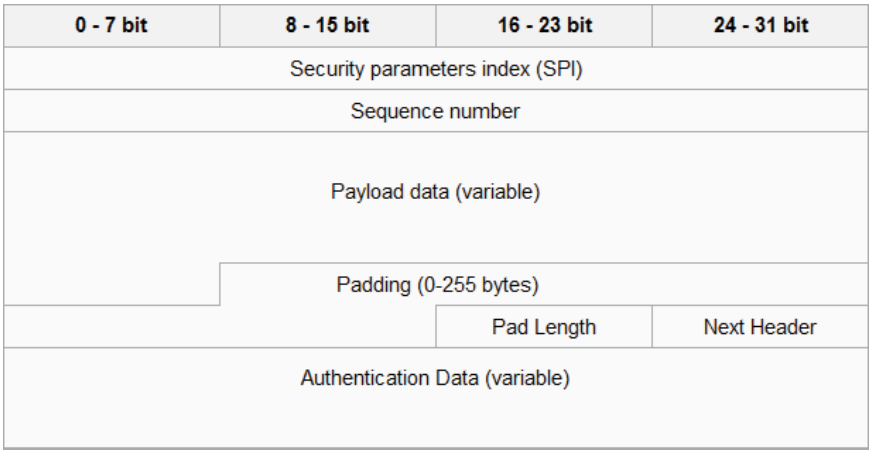


Figura 14. ESP pertenece al nivel de red dentro de TCP/IP.

Tomado de (edeszone.net, 2011)
http://www.redeszone.net/2011/09/06/ipsec-volumen-iii-esp-carga-de-seguridad-encapsulada/

"El área de datos queda totalmente cifrada, también se podría autenticar el propio datagrama para proporcionar mayor seguridad. El cifrado de los datos se realiza mediante algoritmos de clave simétrica, habitualmente se usan cifrados en bloque (como AES), el cifrado de los

datos se hacen mediante múltiplos del tamaño del bloque, por este motivo tenemos el “Padding”, un campo de relleno.

Para cifrar los datos, primero el emisor cifra el mensaje original usando una clave y lo introduce en un nuevo datagrama IP (que es protegido por la cabecera ESP). En el hipotético caso de que alguien intercepte el mensaje (Man In The Middle), sólo obtendrá datos sin sentido ya que no tiene la clave secreta para descifrar el mensaje. Cuando el mensaje llegue al destino, éste aplicará la clave secreta sobre los datos y descifrará el paquete. El algoritmo más utilizado es AES en todas sus versiones versiones (128 y 256bits) y en sus distintas modos de cifrado como AES-CBC, AES-CFB y AES-OFB” (redeszone.net, 2011).

De ahí nace emplear un buen algoritmo de cifrado para proteger todos los datos, la distribución de las claves de forma segura será muy importante.

1.1.2.4.2.2.2.1 Funcionamiento del Protocolo ESP

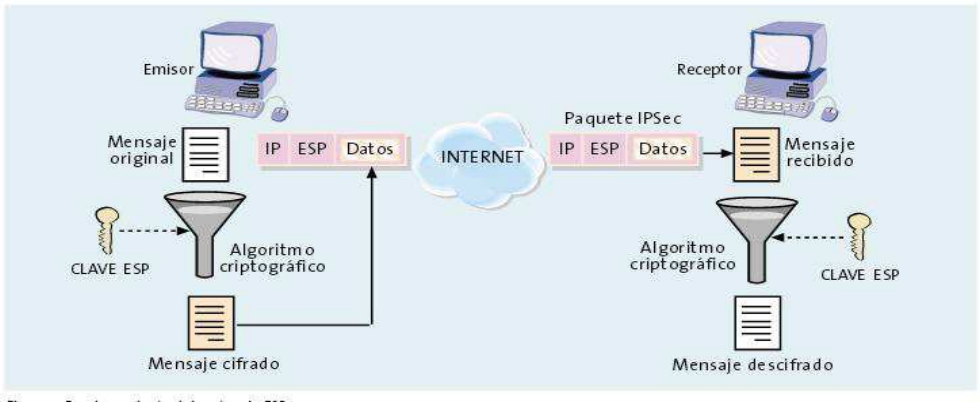


Figura 15. Funcionamiento del Protocolo ESP

Tomado de Pérez, 2001, p.12.

1.1.2.4.2.3 Protocolo de Control IKE

"El IETF ha definido el protocolo IKE para realizar la función de gestión automática de claves como el establecimiento de las SAs correspondientes. Una característica importante de IKE es que su utilidad no se limita a IPSec, si no que es un protocolo estándar de gestión de claves que podría ser útil en otros protocolos como por ejemplo: OSPF o RIPv2. Consiste en establecer una conexión cifrada y autenticada entre dos entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad IPSec" (proyectos.ingeniovirtual,s.f) .

1.1.2.4.2.3.1 Funcionamiento Protocolo IKE

A continuación la gráfica detalla el funcionamiento del Protocolo:

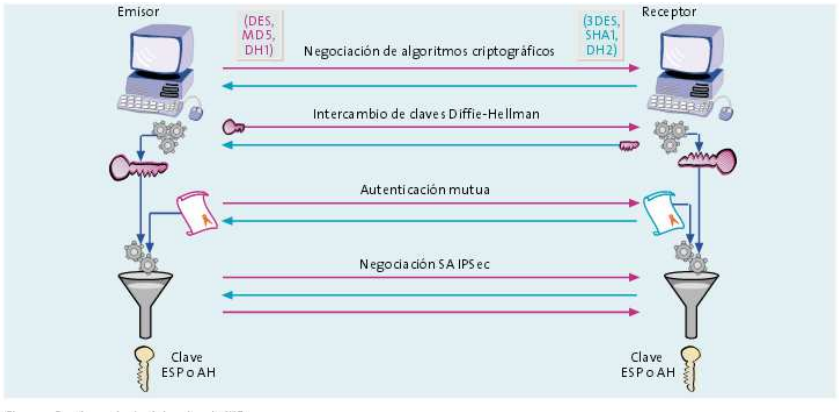


Figura 16. Funcionamiento del Protocolo IKE

Tomado de Pérez, 2001, p.11.

1.1.2.4.3 Multipoint GRE (mGRE)

El protocolo GRE es definido por el RFC 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

1.1.2.4.3.1 Ventajas y Desventajas de GRE.

Ventaja: Es compatible con la encapsulación de los paquetes IP, también de multidifusión y el tráfico IPv6.

Desventaja: La interfaz de túnel es un interfaz virtual, y permanece activa, incluso si el lado remoto está en problemas.

1.1.2.4.3.2 GRE y los protocolos de enrutamiento

Como ya se mencionó, GRE permite que los routers en cada extremo del túnel virtual creado ejecuten los protocolos de enrutamiento.

1.1.2.4.4 Politica ISAKMP (Protocolo de Gestión de Claves y Asociaciones de Seguridad en Internet).

Esta sección hablaremos de las política ISAKMP, “La política ISAKMP define las cargas para el intercambio de generación de claves y autentificación de datos, está definido en el RFC 2408” (Schertler, Schneider, Turner, 2005, p.4-16). Estos estándares facilitaron un nivel estable para la transferencia de claves y autentificación de datos que es aislada de la técnica de generación de claves, algoritmo de encriptación, y mecanismo de autentificación.

ISAKMP, establece con marco común para acordar el formato de los atributos S.A, la negociación, modificación y cancelación de SAS (Asociación de Seguridad).

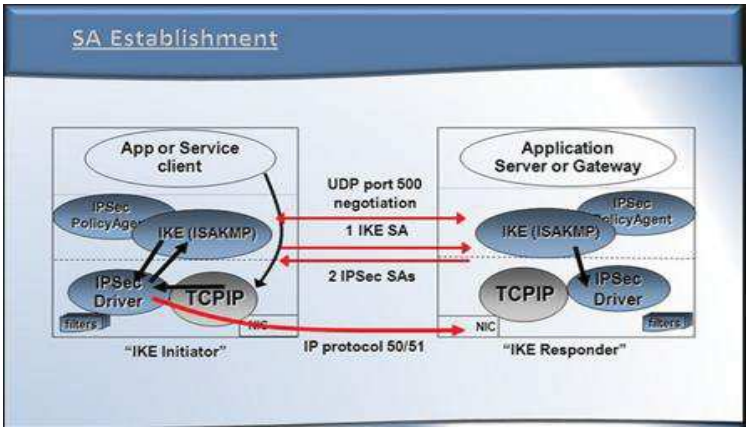


Figura 17. SA POLITICA ISAKMP
Tomada de (slideplayer, s.f)
http://slideplayer.es/slide/159908/

1.1.2.5. Protocolos de Enrutamiento.

1.1.2.5.1. Protocolo EIGRP

El Protocolo de Enrutamiento EIGRP es la abreviatura de Protocolo de Enrutamiento de Gateway Interior Mejorado, de ahí nace el nombre como protocolo de enrutamiento de vector distancia.

1.1.2.5.1.1. Funcionamiento de EIGRP

En un router configurado EIGRP, este sólo envía actualizaciones de enrutamiento como vectores de distancia de las rutas conectadas directamente, más no las rutas que se encuentran en la red. El router sólo envía una actualización de un particular si una variación de topología se ha producido a dicha ruta específica.

Además, esta actualización sólo se envía a los routers vecinos, es decir los que se encuentran directamente conectados. Esto hace que EIGRP un

protocolo de enrutamiento eficiente del ancho de banda. Otros protocolos de enrutamiento tienen regulares actualizaciones de enrutamiento que contienen toda la información de las rutas por defecto.

1.1.2.5.1.2 Los Sistemas Autónomos y el Rango Disponible para Numerarlos.

- Identificaciones de procesos y sistema autónomo (AS)
- Es un grupo de redes controlado por una autoridad única (referencia RFC 1930).
- IANA asigna los números AS
- Entidades que necesitan los números AS:

1.1.2.5.2. Protocolo de Enrutamiento OSPF.

El protocolo OSPF está denominado (Open Shortest Path First – abrir primero la trayectoria más corta) está definido en el RFC 1583. Esto significa que comparte las tablas de enrutamiento entre todos los routers que pertenecen a una misma comunidad de un sistema autónomo. OSPF está basado en la tecnología de estado de enlaces OSPF.

1.1.2.5.2.1. Funcionamiento de OSPF.

En este protocolo ejecuta el mismo algoritmo de forma paralela en todos los rotuteres. Dado que van a existir varias rutas de similar costo hacia el destino, el tráfico es dividido por igualdad entre las rutas, esto es conocido como (balance de Carga).

1.1.2.5.2.2. Algoritmo del estado de enlace

Como se menciona el, protocolo OSPF usa un algoritmo de estado de enlace para generar y calcular el trayecto más corto a todos los destinos conocidos.

- Pasos a seguir para alcanzar la Ruta más corta

1. “Durante la inicialización, o bien cuando se produce algún cambio en la información de enrutamiento, un router generará un anuncio de estado de enlace. Este anuncio representará la agrupación de todos estos estados de enlace en dicho router” (Cisco, 2008, p.3).

2. “Todos los routers intercambiarán estados de enlace mediante la inundación. Cada router que recibe una actualización de estado de enlace debe almacenar una copia de su base de datos de estados de enlace y luego propagar la actualización a otros routers” (Cisco, 2008,p.3).

3. “Una vez que la base de datos de cada router está completa, el router calculará un árbol de trayecto más corto a todos los destinos. Para ello, el router utiliza el algoritmo Dijkstra. Los destinos, el costo asociado y el siguiente salto (next hop) para alcanzar dichos destinos formarán la tabla de IP Routing” (Cisco, 2008,p.3).

4. “En caso de que no se produzcan cambios en la red OSPF, por ejemplo, el costo de un enlace o bien la adición o eliminación de una red, OSPF Gdebería permanecer muy tranquilo. Los cambios que se produzcan se comunicarán a través de paquetes de estado de enlace y se volverá a calcular el algoritmo Dijkstra para encontrar el trayecto más corto”(Cisco, 2008,p.3).

1.1.2.5.2.3 Algoritmo del trayecto más cortó.

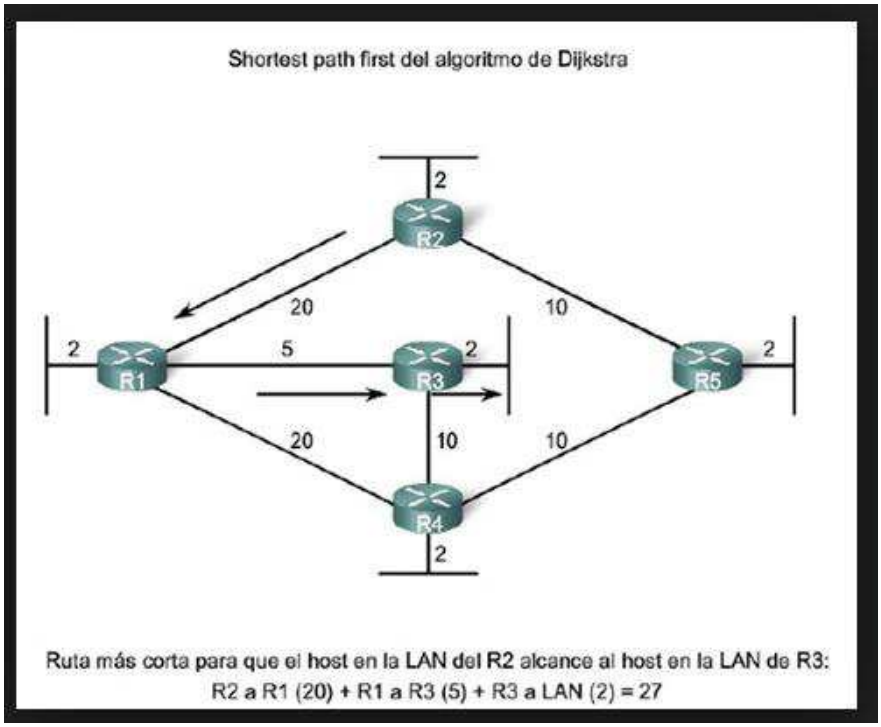


Figura 18. Algoritmo Dijkstra.

Tomado de (electropediadigital.blogspot, 2012)

http://electropediadigital.blogspot.com/2012/10/algoritmo-dijkstra-y-spf.html

El trayecto más corto se calcula con el algoritmo Dijkstra, este fue diseñado para encontrar las rutas más cortas entre el nodo origen y cada uno de los nodos de la red a través de la suma de costos, como se aprecia en la Figura 18.

1.1.2.5.2.4 Tipos de paquetes OSPF.

Encabezamientos de paquetes OSPF: incluye información básica relacionada con el enrutador, como es el caso de la versión de OSPF, el tipo de paquete, el identificador del enrutador y el identificador del área.

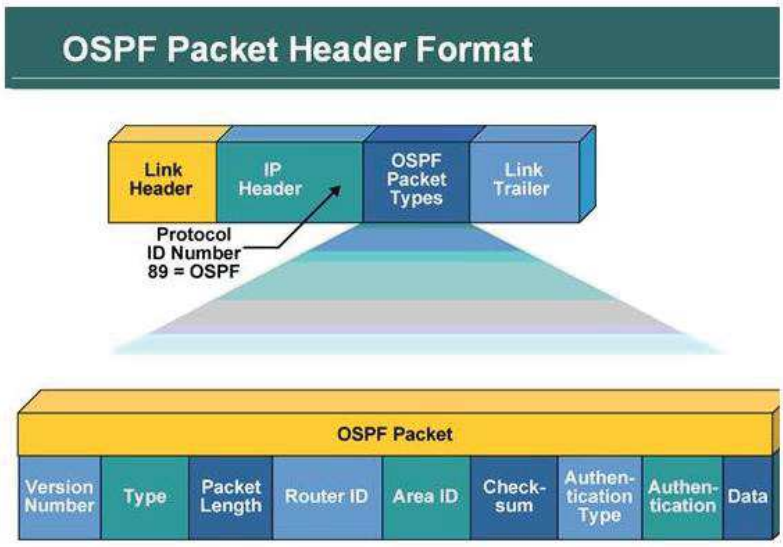


Figura 19. Tipos de Paquetes

Tomado de Ochoa, 2009, p.10.

- **Paquetes tipo 1 (HELLO):** Permiten establecer y mantener adyacencias. Los paquetes de saludo incluyen toda la información necesaria para establecer una realcen e vecindad, incluyendo los intervalos de saludo y de no operatividad, la contraseña, la mascara de red correspondiente al enlace al que se envío el saludo, el indicador de área de modulo, los DR y BDR elegidos y cualquier vecino conocido.

- **Paquetes tipo 2** (Descripción de base de datos): Constituye la base de datos de estado del enlace que hay en el enrutador cuando se inicializa una adyacencia, estos paquetes incluyen encabezamientos LSA, para que el enrutador receptor confirme que tiene todos los LSA requeridos.

- **Paquetes tipo 3** (Petición de estado del enlace): Solicita los LSA específicos desde los vecinos, los paquetes de petición de estado de enlace se envían basándose en las entradas situadas en el listado de petición de estado de enlace.

- **Paquetes tipo 4** (Actualización de estado del enlace): Suministra los LSA a los enrutadores remotos.

- Paquetes tipo 5 (Acuse de recibo de estado de enlace): Envío de un acuse de recibo explicito a uno o más LSA.

2. Metodología.

2.1. Diseño Metodológico.

El presente trabajo de titulación, fue realizado con el método de investigación experimental-inductivo, debido a la naturaleza del trabajo ya que no existe reportes de este tipo de trabajos en el país; sin embargo, se lo puede encontrar en países como EEUU, México, Argentina.

Es realizado en un ambiente de laboratorio para demostrar su funcionamiento lo que lo hace en lo una investigación experimental, e inductivo pues se extrae conclusiones generales resultado de la acumulación de datos particulares. Es por esto que se inicia la investigación con el estudio de las redes privadas virtuales (VPN) base de la tecnología que se muestra en el presente trabajo de titulación. Comprendiendo el funcionamiento de las VPN se busca una forma en que estas últimas sean más fáciles de implementar y no sean enlaces solo punto a punto, llegando así al estudio que comprende DMVPN, es decir realizar la investigación de esta solución y que funcione correctamente para el envió de datos por una red pública, asegurando el envió y protección de la información. En consecuencia se estudia la seguridad de datos utilizando el protocolo de encriptación y autenticación IPsec por las siguientes razones:
1.- Ipsec resulta de un conjunto de estándares que integran funciones de seguridad en IP basados en criptografía.
2.- Proporciona confidencialidad, integridad, y autenticidad de paquetes IP para aquello combina:

- Tecnologías de clave pública (RSA).
- Algoritmo de cifrado AES, DES, 3DES, IDEA, BLOWFISH.
- Algoritmos de HASH (MD5, SHA-1).
- Certificados digitales X509v3.

Figura 20. Tecnologías utilizadas en IPsec.
Tomado de www.utn.edu.ec, s.f.

Dentro de IPsec se distinguen los componentes siguientes:

Dos protocolos de seguridad, IP Authentication Header (AH) e IP Encapsulating Security Payload (ESP) que proporcionan mecanismos de seguridad para proteger tráfico IP.

Un protocolo de gestión de claves Internet Key Exchange (IKE) que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

Además IPsec se utiliza actualmente en soluciones VPN, por consecuencia se dispone de documentación que permite un mejor entendimiento y ayuda a una rápida implementación.
Por otro lado, se elabora un estudio de la capacidad de entablar túneles directos entre los puntos involucrados de forma que su resultado sea una red

mallada, los protocolos NHRP y mGRE utilizados por DMVPN sobre las redes IP son utilizados para este fin debido a que:

- NHRP proporciona un mecanismo para conocer la dirección de red NBMA (Redes de acceso multiple sin difusión) del Destino, o de un enrutador que se encuentre a lo largo de la ruta al destino. NHRP no es un protocolo de enrutamiento, sin embargo podrá hacer uso de la información de enrutamiento.

- mGRE o GRE “es un protocolo de tunneling desarrollado por Cisco que puede encapsular una amplia variedad de tipos de paquete de protocolo dentro de túneles IP, lo que crea un enlace punto a punto virtual a los routers Cisco, en puntos remotos a través de una Internetwork”(Cisco Systems, s.f). Está definido como un estándar IETF (RFC 2784).

2.1.1 Análisis de las Diferentes Soluciones VPN.

Teniendo en cuenta que las soluciones VPN actuales pueden ser de Software o Hardware, y que además la mayoría de ISPs tienen estructurado su red principal o backbone con equipos del proveedor Cisco System tomando como ejemplo ISPs como Telconet S.A y Level 3, se procedió a buscar una solución que tenga la facilidad de utilizar esa estructura, llegando así a escoger DMVPN.

A continuación se muestra las diferentes soluciones y sus características.

Las VPN pueden ser de los siguientes tipos:

- VPN de firewall
- VPN de router y de concentrador
- VPN de sistema operativo
- VPN de aplicación

- VPN de proveedor de servicios

2.1.1.1. VPN de firewall

Se trata de un sistema de seguridad que implanta políticas de control de acceso entre dos o más redes. Un filtro que controla todas las comunicaciones que pasan de una a otra y en función de lo qué sean permite o deniega. Para permitir o denegar el firewall examina el tipo de servicio al que corresponde, como pueden ser el web, correo, IRC, etc.

Es muy común encontrar soluciones VPN basadas en firewall para proporcionar servicios. Empresas como Cisco Systems, Nortel Networks y 3Com incluyen en muchos de sus dispositivos firewall soporte para VPN. Una VPN basada en firewall tiene la ventaja de que simplifica la arquitectura de la red al establecer un único punto de control de seguridad.

2.1.1.2. VPN de router y de concentrador

> “Empresas como Cisco, Nortel y 3Com, entre otros, también ofrecen servicios VPN integrados dentro de un router o un dispositivo llamado concentrador VPN. Tanto el router como el concentrador VPN están especialmente diseñados para las conexiones VPN sitio a sitio y acceso remoto. Cuenta con las tecnologías VPN más importantes y los métodos de autenticación y cifrado para proteger los datos transmitidos” (Arias, 2007, p.10).

2.1.1.3. VPN de sistema operativo

> “Los sistemas operativos como Windows de Microsoft, Netware de Novell o Linux en sus diferentes distribuciones (Red Hat, Debian,etc...) ofrecen servicios de VPN ya integrados. La principal ventaja de esta solución es que resulta ser económica ya que en un mismo sistema

operativo se pueden contar con una gran variedad de servicios (servidor Web, de nombres de dominio, acceso remoto, VPN) y además mejora los métodos de autenticación y la seguridad del sistema operativo. Tiene la desventaja de que es vulnerable a los problemas de seguridad del propio sistema operativo. Estas VPN se utilizan más para el acceso remoto" (Arias, 2007, p.11).

2.1.1.4 VPN de aplicación

"Una VPN de aplicación es un programa que añade posibilidades VPN a un sistema operativo. Sin embargo, este programa no queda integrado con el sistema operativo. La ventaja de este tipo de VPN es que la aplicación añade seguridad extra a la que podría ofrecer una VPN integrada al sistema operativo. Un ejemplo de esta VPN es el programa ViPNet de Infotecs.

La desventaja es que estas VPN no soportan una gran cantidad de usuarios y son mucho más lentas que una VPN basada en hardware. Si se utilizan en Internet, son vulnerables a las fallas de seguridad del sistema operativo que contiene a la aplicación" (Arias, 2007, p.12).

2.1.1.5. VPN de proveedor de servicios

"Este tipo de VPN es proporcionada por un proveedor de servicios. Al principio las VPN de proveedor de servicios se basaban en tecnologías tales como X.25 y Frame Relay, posteriormente ATM y SMDS y finalmente se ofrecen redes basadas en IP. El proveedor de servicios es la empresa propietaria de la infraestructura tales como equipos y líneas de transmisión que ofrece líneas dedicadas virtuales a sus clientes. El cliente se conecta a la red del proveedor de servicios a través de un dispositivo de equipo terminal del cliente (CPE) como pugede ser un router. El CPE se conecta a través de medios de transmisión al equipo del proveedor de servicios, que puede ser X.25, Frame Relay, un

conmutador ATM o un router IP. La línea virtual que se le proporciona al cliente mediante el proveedor de servicios se le llama circuito virtual (VC). Conforme a los análisis realizados, se llegó al desarrollo de la configuración y lo que implica cada línea de la misma" (Arias, 2007, p.12).

2.1.2. DMVPN configuración.

2.1.2.1. Configuración de la política ISAKMP:

Debe haber al menos una política ISAKMP congruente entre dos posibles pares de cifrado.

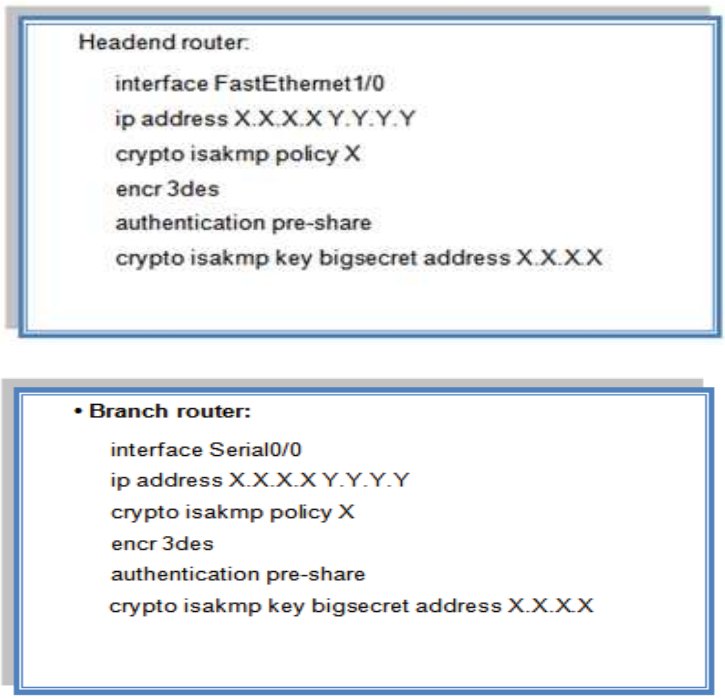


Figura 21. Configuracion de la política ISAKMP.

Tomado de Cisco, 2008, p. 33

Se toma en cuenta lo siguiente:

• En un solo nivel de Arquitectura de Cabecera, la configuración anterior se aplica al router cabecera.

• En un nivel doble de Arquitectura de Cabecera, la configuración anterior se aplica al router cabecera de cifrado.

• En cualquier arquitectura de sistema de cabecera la implementación de una sucursal con una dirección IP pública dinámica, un wildcard PSK o PKI (Pre-Shared Key) debe ser utilizado en el router de cabecera de cifrado.

2.1.2.2. Transformación IPsec y configuración del protocolo

La transformación definida debe coincidir entre los dos pares IPsec. El cambio de nombres definidos sólo es significativo a nivel local. Sin embargo, el algoritmo de encriptación, método de hash, y en particular los protocolos utilizados (ESP o AH) deben tener al menos una concordancia.

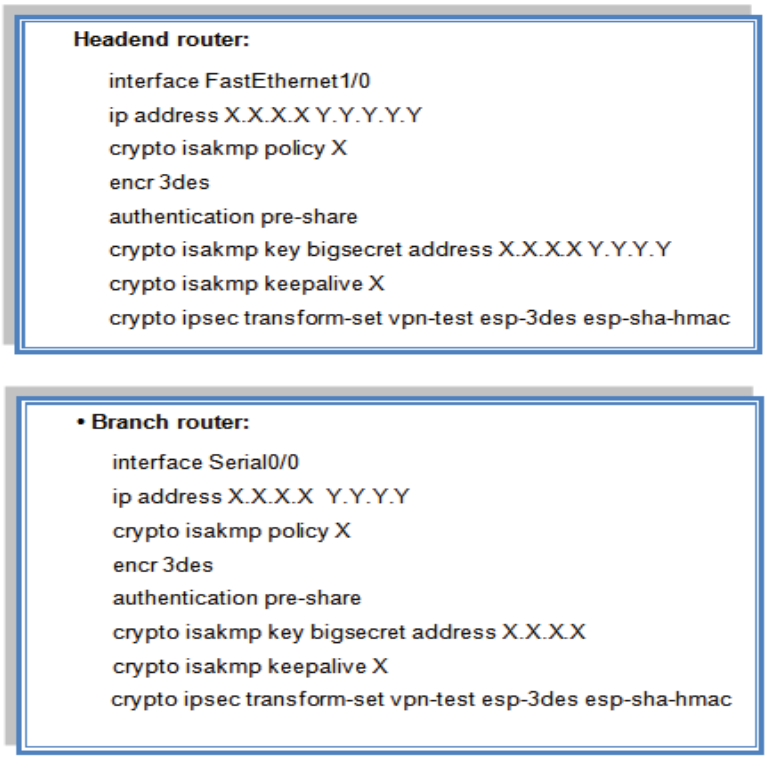


Figura 22. ISAKMP
Tomado de Cisco, 2008, p. 34

2.1.2.3. Configuración de la protección del túnel

La protección del túnel puede ser utilizada cuando los túneles GRE y el túnel cifrado comparten los mismos extremos. Debido a esta restricción, la protección del túnel sólo es aplicable a la arquitectura de cabecera de un solo nivel. En las primeras versiones de configuraciones IPsec, los mapas criptográficos dinámicos o estáticos especifican que transformación de IPsec definir (Intensidad de encriptación y grupo Diffie-Hellman) y además especifican una lista de acceso cifrada. Que define el tráfico importante para el mapa de cifrado. A partir de la versión de software Cisco IOS 12.2 (13)T, el concepto de perfil IPsec existe. El perfil de IPsec comparte la mayoría de los mismos comandos con la configuración del mapa cifrado, pero solamente un subconjunto de los comandos es necesario en un perfil IPsec. Estos comandos se refieren a una directiva IPsec que puede ser emitida bajo un perfil IPsec; no hay necesidad de especificar la dirección del par IPsec o la ACL para coincidir los paquetes que serán encriptados.

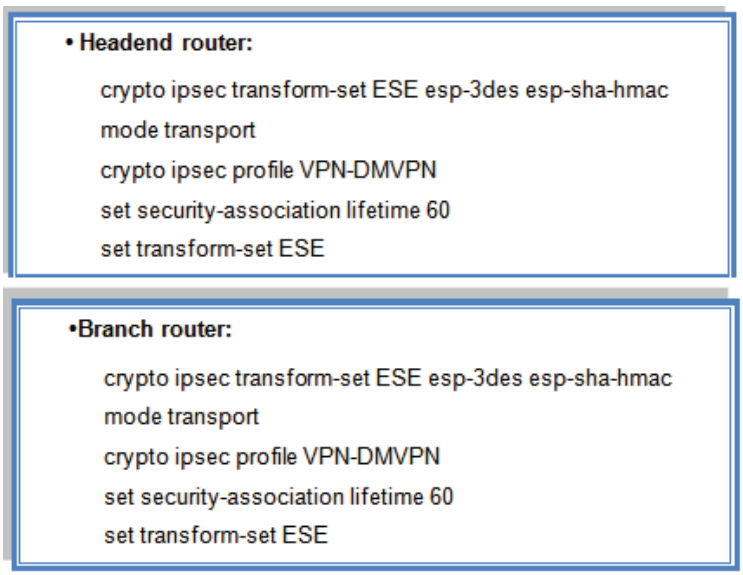


Figura 23. Proteccion del túnel
Tomado de Cisco, 2008, p. 35

El perfil IPsec es asociado con una interface de túnel mediante el comando de perfil de protección del túnel IPsec profile-name, introducido por primera vez en

la versión de software Cisco 12.2(13)T. el comando de la protección del túnel puede ser usado con túneles mGRE y p2p GRE, con túneles p2p GRE, la dirección destino del túnel es usada como la dirección del par IPsec. Con túneles mGRE, son posibles múltiples pares IPsec; las direcciones de destino asignadas a NHRP NBMA correspondientes se utilizan como las direcciones pares de IPsec. Las listas de acceso cifradas que definen el tráfico interesante no necesitan ser configuradas. Si más de un túnel mGRE es configurado en un router (por ejemplo, en un router de una sucursal con nubes DMVPN dobles), es posible hacer referencia a la misma dirección origen del túnel sobre cada interface de túnel. En este caso, la clave compartida es usada en el comando de la protección del túnel en ambas interfaces. Esto no significa que los dos túneles mGRE están alcanzando la misma nube DMVPN; cada interface de túnel requiere un único identificador de red NHRP y ya subred IP.

2.1.2.4. Configuración del Mapa de Cifrado Dinámico

El mapa de cifrado dinámico es requerido solamente en una arquitectura de nivel dual donde la protección del túnel no puede ser utilizada.

El siguiente ejemplo de configuración muestra una dirección IP pública dinámica en el router de la sucursal con una IP pública estática en el router de cabecera utilizando una arquitectura de cabecera de nivel doble.

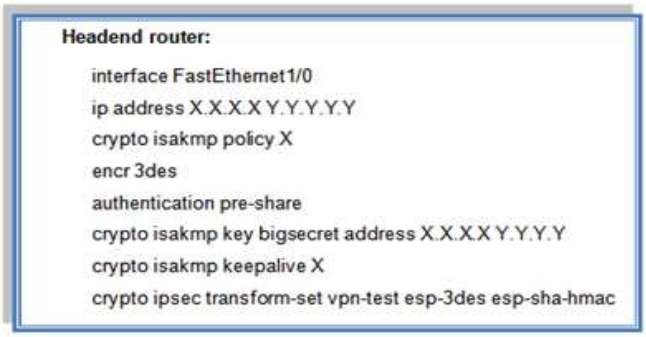


Figura 24. ISAKMP sobre el HUB.

Tomado de Cisco, 2008, p. 35.

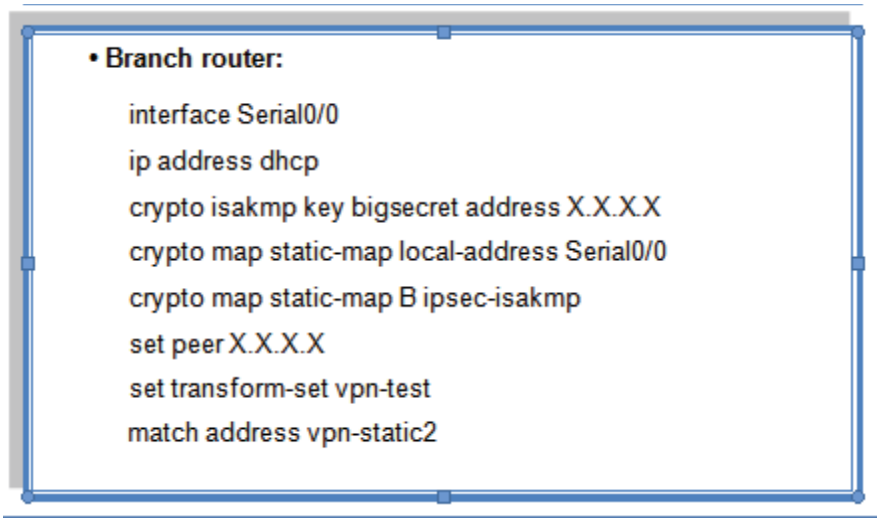


Figura 25. ISAKMP sobre la Sucursal

Tomado de Cisco, 2008, p. 36.

En el router cabecera, un mapeo de cifrado dinamico es utilizado con una wildcard PSK para permitir un par cifrado con la dirección IP pública obtenida dinámicamente del router de la sucursal.

En una arquitectura de cabecera de nivel doble, la configuración es aplicada al router de cifrado de cabecera.

2.1.2.4.1 Aplicar mapas de cifrado

Los mapas de cifrado son requeridos solamente cuando se utiliza una arquitectura de cabecera de doble nivel. El mapa de cifrado se aplica sobre los ruteadores de salida con la dirección pública. El router de la sucursal debe estar configurado con un mapa de cifrado estático cuando se usa una arquitectura de cabecera de doble nivel debido a que el destino del túnel encriptado difiere del destino del túnel GRE.

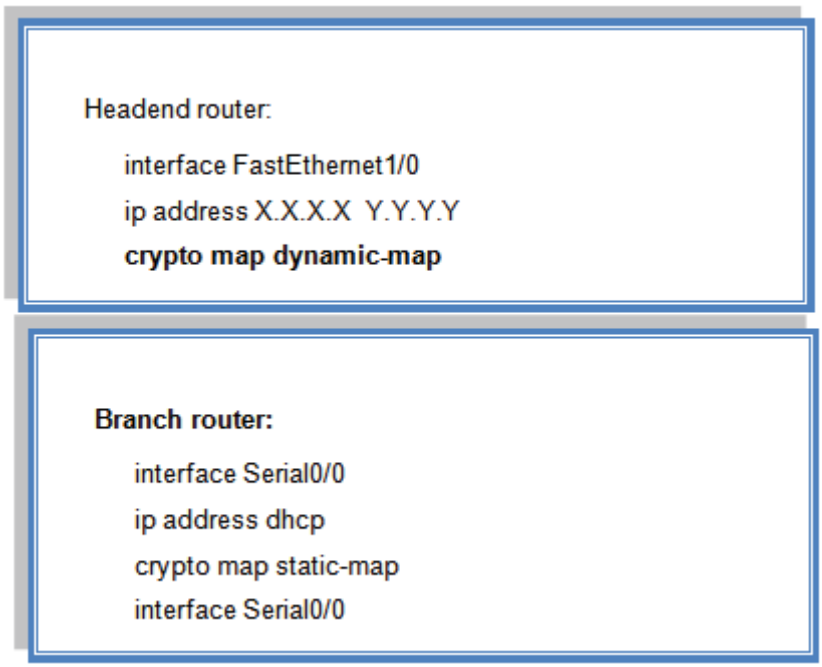


Figura 26. Aplicar cripto maps

Tomado de Cisco, 2008, p. 36.

El anterior ejemplo de configuración se muestra el router en la sucursal con una dirección IP pública dinámica y una dirección IP pública estática en el router cabecera para los pares cifrados en una arquitectura de doble nivel:

En una arquitectura de cabecera de doble nivel, la configuración mostrada se aplica al router cabecera de cifrado.

2.1.2.5. Configuración mGRE.

La configuración de mGRE permite a un túnel tener múltiples destinos. La configuración mGRE sobre un lado de un túnel no tiene ninguna relación con las propiedades de túnel que puedan existir en los puntos de salida. Esto significa que un túnel mGRE en el HUB podría conectarse a un túnel p2p en la sucursal.

A la inversa, un túnel GRE p2p puede conectarse a un túnel mGRE. La característica distintiva entre una interfaz mGRE y una interfaz GRE p2p es el destino del túnel. Una interfaz mGRE no tiene un destino configurado. En su lugar el túnel GRE está configurado con el comando tunnel mode gre multipoint. Este comando se utiliza en lugar del tunnel destination x.x.x.x encontrado con túneles GRE p2p. Además de permitir a múltiples destinos, un túnel mGRE requiere NHRP para resolver los extremos del túnel.

```
interface Tunnel X
bandwidth 1536
ip address X.X.X.X Y.Y.Y.Y
tunnel source Serial0/0
tunnel mode gre multipoint
```

Figura 27. Configuración mGRE

Tomado de Cisco, 2008, p. 37.

2.1.2.5.1. Configuración de la Interface de Túnel (Solamente para topología HUB-and-Spokes).

El siguiente ejemplo de configuración muestra una dirección IP pública estática en la sucursal con una dirección IP pública estática en el ruteador de cabecera, ya sea una arquitectura de cabecera de nivel simple o doble.

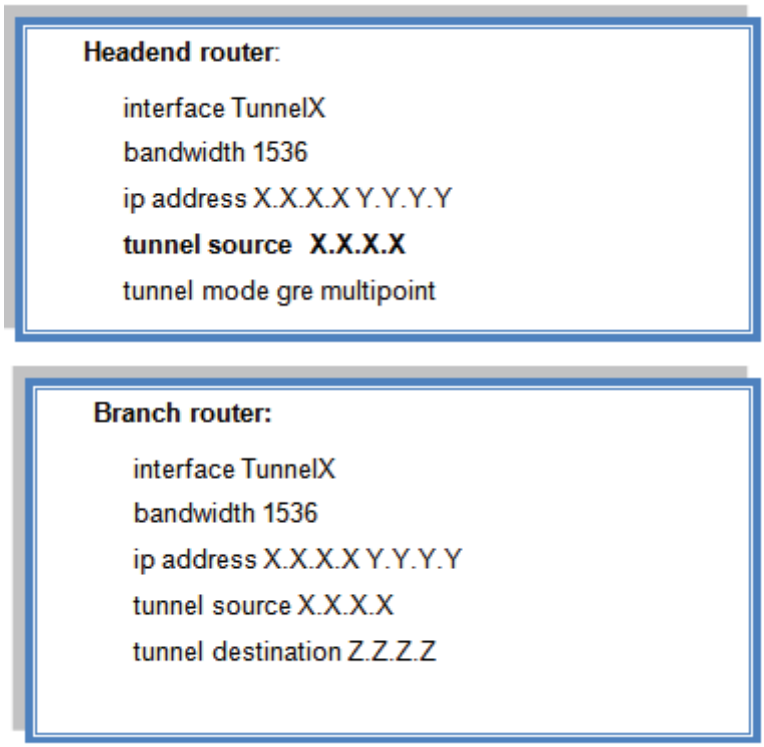


Figura 28. Configuración del túnel

Tomado de Cisco, 2008, p.38.

Nótese que esta configuración aplica solamente en arquitecturas de cabecera de nivel simple.

2.1.2.5.2. Configuración de la Interface de Túnel (Spoke-to-Spoke dinámico).

El siguiente ejemplo de configuración muestra una dirección IP pública dinámica en la sucursal con una dirección IP pública estática en el ruteador de cabecera para el túnel mGRE para una arquitectura de cabecera de nivel simple.

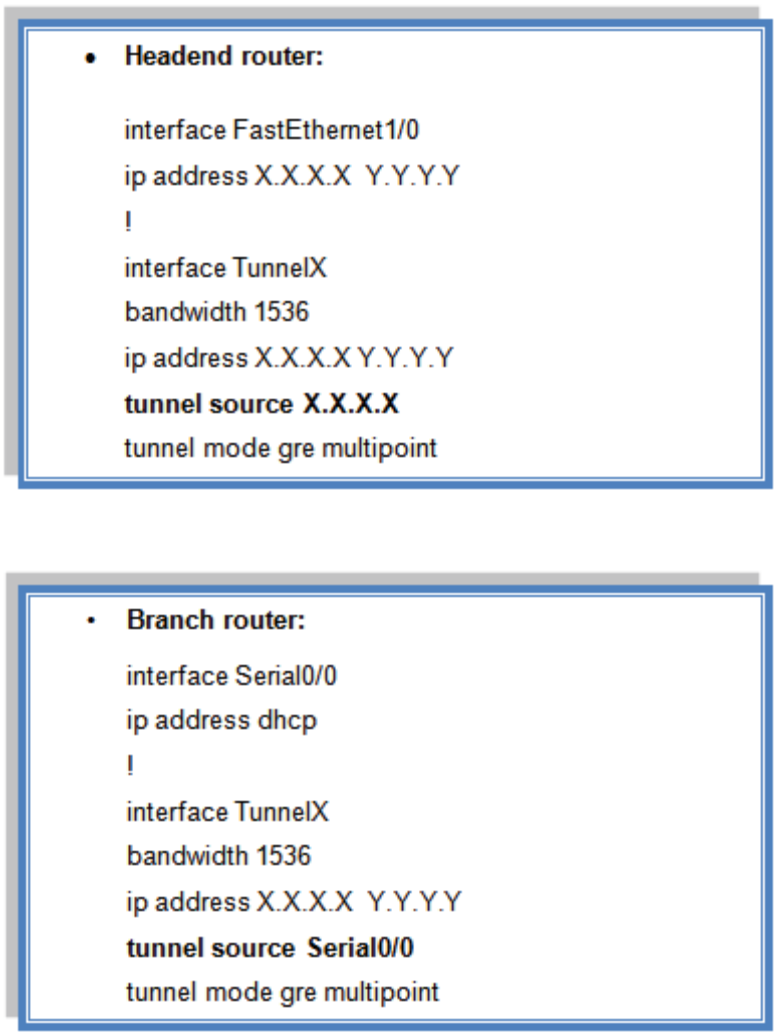


Figura 29. Configuración Tunel spoke-Spoke

Tomado de Cisco, 2008, p. 37.

En una arquitectura de cabecera de nivel simple, la configuración mostrada es aplicada al router cabecera.

En una arquitectura de cabecera de nivel doble, la configuración arriba mostrada es aplicada al router mGRE de la cabecera. El router mGRE de la cabecera tiene una IP pública estática diferente que el router de la cabecera de cifrado. El router mGRE de la cabecera envía todo el tráfico mGRE saliente hacia la sucursal a través de la cabecera de cifrado.

2.1.2.6. Configuración NHRP.

NHRP provee un mapeo entre la dirección de entrada y de salida de un extremo del túnel. Este mapeo puede ser dinámico o estático. En un escenario dinámico, un servidor de siguiente salto (NHS) es utilizado para mantener una lista de posibles destinos de túnel. Cada extremo utilizando el NHS registra su propio mapeo público o privado con el NHS. El mapeo local del NHS debe ser siempre estático.

Es importante notar que la sucursal apunta a la dirección interna o protegida del servidor NHS.

El tiempo de espera NHRP es utilizado para determinar cuánto tiempo los routers adyacentes deberán considerar las entradas en caché de este dispositivo como válidas. El valor configurado es enviado hacia el extremo remoto cuando la sesión spoke-to-spoke es inicializada. El sitio remoto comienza un conteo regresivo, cuando este tiempo expira, el router remoto remueve las entradas de caché hacia el router local. Si el tráfico sigue fluyendo, el router remoto debe pedir nuevamente el mapeo desde el servidor NHS. Los routers remotos pueden tener diferente tiempo de espera, sin embargo esta práctica no es muy común. Si dos Spokes están en sesión, y un temporizador expira antes que el otro, el spoke informa al spoke adyacente que la entrada de cache NHRP debe ser caducada. Cada dispositivo también remueve la sesión de cifrado spoke-to-spoke.

Aunque el tráfico de voz spoke-spoke (VoIP) es factible sobre DMVPN generalmente no se recomienda debido a preocupaciones de QoS, ya que el tiempo de espera de NHRP deberá ser mayor que la duración de la mayoría de llamadas. El tiempo de espera no debe ser tan largo que las sesiones spoke-to.spoke estén inactivas sobre el promedio. Esta recomendación es especialmente cierta para los routers de gama baja donde el software impone un límite inferior sobre el número de túneles de cifrado. Un equilibrio general entre túneles inactivos y un sobre almacenamiento excesivo puede ser logrado configurando el tiempo de inactividad a 600 segundos.

Ejemplo de configuración.

Headend router:

```
interface TunnelX
description NHRP with mGRE
ip address X.X.X.X  Y.Y.Y.Y
ip mtu 1400
ip nhrp map X.X.X.X Z.Z.Z.Z
ip nhrp network-id 12345
ip nhrp holdtime 600
ip nhrp nhs X.X.X.X
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 100000
tunnel protection ipsec profile DMVPN shared
!
```

Figura 30. Configuración del Protocolo NHRP en el Headend

Tomado de Cisco System, 2008, p. 38.

Branch router

```
interface Tunnel0
description NHRP with p2p GRE
ip address X.X.X.X Y.Y.Y.Y
ip mtu 1400
ip nhrp map X.X.X.X Z.Z.Z.Z
ip nhrp network-id ABC
ip nhrp holdtime 600
ip nhrp nhs X.X.X.X
tunnel source FastEthernet0/0
tunnel destination X.X.X.X
tunnel key 100000
tunnel protection ipsec profile DMVPN shared
```

Figura 31. Configuracion del Protocolo NHRP en el Branch.

Tomado de Cisco System, 2008, p. 39.

2.1.2.7 Configuración de EIGRP.

“EIGRP se lanzó originalmente en 1992 como un protocolo exclusivo disponible solamente en los dispositivos de Cisco. En 2013, Cisco cedió una funcionalidad básica de EIGRP como estándar abierto al IETF, como una RFC informativa. Esto significa que otros proveedores de redes ahora pueden implementar EIGRP en sus equipos para que interoperen con routers que ejecuten EIGRP, ya sean de Cisco o de otros fabricantes. Sin embargo, las características avanzadas de EIGRP, como las rutas internas de EIGRP necesarias para la implementación de la red privada virtual dinámica multipunto (DMVPN), no se cederán al IETF. Como RFC informativa, Cisco mantendrá el control de EIGRP” (ecovi.uagro.mx, s.f).

“EIGRP incluye características de protocolos de routing de estado de enlace y vector distancia. Sin embargo, aún se basa en el principio clave del protocolo de routing vector distancia, según el cual la información acerca del resto de la red se obtiene a partir de vecinos conectados directamente” (ecovi.uagro.mx, s.f).

3. Desarrollo del modelo.

El modelo de la tecnología DMVPN propuesto, combina las capacidades ya existentes de los túneles multipunto, basados en encapsulación de enrutamiento genérico (mGRE), protocolo de resolución del siguiente salto (NHRP) y el cifrado IPsec para proporcionar una infraestructura VPN hub-and-spoke.

3.1. Requerimientos

3.1.1. Requerimientos de hardware para la conexión WAN

Como se menciona en el capítulo II, DMPVN hace uso de la red pública o Internet para entablar las conexiones entre los distintos puntos. Por consiguiente el equipamiento necesario para lo antes indicado debe ser:

- Enrutadores.
- Tecnologías de acceso al medio o última milla.

El primer dispositivo mencionado deberá ser capaz de soportar DMVPN. La tabla 2 en el Capítulo II muestra una lista de equipos que cuentan con las características necesarias para levantar DMVPN, cada uno de estos dependiendo de su serie tienen adiciones como por ejemplo el Router Cisco de la serie 870, que son utilizados para Spokes o los Routers de la serie 1841 perfectos para conformar el Hub.

El segundo requerimiento de hardware no es necesariamente un requerimiento específico que depende del empresario, más bien dependerá del ISP, sin embargo si dependerá de los servicios que cursarán por la red debido a que ciertas aplicaciones son más sensibles a retardos, jitter, etc. Por tal motivo se coloca como requerimiento.

3.1.2. Requerimientos de Software.

Estos requerimientos se limitan al sistema operativo que deberán utilizar los dispositivos (Routers). La tabla 3 del capítulo 2 lista la gama de sistemas operativos (IOS) para equipos que soportan DMVPN, uno de los puntos clave que muestra esta lista es que debe ser un IOS actual.

3.1.3. Requerimientos de conexiones

Los enlaces hacia la red pública o Internet y sus respectivos equipos son asignados por el ISP, y, en casos especiales el enrutador será adquirido por la empresa.

Se debe tener claro lo siguiente:

- El concentrador o Hub debe contar con un enlace hacia Internet con direccionamiento público estático.
- Los sitios remotos o sucursales deben contar con una conexión hacia Internet (no es necesario direccionamiento público estático).
- Se debe solicitar administración sobre el equipo del proveedor en el caso de no disponer de un equipo propio.

El último requerimiento listado depende del proveedor de servicio puesto que este último debe ceder la administración del dispositivo de tal forma que la configuración necesaria para habilitar DMVPN sea cargada. Como se ha dicho anteriormente existen casos puntuales en que el enrutador deberá ser adquirido por la empresa, tal como los siguientes casos:

- El equipo del proveedor no soporte DMVPN.
- El equipo del proveedor instalado en la matriz no sea el indicado para ser utilizado como HUB.
- No se tenga administración sobre el equipo instalado.

Los enlaces mencionados son a nivel WAN, las conexiones que se tengan en la red interna dependerá de cada empresa, la aplicación de este modelo ayuda a levantar una red DMVPN con las sedes principales y las sedes remotas o sucursales de modo que se simule una red única.

3.2. Topología de Red

Para que un Spoke sea capaz de entablar un túnel IPsec directo a otro Spoke de la red, este último debe poder alcanzar dicho punto. Para que lo antes indicado sea posible se debe configurar mGRE y NHRP sobre los Spokes que conforman la red DMVPN. Cuando esta opción es activada el tráfico entre los Spokes es recibido y el túnel directo establecido.

Al levantar conexiones entre los distintos puntos tenemos como resultado una topología completamente mallada (Figura 32).

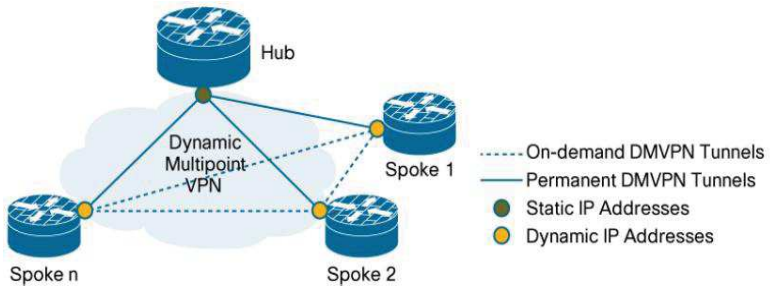


Figura 32. Topología completamente mallada.
Tomado de Cisco Systems, 2009, p.1

La figura 32 muestra una topología lógica completamente mallada la cual resultada de unir los distintos sitios que conformarán la red DMVPN.

3.3. Arquitectura de Red.

Como Cisco menciona IPsec es compatible solamente con IP unicast, por lo que mantener comunicaciones punto – multipunto y multipunto – multipunto seria complicado e ineficiente.

DMVPN combina el uso de tuneles mGRE, IPsec y NHRP de manera que el inconveniente antes indicado sea superado y obteniendo una arquitectura de red completamente compatible y fácil de implementar.

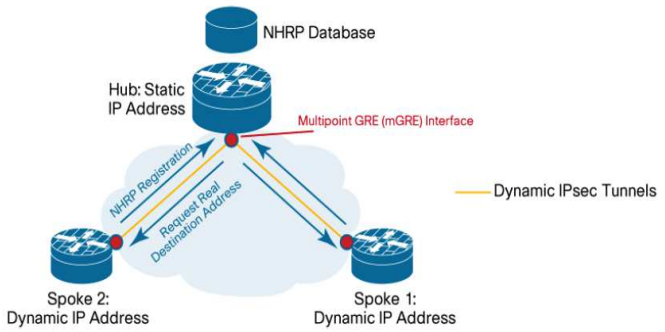


Figura 33. Arquitectura de red DMVPN
Tomado de Cisco Systems, 2009, p.3.

3.3.1. Interface túnel GRE multipunto (mGRE)

Este protocolo permitirá soportar múltiples túneles IPsec, simplificando el tamaño y la complejidad de la configuración al momento de añadir un nuevo dspositivo a la red.

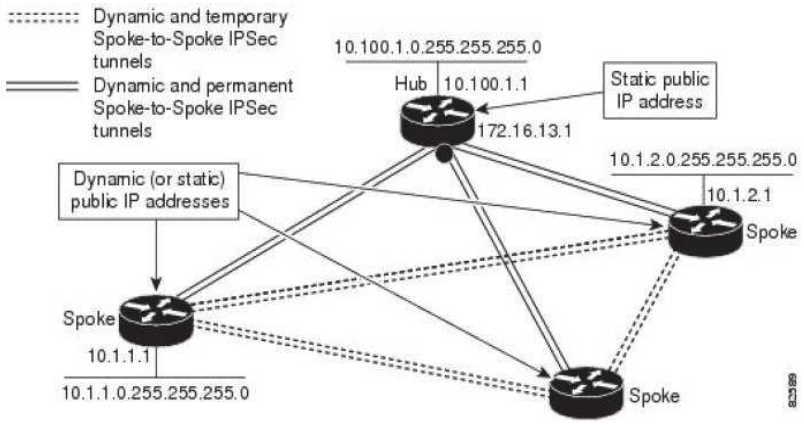


Figura 34. Túnel mGRE
Tomado de Cisco Systems, 2013, p.4.

3.3.2. Descubrimiento dinámico de puntos finales del túnel IPsec y perfiles de cifrados.

Elimina la necesidad de configurar mapas criptográficos estáticos que definen cada par de vecinos IPsec, lo que simplifica aún más la configuración.

3.3.3. NHRP.

Permite a los Spokes ser desplegados con direcciones IP públicas asignadas dinámicamente (por ejemplo detrás de un router del ISP). El HUB contiene una base de datos NHRP de las direcciones de la interface pública de cada uno de los Spokes. Para que el HUB obtenga las direcciones reales, cada uno de los Spoke registra su dirección real cuando inicia su sistema operativo; de esta forma cuando un Spoke requiere conexión directa hacia otro Spoke (armar un túnel) este solicita al HUB la dirección real del spoke destino de modo que lo pueda alcanzar de forma directa.

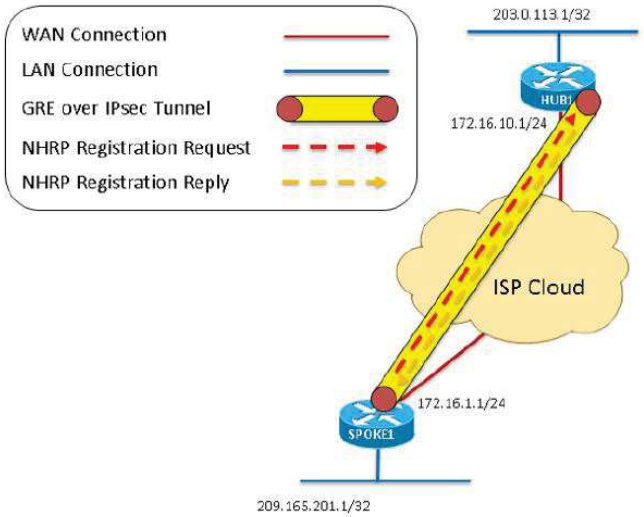


Figura 35. Arquitectura DMVPN.
Tomado de (Cisco System ,2014)
http://www.cisco.com/c/en/us/support/docs/security-vpn/dynamic-multi-point-vpn-dmvpn/116957-technote-dmvpn-00.html

3.4. Configuraciones

A continuación se muestra la configuración necesaria para levantar DMVPN:

3.4.1. Configuración en el HUB.

La configuración siguiente es aplicada en la sede principal o matriz, no obstante tendrá semejanza con la configuración aplicada en los Spokes.

3.4.1.1. Configuración de la Interface WAN.

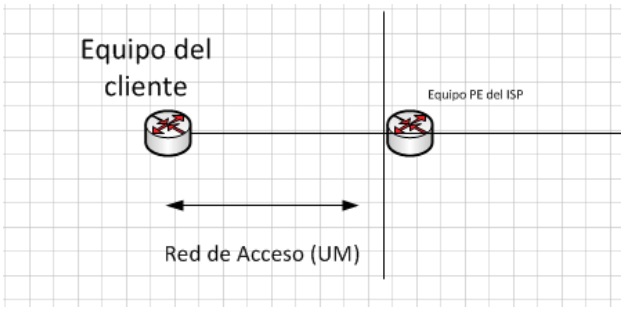


Figura 36. Conexión entre el cliente y el proveedor

Los comandos siguientes permitirán configurar la interface que usaremos como salida al mundo.

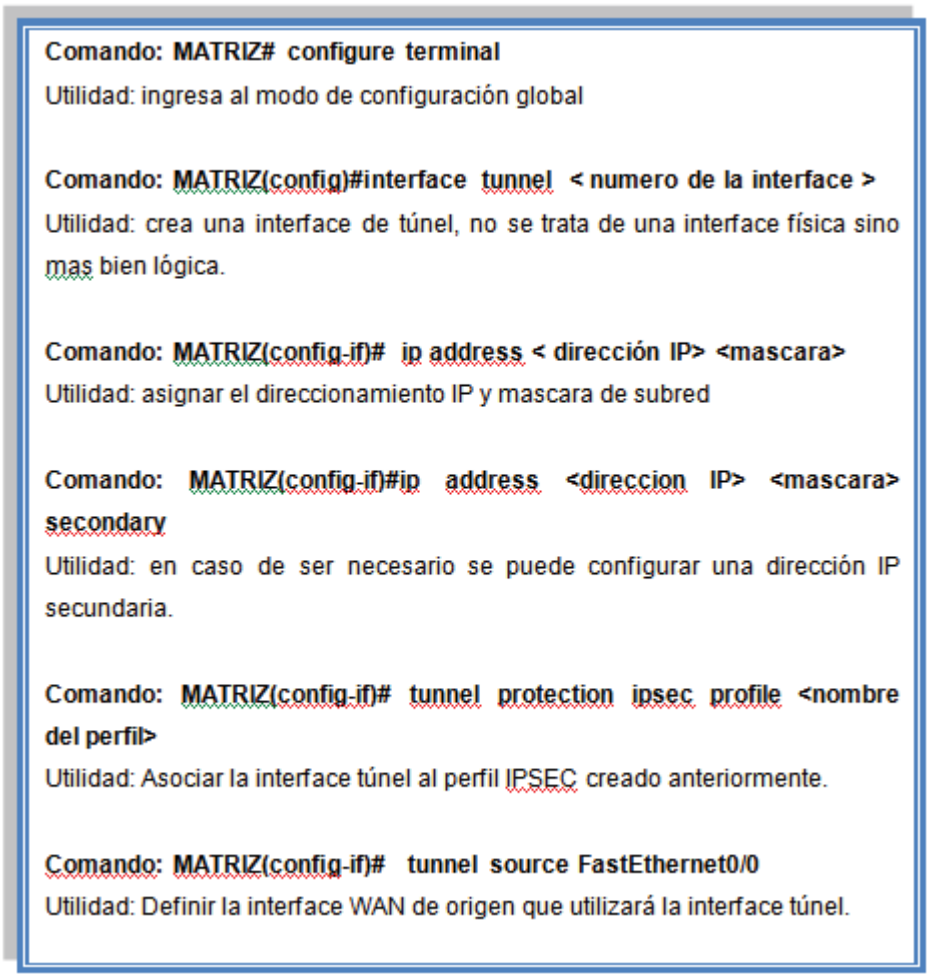


Figura 37.- Configuración de la Interface Wan.

Una vez realizada la configuración se tendrá como el siguiente ejemplo y habremos levantado la conexión entre el Hub y el proveedor:

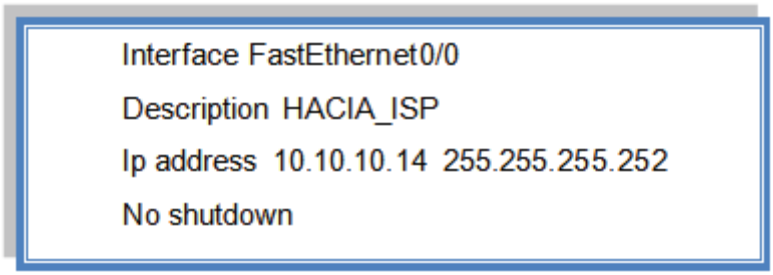


Figura 38. Ejemplo de Configuración.

El direccionamiento IP en la matriz será indicado por el proveedor de Internet debido a que debe ser direccionamiento público estático.

3.4.1.2. Configuración interface LAN

Las líneas de configuración siguientes ayudan a establecer el direccionamiento de la red interna o interface LAN.

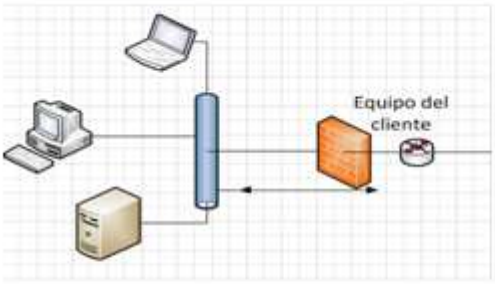


Figura 39. Direccionamiento para la red interna

Comando: MATRIZ(config)#interface fastEthernet <numero de la interface>
Utilidad: ingresa al modo de configuración de la interface.

Comando: MATRIZ(config-if)# ip address < dirección IP> <mascara>
Utilidad: asignar el direccionamiento y mascara de subred

Comando: MATRIZ(config-if)#no shutdown
Utilidad: habilitar la interface WAN.

Comando: MATRIZ(config-if)# Description < descripción >
Utilidad: proponer información sobre el enlace.

Figura 40. Configuración de la Interface Lan

Una vez realizado los pasos anteriores se tendrá como el siguiente ejemplo:

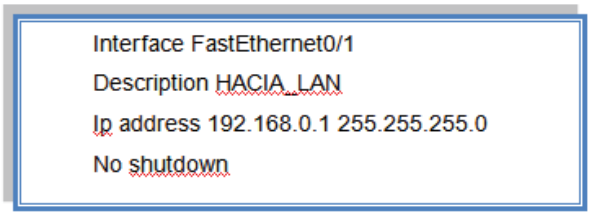


Figura 41. Ejemplo de Configuración.

3.4.1.3 Configuración IPsec

En esta parte del capítulo se indica la configuración de la seguridad del túnel que servirá de conexión segura entre los diferentes puntos.

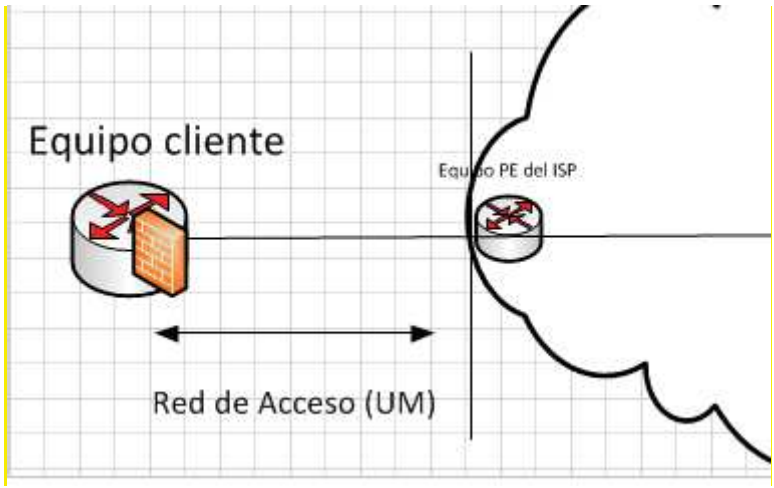
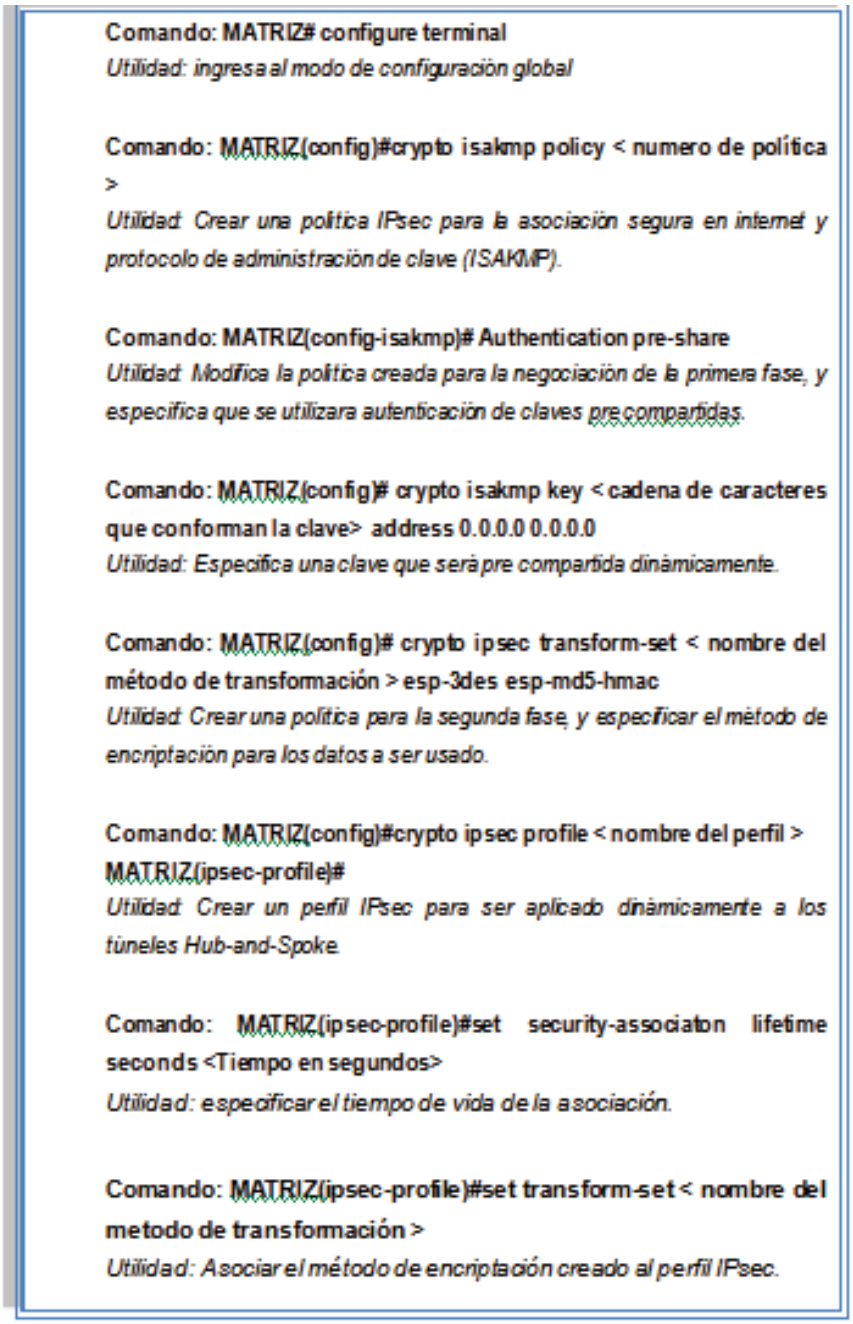


Figura 42. Diagrama de Conexión.

Una vez realizados los pasos anteriores la configuración IPsec se verá como en el siguiente ejemplo:



Comando: MATRIZ# configure terminal
Utilidad: ingresa al modo de configuración global

Comando: MATRIZ(config)#crypto isakmp policy < numero de política >
Utilidad: Crear una política IPsec para la asociación segura en internet y protocolo de administración de clave (ISAKMP).

Comando: MATRIZ(config-isakmp)# Authentication pre-share
Utilidad: Modifica la política creada para la negociación de la primera fase, y especifica que se utilizara autenticación de claves pre compartidas.

Comando: MATRIZ(config)# crypto isakmp key < cadena de caracteres que conforman la clave> address 0.0.0.0 0.0.0.0
Utilidad: Especifica una clave que será pre compartida dinámicamente.

Comando: MATRIZ(config)# crypto ipsec transform-set < nombre del método de transformación > esp-3des esp-md5-hmac
Utilidad: Crear una política para la segunda fase, y especificar el método de encriptación para los datos a ser usado.

Comando: MATRIZ(config)#crypto ipsec profile < nombre del perfil > MATRIZ(ipsec-profile)#
Utilidad: Crear un perfil IPsec para ser aplicado dinámicamente a los túneles Hub-and-Spoke.

Comando: MATRIZ(ipsec-profile)#set security-associaton lifetime seconds <Tiempo en segundos>
Utilidad: especificar el tiempo de vida de la asociación.

Comando: MATRIZ(ipsec-profile)#set transform-set < nombre del metodo de transformación >
Utilidad: Asociar el método de encriptación creado al perfil IPsec.

Figura 43. Configuración IPSEC

```
crypto isakmp policy 1
encr 3des
hash md5
authentication pre-share

group 2
crypto isakmp key firewall.cx address 0.0.0.0 0.0.0.0
crypto ipsec transform-set TS esp-3des esp-md5-
hmac
crypto ipsec profile protect-gre
set security-association lifetime seconds 86400
set transform-set TS
!
```

Figura 44. Ejemplo de configuración.

3.4.1.4. Configuración interface del túnel.

A continuación se muestra la configuración aplicada para crear el túnel que servirá para las conexiones multipunto, cabe mencionar un punto clave, todos los HUB y Spokes que son parte de una misma red DMVPN deben tener el mismo direccionamiento de subred.

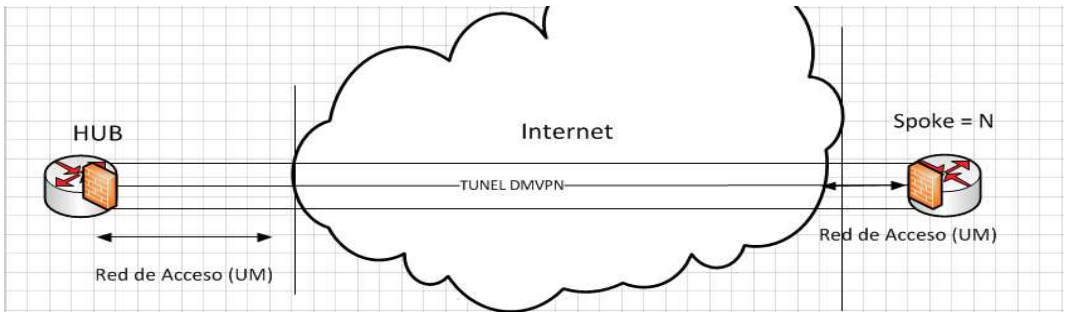


Figura 45. Conexión lógica mediante la creación de un túnel.

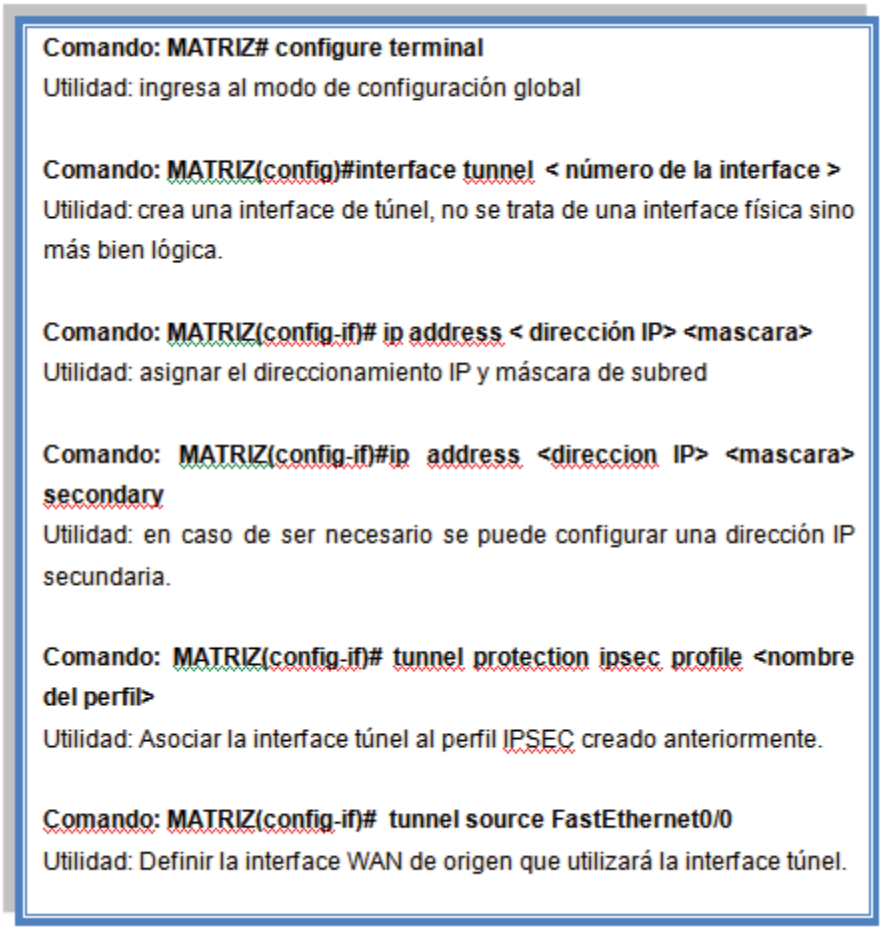


Figura 46.- Configuración Tunnel .

3.4.1.5. Configuración de mGRE sobre la interface del túnel.

Enseguida se muestra la configuración del protocolo mGRE que en resumida teoría ayuda a levantar el túnel multipunto.

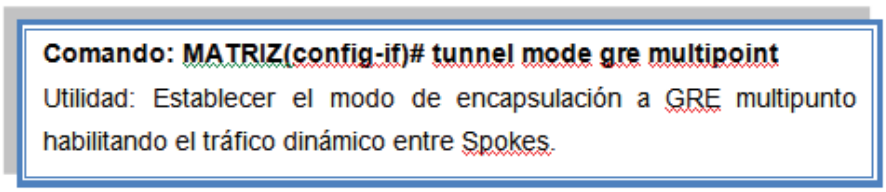


Figura 47. Configuración de MGRE.

3.4.1.6. Configuración del protocolo NHRP sobre la interface del túnel

A continuación la configuración del protocolo NHRP, que ayuda a reconocer la dirección real del destino.

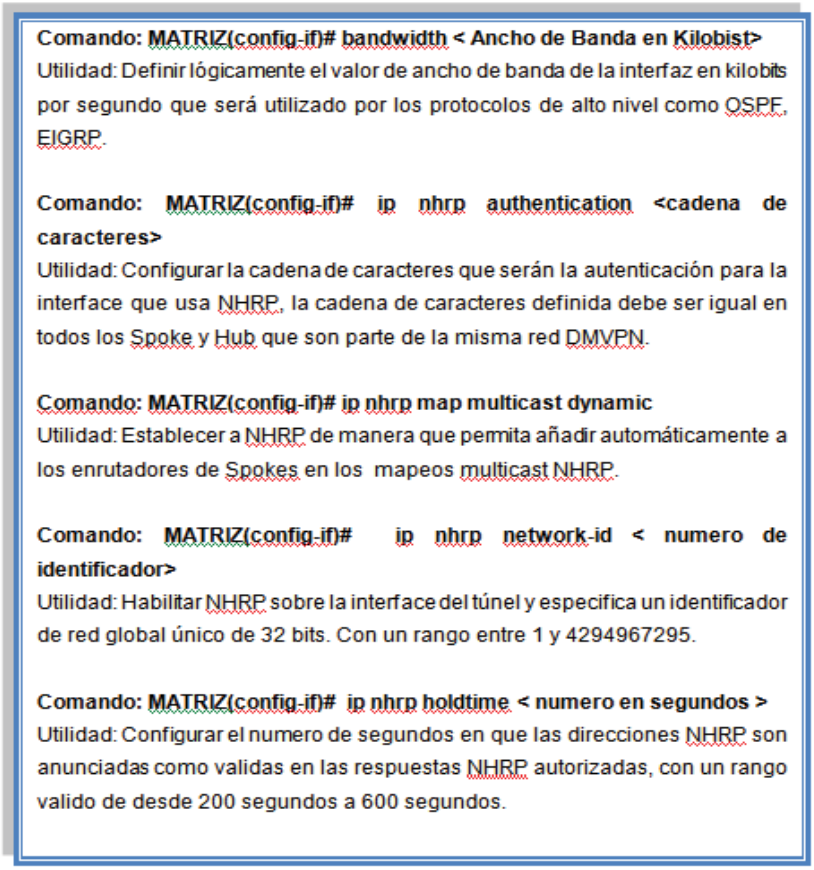


Figura 48. Configuración del NHRP sobre la Interface Túnel.

3.4.1.7. Configuración del Protocolo de enrutamiento dinámico OSPF sobre la interface túnel.

En seguida se muestra las líneas de configuración para habilitar el protocolo de enrutamiento dinámico que anunciará nuestras sub-redes por toda la red DMVPN.

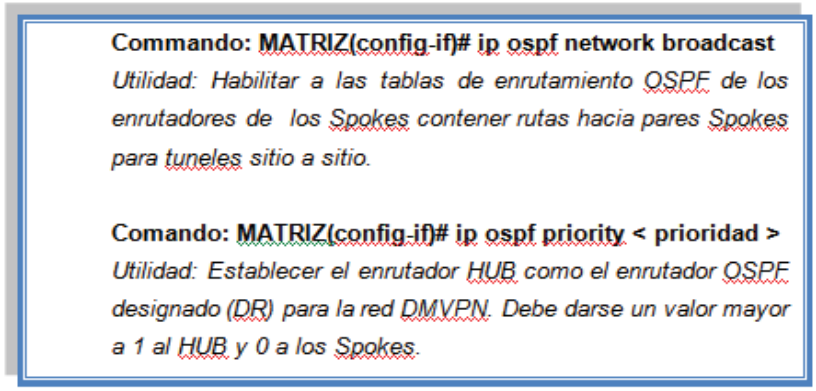


Figura 49. Configuración de Protocolo de Enrutamiento OSPF.

3.4.2. Configuración de los Spokes.

La configuración aplicada en los siguientes pasos es establecida para los Spokes sin importar su ubicación.

3.4.2.1. Configuración de la Interface WAN

Los comandos siguientes permiten configurar la interface que usada como salida hacia la red pública o Internet.

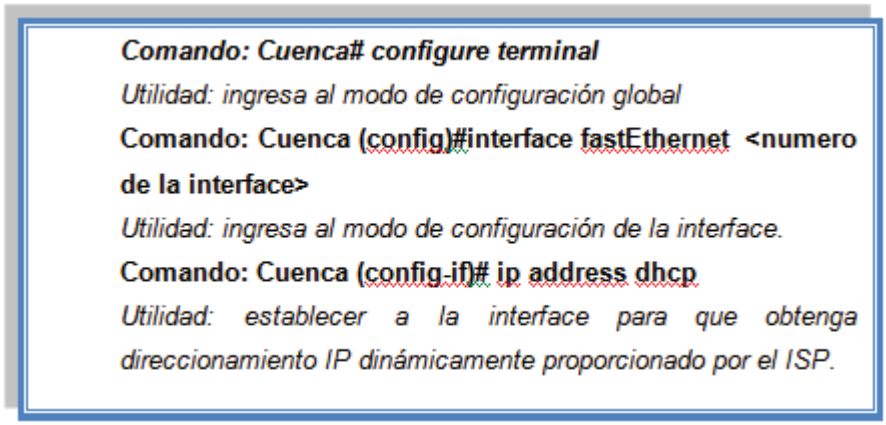


Figura 50. Configuración de Spokes WAN.

En caso de tener la necesidad de un sitio remoto con direccionamiento IP público estático se debe colocar de la manera siguiente:

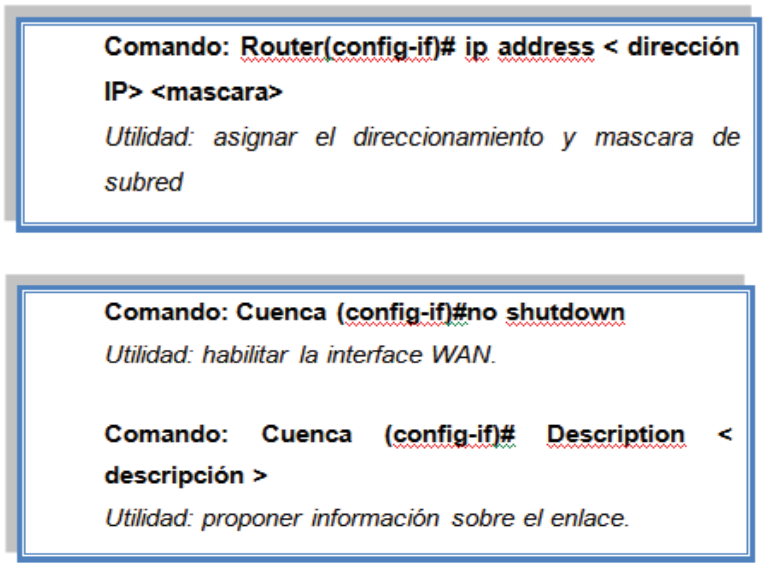


Figura 51. Configuración de Spokes WAN.
Tomado Cisco, s.f.

Una vez realizada la configuración de la interface se tendrá lo siguiente:

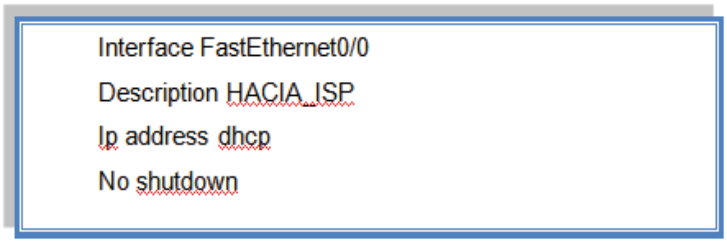


Figura 52. Ejemplo de Configuración

El direccionamiento IP de los Spokes no tiene que ser público estático necesariamente, puede ser automático y dinámico.

3.4.2.2 Configuración interface LAN

A continuación se muestra las líneas para configurar la interface interna o LAN.

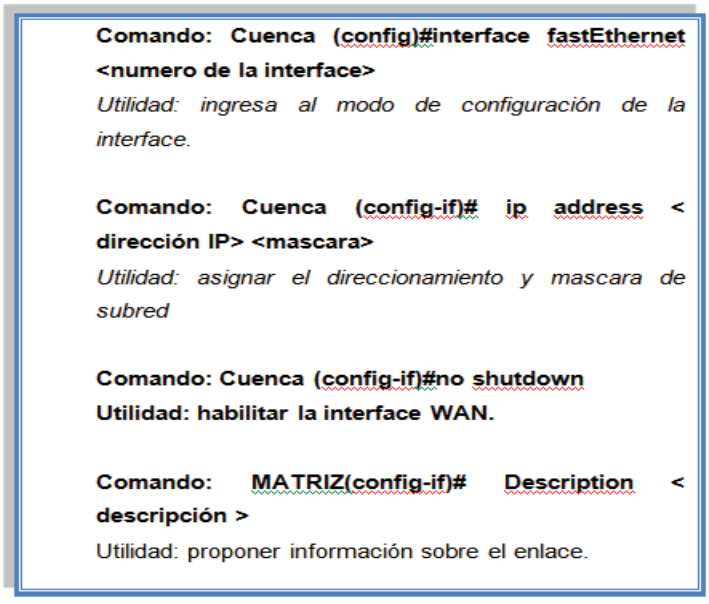


Figura 53. Configuración de Spokes LAN.

Una vez realizado los pasos anteriores se tendrá como el siguiente ejemplo:

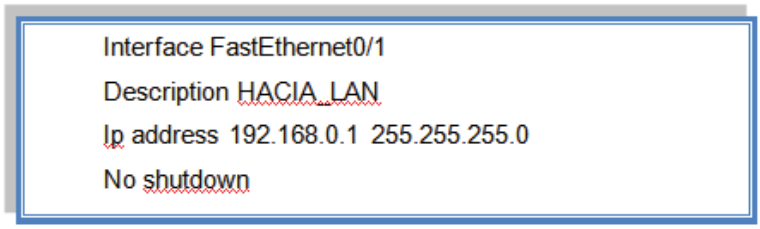


Figura 54. Ejemplo de Configuración

3.4.2.3 Configuración IPsec

En esta parte del capítulo se inicia la configuración de la seguridad del túnel que servirá de conexión entre los diferentes puntos.

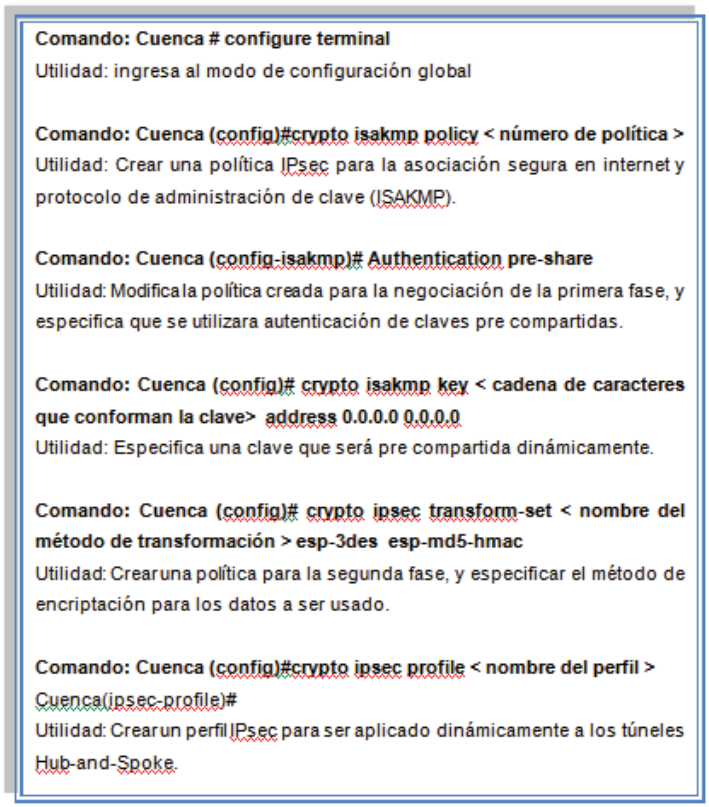


Figura 55. Configuración de IPSEC.

Una vez realizado los pasos anteriores la configuración IPsec será como en el siguiente ejemplo:

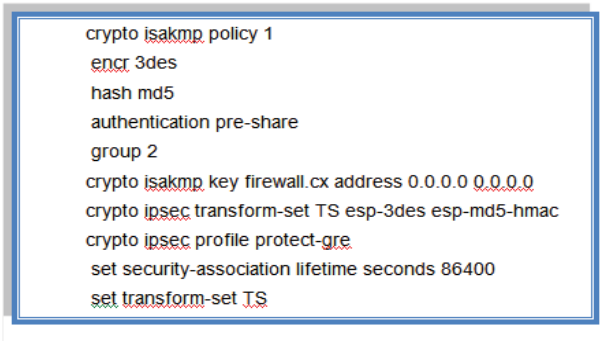


Figura 56. Ejemplo de Configuración.

3.4.2.4 Configuración interface del túnel.

A continuación se muestra la configuración aplicada para crear el túnel que servirá para las conexiones multipunto, cabe mencionar un punto clave, todos los HUB y Spokes que son parte de una misma red DMVPN deben tener el mismo direccionamiento de subred.

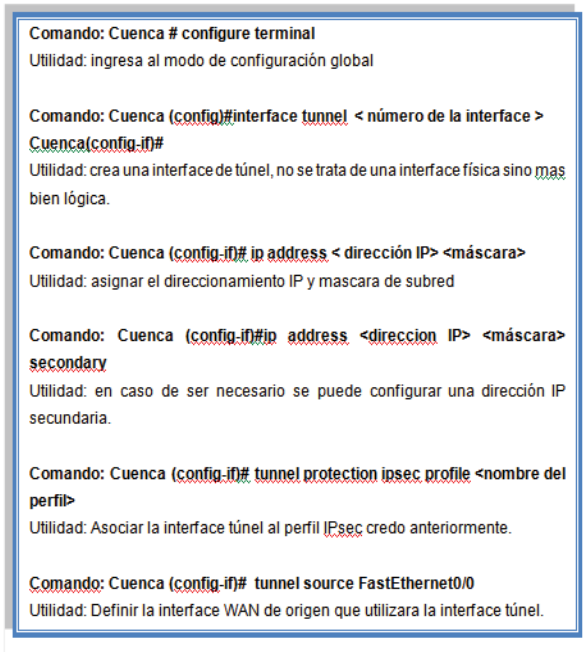


Figura 57. Configuración de Túnel.

3.4.2.5. Configuración de mGRE sobre la interface del túnel

Acto seguido se muestra las líneas correspondientes para habilitar el protocolo que permitirá establecer el túnel multipunto.

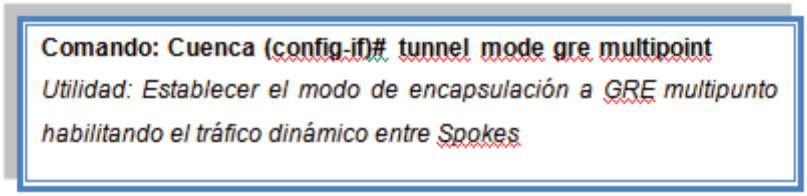


Figura 58.- Configuración de mGRE.

3.4.2.6. Configuración del protocolo NHRP sobre la interface del túnel.

Del mismo modo que los pasos anteriores a continuación se detalla la configuración del protocolo de resolución del siguiente salto.

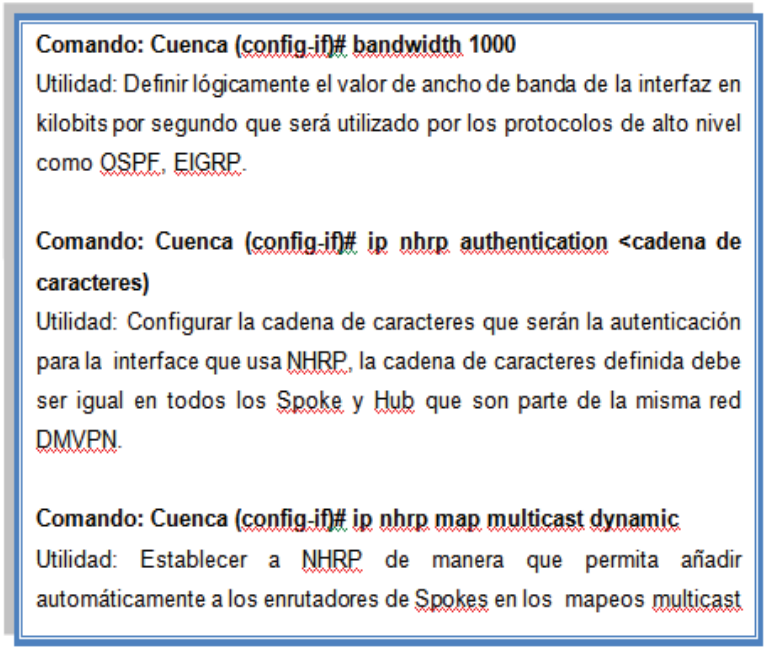


Figura 59. Configuración de NHRP.

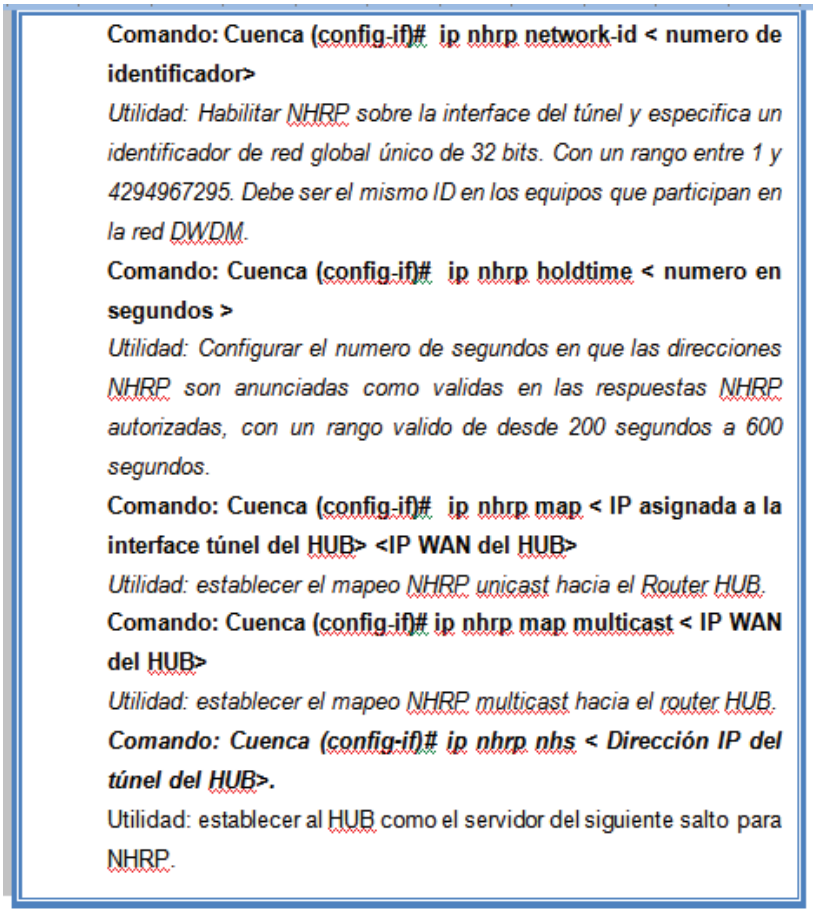


Figura 60. Configuración de NHRP.

3.4.2.7. Configuración del Protocolo de enrutamiento dinámico sobre la interface túnel.

Finalmente en los pasos siguientes se dan a conocer la configuración necesaria para habilitar los protocolos de enrutamiento dinámico que permitan publicar las subredes a toda la red DMVPN.

Se tiene las siguientes alternativas:

- Protocolo de enrutamiento dinámico OSPF.
- Protocolo de enrutamiento dinámico EIGRP.

3.4.2.7.1. Configuración del protocolo OSPF sobre la interface de túnel.

En la red DMVPN se debe configurar un protocolo de enrutamiento dinámico para propagar las redes que serán parte de esta topología, los pasos siguientes muestran como habilitar el protocolo de enrutamiento OSPF sobre la interface de túnel creada.

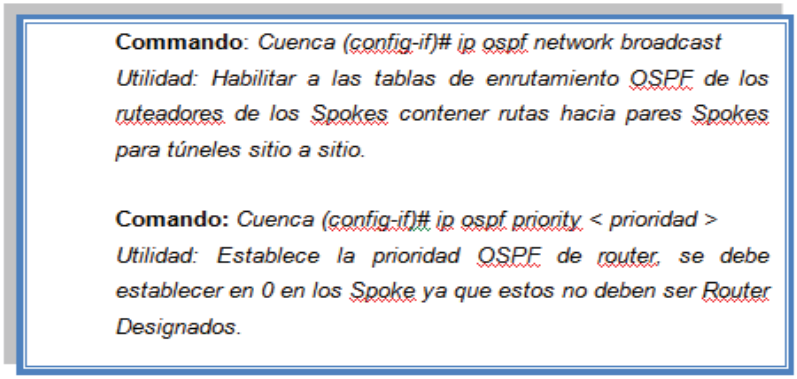


Figura 61. Configuración de Protocolo OSPF en la Interface Tunel.

3.4.2.7.2. Configuración del protocolo dinámico EIGRP sobre la interface de túnel.

A continuación se muestra los pasos para configurar el protocolo de enrutamiento EIGRP sobre la interface de túnel.

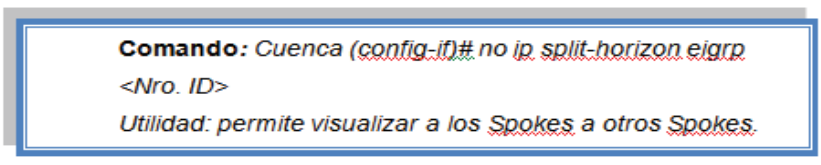


Figura 62. Configuración de Protocolo EIGRP en la Interface Túnel.

3.4.3. Configuración del Protocolo de enrutamiento en el HUB y Spoke.

En base a lo dispuesto en el Capítulo II se requiere configurar un protocolo de enrutamiento dinámico para anunciar nuestras redes a todos los sitios que conforman la red DMVPN, pudiendo tomar como opciones los protocolos dinámicos OSPF o EIGRP.

A continuación se muestra la configuración para el protocolo EIGRP:

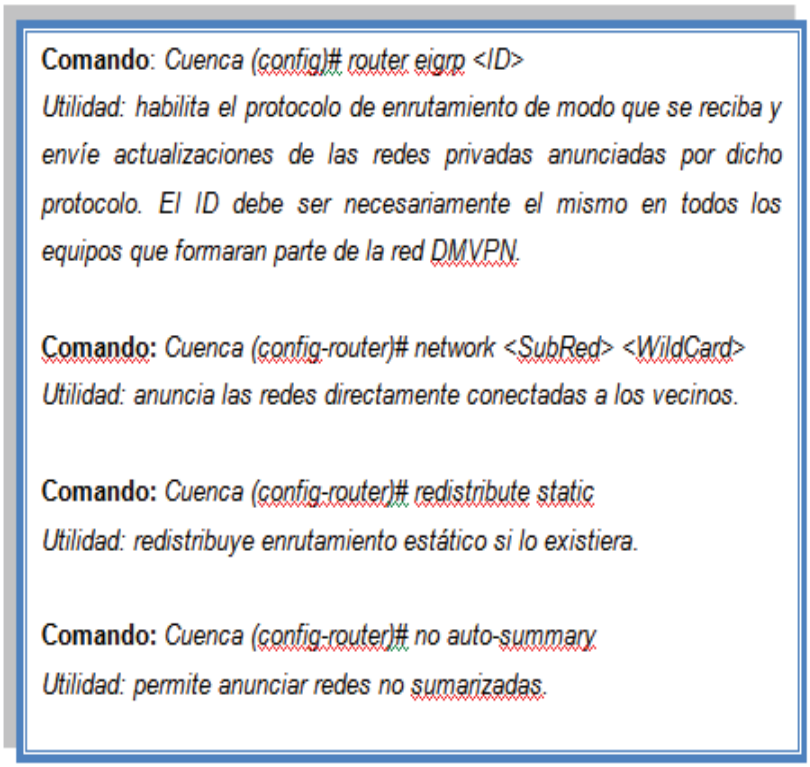


Figura 63. Configuración de Protocolo EIGRP HUB Y SPOKE.

A continuación la configuración del protocolo OSPF:

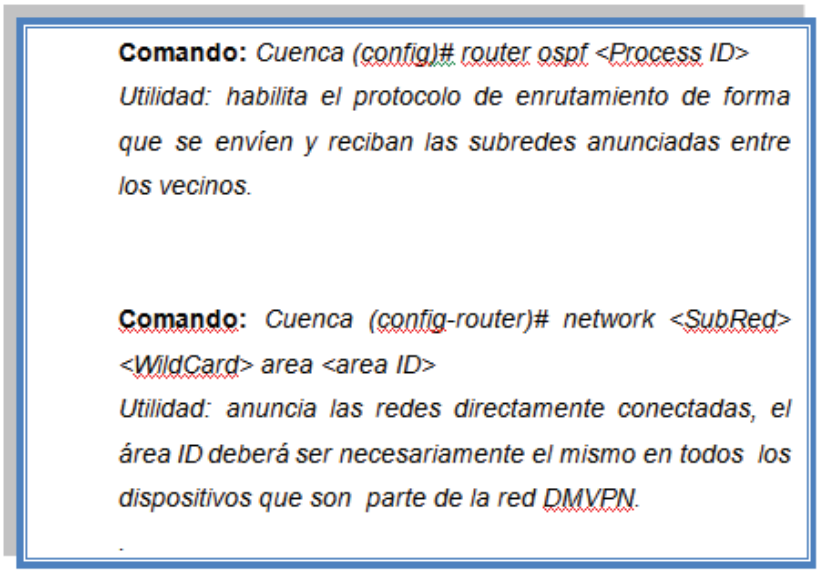


Figura 64. Configuración de Protocolo OSPF HUB Y SPOKE.

3.4.4 Presentación del Modelo de Red DMVPN

El siguiente modelo responde a los puntos mencionados anteriormente, y a las VPNs basadas en dispositivos CE(Customer Edge), la red de acceso o última milla proporciona las conexiones entre los dispositivos CE y router PE(Provider Edge). Puede tratarse de una red de capa 2 (FR, ATM, Ethernet, etc) o una red IP. El equipo CE y PE entablan conectividad de capa 3 sobre la última milla, en el contexto de las redes DMVPN, el túnel VPN establecido entre dos puntos distintos es un túnel IP entre estos de forma dinámica y formando una red privada completamente mallada utilizando la red pública o Internet.

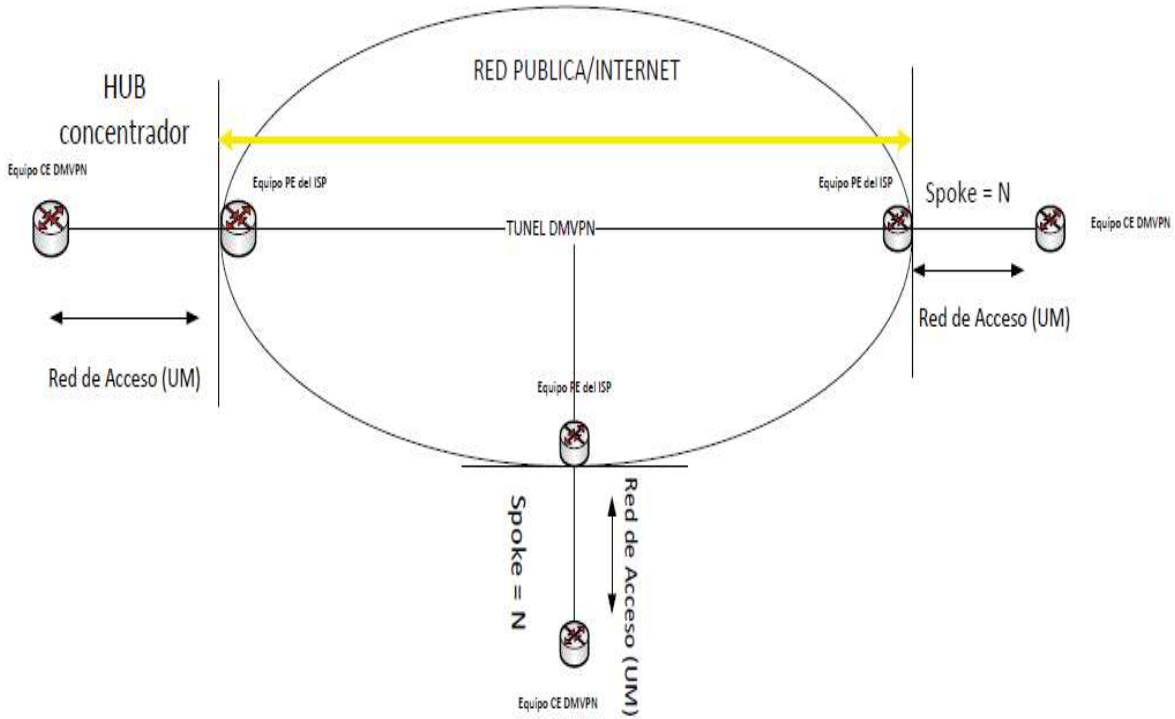


Figura 65. Modelo de Implementación DMVPN.

3.4.5 Análisis de Costos con proveedores de Internet y enlaces dedicados:

A continuación se muestra costos relacionados a dos proveedores de internet que comercializan enlaces de Internet para Pymes:

Tabla 4 . Costos de enlaces de Internet para Pymes proveedor Netlife:

	PLAN PYME 1	PLAN PYME 2	PLAN PYME 3	PLAN PYME 4	PLAN PYME 5
Velocidad Local	6/6 Mbps	9/9 Mbps	15/15 Mbps	24/24 Mbps	48/48 Mbps
Velocidad Internacional	2/2 Mbps	3/3 Mbps	5/5 Mbps	8/8 Mbps	16/16 Mbps
Comparticion	2:1	2:1	2:1	2:1	2:1
Soporte Tecnico	24/7	24/7	24/7	24/7	24/7
Precio Final Incluido IVA	$81 76 DÓLARES	$112 00 DÓLARES	$133 28 DÓLARES	$174 72 DÓLARES	$280 00 DÓLARES

Tomado de (netlife.ec, 2015) http://www.netlife.ec/planes/pymes/internet-de-alta-velocidad/nuestros-planes/

Tabla 5. Costos de enlaces de Internet para Pymes proveedor CNT:

PLAN DE INTERNET PYMES ASIMÉTRICO (Velocidad Bajada x Velocidad Subida)	Tarifa mensual	Inscripción
Hasta 1 x 0,512 Mbps	$45.00	$80.00
Hasta 2 x 0,768 Mbps	$65.00	$80.00
Hasta 3 x 0,768 Mbps	$80.00	$80.00
Hasta 4 x 2 Mbps	$91.51	$250.00
Hasta 6 x 3 Mbps	$109.00	$250.00
Hasta 10 x 5 Mbps	$150.00	$250.00
Hasta 15 x 7 Mbps	$200.00	$380.00
Hasta 20 x 10 Mbps	$260.00	$380.00
Hasta 25 x 15 Mbps	$300.00	$380.00

Tomado de (cnt.gob.ec, 2015) https://www.cnt.gob.ec/internet/plan-corporativo/internet-pymes/

Seguidamente se muestra una tabla de costos referencial de enlaces de Datos dedicados con el proveedor Telconet:

Tabla 6. Costos de enlaces de datos dedicados proveedor Telconet:

Proveedor	Ancho de banda en Kbps	Tarifa Mensual	Instalación
Telconet	3072	300.00	150.00
	2048	248.64	150.00
	1024	150.00	150.00

Tomado de cotización realizada al proveedor Telconet.

3.4.5.1 Análisis de costos proveedores de Internet para Pymes:

Para realizar un análisis con respecto al beneficio del uso de un enlace de Internet sobre un enlace de datos dedicado se realiza lo siguiente:

Con el primer proveedor NetLife tómanos como referencia un ancho de banda de 6/6 Mbps nacional y 2/2Mbps Internacional por un costo de 81,76$ mensual.

Ahora con el segundo proveedor CNT tenemos anchos de banda menores y por ende de menor costo, sin embargo para efectos del análisis se hará referencia con un ancho de banda parecido al primer proveedor NetLife.

Con el proveedor CNT tomamos el ancho de banda de 4Mbps en descarga de datos y 2Mbps en subida de datos con un costo de 91,50$ mensual.

Para determinar un valor promedio entre los dos proveedores se realiza el siguiente cálculo:

Procedemos a calcular un valor promedio de costo entre los dos proveedores realizando la suma de los dos valores y su resultado dividido para 2:

(91,50 + 81,76) /2 = 86,63$

(Ecuación 1)

3.4.5.2 Análisis con respecto al proveedor de enlaces de datos dedicados:

Debido que se ha tomado referencialmente enlaces de Internet no menores a 2Mbps, de igual forma se realizará con el proveedor de un enlace de datos dedicado en este caso Telconet.

El Proveedor Telconet ofrece un enlace de datos de 2048Mbps por un costo de 248.64$ que a simple vista resulta de mayor costo al de un enlace de Internet.

Para efectos del análisis se realizará el siguiente cálculo:

Tomamos el valor de 248.64$ como el 100%, seguidamente calcularemos el porcentaje que corresponde al valor calculado anteriormente correspondiente al resultado del primer cálculo:

Entonces:

248,74$ = 100% (Ecuación 2)

86,63$ = ? (Ecuación 3)

Aplicando una regla de 3 tenemos el siguiente resultado:

(86,63 X 100) / 248,74 = 34,82% (Ecuación 4)

Como se puede visualizar el valor obtenido es del 34,82% que equivale al valor de un enlace de Internet.

Ahora se realiza la siguiente resta para determinar el % de diferencia entre ambos enlaces:

Resta del 100%:

100% - 34,82% = 65,17% (Ecuación 5)

Como conclusión tenemos un resultado de diferencia del 65,17% entre un enlace de Internet y un enlace de datos dedicado.

4. Implementación del Modelo.

Esta parte del proyecto se enfoca en implementar el modelo propuesto en el capítulo III sobre un ambiente de laboratorio con el fin de comprobar su funcionamiento.

Para lo antes mencionado se hará uso del laboratorio y equipos proporcionados por la Universidad de Las Américas.

4.1. Requerimientos.

4.1.1. Requerimientos de hardware.

Se utilizará los dispositivos necesarios para demostrar el funcionamiento de una red DMVPN, y serán los que se detallan a continuación:

Tabla 7. Detalle de equipos utilizados en el laboratorio.

Cantidad	Equipo	Marca	Modelo	Función en la red DMVPN
1	Router	Cisco	2800	Router HUB
1	Router	Cisco	2800	Router Spoke
1	Router	Cisco	2800	Router Spoke
1	Router	Cisco	871	Router Spoke
1	Switch	Cisco	3560	Nube Internet
3	Router	Cisco	2900	Nube Internet

La red DMVPN estará conformada por 4 equipos routers. Y la nube de Internet será emulada con 3 enrutadores y un switch Cisco.

4.1.2 Requerimientos de Software.

A continuación se muestra el sistema operativo IOS que debe ser cargado en los dispositivos:

Tabla 8. Sistema operativo para los equipos Cisco de la serie 2800 que conforman la red.

IOS Router 2800
Cisco IOS Software Release 15.0 or later recommended for Cisco 2800

Tomado de Cisco System Dmvpn Data Sheet, 2009, p.6.

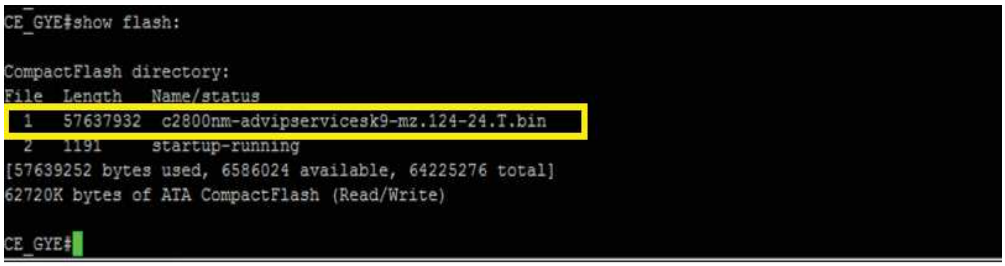


Figura 66. IOS utilizado en los Routers 2800.

Tabla 9. Sistema operativo para los equipos Cisco de la serie 870 que conforman la red.

IOS Router 870
Cisco IOS Software Release 12.3(2)T or later recommended for Cisco 870,

Tomado de Cisco System Dmvpn Data Sheet, 2009, p.6.

4.2. Conexiones realizadas en el laboratorio de cómputo de la UDLA.

4.2.1 Conexiones en el HUB de Quito.

El sitio concentrador/ matriz contiene un router HUB DMVPN (Router Cisco 2800) conectado a la red de un proveedor de Internet (Switch).

Figura 67. Router utilizado como HUB o Matriz.

4.2.2. Conexiones de los Spoke.

Esta parte de la red será representada por los dos enrutadores 2800 y el enrutador cisco 870, serán los que tendrán la función de Spokes conectados hacia la red pública (Switch). Siendo representados por las ciudades de Guayaquil, Cuenca, Ambato.

4.2.2.1. Conexiones en el Spoke de Guayaquil.

Figura 68. Router utilizado como Spoke ubicación GYE.

4.2.2.2. Conexiones en el Spoke de Cuenca.

Figura 69. Router utilizado como Spoke ubicación Cuenca.

4.2.2.3. Conexiones en el Spoke de Ambato.

Figura 70. Router utilizado como Spoke Ambato.

4.2.2.4. Conexiones de los equipos que conforman la Nube de Internet.

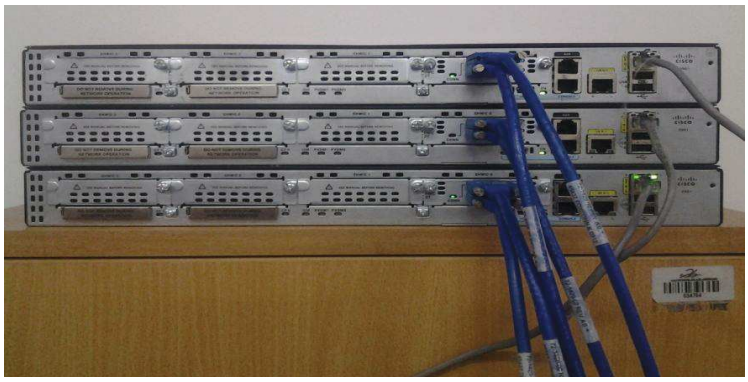


Figura 71. Enrutadores que integran la nube de Internet.

4.2.2.5. Laboratorio completo.

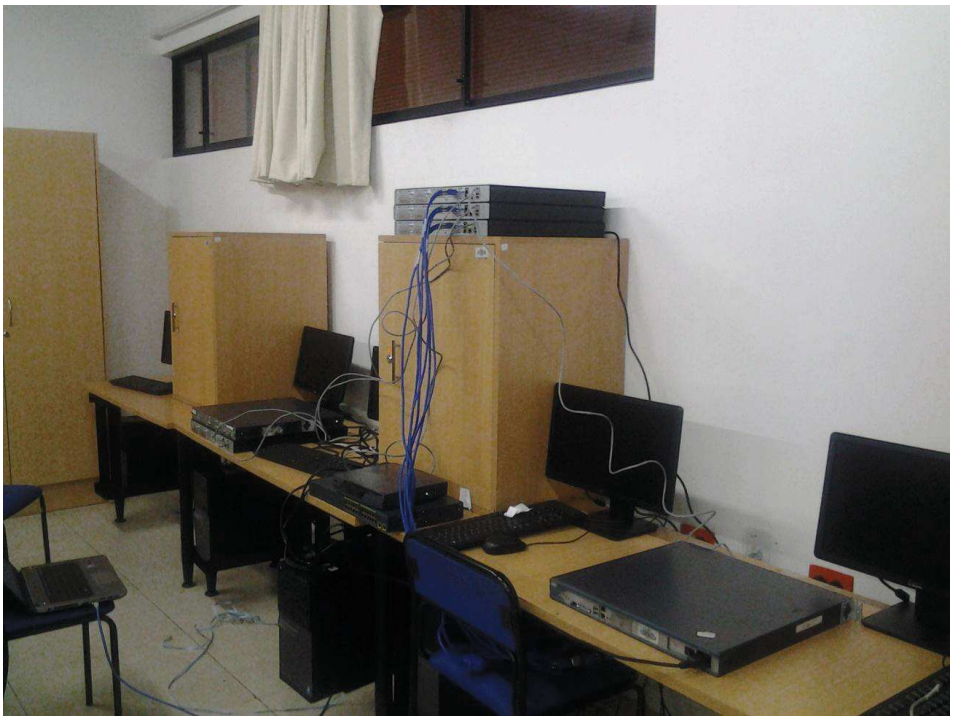


Figura 72. Laboratorio completo con los equipos seleccionados.

4.3. Direccionamiento de RED.

En seguida se muestra las direcciones IP correspondientes a cada punto de la red DMVPN.

4.3.1. Enrutamiento WAN:

Tabla 10. Direccionamiento de red para los distintos enlaces WAN

Ubicación	Equipo	Direccionamiento statico	Direccionamiento dinamico
Quito	Router Cisco 1900	192.200.200.10/30	NA
Guayaquil	Router Cisco 1900	193.200.200.14/30	NA
Cuenca	Router Cisco 1900	NA	194.200.200.0/24
Ambato	Router Cisco 870	NA	192.168.1.0/24

4.3.2. Enrutamiento LAN.

Tabla 11. Direccionamiento de red interna

Ubicación	Equipo	Direccionamiento tunel 0	Direccionamiento LAN (Loopback0)
Quito	Router Cisco 1900	172.16.1.1/24	192.168.10.0/24
Guayaquil	Router Cisco 1900	172.16.1.2/24	192.168.11.0/24
Cuenca	Router Cisco 1900	172.16.1.3/24	192.168.12.0/24
Ambato	Router Cisco 870	172.16.1.4/24	192.168.13.0/24

4.4. Topología de red

A continuación se muestra como estaría la topología lógica y física conforme a la infraestructura elegida y sus ubicaciones respectivas.

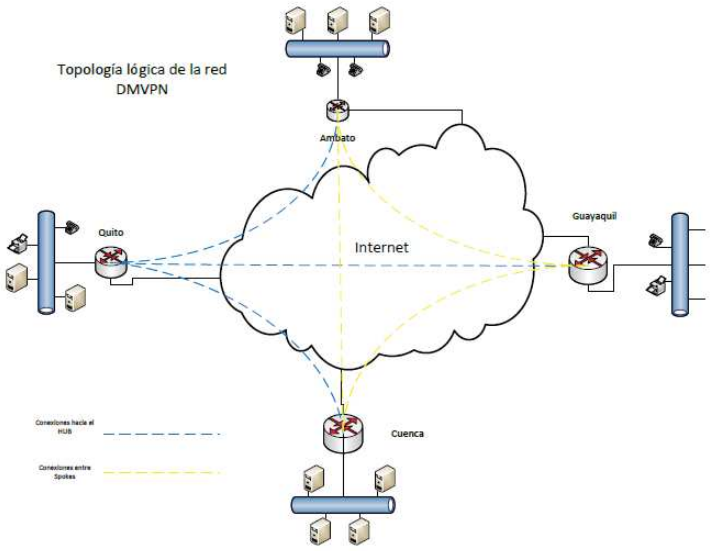


Figura 73. Muestra la topología de conexiones lógicas de la red DMVPN.

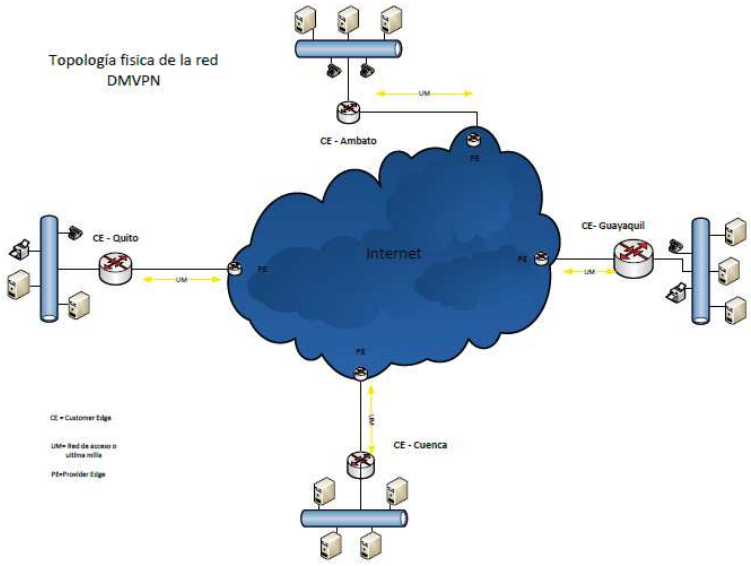


Figura 74. Muestra la topología de conexiones físicas de los diferentes puntos de interconexión.

4.5. Configuración a Ejecutar en los Dispositivos de Red.

4.5.1. Configuración aplicada sobre el router concentrador ubicado en Quito.

CE_QUITO

Hostname CE_QUITO

interface FastEthernet0/0

description HACIA_ISP

ip address 192.200.200.10 255.255.255.252

interface Loopback0

description HACIA_LAN

ip address 192.168.10.1 255.255.255.0

Configuración IPsec:

crypto isakmp policy 1

encr 3des

hash md5

authentication pre-share

group 2

crypto isakmp key Udlakey address 0.0.0.0 0.0.0.0

crypto ipsec transform-set transformacion esp-3des esp-md5-hmac

crypto ipsec profile protect-gre

set security-association lifetime seconds 86400

set transform-set transformacion

interface Tunnel0

ip address 172.16.1.1 255.255.255.0

no ip redirects

```
 ip nhrp authentication Udla
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 no ip split-horizon eigrp 1
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile protect-gre
router eigrp 1
network 172.16.1.0 0.0.0.255
network  192.168.10.0 0.0.0.255
 no auto-summary
```

<Ruta estática hacia el ISP>.

```
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
```

4.5.2. Configuración en el Spoke ubicación Guayaquil.

CE_GYE

```
Hostname CE_GYE
interface FastEthernet0/0
 description HACIA_ISP
 ip address 193.200.200.14 255.255.255.252
interface Loopback0
description HACIA_LAN
ip address 192.168.11.1 255.255.255.0
crypto isakmp policy 1
 encr 3des
 hash md5
```

```
 authentication pre-share
 group 2
crypto isakmp key Udlakey address 0.0.0.0 0.0.0.0
crypto ipsec transform-set transformacion esp-3des esp-md5-hmac
crypto ipsec profile protect-gre
 set security-association lifetime seconds 86400
 set transform-set transformacion
```

<Configuración InterfaceTunnel 0>

```
interface Tunnel0
 ip address 172.16.1.2 255.255.255.0
 no ip redirects
 ip nhrp authentication Udla
 ip nhrp map multicast dynamic
 ip nhrp map multicast 192.200.200.10
 ip nhrp map 172.16.1.1 192.200.200.10
 ip nhrp network-id 1
 ip nhrp nhs 172.16.1.1
 no ip split-horizon eigrp 1
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile protect-gre
```

Enrutamiento dinámico de las redes DMVPN.

```
router eigrp 1
 network 172.16.1.0 0.0.0.255
 network  192.168.11.0 0.0.0.255
 no auto-summary
```

Ruta estática hacia el ISP.

ip route 0.0.0.0 0.0.0.0 FastEthernet0/0

4.5.3. Configuración en el Spoke ubicación Cuenca.

CE_CUENCA

```
Hostname CE_CUENCA
interface FastEthernet0/0
 description HACIA_ISP
 ip address dhcp
interface Loopback0
description HACIA_LAN
ip address 192.168.12.1 255.255.255.0
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key Udlakey address 0.0.0.0 0.0.0.0
crypto ipsec transform-set transformacion esp-3des esp-md5-hmac
crypto ipsec profile protect-gre
 set security-association lifetime seconds 86400
 set transform-set transformacion
interface Tunnel0
 ip address 172.16.1.3 255.255.255.0
 no ip redirects
 ip nhrp authentication Udla
```

```
 ip nhrp map multicast dynamic
 ip nhrp map multicast 192.200.200.10
 ip nhrp map 172.16.1.1 192.200.200.10
 ip nhrp network-id 1
 ip nhrp nhs 172.16.1.1
 no ip split-horizon eigrp 1
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile protect-gre
```

<Enrutamiento dinámico de las redes que conforman DMVPN.>

```
Router eigrp 1
 network 172.16.1.0 0.0.0.255
 network  192.168.12.0 0.0.0.255
 no auto-summary
```

<Ruta estática hacia el ISP>.

```
Ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
```

4.5.4. Configuración en el Spoke ubicación Ambato.

CE_AMBATO

```
Hostname CE_AMBATO
interface FastEthernet0/0
 description HACIA_ISP
 ip address dhcp
interface Loopback0
description HACIA_LAN
ip address 192.168.13.1 255.255.255.0
```

```
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key Udlakey address 0.0.0.0 0.0.0.0
crypto ipsec transform-set transformacion esp-3des esp-md5-hmac
crypto ipsec profile protect-gre
 set security-association lifetime seconds 86400
 set transform-set transformacion
```

<Configuración InterfaceTunnel 0>

```
interface Tunnel0
 ip address 172.16.1.4 255.255.255.0
 no ip redirects
 ip nhrp authentication Udla
 ip nhrp map multicast dynamic
 ip nhrp map multicast 192.200.200.10
 ip nhrp map 172.16.1.1 192.200.200.10
 ip nhrp network-id 1
 ip nhrp nhs 172.16.1.1
 no ip split-horizon eigrp 1
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile protect-gre
```

<Enrutamiento dinámico de las redes DMVPN>.

```
router eigrp 1
```

network 172.16.1.0 0.0.0.255

network 192.168.13.0 0.0.0.255

no auto-summary

<Ruta estática hacia el ISP.>

ip route 0.0.0.0 0.0.0.0 FastEthernet0/0

4.5.5. Configuración en de la nube de Internet.

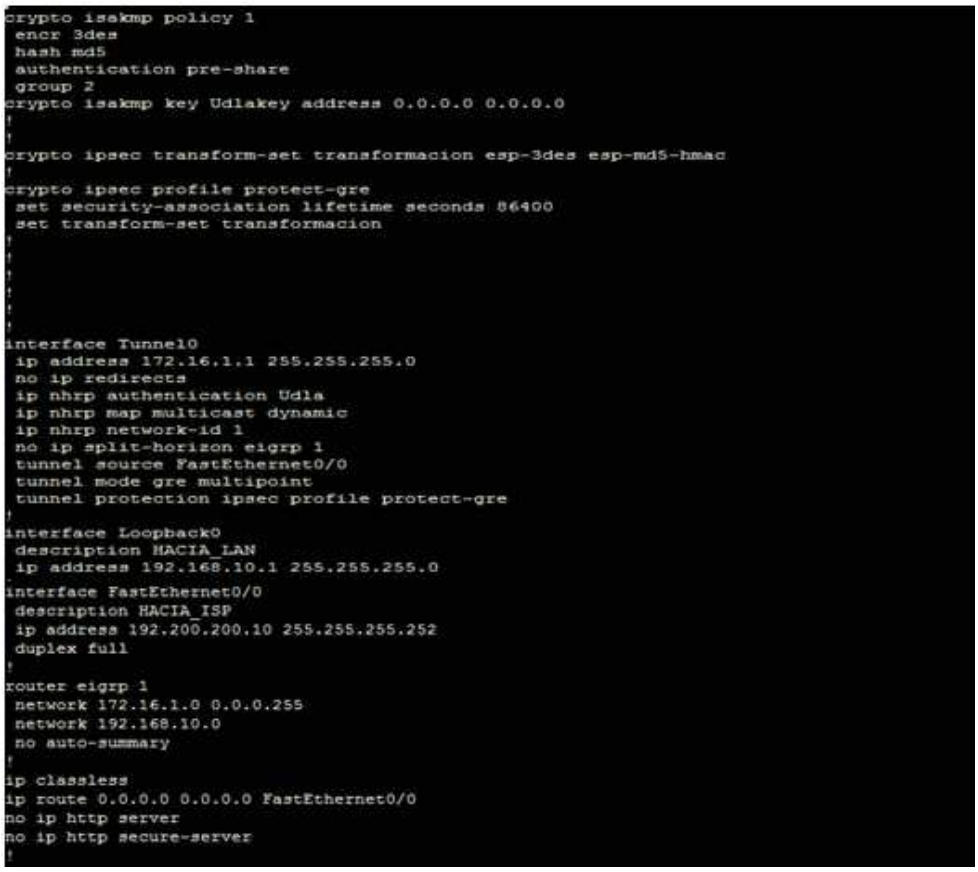
Las configuraciones de la nube serán las de un proveedor de Internet, por lo que se asume que ya están listas. Como información adicional se indica que dentro de la nube esta corriento un protocolo EGP.

4.5.6. Configuración implementada en cada equipo.

```
CE_QUITO#sho running-config
Building configuration...

Current configuration : 1640 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CE_QUITO
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
!
!
!
!
no ip domain lookup
!
!
!
```

Figura 75. Configuración Cargada en la Ciudad Quito

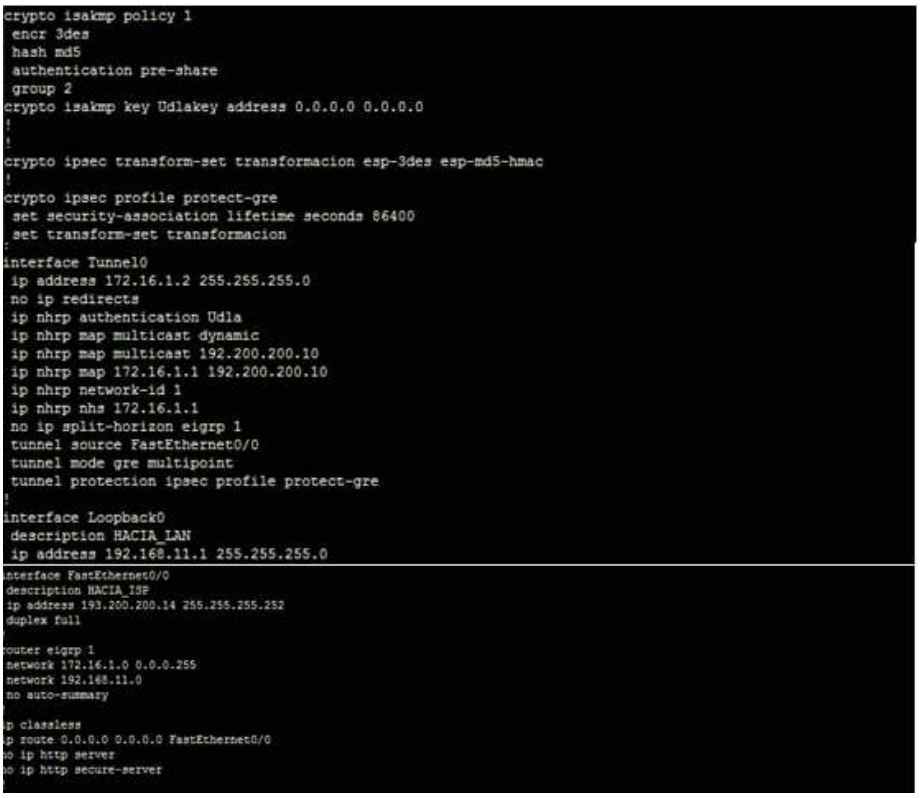


```
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key Udlakey address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set transformacion esp-3des esp-md5-hmac
!
crypto ipsec profile protect-gre
 set security-association lifetime seconds 86400
 set transform-set transformacion
!
!
!
!
!
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 no ip redirects
 ip nhrp authentication Udla
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 no ip split-horizon eigrp 1
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile protect-gre
!
interface Loopback0
 description HACIA_LAN
 ip address 192.168.10.1 255.255.255.0
!
interface FastEthernet0/0
 description HACIA_ISP
 ip address 192.200.200.10 255.255.255.252
 duplex full
!
router eigrp 1
 network 172.16.1.0 0.0.0.255
 network 192.168.10.0
 no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
no ip http server
no ip http secure-server
!
```

Figura 76. Configuración Cargada en la Ciudad Quito.

```
no service password-encryption
!
hostname CE_GYE
!
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
!
no ip domain lookup
!
```

Figura 77. Configuración Cargada en la Ciudad Guayaquil.



```
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key Udlakey address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set transformacion esp-3des esp-md5-hmac
!
crypto ipsec profile protect-gre
 set security-association lifetime seconds 86400
 set transform-set transformacion
!
interface Tunnel0
 ip address 172.16.1.2 255.255.255.0
 no ip redirects
 ip nhrp authentication Udla
 ip nhrp map multicast dynamic
 ip nhrp map multicast 192.200.200.10
 ip nhrp map 172.16.1.1 192.200.200.10
 ip nhrp network-id 1
 ip nhrp nhs 172.16.1.1
 no ip split-horizon eigrp 1
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile protect-gre
!
interface Loopback0
 description HACIA_LAN
 ip address 192.168.11.1 255.255.255.0
nterface FastEthernet0/0
escription HACIA_ISP
p address 193.200.200.14 255.255.255.252
uplex full

outer eigrp 1
etwork 172.16.1.0 0.0.0.255
etwork 192.168.11.0
o auto-summary

p classless
p route 0.0.0.0 0.0.0.0 FastEthernet0/0
o ip http server
o ip http secure-server
```

Figura 78. Configuración Cargada en la Ciudad Guayaquil.

```
CE_CUENCA#sho run
Building configuration...

Current configuration : 1716 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CE_CUENCA
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
```

Figura 79. Configuración Cargada en la Ciudad Guayaquil.

```
E_AMBATO#sho run
uilding configuration...

urrent configuration : 1716 bytes

ersion 12.4
ervice timestamps debug datetime msec
ervice timestamps log datetime msec
o service password-encryption

ostname CE_AMBATO

oot-start-marker
oot-end-marker


o aaa new-model

esource policy

p subnet-zero
o ip icmp rate-limit unreachable
p cef
p tcp synwait-time 5
o ip domain lookup
rypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
rypto isakmp key Udlakey address 0.0.0.0 0.0.0.0

rypto ipsec transform-set transformacion esp-3des esp-md5-hmac

rypto ipsec profile protect-gre
 set security-association lifetime seconds 86400
 set transform-set transformacion

nterface Tunnel0
 ip address 172.16.1.4 255.255.255.0
 no ip redirects
 ip nhrp authentication Udla
 ip nhrp map multicast dynamic
 ip nhrp map multicast 192.200.200.10
 ip nhrp map 172.16.1.1 192.200.200.10
 ip nhrp network-id 1
 ip nhrp nhs 172.16.1.1
 no ip split-horizon eigrp 1
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile protect-gre

nterface Loopback0
 description HACIA_LAN
 ip address 192.168.13.1 255.255.255.0

nterface FastEthernet0/0
 description HACIA_ISP
 ip address dhcp
 duplex full

outer eigrp 1
 network 172.16.1.0 0.0.0.255
 network 192.168.13.0
 no auto-summary

p classless
p route 0.0.0.0 0.0.0.0 FastEthernet0/0
o ip http server
o ip http secure-server
```

Figura 80. Configuración Cargada en la Ciudad Ambato.

4.6. Pruebas

4.6.1 Verificación del estado de las interfaces

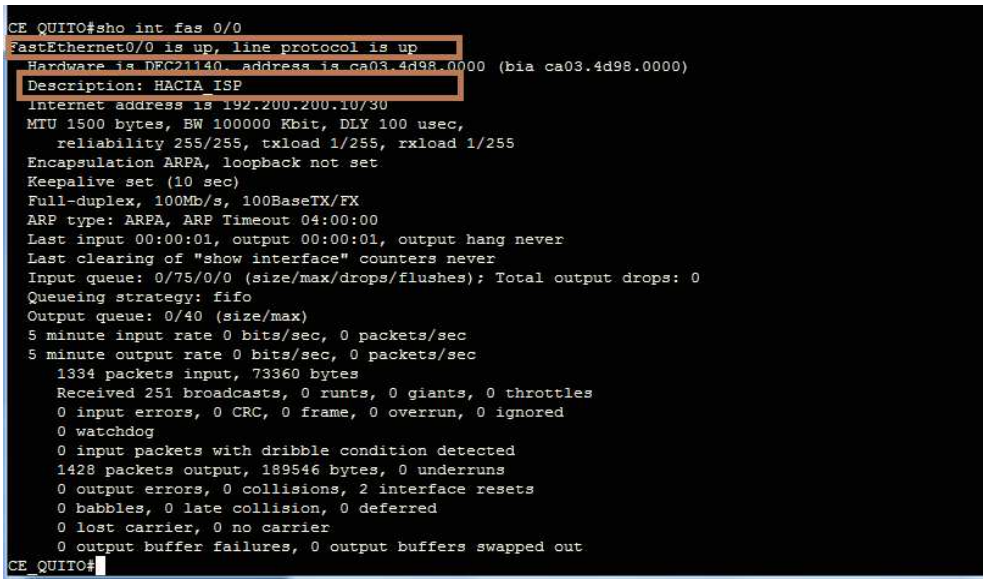


Figura 81. Interface UP Ciudad Quito.

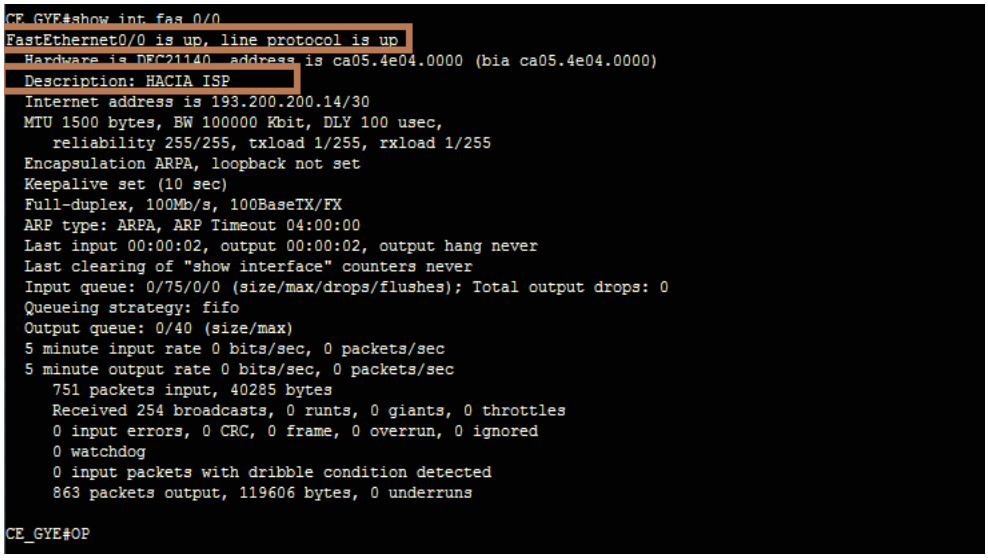


Figura 82. Interface UP Ciudad Guayaquil.

```
CE_AMBATO#sho int fas 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is DEC21140, address is ca04.4e04.0000 (bia ca04.4e04.0000)
  Description: HACIA ISP
  Internet address is 192.168.1.3/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:45, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     58 packets input, 15268 bytes
     Received 44 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     484 packets output, 68668 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
CE_AMBATO#
```

Figura 83. Interface UP Ciudad Ambato.

```
CE_CUENCA#sho int fas 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is DEC21140, address is ca0c.4d10.0000 (bia ca0c.4d10.0000)
  Description: HACIA_ISP
  Internet address is 194.200.200.3/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:02, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     717 packets input, 34922 bytes
     Received 249 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     798 packets output, 122007 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
CE_CUENCA#
```

Figura 84. Interface UP Ciudad Cuenca.

4.6.2 Verificación del establecimiento de la sesión criptográfica.

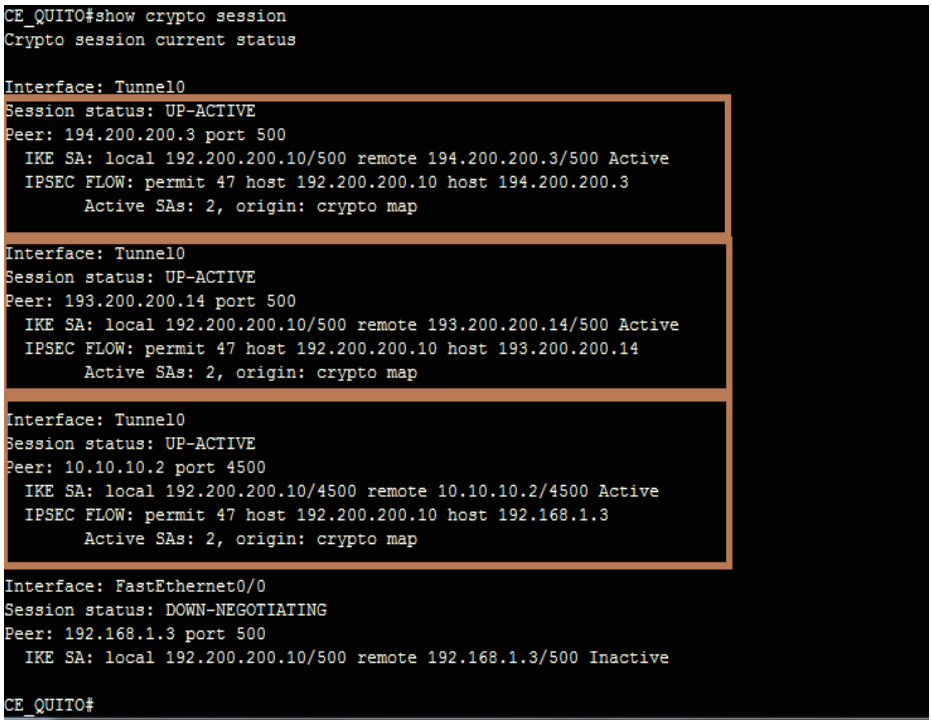


Figura 85. Sesión Criptográfica Ciudad Quito.

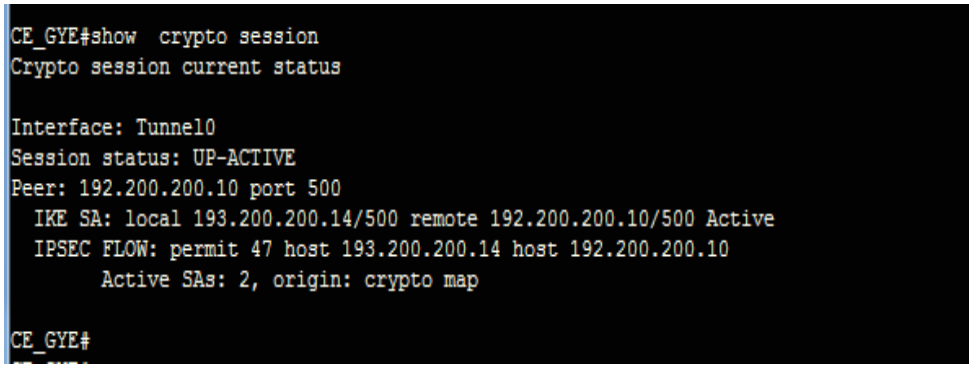


Figura 86. Sesión Criptográfica Ciudad Guayaquil.

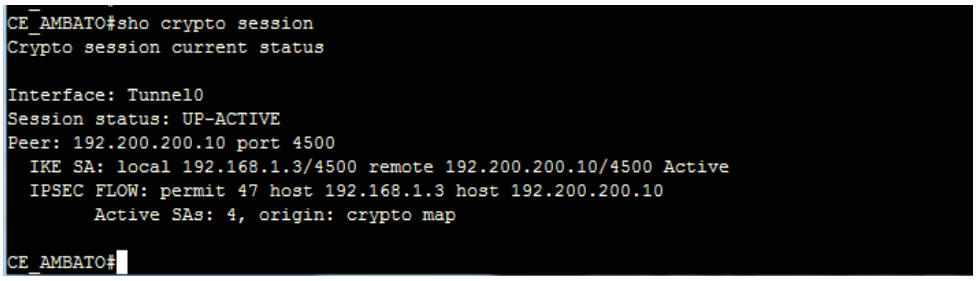


Figura 87. Sesión Criptográfica Ciudad Ambato.

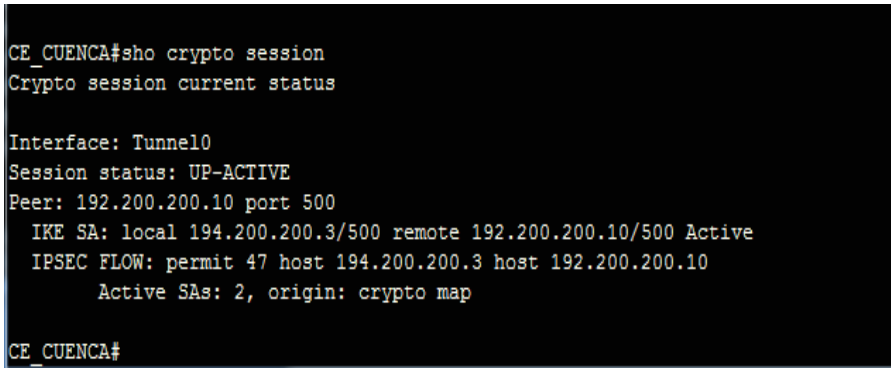


Figura 88. Sesión Criptográfica Ciudad Cuenca.

Hasta este punto se ha confirmado que las conexiones han sido establecidas tras realizar la configuración. Como se puede apreciar en las capturas arriba detalladas se tiene entablado las sesiones criptográficas entre los Spoke y su Hub respectivo.

A continuación se muestra la resolución que realizó el protocolo NHRP para conocer las IPs destinos de cada sitio.

```
CE_QUITO#show ip nhrp
172.16.1.2/32 via 172.16.1.2, Tunnel0 created 00:52:44, expire 01:49:43
  Type: dynamic, Flags: authoritative unique registered used
  NBMA address: 193.200.200.14
172.16.1.3/32 via 172.16.1.3, Tunnel0 created 00:44:03, expire 01:55:34
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 194.200.200.3
172.16.1.4/32 via 172.16.1.4, Tunnel0 created 00:03:09, expire 01:56:50
  Type: dynamic, Flags: authoritative unique registered used
  NBMA address: 192.168.1.3
CE_QUITO#
```

Figura 89. Resolución del Protocolo NHRP en la Ciudad Quito.

```
CE_AMBATO#sho ip nhrp
172.16.1.1/32 via 172.16.1.1, Tunnel0 created 00:53:05, never expire
  Type: static, Flags: authoritative used
  NBMA address: 192.200.200.10
CE_AMBATO#
```

Figura 90. Resolución del Protocolo NHRP en la Ciudad Ambato.

```
CE_GYE#sho ip nhrp
172.16.1.1/32 via 172.16.1.1, Tunnel0 created 00:54:00, never expire
  Type: static, Flags: authoritative used
  NBMA address: 192.200.200.10
CE_GYE#
```

Figura 91. Resolución del Protocolo NHRP en la Ciudad Guayaquil.

```
CE_CUENCA#show ip nhrp
172.16.1.1/32 via 172.16.1.1, Tunnel0 created 00:46:32, never expire
  Type: static, Flags: authoritative used
  NBMA address: 192.200.200.10
CE_CUENCA#
```

Figura 92. Resolución del Protocolo NHRP en la Ciudad Cuenca.

4.6.3 Pruebas de confirmación de negociación y conectividad.

Se aplicó el comando “Show dmvpn details” para conocer toda la información detallada de la negociación, como los pares formados, el detalle de las sesiones crittograficas, el servido nhrp, el estado de la interface.

Se aplicó el comando “Show dmvpn peer tunnel 172.16.1.1” para verificar la adyacencia con el HUB.

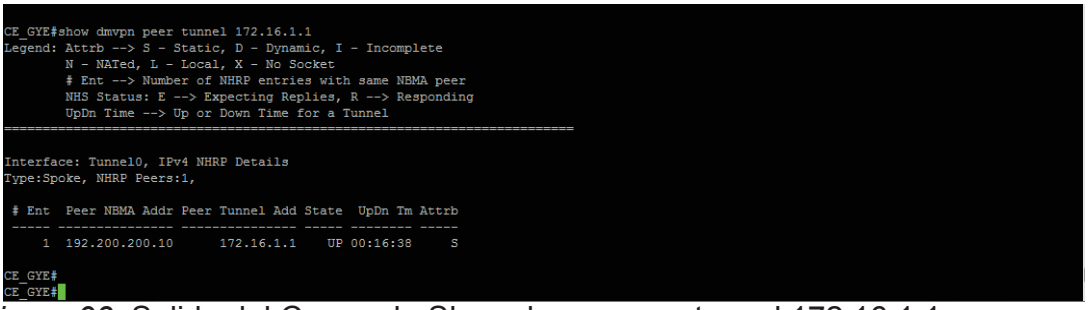


Figura 93. Salida del Comando Show dmvpn peer tunnel 172.16.1.1.

Continuando con las pruebas una vez confirmado que se entablaron las conexiones respectivas se procede hacer pruebas de enrutamiento ayudados del protocolo ICMP.

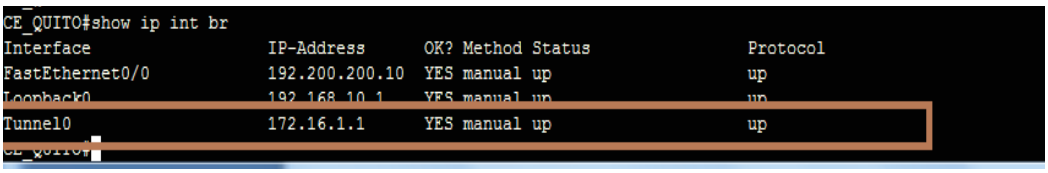


Figura 94. Estado de Túnel enlace Quito – Guayaquil

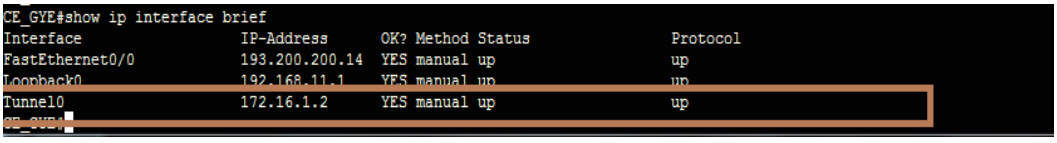


Figura 95.- Estado de Túnel enlace Guayaquil – Quito

```
CE_GYE#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 152/185/236 ms
CE_GYE#
```

Figura 96.- Conectividad Guayaquil – Quito

```
CE_QUITO#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.200.200.10  YES manual up                    up
Loopback0              192.168.10.1    YES manual up                    up
Tunnel0                172.16.1.1      YES manual up                    up
CE_QUITO#
```

Figura 97. Estado de Túnel enlace Quito – Cuenca.

```
CE_CUENCA#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        194.200.200.3   YES DHCP   up                    up
Loopback0              192.168.12.1    YES manual up                    up
Tunnel0                172.16.1.3      YES manual up                    up
CE_CUENCA#
```

Figura 98. Estado de Túnel enlace Quito – Cuenca.

```
CE_CUENCA#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 104/114/128 ms
CE_CUENCA#
```

Figura 99. Conectividad enlace Quito – Cuenca

```
CE_QUITO#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.200.200.10  YES manual up                    up
Loopback0              192.168.10.1    YES manual up                    up
Tunnel0                172.16.1.1      YES manual up                    up
CE_QUITO#
```

Figura 100. Estado de Túnel enlace Quito – Ambato.

```
CE_AMBATO#sho ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.1.3     YES DHCP   up                    up
FastEthernet0/1            unassigned      YES unset  administratively down down
Loopback0                  192.168.13.1    YES manual up                    up
Tunnel0                    172.16.1.4      YES manual up                    up
CE_AMBATO#
```

Figura 101. Estado de Túnel enlace Ambato – Quito.

```
CE_AMBATO#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 160/180/216 ms
```

Figura 102. Estado de Túnel enlace Quito – Ambato.

```
CE_QUITO#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 136/154/172 ms
CE_QUITO#ping 172.16.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 148/192/236 ms
CE_QUITO#ping 172.16.1.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 136/200/264 ms
CE_QUITO#
```

Figura 103. Conectividad enace Quito, Guayaquil, Cuenca y Ambato.

Como se indicó en el desarrollo del presente proyecto con DMVPN se puede tener una conexión completamente mallada. De tal modo que las siguientes

pruebas de conectividad entre los Spoke, comprobarán que la topología malla fue establecida.

```
CE_GYE#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 136/207/240 ms
CE_GYE#
```

Figura 104. Conectividad enlace Guayaquil- Quito

```
CE_GYE#ping 172.16.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 300/346/408 ms
CE_GYE#
```

Figura 105. Conectividad enlace Guayaquil- Cuenca.

```
CE_GYE#ping 172.16.1.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 292/344/428 ms
CE_GYE#
```

Figura 106. Conectividad enlace Guayaquil- Ambato

```
CE_CUENCA#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 168/194/216 ms
CE_CUENCA#
```

Figura 107. Conectividad enlace Cuenca- Quito.

```
CE_CUENCA#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 168/224/276 ms
CE_CUENCA#
```

Figura 108. Conectividad enlace Cuenca- Guayaquil.

```
CE_CUENCA#ping 172.16.1.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 228/317/440 ms
CE_CUENCA#
```

Figura 109. Conectividad enlace Cuenca- Ambato.

```
CE_AMBATO#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 296/357/424 ms
CE_AMBATO#
```

Figura 110. Conectividad enlace Ambato-Guayaquil.

```
CE_AMBATO#ping 172.16.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 212/312/384 ms
CE_AMBATO#
```

Figura 111. Conectividad enlace Ambato-Cuenca.

```
CE_AMBATO#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 168/208/300 ms
CE_AMBATO#
```

Figura 112. Conectividad enlace Ambato-Quito.

5 Conclusiones Y Recomendaciones

5.1. Conclusiones

El presente proyecto se realizó basándose en la problemática de interconectar los distintos sitios que una empresa podría llegar a tener, sean nacionales e internacionales. En el proceso se ha indicado la adecuada configuración de los equipos así como la ubicación de cada uno de ellos dentro de la infraestructura de red, además de la importancia de la información y su seguridad. Conforme a lo realizado se propuso un modelo de implementación que utiliza la tecnología DMVPN. Se pretende que este proyecto sirva de ayuda para reducir los costos que una empresa adquiere cuando requiere conectar sus oficinas, y no depender de los enlaces dedicados.

Se ha establecido el proceso o los procesos necesarios para implementar esta solución de tal forma que sea fácil y rápida.

Se debe tomar en cuenta que cada aplicación que se use en la red interna es diferente y por ende algunas necesitarán mayor eficiencia que otras, por lo que incluir configuraciones de QoS sería importante.

Se llegó a la conclusión mediante el laboratorio realizado que DMVPN puede ser usado para entablar conexiones utilizando la infraestructura de Internet tal cual lo hace una VPN normal que actualmente se usa, sin embargo Dmvpn funciona de una forma diferente que permite tener conexiones entre todas las oficinas involucradas y no solo con la matriz como lo hace una VPN normal.

Tambien se confirmó que los enlaces o túneles entre cada uno de los sitios participantes es establecido de forma dinámica facilitando la convergencia de cada punto.

Los proveedores de Internet y Datos actualmente tienen redes MPLS las cuales combinan el uso de las VPN, esto significa que ya existe una solución más para el problema planteado, sin embargo aun cuando una empresa ya

disponga de un enlace dedicado de datos por el cual envíen su información, Dmvpn puede ser utilizado como un enlace de respaldo.

El servicio ayudará a las pequeñas y medianas empresas e incluso a las grandes empresas a tener conectividad total sobre sus oficinas.

El estudio del presente proyecto de titulación ayudó a obtener conocimientos muy profundos y avanzados sobre las redes, así mismo del vital cuidado que se debe tener al momento de implementar configuración sobre los equipos de telecomunicaciones, ya que se trata de empresas que están en funcionamiento.

La razón por la cual DMVPN puede entablar conexiones con todas las oficinas o sitios involucrados es debido a que se apoya de los protocolos NHRP y mGRE, con lo que el resultado es una administración fácil y eficiente con enlaces de transmisión seguros.

El enfoque de esta tesis podría ser mejorado en el futuro, con el direccionamiento IPv6, QoS para los próximos modelos de diseño.

Para finalizar, el presente proyecto de titulación es de alguna forma pequeño y se podría decir que es un demo de lo que en realidad puede realizar dmvpn, sin embargo funcionará muy bien al momento de implementarlo tal cual se vió en el laboratorio creado.

El proyecto puede servir de ejemplo e iniciación para buscar una solución más viable, e incluso a que los estudiantes de la Universidad de las Américas puedan crear un diseño propio.

5.2. Recomendaciones

Se recomienda hacer el estudio de esta tecnología sobre el protocolo de Internet IPv6, debido a que está en crecimiento y las redes convergen hacia IPv6.

Se recomienda utilizar QoS en el caso de tener alguna aplicación que demande mayor confiabilidad de la red.

Se recomienda que el equipo de la matriz o concentrado (HUB) sea de una gama más alta que el utilizado en el laboratorio (Cisco 2800), para administrar las conexiones y no sean un limitante.

También se recomienda hacer un estudio de soluciones con otros vendors más conocidos en el mercado como puede ser Juniper, HP.

Se recomienda que se haga un estudio de mercadeo para tener valores concretos de las empresas que saldrán favorecidas con este proyecto.

REFERENCIAS

Bitacoraderedes.wordpress. (2013). *LA ARQUITECTURA DE LA RED El pilar de Internet Parte 2º El modelo Osi vs TCP.* Recuperado el 12 de Junio de 2013 de https://bitacoraderedes.wordpress.com/2013/04/24/la-arquitrectura-de-la-red-el-pilar-de-internet-parte-2o-el-modelo-osi-vs-tcp/

Blog.ccna.com.br. (2008). *Tuneles GRE*. Recuperado 17 de Julio de 2014 de http://blog.ccna.com.br/

Cisco System. (2007). *Dynamic Multipoint VPN (DMVPN) Design Guide (Version 1.1).* Recuperado el 1 de Febrero de 2014 de http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/DMVPDG.pdf

Cisco Systems Inc.(2008). *Guía de diseño de OSPF.* Recuperado el 15 de Febrero de 2014 de http://www.cisco.com/cisco/web/support/LA/7/73/73214_1.html

Cisco. (2008). *Cisco IOS DMVPN Overview*. Recuperado el 10 de Julio de de 2014 de http://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/DMVPN_Overview.pdf

Cisco. (2009). *Dynamic Multipoint VPN (DMVPN).* Recuperado el 6 de Noviembre del 2014 de

http://www.cisco.com/cisco/web/support/LA/107/1074/1074085_sec_DVPN_ps6922_TSD_Products_Configuration_Guide_Chapter.pdf

Cisco. (2009). *Dynamic Multipoint VPN (DMVPN)*. Recuperado el 3 de abril de 2014 de http://www.cisco.com/cisco/web/support/LA/107/1074/1074085_sec_DMVPN_ps6922_TSD_Products_Configuration_Guide_Chapter.pdf

Cisco. (2008). *Guía de Diseño OSPF*. Recuperado 21 de Noviembre de 2014 de http://www.cisco.com/cisco/web/support/LA/7/73/73214_1.html

Cisco. (2014). *Guía del Troubleshooting de los debugs de la fase 1 DMVPN.* Recuperado el 07 de septiembre de 2014 de http://www.cisco.com/cisco/web/support/LA/112/1121/1121979_116957-technote-dmvpn-00.html

Cnt.gob.ec. (2015). *Internet Pymes*. Recuperado el 21 de Enero de 2015 de https://www.cnt.gob.ec/internet/plan-corporativo/internet-pymes/

Electropediadigital.blogspot. (2012). *ALGORITMO DIJKSTRA Y SPF*. Recuperado 21 de Noviembre de 2014 de http://electropediadigital.blogspot.com/2012/10/algoritmo-dijkstra-y-spf.html

Edeszone.net, (2011). *IPsec. Volumen. AH (Cabecera de autenticación)*. Recuperado el 20 de Noviembre del 2014 de

http://www.redeszone.net/2011/08/30/ipsec-volumen-ii-ah-cabecera-de-autenticacion/.

Edeszone.net. (2011). *IPsec. Volumen III: ESP (Carga de seguridad encapsulada)*. Recuperado el 20 de Noviembre de 2014 de http://www.redeszone.net/2011/09/06/ipsec-volumen-iii-esp-carga-de-seguridad-encapsulada/

Estrada, A. (2004). *Protocolos TCP/IP DE Internet*. Recuperado el 10 de Octubre de 2014 de http://www.revista.unam.mx/vol.5/num8/art51/sep_art51.pdf

EKosNegocios. (2012). *Rankin 2013 PYMS*. Recuperado el 7 de Octubre 2014 de http://www.ekosnegocios.com/revista/pdf/234.pdf#page=21&zoom=auto,-100,605

Freebsd. (s.f). *VPN over IPsec*. Recuperado el 17 de marzo de 2014 de https://www.freebsd.org/doc/en/books/handbook/ipsec.html

Garcia, L. (s.f). *IPSEC.* Recuperado el 10 de Enero de 2014 de http://slideplayer.es/slide/159908/

Garcia, J. (2012). *Conceptos Basicos de Redes e Internet*. Recuperado el 10 de Octubre 2014 de http://es.slideshare.net/jegarba/presentacion-sobre-los-20-terminos-de-redes-e-Internet

It.uc3m.es. (2003). *IPSEC*. Recuperado el 10 de Noviembre de http://www.it.uc3m.es/~teldat/TeldatC/castellano/protocolos/Dm739v10_10_IPSec.PDF.

Netlife.ec. (2015). *PYMES INTERNET DE ALTA VELOCIDAD.* Recuperado el 20 de Enero de 2015 de http://www.netlife.ec/planes/pymes/internet-de-alta-velocidad/nuestros-planes/

Networkknerd.blogspot. (2014). *DMVPN - Part 2, BGP with dyanmic neighbors*. Recuperado el 5 de Septiembre de 2014 de http://networkknerd.blogspot.com/search?q=dmvpn

Networkknerd.blogspot. (2014). *Traffic filtering on Lan-2-Lan VPNs (ASA)* Recuperado el 10 de Octubre de 2014 de http://networkknerd.blogspot.com/2014/09/traffic-filtering-on-lan-2-lan-vpns-asa.html

Ochoa,f. (2009). *"DISEÑAR ESTRATEGIAS PARA LA MIGRACIÓN DE UN PROTOCOLO PROPIETARIO A UN PROTOCOLO ESTÁNDAR DE ENRUTAMIENTO IP EN LAS REDES DE PEQUIVEN"*. Recuperado el 21 de Noviembre de 2014 de http://www.geocities.ws/feochoa/Tesis/tesisospf.htmle

Packetlife. (2008). *Dynamic Multipoint VPN (DMVPN)*. Recuperado el 5 de marzo de 2014 de http://packetlife.net/blog/2008/jul/23/dynamic-multipoint-vpn-dmvpn/

Posada, O. (2013). *Tecnologías de la Información*. Recuperado el 6 de Noviembre de 2014 de http://oscaromarposadasanchez.blogspot.com/2013/01/ipsec.html

Proyectos.ingeniovirtual. (s.f). *IPSec.* Recuperado el 10 de enero de 2014 de https://proyectos.ingeniovirtual.com.ar/projects/ipv6/wiki/IPSec

Schertler, M., Schneider, M. y Turner,J. (2005). *Protocolo de Gestión de Claves y Asociaciones de Seguridad en Internet (ISAKMP)*. Recuperado el 20 de Noviembre de 2014 de http://www.rfc-es.org/pendientes/rfc2408-es.txt

Tejada,K., León, S. y Astudillo, C. (2001*). Diseño de una intranet usando tecnología VPN (Virtual Private Network), que comunique la matriz de SECOHI con sus oficinas sucursales y que además permita el acceso remoto de usuarios móviles*. Guayaquil, Ecuador: Escuela superior politécnica del Litoral.

Teleamazonas. (2012). *Huawei y CNT lanzan Smartphones al mercado ecuatoriano*. Recuperado el 17 de Julio de 2014 de http://72.55.165.243/index.php/actualidad/tecnologia/17115-huawei-y-cnt-lanzan-smartphones-al-mercado-ecuatoriano

Wordreference. (s.f). *Online Language Dictionaries*. Recuperado el 21 de mayo de 2014 de http://www.wordreference.com/es/

ANEXOS

ANEXO 1

Terminología

- **VPN**.- red privada virtual,
- **DMVPN.**- VPN Multipunto Dinámica
- **NHRP.** Protocolo de Resolución del Siguiente Salto
- **NBMA**.- red de acceso múltiple de no difusión
- **RFC**.- Request For Comments
- **MGRE**.- Generic Routing Encapsulation
- **IPSEC**.- Seguridad de protocolos en Internet
- **IPK**.- Internet Key Exchange
- **IETF**.- Grupo de Trabajo de Ingeniería de Internet
- **RSA**.- Rivest, Shamir y Adleman
- **AES**.- Advanced Encryption Standard
- **DES.**- Data Encryption Standard
- **3DES.**- Algoritmo de cifrado de datos triple (TDEA o Triple DEA)
- **BLOWFISH.**.- Codificador de bloques simétricos,
- **EIGRP** Enhanced Interior Gateway Routing Protocol
- **OSFP** Open Shortest Path First
- **MD5** Message-Digest Algorithm 5,
- **FIREWALL.** Cortafuegos
- **Cisco IOS** Internetwork Operating System

ANEXO 2.

RFC	
RFC 2333 **Protocolo NHRP aplicabilidad Abril 1998**	Con un inter-LIS mecanismo de la resolución de la dirección al final de la cual Ambas estaciones pueden intercambiar paquetes sin tener que utilizar los servicios de los routers intermedios. Esta función también se denomina "Atajo" de enrutamiento. Si la estación de destino no es parte de la NBMA lógica de red, NHRP proporciona la fuente con la dirección NBMA De la actual salida del router hacia el destino.
RFC 2403-es Uso de HMAC-MD5-96 en ESP y AH	MD5 [RFC-1321] combinado con HMAC [RFC-2104], como un mecanismo de autentificación de claves dentro del contexto de ESP y AH dentro de IPsec. El propósito de HMAC-MD5-96 es asegurar que el paquete es autentico y que no puede ser modificado en tránsito
RFC 2411-es **Documento de Guía para IPSEC**	El conjunto de protocolos IPsec se utiliza para proporcionar servicios de privacidad y autentificación en la capa IP.
RFC -791	El Protocolo Internet está específicamente limitado a proporcionar las funciones necesarias para enviar un
RFC 2784Encapsulación de enrutamiento genérico (GRE)	Una serie de diferentes propuestas [RFC1234, RFC1226] Actualmente existe para la encapsulación de un protocolo sobre otro protocolo. Otros tipos de encapsulados [RFC1241, RFC1479] se han propuesto para el transporte de IP sobre IP con fines de política.
RFC 2408 **Protocolo ISAKMP**	Un protocolo que utiliza los conceptos de seguridad necesarias para el establecimiento de asociaciones de seguridad (SA) y claves criptográficas en un entorno de Internet. [NORMAS-TRACK].
RFC 1583 **Protocolo OSPF**	Se distribuye la información de enrutamiento entre los routers que pertenecen a un único sistema autónomo. El protocolo OSPF se basa en el estado de enlace o la tecnología SPF.