UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:
INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:
INGENIERA DE SISTEMAS

TEMA:
DISEÑO DE UNA INFRAESTRUCTURA DE SEGURIDAD DE CAPA TRES BASADA EN IPSEC SOBRE TÚNELES MULTIPUNTO USANDO GRE PARA LA INTERCONEXIÓN DE LAS SEDES QUITO, GUAYAQUIL Y CUENCA DE LA UNIVERSIDAD POLITÉCNICA SALESIANA.

AUTORA:
XIMENA ELIZABETH BAUTISTA TAPIA

TUTOR:
JORGE ENRIQUE LOPEZ LOGACHO

Quito, diciembre del 2016

CESIÓN DE DERECHOS DE AUTOR

Yo, Ximena Elizabeth Bautista Tapia con documento de identificación N° 1719443317, manifiesto de mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy la autora del trabajo de titulación con el tema :" DISEÑO DE UNA INFRAESTRUTURA DE SEGURIDAD DE CAPA TRES BASADA EN IPSEC SOBRE TÚNELES MULTIPUNTO USANDO GRE PARA LA INTERCONEXIÓN DE LAS SEDES QUITO, GUAYAQUIL Y CUENCA DE LA UNIVERSIDAD POLITÉCNICA SALESIANA" ,mismo que ha sido desarrollado para optar por el título de INGENIERA DE SISTEMAS, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En la aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autora me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

Ximena Elizabeth
Bautista Tapia

CC: 171944331-7

Quito, diciembre del 2016

DECLARATORIA DE COAUTORÍA DEL TUTOR

Yo, declaro que bajo mi dirección y asesoría fue desarrollado el trabajo de titulación: DISEÑO DE UNA INFRAESTRUTURA DE SEGURIDAD DE CAPA TRES BASADA EN IPSEC SOBRE TÚNELES MULTIPUNTO USANDO GRE PARA LA INTERCONEXIÓN DE LAS SEDES QUITO, GUAYAQUIL Y CUENCA DE LA UNIVERSIDAD POLITÉCNICA SALESIANA realizado por Ximena Elizabeth Bautista Tapia obteniendo un trabajo que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Quito, diciembre 2016

JORGE ENRIQUE LÓPEZ LOGACHO

CI: 1712082484

Dedicatoria

A Dios, a mi Familia, a mis Queridos Padres por haberme dado la vida, por ser mi pilar fundamental en cada paso de mi existencia, por cada uno de sus consejos, de su paciencia, por su amor y apoyo incondicional sin ustedes no sería la persona que soy ahora.

A mi hermano por sus consejos y por brindarme siempre una palabra de ánimo, a mis sobrinos por cada día demostrarme su amor y ser un ejemplo para ellos. También dedico este proyecto de titulación a mi mejor amigo por los buenos y malos momentos que hemos pasado, por su comprensión, su apoyo, sus consejos, por cada día tratarme de sacar una sonrisa cuando el cansancio me ha ganado y demostrarme que nada es imposible.

Ximena Elizabeth Bautista Tapia

Agradecimiento

Mis más profundos y sinceros agradecimientos a todos mis queridos docentes que he conocido durante toda mi vida universitaria, en especial a mi tutor el Ingeniero Jorge López quien con sus sabios consejos y ayuda incondicional supo guiarme para la culminación de este proyecto de titulación.

Ximena Elizabeth Bautista Tapia

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Resumen

El objetivo principal de este proyecto técnico es realizar el diseño de una Infraestructura de capa tres utilizando IPSEC sobre túneles multipunto GRE que es uno de los mecanismos que ha permitido establecer canales o túneles de comunicación privada para encaminar paquetes sobre redes públicas, de tal manera que brindara la garantía de maximizar las redes propietarias sobre redes ya existentes que serían las redes públicas, cabe destacar que al momento de poner en marcha este protocolo sobre los paquetes IP se podrá brindar la características más eficientes de seguridad mediante la pila de IPSEC y la robustez de IPV6 convirtiéndose de esta manera en una magnifica opción para la protección de todos los datos críticos; así como también la interconexión de cada una de las sedes de la Universidad Politécnica Salesiana que se encuentran localizadas en Quito, Guayaquil y Cuenca.

Abstract

The main objective of this technical project is to design an Infrastructure Layer three using IPSEC over tunnels multipoint GRE which is one of the mechanisms that has established channels or tunnels private communication to route packets over public networks , such that would provide assurance to maximize proprietary networks on networks already exist that would be public networks , it should be noted that when implementing this protocol on IP packets may provide the most efficient security features through the stack of IPSEC and robustness IPV6 thus becoming a great option for protecting all critical data as well as the interconnection of each of the headquarters of the Salesian Polytechnic University that are located in Quito , Guayaquil and Cuenca.

INTRODUCCIÓN

En pleno siglo XVI se ha podido apreciar la evolución de las tecnologías de comunicación permitiendo el paso de los datos de un lugar a otro.

Con el pasar de los años las organizaciones tanto privadas, públicas han ido creciendo gradualmente y junto con ellas la necesidad de poder proteger sus datos más críticos resguardando la integridad de sus empresas.

La escasa importancia dada a las medidas de seguridad de las redes de comunicación, ha creado una gran limitante que con el pasar del tiempo se vuelve cada vez más difícil identificar las amenazas que podrían desestabilizar a cada una de las instituciones, así como el funcionamiento de las mismas. Para lo cual se ha llevado a cabo varias investigaciones que permitan establecer dispositivos, protocolos y herramientas que cubran con la demanda de proteger la información vital que se envía a través de la red de datos llamada Internet.

Antecedentes

En la actualidad, uno de los requerimientos más principales de las redes dentro de las empresas es la seguridad de su información debido a la importancia y la criticidad de dicha información.

En la tesis publicada en enero del 2014 llamada “FACTIBILIDAD DE IPSEC PARA IPV6 EN LA RED DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, SEDE QUITO” por el autor Ing. Jorge López, menciona que IPSec ofrece seguridad a nivel de capa 3, por medio de algoritmos criptográficos que permiten proporcionar servicios de transporte seguros entre dos extremos, adicionalmente se lo usa para proteger una o más trayectorias entre un par de host, o entre un par security gateway (pág. 36).

Además de las técnicas criptográficas que se menciona dentro de IPSec es importante recalcar un elemento fundamental como es los túneles punto a multipunto conocido como el protocolo mGRE, como lo dice Cisco en su documento titulado “Dynamic Multipoint VPN Configuration Guide” menciona que una interfaz de túnel mGRE permite una única interfaz GRE para soportar múltiples túneles IPSec y simplifica el tamaño y la complejidad de la configuración, la función DMVPN combina el enrutamiento NHRP, los túneles mGRE y el cifrado IPSec para proporciona a los usuarios la facilidad de configuración a través de perfiles criptográficos, dicha tecnologías mejoradas por Cisco (CISCO, 2012).

Planteamiento del Problema

La elaboración del presente proyecto técnico es garantizar un nivel de seguridad eficaz para el envió de información crítica como notas, registros entre otros; proporcionando también a su vez una interconexión y unificación entre las 3 Sedes de la Universidad Politécnica Salesiana ubicada en Quito, Guayaquil y Cuenca respectivamente.

Justificación

El presente proyecto técnico tiene como propósito dar a conocer los elementos, el análisis, diseño y funcionamiento de una red piloto con infraestructura IPSec con Tunelización Generic Routing Encapsulation (GRE) Multipunto, en un entorno IPv6, debido a que este mecanismo proporciona encapsulación de todos los datos que se pueden enviar a través de la red, permitiendo así una interconexión de diferente tipos de dispositivos con un alto grado de seguridad y calidad de servicio (QoS), brindando una mayor seguridad, encriptación e interconexión en el entorno IPv6 de las Sedes de la Universidad Politécnica Salesiana que se encuentran localizadas en Quito, Guayaquil y Cuenca respectivamente.

Al combinar estos elementos dentro de una red va a permitir que dicha red con GRE multipunto pueda soportar múltiples túneles IPSEC de tal manera que reduzca drásticamente el tamaño y la complejidad de la configuración, además dentro de GRE se permitirá establecer canales de comunicación privadas y expansión de la red propietaria.

Objetivos

Objetivo General

Realizar el diseño de una infraestructura de seguridad de capa tres basadas en IPSec sobre túneles multipunto usando GRE IPv6 para la interconexión de las Sedes Quito, Guayaquil y Cuenca de la Universidad Politécnica Salesiana.

Objetivos Específicos

Conocer los conceptos, funcionalidad y operación de GRE.

Analizar la red existente de la Universidad Politécnica Salesiana para la implementación de túneles GRE.

Diseñar la infraestructura de seguridad con túneles GRE con IPSEC en IPv6 para este tipo de redes.

Implementar los túneles GRE con IPSEC IPv6 en un entorno de simulación.

Evaluar técnicamente los resultados de la infraestructura de seguridad obtenidos de la simulación de la red que usa túneles en GRE, con IPSEC en un entorno IPv6.

CAPÍTULO 1
FUNDAMENTO TÉORICO

1 Seguridades en IPv6

INTRODUCCIÓN

Para resguardar los datos que se envían a través de las redes, dentro de la seguridad se deben tomar en consideración el uso de los protocolos que permiten brindar 3 aspectos importantes que son confidencialidad, integridad y autentificación.

Dentro de la seguridad se debe tomar en cuenta, que durante el envió de datos dentro de una red, esta información crítica no debe ser modificada, reemplazada o peor aún eliminada por usuarios que no tengan la autorización para manipular dicha información.

Al momento que se realice la manipulación de dichos datos, se deberá garantizar la disponibilidad de los diferentes servicios que se encuentren operando dentro de la red, ya que puede existir el riesgo que personas no autorizadas mediante invasión saturen o produzcan el mal funcionamiento de dichos servicios y la información que se maneje no se encuentre disponible o denegada.

1.1 Aspectos de Seguridad en IPv6

Dentro del Protocolo de IPv6 se puede destacar los siguientes ámbitos de seguridad que se debería tomar en consideración al momento de implementar IPv6 en redes de datos son las siguientes:

Las redes IPv6 son con carácter general es decir son más seguras que las redes IPv4 (Gobierno de España , 2015).

En IPv6 se puede utilizar seguridad de extremo a extremo, lo cual no siempre es posible en IPv4 pues el protocolo NAT lo impide. (Gobierno de España , 2015).

IPv6 proporciona protección frente a posibles ataques de negación de servicios denominados “ataques de fuerza bruta”. (Gobierno de España , 2015)

IPSec es obligatorio en IPv6 lo cual siempre debe estar presente, mientras que en IPv4 es opcional. (Gobierno de España , 2015).

1.2 GRE

GRE (Generic Router Encapsultion), es un protocolo de túnel desarrollado por Cisco, que permite encapsular varios protocolos de capa red entre dos ubicaciones punto a punto a través de una red pública, como Internet (CISCO, s.f., pág. 2).

Esquema del Funcionamiento de GRE en IPv4

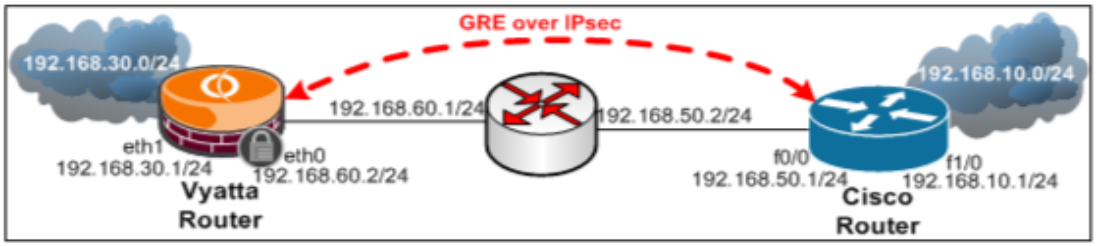

Figura 1. GRE en IPV4
Fuente: Configure GRE/IPSEC

1.2.1 Encapsulamiento GRE.

La implementación del protocolo GRE (Generic Routing Encapsulation), permite tener un camino viable para ser aplicado en infraestructuras pequeñas, debido al tipo y la cantidad de la información permite la utilización de menos recursos. (Aimacaña Valladares, 2014, pág. 35).

De acuerdo a las especificaciones RFCs (1701 y 1072), los paquetes que se encuentran en GRE encierran paquetes de carga útil que tienen los detalles de una ruta de origen,

así como los paquetes que han sido procesados y encapsulados por el protocolo de entrega (Aimacaña Valladares, 2014, pág. 35).

Esquema de Encapsulamiento de GRE

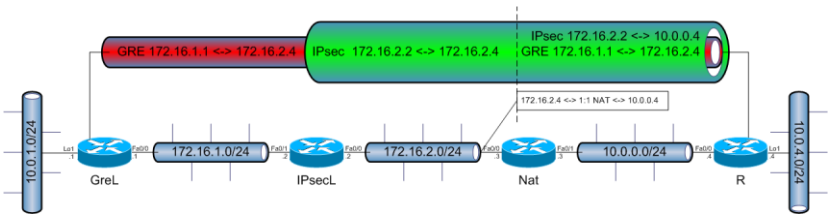

Figura 2. Encapsulación GRE
Fuente: Cisco

1.2.2 Cabecera GRE.

La cabecera GRE tendrá 4 bytes en caso de no tener configurada ninguna de las opciones. El primer par de bytes (del 0 a15) contiene las etiquetas que indican la presencia de las opciones de GRE y que en caso de estar activas se añade más bytes a la cabecera. (Ariganello & Sevilla Barriento , 2010, pág. 645).

El segundo par es el campo del protocolo e indica que tipo de datos se están transportando en el túnel (Ariganello & Sevilla Barriento , 2010, pág. 646).

La siguiente Figura 3, nos describe las opciones de la cabecera GRE.

Cabecera de GRE

Bit en la cabecera GRE	Opción	Añadido
0	Checksum	4 bytes
2	Clave	4 bytes
3	Número de secuencia	4 bytes
13–15	Versión	0 GRE básico y 1 PPTP

Figura 3. Cabecera GRE
Fuente: CCNP A FONDO

Checksum Present: Permite añadir un campo adicional de checksum a la cabecera GRE (Ariganello & Sevilla Barriento , 2010, pág. 647).

Key Present: Permite añadir un campo opcional de seguridad, que proporciona un sistema básico de seguridad comprobando que a cada uno de los extremos del túnel tenga la misma clave (Ariganello & Sevilla Barriento , 2010, pág. 647).

Sequence Number: Permite añadir un campo opcional de números de secuencia, como ocurre en el checksum, no es muy ocupado ya que protocolos de capas superiores realizan la misma función (Ariganello & Sevilla Barriento , 2010, pág. 647).

Versión: Indican el número de versión de GRE, el valor 0 representa GRE (Ariganello & Sevilla Barriento , 2010).

Datagrama de la Cabecera de GRE

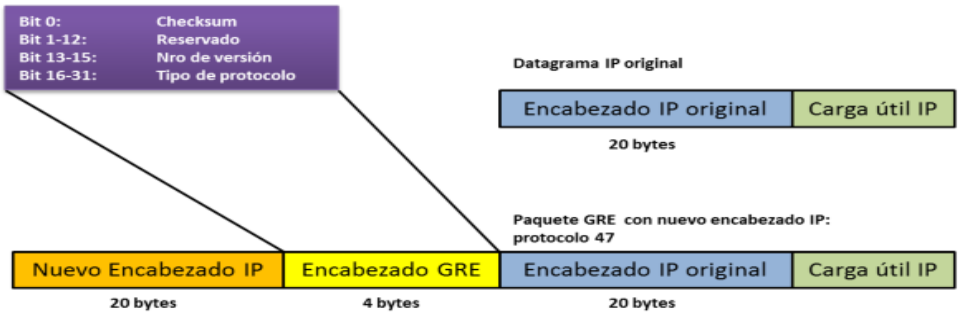

Figura 4. Cabecera GRE
Fuente: Virtualización de Redes en la Empresa

1.2.3 Ventajas de GRE.

El protocolo GRE se puede utilizar en diferentes escenarios los cuales se citarán a continuación:

Permite conexiones de redes IPv6 sobre IPv4 (CISCO, s.f., pág. 2).

Paquetes de multidifusión, como OSPF, EIGRP y aplicaciones de transmisión (CISCO, s.f., pág. 2).

GRE cuenta con un método de "keep-alive" para mantener el estatus de la red (Samaniego Fuentes, 2013, pág. 5).

GRE se puede utilizar para canalizar el tráfico que no es IP a través de una red IP, lo que permite la expansión de la red mediante la conexión de subredes multiprotocolo en un entorno de backbone de protocolo único (CISCO , s.f.).

GRE admite el tunneling de multidifusión IP, lo que permite la utilización de protocolos de routing a través de túnel(CISCO , s.f.).

1.3 Tunelización

Es un mecanismo que proporciona el transporte de paquetes de un protocolo dentro de otro protocolo, el protocolo que es transportado es llamado protocolo pasajero mientras que, el protocolo utilizado para transportar al protocolo pasajero se lo conoce como protocolo transporte.

1.3.1 Tunelización Punto a Punto.

Es un protocolo a nivel de enlace que permite la comunicación mediante túneles privados, para el intercambio seguro de los datos de un cliente a un servidor formando una red privada (VPN), basada en una red de trabajo TCP/IP. La encapsulación de punto a punto permite que diferentes protocolos de la red operen sobre un mismo enlace.

GRE se considera una VPN porque es una red privada que se crea con tunneling a través de una red pública. Mediante la encapsulación, un túnel GRE crea un enlace virtual punto a punto a los routers Cisco en puntos remotos a través de una internetwork IP (CISCO, s.f.).

1.3.2 Tunelización Punto a Multipunto.

En un enlace punto a multipunto, existe un punto central que se comunica con varios otros puntos remotos, generalmente esto implica que la comunicación es solamente de un punto central y los remotos, de estos hacia el central (Caprile R, 2009).

Para ello se tiene un ejemplo muy destacado que son los túneles multipunto GRE(mGRE), permiten que existan más de dos extremos y es tratado como una red de acceso múltiple sin broadcast (NBMA) (Gumucio Torrico, 2015).

1.3.3 mGRE.

mGRE (Multipoint Generic Rounting Encapsulation) permite, que una única interfaz GRE pueda soportar múltiples túneles IPSec de esta manera garantizará la disminución del tamaño y la complejidad de la configuración.

Los túneles GRE multipunto es una tecnología poco conocida, con el mismo potencial que un túnel GRE, pero con el añadido de poder crear un segmento de red punto multipunto, emulando lo que por ejemplo podría ser una conexión de Frame-Relay punto multipunto (Networking, 2012).

A la hora de configurar túneles GRE multipunto se debe tener en cuenta, que se está configurando un túnel GRE con sus propiedades y limitaciones, pero además hay que añadirle las propiedades y limitaciones de una red punto multipunto, esto supone que tendrá que existir un punto que hará la función de hub, donde se concentrará todas la conexiones y, varios spokes, que serán sitios remotos que solo tendrán conexión con el hub y, si quieren llegar al resto de spokes deberán hacerlo a través de hub (Networking, 2012).

Esquema de una Red con mGRE

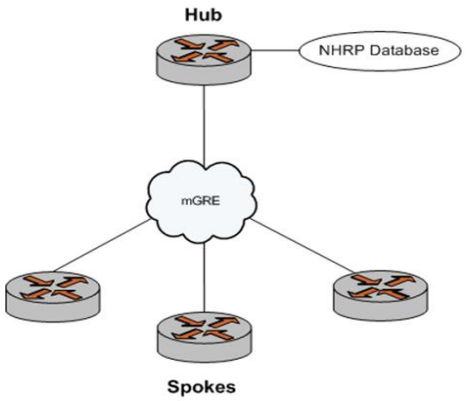

Figura 5. Diseño de mGRE
Fuente: Brocade de Multipoint GRE

1.3.4 Especificaciones de mGRE.

Tecnología que se basa en DMVPN (Dynamic Multipoint VPN) para tener una interfaz para trabajar con mGRE e IPSec.

Maneja una topología Hub-Spoke (similar a la topología estrella) donde el Hub se encuentra en el centro y Spoke es un punto remoto.

mGRE sobre IPv6 permite a sus proveedores de servicios desplegar IPv6 sobre su infraestructura central (CISCO , 2014).

NHRP (Next Hop Resolution Protocol) Protocolo de resolución del siguiente salto permite crear un ID para la configuración de túneles multipunto (mGRE) (CISCO , 2014).

1.4 DMVPN

DMVPN (Dinamic Multipoint VPN) es una tecnología que se basa en la generación de túneles GRE (mGRE desde varios puntos remotos (spokes) hacia un nodo central conocido como Hub). Con DMVPN cualquier flujo de tráfico entre los routers se envía en túnel GRE, pero la característica más interesante es que distingue a DMVPN de otras implementaciones VPN es que el túnel GRE sobre DMPVN es un túnel multipunto (Aimacaña Valladares, 2014, pág. 33). Con esto el hub y spokes requerirán de un túnel cada uno para alcanzar la conectividad DMVPN completamente mallada, por lo que las ventajas son las siguientes:

Simplificar la porción de la configuración del router hub (Aimacaña Valladares, 2014, pág. 33).

Los routers spoke pueden obtener sus direcciones IP dinámicamente por ejemplo un router de borde de Internet conectado con un enlace ADSL puede obtener su IP

automáticamente del ISP y entonces el túnel se registrará con el hub usando NHRP (Aimacaña Valladares, 2014, pág. 33).

1.4.1 Funcionamiento de DMVPN.

La característica del Dynamic Multipoint VPN (DMVPN) combina los túneles GRE, la encriptación de IPSec, y el encaminamiento. NHRP para proporcionar a los usuarios una facilidad de la configuración vía los perfiles crypto que reemplazan el requisito para definir las correspondencias de criptografía estática y de la detección dinámica de puntos finales del túnel (CISCO, 2013).

Esta característica confía en las siguientes tecnologías estándar:

NHRP: Un protocolo de cliente y servidor donde el hub es el servidor y las radios son los clientes. El hub mantiene una base de datos NHRP de las direcciones de interfaz pública de cada radio. Cada spoke registra su dirección real cuando arranca y consulta en la base de datos NHRP las direcciones reales de los spokes de destino con el fin de crear túneles directos (CISCO, 2013).

Interfaz de túnel mGRE: Permite que una sola interfaz GRE soporte los túneles IPSec múltiples y simplifica los tamaños y la complejidad de la configuración (CISCO, 2013).

Esquema del Funcionamiento de DMVPN

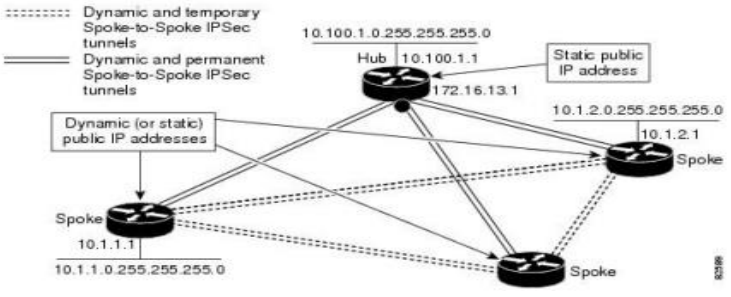

Figura 6. Funcionamiento DMVPN
Fuente: Dynamic Multipoint VPN

1.4.2 Topologías DMVPN.

Dentro de DMVPN se puede implementar dos tipos de topologías que son las siguientes:

Dual hub-dual DMVPN Cloud: Una topología Dual hub-dual DMVPN cloud es un conjunto de routers que se configura ya sea con una interfaz multipunto (mGRE), punto a punto, interfaz GRE (combinación de ambos) que comparten la misma dirección de subred (Aimacaña Valladares, 2014, pág. 34).

Esquema de la Topología Dual Hub-Dual DMVPN

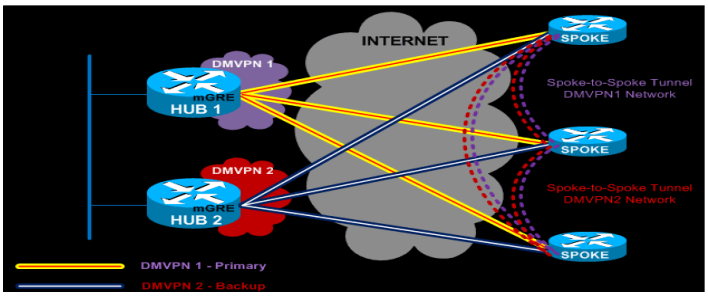

Figura 7. Topología Dual hub-dual DMVPN Cloud
Fuente: DMVPN Modelos y Arquitecturas CISCO

Dual hub-single DMVPN Cloud: La topología Dual hub-single DMVPN cloud no se recomienda porque es basada en mecanismos que se aplicarían fuera del túnel (Aimacaña Valladares, 2014).

Esquema de la Topología Dual Hub-Single DMVPN

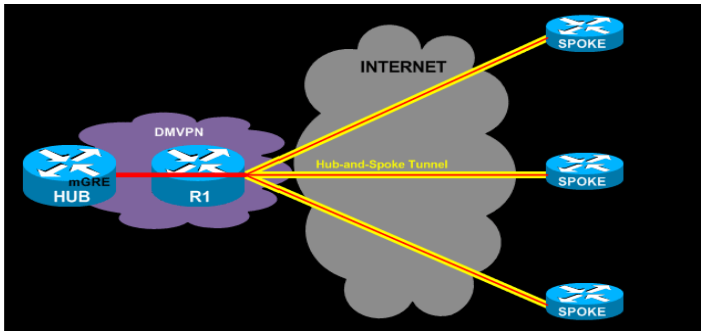

Figura 8. Topología Dual hub-single DMVPN Cloud
Fuente: DMVPN Modelos y Arquitecturas CISCO

1.5 Protocolo NHRP

NHRP (Next Hop Resolution Protocol) permite la simplificación de la configuración de los equipos tanto spokes como hubs, los equipos que actúan como hubs no necesitan tener una configuración de la dirección de ninguno de los spokes de la red y por tanto las direcciones de los spokes pueden haber sido asignados de una manera dinámica.

1.5.1 Funcionamiento del Protocolo NHRP.

Las DMVPN's se configuran sobre un interfaz virtual de tipo túnel llamado TNIP (abreviatura de túnel IP). El interfaz TNIP tiene su propia dirección IP y sobre él se configura el protocolo mGRE. En el interfaz TNIP se configuran también los parámetros de funcionamiento del protocolo NHRP que da servicio al protocolo mGRE (Telnat , 2006, pág. 4).

El objetivo de NHRP es descubrir la dirección pública del interfaz TNIP del equipo remoto con el que se quiere establecer comunicación a través de un túnel. (Telnat , 2006, pág. 4). La dirección privada ya se conoce por medio del protocolo de routing dinámico que está corriendo en la red:

Cada spoke se registra periódicamente, en el hub o hubs que tenga configurados y mantiene activos los túneles que establece con éstos. (Telnat , 2006, pág. 4)

A través de estos túneles viajan los paquetes multicast del protocolo de rutado dinámico.(Telnat , 2006, pág. 4).

El hub transmite a los spokes las rutas del resto de equipos de la DMVPN a través del túnel mencionado, es decir, se transmite el siguiente salto, que normalmente coincide con la dirección privada (Telnat , 2006, pág. 4).

Para descubrir la dirección IP destino del túnel, el protocolo mGRE realiza una petición al protocolo NHRP con la dirección privada del siguiente salto (Telnat , 2006, pág. 4).

Esquema del Funcionamiento de NHRP

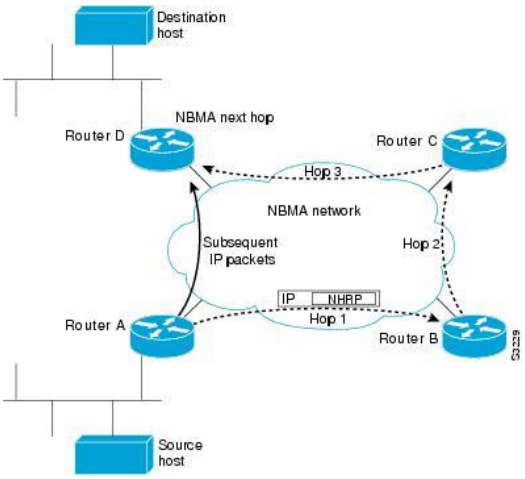

Figura 9. Funcionamiento de NHRP
Fuente: CISCO

1.6 IPSec

IPSec (Internet Protocolo Security IP) es un protocolo que permitirá ofrecer servicios de seguridad en la capa 3, así como a los protocolos superiores que se encuentran basados en IP(TCP-UDP), la seguridad que ofrece IPSec es mediante algoritmos criptográficos cuya función será proteger las comunicaciones sobre el protocolo IP, esta protección puede darse en una o más conexiones entre dos hosts.

IPSec emplea dos tipos de protocolos: AH y ESP para asegurar la autentificación, integridad y confidencialidad de la comunicación, ofreciendo la protección del datagrama IP completo o solo los protocolos de capa superiores (Müller, 2011, pág. 3).

La interfaz del túnel virtual de IPSec (VTI) ofrece IPv6 la protección criptográfica de sitio a sitio, dentro de IPV6 nativo IPSec la encapsulación se utiliza para proteger a los tipos tráfico unicast IPv6, así como el tráfico de multidifusión.

Como se ve en la Figura 10, IPSec (VTI) permite que los dos routers que trabajan como security gatways de seguridad, permiten establecer túneles IPSec entre estos, así como las puertas de enlace de seguridad proporciona una protección de cifrado IPSec para el tráfico de las redes internas como se envía a través del internet público IPv6 (CISCO , 2011, pág. 3).

Esquema del Funcionamiento de IPSec Sitio a Sitio

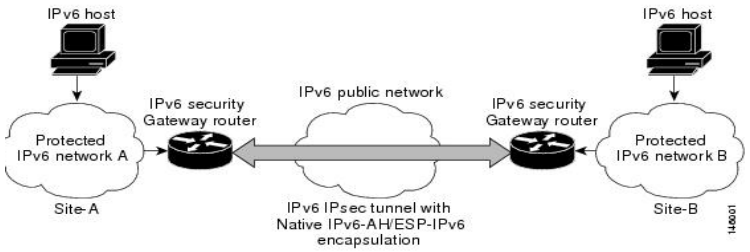

Figura 10. IPSec Sitio a Sitio
Fuente: Implementing IPSec in IPv6 Security

1.6.1 Arquitectura de IPSEC.

IPSec es un conjunto de estándares abiertos que proporcionan confidencialidad, integridad y autentificación de los datos en la capa IP. IPSec se lo puede utilizar para proteger uno o más flujos de datos entre iguales de IPSec (Ramirez Acuña, s.f., pág. 47), ofrece la protección criptográfica, tanto para los datagramas IP en paquetes de redes IPv4 e IPv6 (Ramirez Acuña, s.f., pág. 47).

1.6.2 Modos de Transporte de IPSec.

IPSec permitirá dos modelos de funcionamiento que se utiliza en ESP y AH respectivamente como se detalla a continuación:

Modo Túnel: Empleado principalmente por los gateways IPSec, con objeto de identificar la red que protegen bajo una misma dirección IP y centralizar de este modo el procesado del tráfico de IPSec en un equipo (Pérez Iglesias, 2001, pág. 55).

El contenido del datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. Así, se toma un datagrama IP cual se añade inicialmente una cabecera AH o ESP, posteriormente se añade una nueva cabecera IP que es la que se utiliza para encaminar los paquetes a través de la red. El modo túnel se usa normalmente cuando, el destino final de los datos no coincide con el dispositivo que realiza las funciones de IPSec (Pérez Iglesias, 2001, pág. 55).

Como se muestra en la Figura 11, se observa dos redes que para comunicarse utilizan dos routers como gateways IPSec que implementan el modo túnel. Para la comunicación se realizará a través de una red pública de datos entre dos PC’s una de ellas ubicada en una red local y la otra en una red remota, de tal manera que entre los routers gateways IPSec se establecerá el modo túnel, que permitirá la protección de las comunicaciones de ambas redes.

Modo Túnel en IPSec

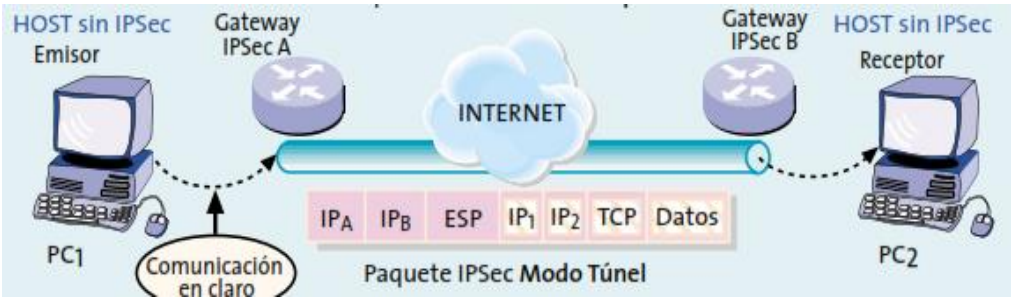

Figura 11. Modo Túnel IPSec
Fuente: Unex

Modo Transporte: En este modo el contenido transportado dentro del datagrama AH o ESP son los datos de la capa de transporte (datos TCP o UDP). Por lo tanto, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger.

El modo transporte tiene la ventaja de que asegurar la comunicación de extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPSec (Pérez Iglesias, 2001, pág. 55).

Como se muestra en la Figura 12, se observa dos dispositivos con el protocolo IPSec y que permitirá la comunicación entre ellas de manera segura, este tipo de comunicación se encontrará en modo transporte, los datos que se debe resguardar es solo el protocolo TCP o UDP, así como también datos de aplicación.

Modo Transporte en IPSec

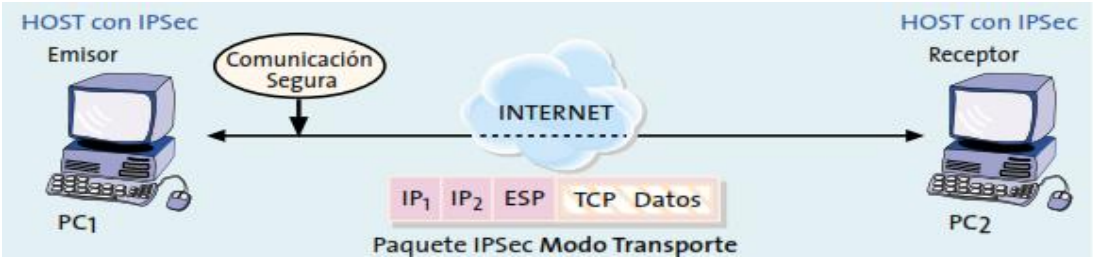

Figura 12. Modo Transporte IPSec
Fuente: Unex

1.6.3 Funcionamiento de IPSEC.

DOI (Domain of Interpretation) define todos los parámetros que se negocian para establecer canales seguros, incluyendo identificadores únicos para algoritmos de autentificación y de encriptación durante el proceso de comunicación, además de los procesos para crear conexión tipo AH o ESP (López Logacho, 2014, pág. 37). La política de seguridad (SP, Security Policy), define que tráfico proteger y cuando hacerlo (López Logacho, 2014, pág. 37). La arquitectura de IPSec se encuentra divida en 7 secciones y como se encuentran unidos a cada uno de estos, como se puede apreciar en la Figura 13.

Esquema de la Arquitectura de IPSec

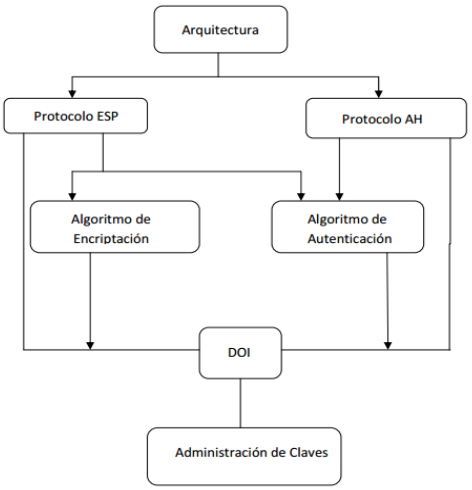

Figura 13. Arquitectura de IPSec
Fuente: Protocolo Seguro de Internet IPS

1.6.4 Asociaciones de Seguridad IPSec.

Una asociación de seguridad (SA) IPSec, especifica las propiedades de seguridad que se reconocen mediante host comunicados. Una única SA protege los datos en una dirección. La protección es para un solo host o para una dirección de grupo (multidifusión) (Ramirez Acuña, s.f., pág. 50). Dado que la mayoría de las comunicaciones es de igual a igual o de cliente-servidor, debe haber dos SA para proteger el tráfico en ambas direcciones.

Los tres elementos que identifican una SA IPSec de modo exclusivo es:

Índice de Parámetros de Seguridad (SPI): Valor entero que indica la fila de la base de datos de asociaciones de seguridad (SDAB), que debe utilizar un destinatario para descifrar un paquete recibido (Ramirez Acuña, s.f., pág. 50).

Dirección IP de Destino: Puede ser una dirección unicast, una dirección de difusión IP, o una dirección de grupo multicast, sin embargo, los mecanismos de IPSec para la gestión de SA se define solamente para unicast (Ramirez Acuña, s.f., pág. 50).

Identificador de protocolo de seguridad (AH o ESP) (Ramirez Acuña, s.f., pág. 50).

1.6.5 Funcionamiento de una SA.

El conjunto de servicios de seguridad ofrecidos por una SA depende del protocolo de seguridad seleccionado, dentro del modo de los SA, de los extremos de la SA y de la elección de los servicios opcionales seleccionados dentro del protocolo (Ramirez Acuña, s.f., pág. 51). AH ofrece además un servicio de anti-replay (integridad de la secuencia) según el deseo del receptor, esto ayudara a prevenir ataques contra denegación de servicios. AH es un protocolo apropiado para emplearse cuando la confidencialidad no es requerida (Ramirez Acuña, s.f., pág. 52).

ESP proporciona de forma opcional confidencialidad del tráfico, ESP también proporciona de forma opcional la autentificación, si la autentificación es negociada por una SA ESP (Ramirez Acuña, s.f., pág. 53). El receptor también puede elegir implementar el servicio de anti-replay, con las mismas características de anti-replay de AH (Ramirez Acuña, s.f., pág. 53).

1.6.6 Combinaciones de Asociaciones de Seguridad.

Los datagramas IP transmitidas por una SA, permite la protección de un protocolo de seguridad AH o ESP; pero no ambos. En ocasiones una política de seguridad puede

determinar una combinación de servicios para flujo de tráfico específico que no se puede por una única SA (Ramirez Acuña, s.f., pág. 53).

El término de “grupo de asociaciones de seguridad” o “grupo de SA” se aplica a una secuencia de SAs las cuales deben procesar el tráfico para satisfacer una política de seguridad (Ramirez Acuña, s.f., pág. 53).

Las SAs pueden combinarse entre grupos de dos formas que son:

Transporte Adyacente: Se aplica más de un protocolo de seguridad sobre el mismo datagrama IP, sin utilizar túneles(Ramirez Acuña, s.f., pág. 53).

Este método combina a AH Y ESP permitiendo solamente un nivel de combinación, el anidado adicional no produce un beneficio adicional (asumiendo el uso de algoritmos adecuados en cada protocolo), puesto que el proceso se realiza en una instancia de IPSec en el destino (Ramirez Acuña, s.f., pág. 53).

Escenario Adyacente de una SA

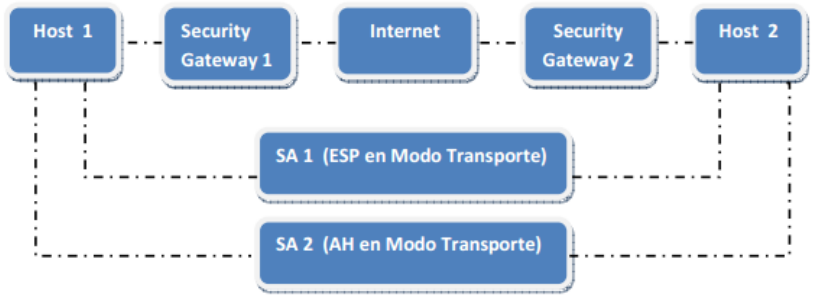

Figura 14. Transporte Adyacente SA
Fuente: Protocolo Seguro de Internet IP

Entre túneles: Se refiere a la aplicación de múltiples capas del protocolo de seguridad efectuado múltiples túneles. Este método permite niveles anidados, puesto que cada túnel se puede originar o terminar en nodos diferentes a lo largo de la trayectoria (Ramirez Acuña, s.f., pág. 54).

CASO 1: Ambos extremos de las SAs son las mismas, los túneles (interno o externo) pueden ser AH o ESP, aunque improbable que el host 1 especifique ambos túneles iguales es decir AH a dentro de AH o ESP dentro de ESP (Ramirez Acuña, s.f., pág. 54).

Esquema del Caso 1 de una SA

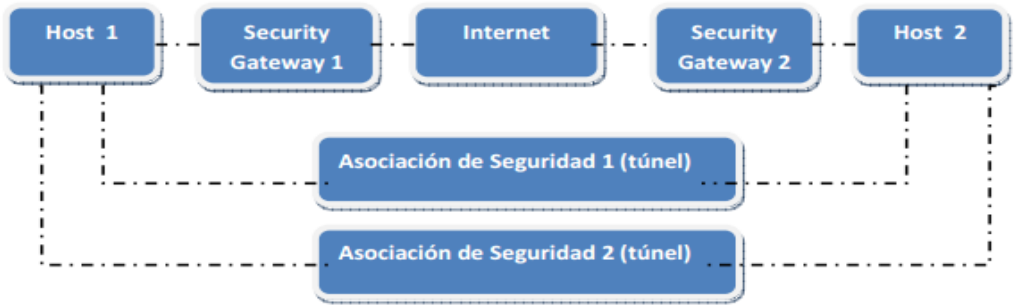

Figura 15. CASO 1 DE SA
Fuente: Protocolo Seguro de Internet IP

CASO 2: Un extremo de las SAs es igual, los túneles (interno o externo) puede ser AH o ESP (Ramirez Acuña, s.f., pág. 54).

Esquema del Caso 2 de una SA

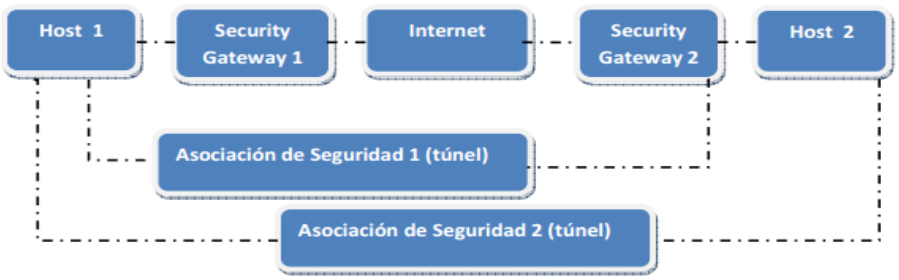

Figura 16. CASO 2 SA
Fuente: Protocolo Seguro de Internet IP

CASO 3: Ninguno de los extremos es igual, los túneles (internos o externos) pueden ser AH o ESP (Ramirez Acuña, s.f., pág. 54).

Esquema del Caso 3 de una SA

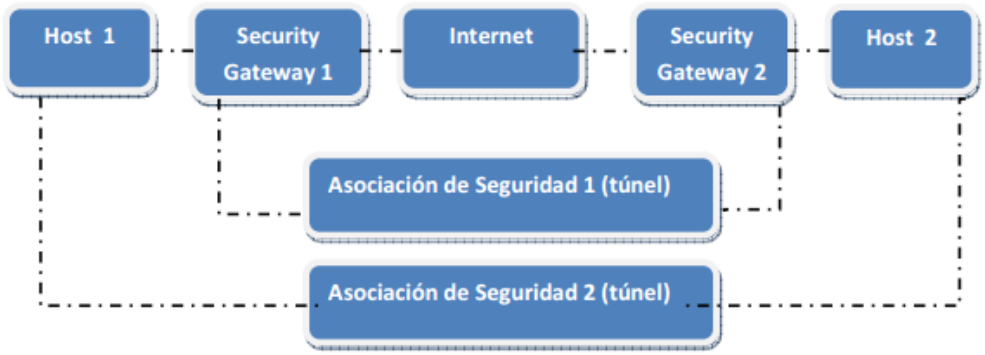

Figura 17. CASO 3 de SA
Fuente: Protocolo Seguro de Internet IP

1.6.7 Características de Protección de IPSec.

Protocolos de Seguridad: El encabezado de autentificación (AH) firma los paquetes IP y garantiza la integridad. El contenido de este datagrama no es cifrado, pero el receptor tiene la seguridad de que el contenido del paquete no sea modificado. El receptor también tiene la garantía de que los paquetes los ha enviado el remitente. Así como (ESP) cifra los datos IP, con lo cual codifica el contenido durante la transmisión de paquetes, ESP también puede garantizar la integridad de los datos mediante el algoritmo de autentificación (Ramirez Acuña, s.f., pág. 48).

Base de datos asociados de seguridad (SADB): La base de datos asocia un protocolo de seguridad con una dirección de destino IP y un numero de índice. El número de índice se denomina índice de parámetros de seguridad. Estos tres elementos (protocolo de seguridad, la dirección de destino y el SPI) identifican de forma exclusiva a un paquete IPSec (Ramirez Acuña, s.f., pág. 48).

Administración de Claves: La generación y distribución de claves para los algoritmos criptográficos y SPI (Ramirez Acuña, s.f., pág. 48).

Mecanismo de Seguridad: Los algoritmos de autentificación y cifrado que protege los datos de los datagramas IP (Ramirez Acuña, s.f., pág. 49).

Base de datos de directivas de seguridad(SPD): La base de datos que especifica el nivel de protección que se aplica a un paquete. SPD filtra el tráfico IP para determinar el modo en que se debe procesar los paquetes. Para los paquetes salientes SPD, SADB determinan el nivel de protección que se aplicará (Ramirez Acuña, s.f., pág. 49).

1.7 Protocolo AH

Dentro de IPSec para garantizar la integridad y autentificación de los datagramas IP. Esto es, proporcionar un medio al receptor de los paquetes IP para autentificar el origen de los datos y para verificar que dichos datos no han sido alterados en tránsito. Sin embargo, no proporciona ninguna garantía de confidencialidad, es decir, los datos transmitidos pueden ser vistos por terceros (Pérez Iglesias, 2001, pág. 52). AH se inserta en la cabecera IP estándar (IPv4 como IPv6) (Pérez Iglesias, 2001, pág. 52).

Como se observa en la Figura 18, IANA al protocolo AH a asignado un valor que es el 51, el significado de este número es la cabecera IP, en vez de los valores 6 o 17 que representan a TCP y UDP en la cabecera AH (Pérez Iglesias, 2001, pág. 52),su principal ventaja es la integridad y autentificación de datos que son encaminados.

Datagrama del Protocolo AH

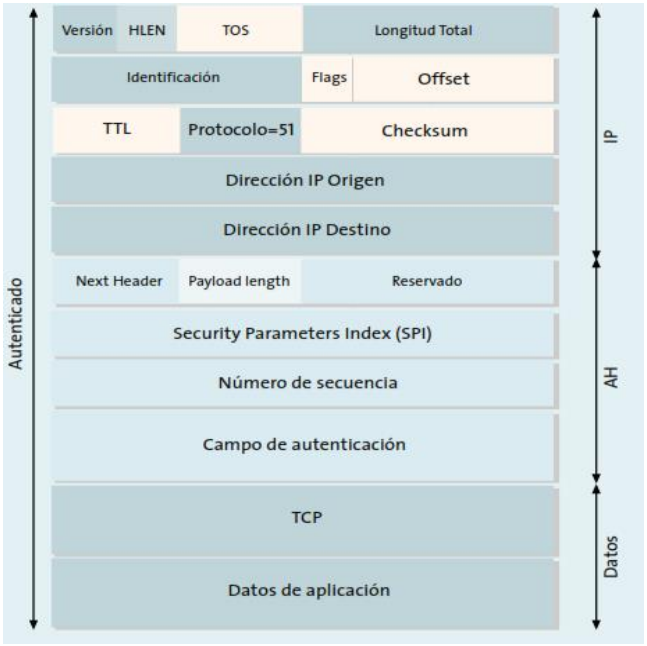

Figura 18. Datagrama AH
Fuente: Análisis del Protocolo IPSec

1.7.1 Funcionamiento del Protocolo AH.

El funcionamiento de AH se basa en un algoritmo HMAC, esto es un código de autentificación de mensajes. Este algoritmo consiste en aplicar una función hash a la combinación de unos de los datos de entrada y una clave, siendo la salida una pequeña cadena de caracteres que se denomina extracto (Pérez Iglesias, 2001, pág. 53). Es una huella personal asociada a los datos y a la persona que lo ha generado, puesto que es la única que conoce la clave (Pérez Iglesias, 2001, pág. 53).

Como se observa en la Figura 19, el modo transporte del protocolo AH, se tiene dos PC's el receptor y el emisor, el emisor permite calcular una parte del mensaje original, este mensaje es copiado en uno de los campos que forman la cabecera AH, una vez que el paquete es ensamblado se envía a la red, esta acción igual es repetida en el extremo es decir en el receptor de tal manera que verifica con el paquete recibido.

Esquema del Funcionamiento del Protocolo AH

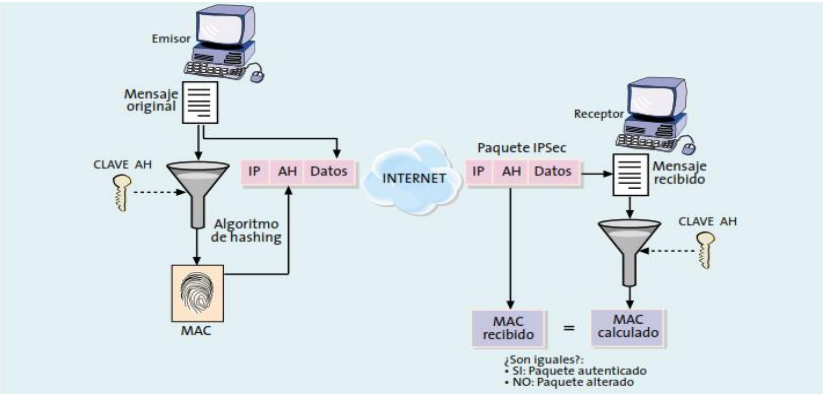

Figura 19. Funcionamiento del Protocolo AH
Fuente: Análisis del Protocolo IPSec

1.8 Protocolo ESP

Permite proporcionar confidencialidad, para ello especifica el modo de cifrar los datos que se desea enviar y como este contenido cifrado incluye en un datagrama IP (Pérez Iglesias, 2001, pág. 54). Adicionalmente, puede ofrecer los servicios de integridad y autenticación del origen de los datos incorporando un mecanismo similar al de AH. Dado que ESP proporciona más funciones que AH, el formato de la cabecera es más complejo, este formato consta de una cabera y una cola que rodean a los datos transportados(Pérez Iglesias, 2001, pág. 54).

Como se muestra en la Figura 20, el protocolo ESP en su datagrama se encontrará estructurado por un campo adicional conocido como campo de relleno. Una de las características más notables es que ESP permitirá tener campos que actúan como rellenos de datos; que servirá para ocultar la longitud real, disfrazando los datos importantes del tráfico.

Datagrama del Protocolo ESP

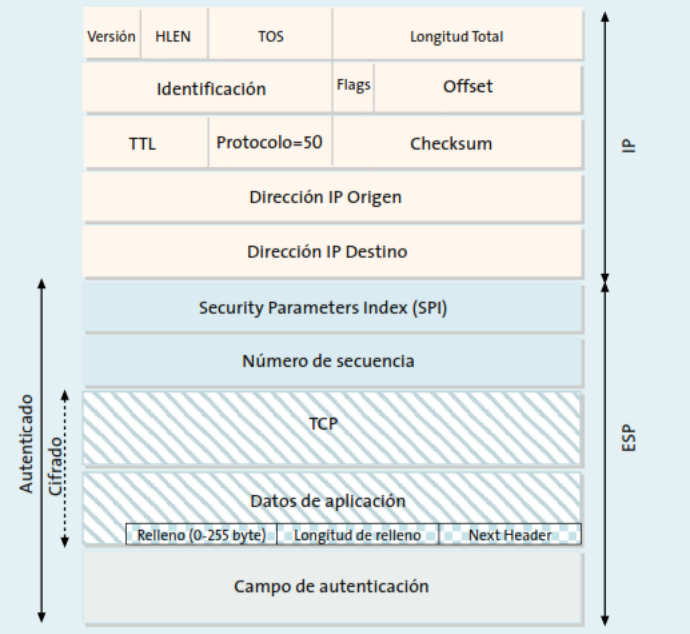

Figura 20. Datagrama de Protocolo ESP
Fuente: Análisis del Protocolo IPSec

1.8.1 Funcionamiento de Protocolo ESP.

La función de cifrado dentro del protocolo ESP, es desempeñada por un algoritmo de cifrado de clave simétrica. Típicamente se usan algoritmos de cifrado bloque, de modo que la longitud de los datos tiene que ser un múltiplo del tamaño de bloque (8 a 16 bytes) (Pérez Iglesias, 2001, pág. 54). La distribución de las claves de forma segura es por consiguiente un requisito esencial para el funcionamiento de ESP, también de AH, es fundamental que el emisor y receptor estén de acuerdo tanto en el algoritmo de cifrado hash y como en el resto de los parámetros comunes que utilizan (Pérez Iglesias, 2001, pág. 55).

Esta labor de puesta en contacto y negociación es realizada por un protocolo de control, denominado IKE (Pérez Iglesias, 2001, pág. 55).

Como se muestra en la Figura 21, ESP envía la información de una manera confidencial, en este caso el emisor tiene el mensaje original, este lo cifra usando una clave específica y lo insertará dentro del paquete IP, a lado de la cabecera ESP.

Mientras el paquete es enviado a su destino, este es atrapado por un tercero que solo podrá observar unos cuantos bytes, en el receptor se ejecuta de nuevo el algoritmo de cifrado en la misma clave, obteniendo así los datos que fueron enviados originalmente, la seguridad de ESP es la robustez de dicho algoritmo de cifrado, esto quiere decir que un hacker no puede descifrar los datos del mensaje sin conocer la clave principalmente, ya que dicha clave solo conoce tanto el emisor como el receptor.

Esquema del Funcionamiento del Protocolo ESP

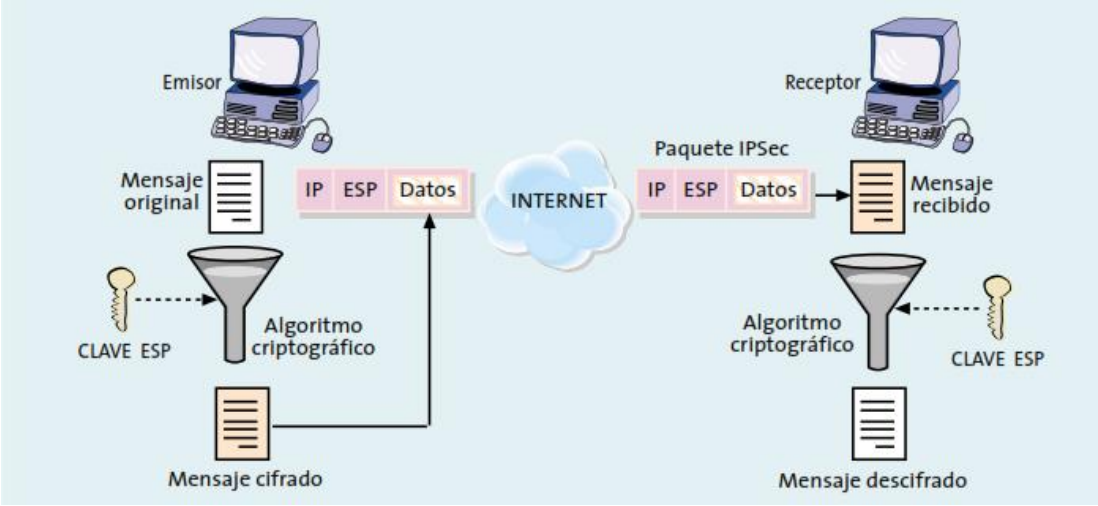

Figura 21. Funcionamiento del Protocolo ESP
Fuente: Análisis del Protocolo IPSec

1.9 Algoritmos de Encriptación

Los protocolos de seguridad de IPSec utiliza dos tipos de algoritmos, de autentificación y de cifrado. El módulo AH utiliza algoritmos de autentificación y el módulo ESP puede utilizar tanto cifrado como de autentificación (Ramirez Acuña, s.f., pág. 79).

IPSec cuenta con diferentes protocolos los cuales se enlistan a continuación:

Cifrado: DES, 3DES, AES (Ramirez Acuña, s.f.).

Funciones Resumen: HMAC, MD5 o SHAI (Ramirez Acuña, s.f.).

Firma Digital: RSA o secreto compartido (Ramirez Acuña, s.f.).

Intercambio de claves: Mediante CA(certificados) o Diffie-Hellman (Ramirez Acuña, s.f.).

Negociación de Seguridad:

IKE (Internet Key Exchange) (Ramirez Acuña, s.f.).

ISAKMP (Internet Security Asssociation and Key Management Protocol) (Ramirez Acuña, s.f.).

Las asociaciones de seguridad son simplemente un paquete de algoritmos y parámetros que se usan para cifrar y autentificar un flujo particular en una dirección (Ramirez Acuña, s.f., pág. 79), por tanto, en el tráfico normal bidireccional, los flujos son asegurados por parte de las asociaciones de seguridad, la decisión final de los algoritmos de cifrado y autentificación le corresponde al administrador de IPSec (Ramirez Acuña, s.f., pág. 79).

1.9.1 Algoritmo DES.

DES utiliza una clave de 56 bits, asegurando un cifrado de alto rendimiento. Se utiliza para cifrar y descifrar datos de los paquetes. DES convierte texto normal en texto cifrado con un algoritmo de cifrado, el algoritmo de cifrado en el extremo remoto restablece el texto normal a partir del cifrado (Ramirez Acuña, s.f., pág. 79).

1.9.2 Algoritmo Triple Des (3DES).

EL algoritmo triple DES(3DES) es una variante del algoritmo DES de 56 bytes. 3DES opera de forma similar a DES en cuanto que los datos se fragmentan en bloques de 64 bits. 3DES entonces procesa cada bloque tres veces, cada vez con una clave de 56 bits independiente (Ramirez Acuña, s.f., pág. 79).

3DES efectivamente duplica la fuerza de cifrado respeto al algoritmo DES de 56 bits (Ramirez Acuña, s.f., pág. 79).

1.9.3 **Diffie-H**ellman **(D-H).**

Es un protocolo de cifrado de clave pública, el algoritmo DH especifica un método de intercambio de clave pública que proporciona de una manera que dos peers establezcan una clave secreta compartida que solo ellos conozcan, aunque se comuniquen a través de un canal inseguro como se muestra en la Figura 22 (CISCO, s.f.).

Como todos los algoritmos criptográficos el intercambio de claves DH se basa en una secuencia matemática de pasos (CISCO , s.f.).

Este es utilizado dentro del IKE para establecer claves de sesión. Los grupos de DH de 768 bits y 1024 bits son soportados en los routers Cisco y los firewalls PIX, el grupo de 1024 bits es más seguro a causa del mayor tamaño de la clave (Ramirez Acuña, s.f., pág. 80).

Esquema del Funcionamiento del Intercambio de Claves Diffie-Hellman

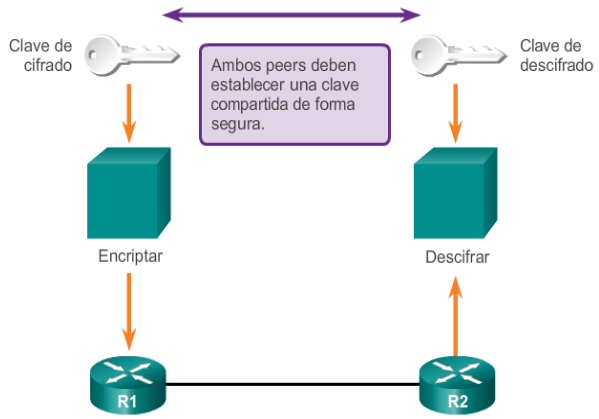

Figura 22. Intercambio de Claves Diffie-Hellman
Fuente: CISCO

1.10 Protocolo ISAKMP

ISAKMP Protocolo de manejo de claves y Asociación de Seguridad, permite la combinación de conceptos de seguridad y autentificación de claves, asociaciones de seguridad para establecer la seguridad requerida.

Está diseñado para soportar negociaciones de SAs de los protocolos de seguridades de todas las capas de la pila de protocolos de red (IPSec, TLS, OSPF, etc.), ISAKMP reduce el costo de la funcionalidad duplicada dentro de un protocolo de seguridad.

1.10.1 Funcionamiento de ISAKMP.

Este protocolo define los procedimientos de autentificar comunicaciones entre los hosts, la creación y la administración de SA, técnicas de generación de claves; negocia, establece y modifica y cancela las SA (López Logacho, 2014, pág. 62).

Negociación de ISAKMP: Las SA deben soportar algoritmos de encriptación, autentificación y mecanismos de establecimiento de claves para IPSEC. ISAKMP no está sujeto a ningún algoritmo criptográfico específico (López Logacho, 2014, pág. 62).

Para la negociación de ISAKMP se encuentra divido en dos fases que se las detalla a continuación:

FASE 1: Dos entidades concuerdan en como proteger futuras negociaciones del tráfico entre ellas mismas, establecido una SA ISAKMP, que es luego usada para proteger las negociaciones requeridas por las SA (López Logacho, 2014, pág. 62).

FASE 2: La negociación es usada para establecer los SA para otros protocolos de seguridad que pueden ser usadas para proteger los intercambios de datos o mensajes (López Logacho, 2014, pág. 62).

1.10.2 Arquitectura de ISAKMP.

Tiene una cabecera de tamaño fijo seguido por un número de cargas variables, donde cada campo realiza una función específica para la seguridad del mensaje (Francisconi, 2009, pág. 131), como se muestra en la Figura 23.

Cabecera de ISAKMP del Protocolo IPSec

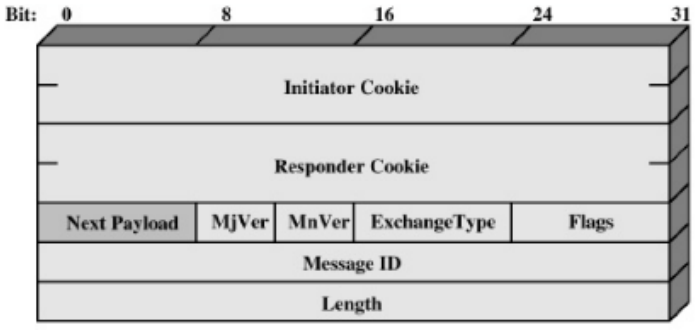

Figura 23. Cabecera de ISAKMP en IPSec
Fuente Seguridad de Sistemas IPSec

Cookie del Iniciador (8 octetos) : Cookie de la entidad que inicia el establecimiento, modifica o cancela la SA (Francisconi, 2009, pág. 131).

Cookie del Respondedor (8 octetos) : Cookie de la entidad que responde al requerimiento del establecimiento de una SA, o cancelación de la SA (Francisconi, 2009, pág. 132).

Carga siguiente (1 octeto) : Indica el tipo de carga en el primer mensaje el formato de cada carga (Francisconi, 2009, pág. 132).

Versión Mayor (4 bits) : Indica la versión mayor del protocolo ISAKMP en uso, las implicaciones basadas en esta versión de Draft-Internet de ISAKMP deben fijar la versión mayor en uno (Francisconi, 2009, pág. 132).

Versión Menor (4 bits) : Indica la versión menor del protocolo ISAKMP en uso, las implicaciones basadas en los Draft-Internet basadas en las versiones previas debe fijarse la versión menor en cero (Francisconi, 2009, pág. 132).

Tipo de Intercambio (1 octeto): Indica el tipo de intercambio usado, esto indica los ordenamientos de los mensajes y la carga en los intercambios ISAKMP (Francisconi, 2009, pág. 132).

Banderas (1 octeto): Indican las opciones específicas que se dejan para el intercambio ISAKMP, las banderas enumeras debajo son específicas del campo de banderas comenzando con el bit menos significativo (Francisconi, 2009, pág. 133).

Bit de Encriptación (1 bit): Si esta en 1, todas las cargas que siguen a la cabecera son encriptadas usando algoritmos de encriptación, identificados por la SA ISAKMP (Francisconi, 2009, pág. 133).

Bit de Commit (1 bit) : Este bit es usado para señalar la sincronización del intercambio de claves, es usado para asegurar que el material encriptado no se reciba antes del término del establecimiento del SA (Francisconi, 2009, pág. 133)

Bit de Autentificación (1 bit): Este bit está diseñado para ser usado con el intercambio informativo de una carga de notificaciones y permitirá la transmisión de la información con comprobación de integridad (Francisconi, 2009, pág. 134).

Identificador (ID) de Mensaje (4 octetos): El identificador de mensaje solamente se usa para identificar el protocolo durante las negociaciones (Francisconi, 2009, pág. 134).

Longitud(4 octetos): Longitud total del mensaje (cabecera más cargas) en octetos, la encriptación puede expandir el tamaño de un mensaje ISAKMP (Francisconi, 2009, pág. 134).

1.11 Protocolo IKE

El objetivo principal de IKE consiste en establecer una conexión cifrada y autentificada entre dos entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad IPSec (Pérez Iglesias, 2001, pág. 57).

Esta negociación se encuentra dividida en dos etapas que se mencionan a continuación:

Primera Fase: La fase común a cualquier aplicación, en la que ambos nodos establecen un canal seguro de autentificado. Dichos canales seguro se consigue mediante el uso de un algoritmo de cifrado simétrico y un algoritmo HMAC, las claves necesarias se derivan de una clave maestra que se obtiene mediante un algoritmo de modo de intercambio de claves Diffie-Hellman de los nodos, para ellos es necesario un paso adicional que es la autentificación (Pérez Iglesias, 2001, pág. 57).

Para la autentificación existen dos métodos que se detallará continuación:

El primer método de autentificación se basa en el conocimiento de un secreto compartido que, como su propio nombre lo indica es una cadena de caracteres que únicamente conocen dos extremos que quieren establecer una comunicación IPSec, mediante el uso de funciones hash cada extremo sin revelar su valor; así los dos se autentifican mutuamente (Pérez Iglesias, 2001, pág. 57).

En los estándares IPSec está previsto de uso de un método de autentificación que se basa en utilizar certificados digitales X509v3, el uso de los certificados permite distribuir de forma segura la clave pública de cada nodo, de modo que se puede probar la identidad mediante posesión de la clave privada y ciertas operaciones de criptografía (Pérez Iglesias, 2001, pág. 57).

En la segunda fase el canal seguro IKE es usado para negociar los parámetros de seguridad específicos asociados a un protocolo determinado en nuestro caso IPSec. Durante esta fase se negocian la característica de la conexión ESP o AH y todos los parámetros necesarios (Pérez Iglesias, 2001, pág. 57).

El equipo que ha iniciado la comunicación ofrecerá todas las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se haya configurado, el sistema receptor aceptara la primera que coincida con los parámetros de seguridad que tengan definidos, así ambos nodos se informaran del tráfico que van a intercambiarse a través de dicha conexión (Pérez Iglesias, 2001, pág. 57).

El funcionamiento de IKE permite la obtención de una clave para la sesión que es utilizada para proteger de una manera segura las conexiones ESP o AH como se muestra en la Figura 24.

Esquema del Funcionamiento de IKE en Protocolo IPSec

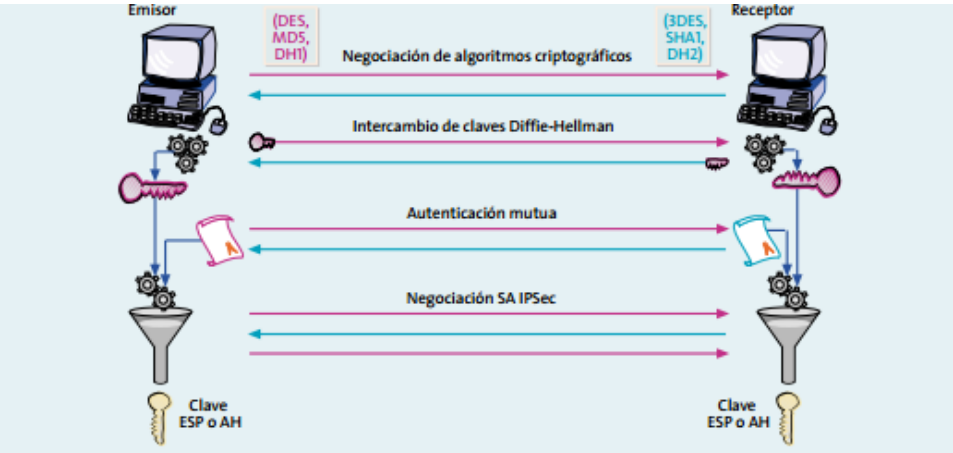

Figura 24. Funcionamiento de IKE en IPSec
Fuente: Análisis del Protocolo IPSec

1.12 Herramientas Utilizadas

1.12.1 GNS3.

Es un simulador gráfico de redes que permite diseñar y configurar topologías complejas y ponerlas en marcha.

Permite trabajar este simulador con ISO de Cisco de diferentes series, permitiendo así que la simulación junto con la configuración sea más real.

1.12.2 Oracle VM Virtual Box.

Es un software de virtualización que permite emular Sistemas Operativos de x86/amd64, permitiendo así al usuario tener un Sistema Operativo dentro de otro, a su vez también de estas máquinas virtuales se les puede enlazar a GNS3 permitiendo así tener un ambiente más real.

CAPÍTULO 2

2 DISEÑO DE LA RED

2.1 Diseño Lógico

Para el diseño lógico de la red piloto el simulador que se utilizará es GNS3, esta aplicación que permitirá cargar routers reales de CISCO, edificando así los dispositivos que se usará para el diseño de red piloto.

2.1.1 Mapa del diseño lógico de la red piloto.

Como se muestra en la Figura 25, el IPS se encontrará en una topología full-mesh, donde cada uno de los nodos estará conectado con todos los nodos restantes, para dicha topología se usarán 12 Routers Cisco 7200, así como también dentro de esta red se tendrá 3 redes LAN que será un grupo de equipos que representará a las 3 sedes de la Universidad Politécnica Salesiana que se encontrarán en Quito, Guayaquil y Cuenca respetivamente.

Para un ambiente más real se utilizarán máquinas virtuales que permitirá cargar servicios como HTTP, FTP en un ambiente IPv6 para la simulación de tráfico.

La red se encontrará compuesta por los siguientes elementos:

Router Cisco 7200

HOST

Servidores

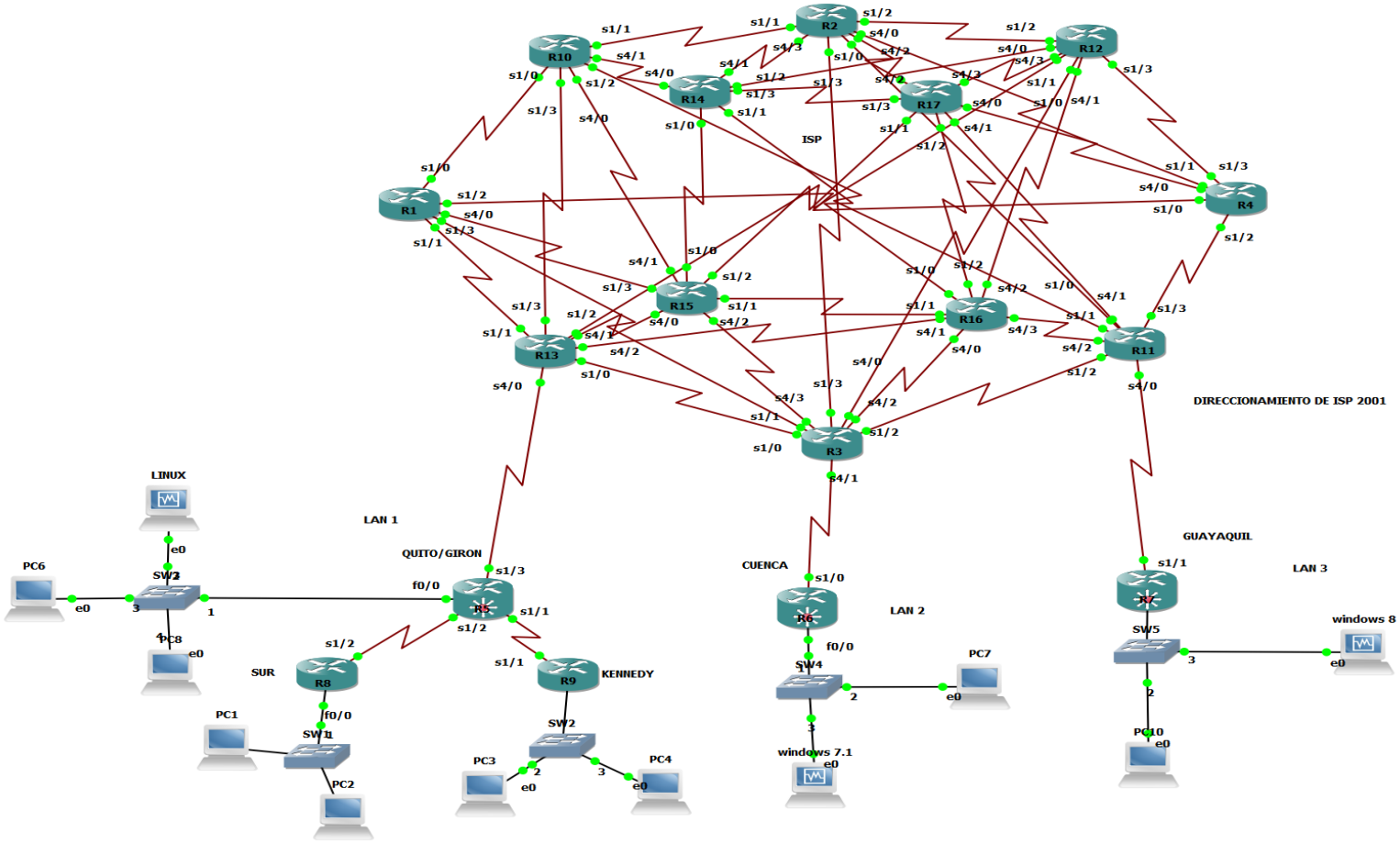

Figura 25. Diseño de la Red Piloto
Fuente: Ximena Bautista

2.1.2 Tabla de direcciones de IPS.

Las direcciones 2001 que se utilizarán en el ISP de la Red Piloto se escogió bajo el criterio de que pertenece a las direcciones Unicast Global que se uso es exclusivamente para Internet, cabe mencionar que el prefijo de sitio que es 2001.

Define la topología de la red, ya que el prefijo para el ISP o RIR es proporcionado por las empresas (ORACLE, 2010).

Tabla 1. Direccionamiento IPv6 de ISP de la Red Piloto

DIRECCIONAMIENTO IPV6 ISP					
Red	***Host***	***Prefijo***	***Red***	***Host***	***Prefijo***
2001:acad:1234:acde	aaaa:abcd:a1b1:abc1	/64	2001:acad:1234:acde	aaaa:abcd:a1b1:abc2	/64
2001:aaaa:bbbb:cccc	acad:cada:3421:dfe7	/64	2001:aaaa:bbbb:cccc	acad:cada:3421:dfe8	/64
2001:dbac:1234:acad	1234:5678:a123:cca7	/64	2001:dbac:1234:acad	1234:5678:a123:cca8	/64
2001:dddd:4321:1234	1234:acad:bcda:ccca	/64	2001:dddd:4321:1234	1234:acad:bcda:cccb	/64
2001:aaaa:bbbb:adca	aaaa:abcd:a1b1:aa12	/64	2001:aaaa:bbbb:adca	aaaa:abcd:a1b1:aa13	/64

Nota: Rango de Direcciones IPv6 para ISP, tabla completa en anexos.
Fuente: Ximena Bautista

2.1.3 Tabla de direccionamiento de LAN (UIO, GYE, CUE).

Las direcciones 2800:68:0016 que se utilizará en la LAN de Quito, Guayaquil, Cuenca de la Red Piloto se la escogió bajo el criterio, a la red CEDIA se le asigno la dirección 2800:68::/32, y su vez se ha subdivido en redes /48 para las Universidades y Centro de Investigación. CEDIA para la Universidad Politécnica Salesiana se le asignó la red 2800:68:0016::/48 (Arguello Tello, 2013).

Para la simulación de la Red piloto se utilizará ::/64 debido a que en IPv6 no afectan las máscaras, por el motivo de que es un protocolo de mayor seguridad y una gran cantidad de direcciones.

Tabla 2.Direcciones IPv6 para Red LAN de la Red Piloto (Quito, Guayaquil, Cuenca)

DIRECCIONAMIENTO IPV6 LAN					
Red	***Host***	***Prefijo***	***Red***	***Host***	***Prefijo***
2008:0068:0016:1001	0A01:1200:0010:0001	/64	2008:0068:0016:1001	0A01:1200:0010:0002	/64
2008:0068:0016:2001	0A01:1200:0020:0010	/64	2008:0068:0016:2001	0B01:1200:0020:0011	/64
2008:0068:0016:3001	0A01:1200:0030:0020	/64	2008:0068:0016:3001	----------	/64
2008:0068:0016:4001	0A01:1200:0010:0020	/64	2008:0068:0016:4001	----------	/64
2008:0068:0016:5001	0A01:1200:0030:0010	/64	2008:0068:0016:5001	----------	/64

Nota: Rango de Direcciones IPv6 para LAN (Quito, Guayaquil, Cuenca), tabla completa en anexos
Fuente: Ximena Bautista.

2.1.4 Tabla de direccionamiento de mGRE.

Tabla 3. Direccionamiento IPv6 para Túneles mGRE (Quito, Cuenca, Guayaquil)

DIRECCIONAMIENTO PARA TÚNEL MGRE			
Red	***Host***	***Prefijo***	***Interfaz***
	ABCD:ABCD:ABCD:ABC1	/64	QUITO-HUB Túnel 10
2012: ABCD: ABCD: ABCD	ABCD:ABCD:ABCD:ABC2	/64	CUENCA-SPOKE 1 Túnel 20
	ABCD:ABCD:ABCD:ABC3	/64	GUAYAQUIL-SPOKE 2 Túnel 30
	ABCD:ABCD:ABCD:ABC4	/64	SUR-QUITO-SPOKE 3 Túnel 40
	ABCD:ABCD:ABCD:ABC5	/64	KENNEDY-QUITO-SPOKE 4 Túnel 50

Nota: Rango de Direcciones IPv6 para Túneles mGRE
Fuente: Ximena Bautista

2.2 Configuraciones

2.2.1 Implementación del ISP.

Se empezará la configuración de la Red por el ISP en GNS3, para lo cual lo primero es añadir la IOS de los Routers que se utilizarán en este caso se usará la IOS de un Router 7200. El siguiente paso es asignar las direcciones a cada uno de los Routers, así como también el tipo de enrutamiento que se utilizará es OSFP, para lo cual se seguirá el direccionamiento de la Tabla 1.

Diseño del ISP para la Red Piloto

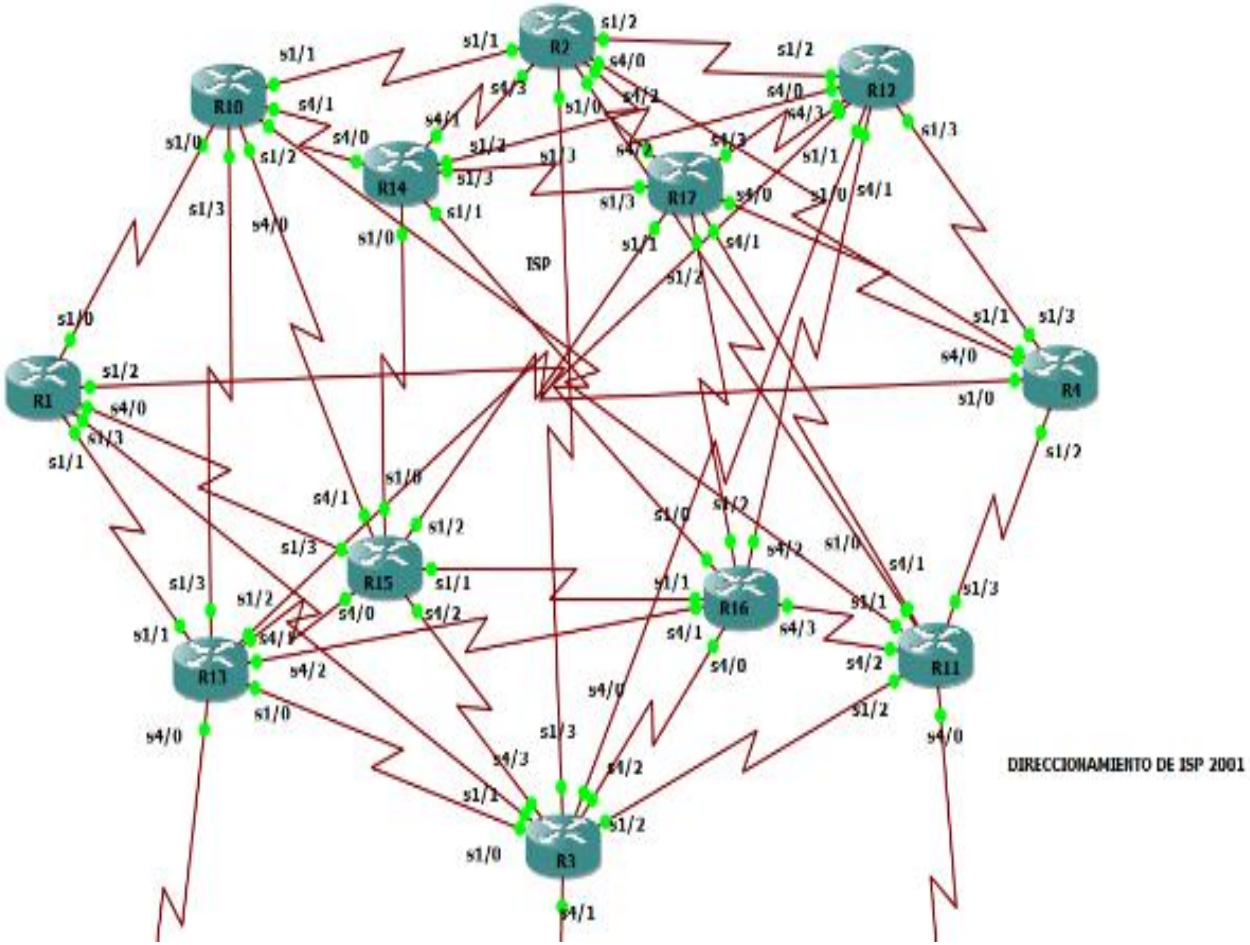

Figura 26. Diseño del ISP
Fuente: Ximena Bautista

EJEMPLO:

R1

R1#configure terminal //Ingresará a la terminal del Router 1.

R1(config)#ipv6 unicast-routing //Habilitará el ruteo unicast para IPv6.

R1(config)#int s1/1 //Ingresará a la interfaz serial de Router 1.

R1(config-if)#ipv6 enable // Activará el Protocolo IPv6 en el Router 1.

R1(config-if)#ipv6 address 2001:acad:1234:acde:aaaat:abcd:a1b1:abc1/64 //Asignará de la dirección IPv6 .

R1(config-if)#no shutdown //Encenderá de la interfaz s1/1.

R1(config-if)#exit //Saldrá del interfaz s1/1.

R1(config)#ipv6 router ospf 1 //Habilitará el enrutamiento OSPFv3 para IPv6.

R1(config-rtr)#router-id 1.1.1.1 //Identificará del R1 con OSPF.

R1(config-rtr)#exit //Saldrá del enrutamiento OSPF.

R1(config)#int s1/1 //Ingresará a la interfaz serial de Router 1.

R1(config)#ipv6 ospf 1 area 0 // Asignará el Área al OSPFv3 para IPv6.

R1(config)#exit //Saldrá de la interfaz s1/1.

R1(config)#do wr //Se guardará las configuraciones realizadas.

CONFIGURACIÓN DEL R13 DEL ISP

R13#configure terminal //Ingresará a la terminal del Router 13.

R13(config)#ipv6 unicast-routing //Habilitará el ruteo unicast para IPv6.

R13(config)#int s1/1 //Ingresará a la interfaz serial de Router 13.

R13(config-if)#ipv6 enable // Activará el Protocolo IPv6 en el Router 13.

R13(config-if)#ipv6 address 2001:ACAD:1234:ACDE:AAAAT:ABCD:

A1B1:ABC2/64 //Asignará de la dirección IPv6.

R13(config-if)#no shutdown //Encenderá de la interfaz s1/1.

R13(config-if)#exit //Saldrá de la interfaz s1/1.

R13(config)#ipv6 router ospf 1 //Habilitará el enrutamiento OSPFv3 para IPv6.

R13(config-rtr)#router-id 1.1.1.1 //Identificará del R1 con OSPF.

R13(config-rtr)#exit //Saldrá del OSPF.

R13(config)#int s1/1 //Ingresará a la interfaz serial de Router 13.

R13(config)#ipv6 ospf 1 area 0 // Asignará del Área al OSPFv3 para IPv6.

R13(config)#exit //Saldrá de la interfaz s1/1.

R13(config)#do wr //Se guardará las configuraciones realizadas.

Nota: Los pasos anteriores de configuración se deberán realizar en todos los routers del IPS con cada una de sus interfaces.

2.2.2 Implementación de la LAN QUITO.

El siguiente escenario es la configuración de la LAN de Quito que se divide en Girón, Kennedy y Sur en GNS3, para lo cual primero es añadir la IOS de los Routers que se utilizarán en este caso se empleará el IOS de un Router 7200.

El siguiente paso será asignar las direcciones a cada uno de los Routers, así como también el tipo de enrutamiento que se utilizará que es OSFP, para lo cual se seguirá el direccionamiento de la Tabla 2.

Diseño de la LAN de Quito

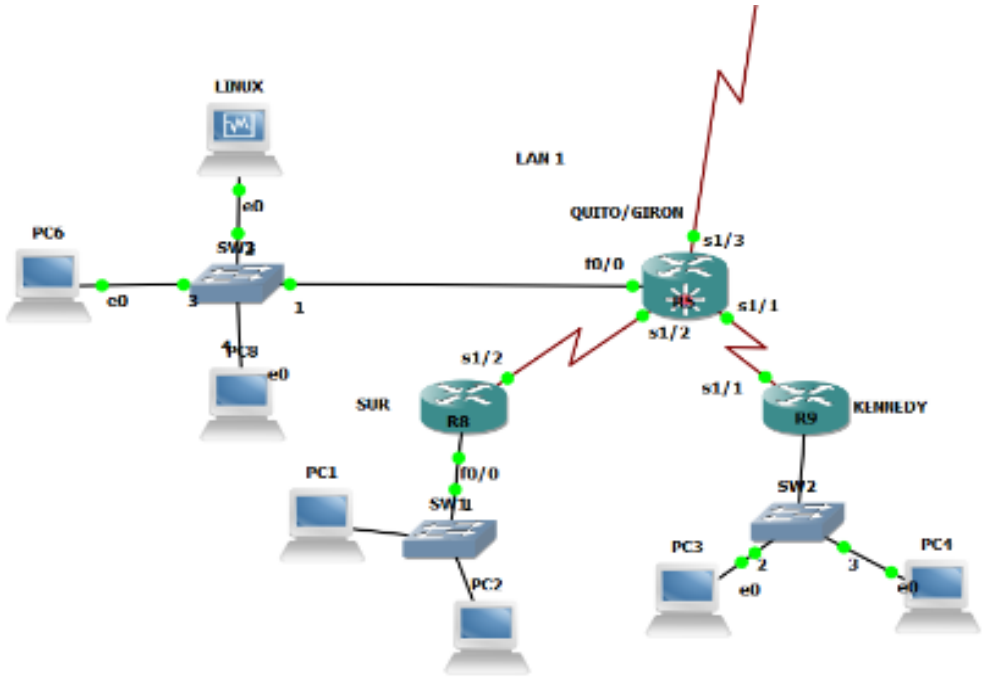

Figura 27. Diseño de LAN de Quito
Fuente: Ximena Bautista

EJEMPLO:

QUITO-GIRON #configure terminal //Ingresará a la terminal del Router QUITO-GIRÓN(R5).

QUITO-GIRON (config)#ipv6 unicast-routing //Habilitará el ruteo unicast para IPv6.

QUITO-GIRON (config)#int s1/2 //Ingresará a la interfaz serial de Router QUITO-GIRÓN(R5).

QUITO-GIRON (config-if) #ipv6 enable //Activará el Protocolo IPv6 en el Router QUITO-GIRÓN(R5).

QUITO-GIRON (config-if)#ipv6 address 2800:0068:0016:1001:0A01:1200:

0010:0001/64 //Asignará de la dirección IPv6.

QUITO-GIRON (config-if)#no shutdown //Encenderá de la interfaz s1/2.

QUITO-GIRON (config-if)#exit //Saldrá del interfaz s1/2.

QUITO-GIRON (config)#ipv6 router ospf 1 //Habilitará del enrutamiento OSPFv3 para IPv6.

QUITO-GIRON (config-rtr)#router-id 5.5.5.5 //Identificará el Router QUITO-GIRÓN(R5) con OSPFv3.

QUITO-GIRON (config-rtr)#exit //Saldrá del OSPF.

QUITO-GIRON (config)#int s1/2 //Ingresará a la interfaz serial de Router QUITO-GIRÓN(R5) con OSPFv3.

QUITO-GIRON (config)#ipv6 ospf 1 area 0 // Asignará el Área al OSPFv3 para IPv6.

QUITO-GIRON (config)#exit //Saldrá de la interfaz s1/2.

QUITO-GIRON (config)#do wr //Se guardará las configuraciones realizadas.

QUITO-SUR #configure terminal //Ingresará a la terminal del Router QUITO-SUR(R8).

QUITO-SUR (config)#ipv6 unicast-routing //Habilitará el ruteo unicast para IPv6.

QUITO-SUR (config)#int s1/2 //Ingresará a la interfaz serial de Router QUITO-SUR(R8).

QUITO-SUR (config-if)#ipv6 enable // Activará el Protocolo IPv6 en el Router QUITO-SUR(R8).

QUITO-SUR (config-if)#ipv6 address 2800:0068:0016:1001:0A01:1200:0010:0002/64 //Asignará la dirección IPv6 .

QUITO-SUR (config-if)#no shutdown //Encenderá de la interfaz s1/2.

QUITO-SUR (config-if) #exit //Saldrá del interfaz s1/2.

QUITO-SUR (config)#ipv6 router ospf 1 //Habilitará el enrutamiento OSPFv3 para IPv6.

QUITO-SUR (config-rtr)#router-id 8.8.8.8 //Identificará al Router QUITO-SUR(R8) con OSPFv3.

QUITO-SUR (config-rtr) #ext. //Saldrá del OSPF.

QUITO-SUR (config)#int s1/2 //Ingresará a la interfaz serial de Router QUITO-SUR(R8) con OSPFv3.

QUITO-SUR (config)#ipv6 ospf 1 area 0 // Asignará del Área al OSPFv3 para IPv6.

QUITO-SUR (config)#exit //Saldrá de la interfaz s1/2.

QUITO-SUR (config)#do wr //Se guardará las configuraciones realizadas.

Nota: Los pasos anteriores de configuración se deben realizar en todos los routers de la LAN que corresponde a Quito, Cuenca, Guayaquil, así como de sus conexiones con el IPS y las interfaces Fast-ethernet con cada una de sus interfaces.

2.2.3 Implementación de mGRE en los Quito, Cuenca y Guayaquil.

El siguiente paso una vez terminado la configuración del ISP y de las Redes LAN, se procederá a la configuración de los túneles mGRE, para lo cual se utilizará una topología Hub-Spoke como router principal será Quito y como spokes serán Cuenca y Guayaquil.

Para su implementación se ha usado la ISO de Cisco 7200 que soporta mGRE en IPv6, cabe recalcar que no todas las ISO soporta mGRE para Ipv6, únicamente soporta para IPv4.

Para las direcciones que se utilizarán dentro de los túneles, se usará las que se encuentran en la Tabla 3.

Diseño de la mGRE en IPv6

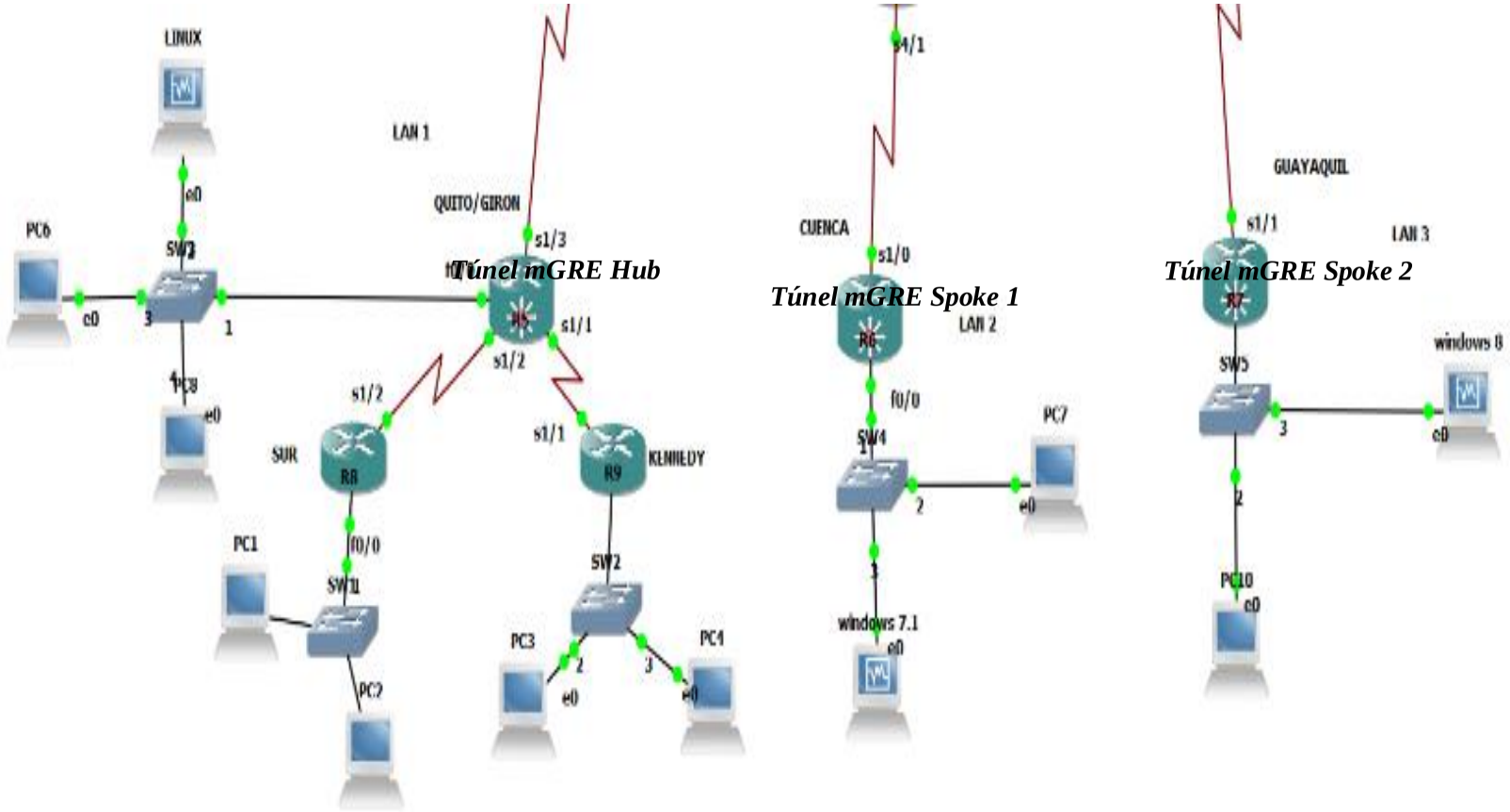

Figura 28. Diseño de mGRE para IPv6
Fuente: Ximena Bautista

EJEMPLO

QUITO-GIRON #configure terminal //Ingresará a la terminal del Router QUITO-GIRÓN(R5).

QUITO-GIRON (config)#ipv6 unicast-routing //Habilitará el ruteo unicast para IPv6.

QUITO-GIRON (config)# interface Tunnel 10 //Ingresará a la interfaz túnel 10 de Router QUITO-GIRÓN(R5).

QUITO-GIRON (config-if) #description DMVPN HUB // Información específica de la Interfaz.

QUITO-GIRON(config-if)#ipv6 address 2012:ABCD:ABCD:ABCD:ABCD:
ABCD:ABCD:ABC1/64 //Asignará de la dirección IPv6 para el HUB.

QUITO-GIRON(config-if)#ipv6 nhrp map multicast dynamic //Habilitará NHRP para iniciar los túneles multipunto (mGRE) y registrará sus asignaciones unicast NHRP.

QUITO-GIRON(config-if) #ipv6 nhrp network-id 100 //Será un identificador de red único que consta de 32 bits, como identificador de una red no difusión de acceso múltiple (NBMA).

QUITO-GIRON(config-if)#ipv6 nhrp holdtime 100 //Permitirá la configuración del tiempo en segundos que NBMA direcciones están anunciadas como respuestas válidas en NHRP.

QUITO-GIRON(config-if)#tunnel source 2001:1111:AAAA:BBBB: 5489:5647:

AD12:54AC //Se configurará la dirección de origen de la interfaz del Túnel 10, también en vez de la dirección se podrá usar la interfaz en este caso es la S1/3.

QUITO-GIRON(config-if) #modo túnel GRE multipunto ipv6//Se establecerá el modo de encapsulación del túnel en este caso será gre multipunto para ipv6.

QUITO-GIRON(config-if)#exit Saldrá de la interfaz túnel 10.

QUITO-GIRON(config)#do wr //Se guardará las configuraciones realizadas.

CUENCA #configure terminal //Ingresará a la terminal del Router CUENCA(R6).

CUENCA (config)#ipv6 unicast-routing //Habilitará el ruteo unicast para IPv6.

CUENCA (config)# interface Tunnel 1 //Ingresará a la interfaz túnel 10 de Router. CUENCA(R6).

CUENCA (config-if) #description DMVPN Spoke 1 // Información específica de la Interfaz.

CUENCA(config-if)#ipv6 address 2012:ABCD:ABCD:ABCD:ABCD:
ABCD:ABCD:ABC2/64 //Asignará la dirección IPv6 para el Spoke 1.

CUENCA(config-if)#ipv6 nhrp map multicast dynamic //Habilitará NHRP para iniciar los túneles multipunto (mGRE) y registrará sus asignaciones unicast NHRP.

CUENCA(config-if)#ipv6 nhrp map multicast dynamic
2001:1111:AAAA:BBB:5489:5647:AD12:54AC //Permitirá que NHRP agregué automáticamente a todos los routers asignaciones de multidifusión de NHRP en este caso utilizará dando una dirección IPv6.

CUENCA(config-if)#ipv6 nhrp network-id 100 //Se establecerá un identificador de red único que constará de 32 bits, como identificador de una red no difusión de acceso múltiple (NBMA).

CUENCA(config-if) #ipv6 nhrp holdtime 100 // Permitirá la configuración del tiempo en segundos que NBMA direcciones estarán anunciadas como respuestas válidas en NHRP.

CUENCA(config-if)#ipv6 nhrp nhs 2012:ABCD:ABCD:

ABCD:ABCD:ABCD:ABCD:ABC1 // Permitirá especificar el prefijo IPv6 de uno o más servidores NHRP, se utilizará la dirección del túnel del HUB.

CUENCA(config-if)#tunnel source 2001:DBAC:1234:1234: 1234:ACAD:

4512:5463 //Se configurará la dirección de origen de la interfaz del Túnel 1, también en vez de la dirección se podrá usar la interfaz en este caso es la S1/0.

CUENCA(config-if) #modo túnel GRE multipunto ipv6//Establecerá el modo de encapsulación del túnel en este caso será gre multipunto para IPv6.

CUENCA(config-if)#exit //Saldrá de la interfaz túnel 1.

CUENCA(config)#do wr //Se guardará las configuraciones realizadas.

Nota: Los pasos anteriores de configuración se deben realizar en todos los Spoke que se encuentran en Guayaquil.

2.2.4 Implementación de IPSEC en Quito, Cuenca, Guayaquil.

EJEMPLO

ROUTER DE CUENCA

CUENCA(config)#crypto isakmp policy 5 //Permitirá la configuración de la política IKE, con una prioridad de 5, este valor puede ir de 1 a 1000.

CUENCA(config-isakmp)#authentication pre-share //Permitirá establecer un modo de autentificación con una clave pre-compartida y soporta IPv6.

CUENCA(config-isakmp)#hash md5// Permitirá establecer el algoritmo hash que se usará para determinar la integridad.

CUENCA(config-isakmp)#group 2//Permitirá especificar un método de intercambio de claves, en el identificador del grupo Diffie-Hellman para la política IKE, tiene varias opciones que son grupo 1 identifica un grupo de 786 bits, el grupo 2 identifica un grupo de 1024 bits y por último el grupo 5 identifica un grupo de 1536.

CUENCA(config-isakmp)#encryption 3des //Permitirá escoger un algoritmo de encriptación, en este caso hemos escogido 3DES, por ser uno de los algoritmos usados para la seguridad de los datos.

CUENCA(config-isakmp)#lifetime 86400 //Permitirá especificar el tiempo de vida que se encontrará en segundos para la SA, éste es un valor de tiempo máximo en que la política de seguridad se va a usar sin realizar una negociación nueva. Para esto el valor se ha elegido para que esta política pueda durar 1 día.

CUENCA(config-isakmp)#exit //Saldrá de isakmp.

CUENCA(config)#crypto isakmp keepalive 30 30 //Permitirá establecer el número de segundos entre mensajes DPD(Dead Peer Dectection), este rango va de 10 a 3600 segundos.

CUENCA(config)#crypto isakmp key 1mgreipv6 address ipv6 2001:1111:AAAA:

BBBB:5489:5647:AD12:54AC/64 //Permitirá definir una clave pre-compartida, dicha clave utilizará la dirección IPv6 de la interfaz de entrada.

CUENCA(config)#crypto keyring mgreups // Permitirá definir el nombre del keyring que se utilizará para la autentificación, esta clave realizará la negociación con IPSec.

CUENCA(conf-keyring)#pre-shared-key address ipv6
2001:1111:AAAA:BBBB:5489:56:47:AD12:54AC/64 key 73abcbx //Permitirá definir una clave pre compartida que se utilizará en la autentificación IKE, la dirección IPv6 deberá ser de la interfaz de entrada del otro extremo.

CUENCA(conf-keyring)#exit //Saldrá del modo de configuración de conf-keyring

CUENCA(config)#crypto ipsec transform-set IPV6UPS esp-3des esp-md5-hmac // Permitirá definir el transform-set que se utilizará para tener una combinación estable de protocolos y algoritmos que serán usados por IPSec.

CUENCA(cfg-crypto-trans)#modo tunnel // Permitirá especificar de que modo se utilizará el túnel.

CUENCA(cfg-crypto-trans)#exit //Saldrá del modo de configuración de crypto.

CUENCA(config)#crypto ipsec profile MGRE // Permitirá definir las características que se utilizará en el cifrado de IPSEC .

CUENCA(ipsec-profile)#set transform-set IPV6UPS// Permitirá especificar un nombre del set transfrom-set que se usará, este nombre distinguirá el proceso, de las políticas de seguridad que se proyectará en el tráfico.

CUENCA (config)# interface Tunnel 1//Ingresará a la interfaz túnel 1 de Router CUENCA(R6).

CUENCA (config-if) # tunnel protection ipsec profile MGRE // Permitirá asociar el túnel 1 con el perfil.

ROUTER DE GUAYAQUIL

GUAYAQUIL(config)#crypto isakmp policy 5 //Permitirá la configuración de la política IKE, con una prioridad de 5, este valor puede irá de 1 a 1000.

GUAYAQUIL (config-isakmp)#authentication pre-share //Permitirá establecer un modo de autentificación con una clave pre-compartida y soportará IPv6.

GUAYAQUIL (config-isakmp)#hash md5// Permitirá establecer el algoritmo hash que se usará para determinar la integridad.

GUAYAQUIL (config-isakmp)#group 2//Permitirá especificar un método de intercambio de claves, en el identificador del grupo Diffie-Hellman para la política IKE, tiene varias opciones que son grupo 1 identifica un grupo de 786 bits, el grupo 2 identifica un grupo de 1024 bits y por último el grupo 5 identifica un grupo de 1536.

GUAYAQUIL (config-isakmp)#encryption 3des //Permitirá escoger un algoritmo de encriptación, en este caso hemos escogido 3DES, por ser uno de los algoritmos usados para la seguridad de los datos.

GUAYAQUIL (config-isakmp)#lifetime 86400 //Permitirá especificar el tiempo de vida que se encuentra en segundos para la SA, este es un valor de tiempo máximo en

que la política de seguridad se va a usar sin realizar una negociación nueva. Para esto el valor se ha elegido para que esta política puede durar 1 día.

GUAYAQUIL (config-isakmp)#exit //Saldrá de isakmp.

GUAYAQUIL (config)#crypto isakmp keepalive 30 30 //Permitirá establecer el número de segundos entre mensajes DPD (Dead Peer Detección), este rango va de 10 a 3600 segundos.

GUAYAQUIL (config)#crypto isakmp key 1mgreipv6 address ipv6 2001:1111:AAAA:BBBB:5489:5647:AD12:54AC/64 //Permitirá definir una clave pre-compartida, dicha clave utilizará la dirección IPv6 de la interfaz de entrada.

GUAYAQUIL (config)#crypto keyring mgreups // Permitirá definir el nombre del keyring que se utilizará para la autentificación, esta clave realizará la negociación con IPSec.

GUAYAQUIL(conf-keyring)#pre-shared-key address ipv6 2001:1111:AAAA:BBBB:5489:56:47:AD12:54AC/64 key 73abcbx //Permitirá definir una clave pre compartida que se utilizará en la autentificación IKE, la dirección IPv6 debe ser de la interfaz de entrada del otro extremo.

GUAYAQUIL (conf-keyring)#exit //Saldrá del modo de configuración de conf-keyring.

GUAYAQUIL config)#crypto ipsec transform-set IPV6UPS esp-3des esp-md5-hmac // Permitirá definir el transform-set que tendrá una combinación estable de protocolos y algoritmos que serán usados por IPSec.

GUAYAQUIL (cfg-crypto-trans)#modo tunnel // Permitirá especificar de qué modo se utilizará el túnel,

GUAYAQUIL (cfg-crypto-trans)#exit //Saldrá del modo de configuración de crypto

GUAYAQUIL (config)#crypto ipsec profile MGRE // Permitirá definir las características que se utilizarán en el cifrado de IPSEC.

GUAYAQUIL (ipsec-profile)#set transform-set IPV6UPS// Permitirá especificar un nombre del set transfrom-set que se usará, este nombre permitirá distinguir el proceso, de las políticas de seguridad que se proyectará en el tráfico.

GUAYAQUIL (config)# interface Tunnel 1//Ingresará a la interfaz túnel 1 de Router GUAYAQUIL(R7).

GUAYAQUIL (config-if) # tunnel protection ipsec profile MGRE // Permitirá asociar el túnel 1 con el perfil.

ROUTER DE QUITO-GIRON

QUITO-GIRON (config)#crypto isakmp policy 5 //Permitirá la configuración de la política IKE, con una prioridad de 5, este valor puede ir de 1 a 1000.

QUITO-GIRON (config-isakmp)#authentication pre-share //Permitirá establecer un modo de autentificación con una clave pre-compartida y soporta IPv6.

QUITO-GIRON (config-isakmp)#hash md5// Permitirá establecer el algoritmo hash que se usará para determinar la integridad.

QUITO-GIRON(config-isakmp)#group 2//Permitirá especificar un método de intercambio de claves, en el identificador del grupo Diffie-Hellman para la política IKE, tiene varias opciones que son grupo 1 identifica un grupo de 786 bits, el grupo 2 identifica un grupo de 1024 bits y por último el grupo 5 identifica un grupo de 1536.

QUITO-GIRON (config-isakmp)#encryption 3des //Permitirá escoger un algoritmo de encriptación en este caso hemos escogido 3DES, por ser uno de los algoritmos usados para la seguridad de los datos.

QUITO-GIRON (config-isakmp)#lifetime 86400 //Permitirá especificar el tiempo de vida que se encuentra en segundos para la SA, este es un valor de tiempo máximo en que la política de seguridad se va a usar sin realizar una negociación nueva. Para esto el valor se ha elegido para que esta política puede durar 1 día.

QUITO-GIRON (config-isakmp)#exit //Saldrá de isakmp.

QUITO-GIRON (config)#crypto isakmp keepalive 30 30 //Permitirá establecer el número de segundos entre mensajes DPD(Dead Peer Detección), este rango irá de 10 a 3600 segundos .

QUITO-GIRON(config)#crypto isakmp key 1mgreipv6 address ipv6 2001:DBAC:1234:1234:1234:ACAD:4512:5463/64 //Permitirá definir una clave pre-compartida, dicha clave utilizará la dirección IPv6 de la interfaz de entrada del túnel 1 de Cuenca.

QUITO-GIRON(config)#crypto isakmp key 1mgreipv6 address ipv6 2001:DCAD:DCAE:FACA:3654:8564:A241:BCA1/64 //Permitirá definir una clave pre-compartida, dicha clave utilizará la dirección IPv6 de la interfaz de entrada del túnel 1 de Guayaquil.

QUITO-GIRON(config)#crypto keyring mgreups // Permitirá definir el nombre del keyring que se utilizará para la autentificación, esta clave realizará la negociación con IPSec.

QUITO-GIRON (conf-keyring)#pre-shared-key address ipv6 2001:DBAC:1234:1234:1234:ACAD:4512:5463/64 key 73abcbx //Permitirá definir una clave pre compartida que se utilizará en la autentificación IKE, la dirección IPv6 debe ser de la interfaz de entrada del otro extremo del túnel 1 de Cuenca.

QUITO-GIRON (conf-keyring)#pre-shared-key address ipv6 2001:DCAD:DCAE:FACA:3654:8564:A241:BCA1/64 key 73abcbx //Permitirá definir una clave pre compartida que se utilizará en la autentificación IKE, la dirección IPv6 debe ser de la interfaz de entrada del otro extremo del túnel 1 de Guayaquil.

QUITO-GIRON (conf-keyring)#exit //Saldrá del modo de configuración de conf-keyring.

QUITO-GIRON config)#crypto ipsec transform-set IPV6UPS esp-3des esp-md5-hmac // Permitirá definir el transform-set que tendrá una combinación estable de protocolos y algoritmos que serán usados por IPSec.

QUITO-GIRON (cfg-crypto-trans)#modo tunnel // Permitirá especificar de que modo se va a utilizar.

QUITO-GIRON (cfg-crypto-trans)#exit //Saldrá del modo de configuración de crypto.

QUITO-GIRON (config)#crypto ipsec profile MGRE // Permitirá definir las características que se utilizarán en el cifrado de IPSEC.

QUITO-GIRON (ipsec-profile)#set transform-set IPV6UPS//Permite especificar un nombre del set transfrom-set que se va a usar, este nombre va a permitir distinguir el proceso, que permitirá las políticas de seguridad que se proyectará en el tráfico

QUITO-GIRON (config)# interface Tunnel 10//Ingresará a la interfaz túnel 10 de Router QUITO-GIRON(R5).

QUITO-GIRON (config-if) # tunnel protection ipsec profile MGRE // Permitirá asociar el túnel 1 con el perfil.

2.2.5 Pruebas de conectividad.

Para la verificación de la conectividad del IPS en la red piloto se realizará entre el R1 y R11 a la S4/2 como se observa en la Figura 29, además de esto se mostrará las seriales configuradas dentro de R11.

Entre ellas se tiene la Serial 4/2 que especificará la dirección IPv6 de dicha interfaz, así como también el tipo de enrutamiento que se utilizó OSPF y su respectiva área.

Direccionamiento de la Interfaz S4/2 del R11

```
!
interface Serial4/0
 no ip address
 ipv6 address 2001:DCAD:DCAE:FACA:3654:8564:A241:BCA2/64
 ipv6 enable
 ipv6 ospf 1 area 0
 serial restart-delay 0
!
interface Serial4/1
 no ip address
 ipv6 address 2001:BCAE:FACD:1111:5662:8542:1381:DDE7/64
 ipv6 ospf 1 area 0
 serial restart-delay 0
!
interface Serial4/2
 no ip address
 ipv6 address 2001:43AB:5EEB:55AE:EEEE:DD11:CC22:BB13/64
 ipv6 ospf 1 area 0
 serial restart-delay 0
!
interface Serial4/3
```

Figura 29. Direccionamiento de la Interfaz S4/2 de R11
Fuente: Ximena Bautista

En la Figura 30, se observa que mediante el comando Ping se envia un paquete ICMP a la direccion destino, en este caso el host destino responde al ping solicitado mediante un paquete denominado ICPM echo reply, dicho así se tiene que el comando Ping envia primero un paquete esperando asi la respuesta , una vez que responda el comando

muestra un signo de exclamación invertido "¡", por defecto las IOS de Cisco mediante el comando Ping envian 5 paquetes de manera predeterminada.

En este caso se han enviado 5 paquetes que correponden al 100% de dichos paquetes enviados, se tiene así un valor menor de tiempo de ida y vuelta menor a 12 milisegundos, con un promedio de 30 milisegundos y un valor máximo de 53 milisegundos.

Conectividad desde R1 a la Interfaz S4/2 del R11

```
*Jul 30 14:12:08.319: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Jul 30 14:12:08.323: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
*Jul 30 14:12:08.351: %LINK-5-CHANGED: Interface Serial4/3, changed state to administratively down
*Jul 30 14:12:08.531: %OSPFv3-5-ADJCHG: Process 1, Nbr 13.13.13.13 on Serial1/1 from LOADING to FULL, Loading
Done
*Jul 30 14:12:08.555: %OSPFv3-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial1/2 from LOADING to FULL, Loading Done
*Jul 30 14:12:08.927: %LINEPROTO-5-UPDOWN: L
R1#ine protocol on Interface FastEthernet2/1, changed state to down
*Jul 30 14:12:08.931: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet3/0, changed state to dow
n
*Jul 30 14:12:08.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial4/1, changed state to down
*Jul 30 14:12:09.159: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial4/2, changed state to down
*Jul 30 14:12:09.303: %OSPFv3-5-ADJCHG: Process 1, Nbr 10.10.10.10 on Serial1/0 from LOADING to FULL, Loading
Done
*Jul 30 14:12:09.351: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial4/3, changed state to down
*Jul 30 14:12:10.323: %OSPFv3-5-ADJCHG: Process 1, Nbr 15.15.15.15 on Serial4/0 from LOADING to FULL, Loading
Done
*Jul 30 14:12:12.251: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial1/3 from LOADING to FULL, Loading Done
R1#ping 2001:43AB:5EEB:55AE:EEEE:DD11:CC22:BB13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:43AB:5EEB:55AE:EEEE:DD11:CC22:BB13, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/30/52 ms
R1#
```

Figura 30. Conectividad del R1 a la S4/2 de R11
Fuente: Ximena Bautista

El siguiente paso será verificar la conección desde las PC´s que se encuentra en Quito, Guayaquil y Cuenca, probando asi la conectividad entre las LAN.

En la siguiente Figura 31, se muestra que mediante el comando show ipv6, se observará la direccion IPv6 de la PC7 que se encuentra conectada al Router CUENCA, así como tambien la MAC 00:50:79:66:68:04 del dispositivo que es un identificador único, la MTU (unidad máxima de transferencia) que para este dispositivo será de 1500 en bytes.

Direccionamiento de la PC7 ubicado en la LAN de Cuenca

```
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file


PC7> show ipv6

NAME                : PC7[1]
LINK-LOCAL SCOPE    : fe80::250:79ff:fe66:6804/64
GLOBAL SCOPE        : 2800:68:16:4001:2050:79ff:fe66:6804/64
ROUTER LINK-LAYER   : ca:11:07:28:00:00
MAC                 : 00:50:79:66:68:04
LPORT               : 10029
RHOST:PORT          : 127.0.0.1:10028
MTU:                : 1500

PC7>
```

Figura 31. Direccionamiento de la PC7 en Cuenca.
Fuente:Ximena Bautista

En la Figura 32, se muestra la conectividad que entre la PC6 de QUITO-GIRON a la PC7 de CUENCA, observando así que el tiempo de vida (TTL) de cada uno de los ping´s se obtiene un valor de 56 cada uno, especificando así que dicho ping recorrio 5 dipositivos de la red , con un tiempo aproximado de 128.714 milisegundos sin haber perdido ninguno de los paquetes enviados.

Conectividad entre la PC6 y PC7

```
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file


PC6> ping 2800:68:16:4001:2050:79ff:fe66:6804

2800:68:16:4001:2050:79ff:fe66:6804 icmp6_seq=1 ttl=56 time=128.714 ms
2800:68:16:4001:2050:79ff:fe66:6804 icmp6_seq=2 ttl=56 time=104.818 ms
2800:68:16:4001:2050:79ff:fe66:6804 icmp6_seq=3 ttl=56 time=142.277 ms
2800:68:16:4001:2050:79ff:fe66:6804 icmp6_seq=4 ttl=56 time=110.003 ms
2800:68:16:4001:2050:79ff:fe66:6804 icmp6_seq=5 ttl=56 time=115.393 ms

PC6>
```

Figura 32. Direccionamiento de la PC6 en Quito-Girón
Fuente: Ximena Bautista

En la Figura 33, mediante el comando show ipv6, se muestra la dirección IPv6 de la PC10 que se encuentra conectada al Router GUAYAQUIL, así como tambien la MAC 00:50:79:66:68:03 del dispositivo que es un identificador único, la MTU (unidad máxima de transferencia) que para este dispositivo será de 1500 en bytes.

Direccionamiento de la PC10 ubicado en la LAN de GUAYAQUIL

```
VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file


PC10> show ipv6

NAME                : PC10[1]
LINK-LOCAL SCOPE    : fe80::250:79ff:fe66:6803/64
GLOBAL SCOPE        : 2800:68:16:5001:2050:79ff:fe66:6803/64
ROUTER LINK-LAYER   : ca:12:13:04:00:00
MAC                 : 00:50:79:66:68:03
LPORT               : 10037
RHOST:PORT          : 127.0.0.1:10036
MTU:                : 1500

PC10>
```

Figura 33. Direccionamiento de la PC10 en Guayaquil
Fuente: Ximena Bautista

En la Figura 34, se muestra la conectividad entre la PC8 de QUITO-GIRON a la PC10 de GUAYAQUIL,observando así que el tiempo de vida (TTL) de cada uno de los ping´s se obtiene un valor de 54 cada uno y dicho ping recorrio 5 dipositivos de la red, con un tiempo aproximado de 278.432 milisegundos sin haber perdido ningún paquete.

Conectividad de la PC8 a la PC10

```
VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file


PC8> ping 2800:68:16:5001:2050:79ff:fe66:6803

2800:68:16:5001:2050:79ff:fe66:6803 icmp6_seq=1 ttl=54 time=278.432 ms
2800:68:16:5001:2050:79ff:fe66:6803 icmp6_seq=2 ttl=54 time=106.202 ms
2800:68:16:5001:2050:79ff:fe66:6803 icmp6_seq=3 ttl=54 time=125.301 ms
2800:68:16:5001:2050:79ff:fe66:6803 icmp6_seq=4 ttl=54 time=122.541 ms
2800:68:16:5001:2050:79ff:fe66:6803 icmp6_seq=5 ttl=54 time=125.272 ms

PC8>
```

Figura 34. Conectividad del PC8 en Quito a la PC10 en Guayaquil
Fuente: Ximena Bautista

El siguiente paso se demostrará que se encuentra configurado mGRE en Quito, con los siguientes comandos que también se puede utilizar en Cuenca y Guayaquil.

- show tunnel endpoints tunnel <0-21474837647> // Permitirá la verificación de los puntos finales del túnel se hayan creado correctamente.
- show dmvpn //Permitirá especificar la sesión de información.

- show interface tunnel10 //Permitirá verificar el estado del túnel 10

En la Figura 35, permite la verificación del túnel 10, se podrá observar que el túnel está configurado en mGRE sobre IPv6.

Resultados del comando show tunnel endpoints tunnel 10

```
QUITO-GIRON#show tunnel endpoints tu
QUITO-GIRON#show tunnel endpoints tunnel 10
 Tunnel10 running in multi-GRE/IPv6 mode

 Endpoint transport 2001:DBAC:1234:1234:1234:ACAD:4512:5463 Refcount 4 Base 0x6B0B43D8 Create Time 00:38:30
   overlay 2012:ABCD:ABCD:ABCD:ABCD:ABCD:ABCD:ABC2 Refcount 2 Parent 0x6B0B43D8 Create Time 00:38:30
   Tunnel Subblocks:
      tunnel-nhrp-sb:
         NHRP subblock has 1 entries
   overlay FE80::C811:7FF:FE28:0 Refcount 2 Parent 0x6B0B43D8 Create Time 00:38:30
   Tunnel Subblocks:
      tunnel-nhrp-sb:
         NHRP subblock has 1 entries
 Endpoint transport 2001:DCAD:DCAE:FACA:3654:8564:A241:BCA1 Refcount 4 Base 0x6B0B4240 Create Time 00:38:21
   overlay 2012:ABCD:ABCD:ABCD:ABCD:ABCD:ABCD:ABC3 Refcount 2 Parent 0x6B0B4240 Create Time 00:38:21
   Tunnel Subblocks:
      tunnel-nhrp-sb:
         NHRP subblock has 1 entries
   overlay FE80::C812:13FF:FE04:0 Refcount 2 Parent 0x6B0B4240 Create Time 00:38:21
   Tunnel Subblocks:
      tunnel-nhrp-sb:
         NHRP subblock has 1 entries
QUITO-GIRON#
QUITO-GIRON#
```

Figura 35. Resultado del comando show tunnel endpoints
Fuente: Ximena Bautista

En la Figura 36, se observa la verificación de los NHRP, así como también los atributos asociados a la sesión actual que en este caso será del túnel 10, el cual se encontrará dos túneles remotos (peer) levantados y cada uno de ellos con un atributo (D) Dinámico, determinando así también las direcciones remotas de NBMA.

Resultados del comando show dmvpn

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

Interface: Tunnel10, IPv6 NHRP Details
Type:Hub, Total NBMA Peers (v4/v6): 2
    1.Peer NBMA Address: 2001:DBAC:1234:1234:1234:ACAD:4512:5463
        Tunnel IPv6 Address: 2012:ABCD:ABCD:ABCD:ABCD:ABCD:ABCD:ABC2
        IPv6 Target Network: 2012:ABCD:ABCD:ABCD:ABCD:ABCD:ABCD:ABC2/128
        # Ent: 1, Status: UP, UpDn Time: 00:39:58, Cache Attrib: D
    2.Peer NBMA Address: 2001:DCAD:DCAE:FACA:3654:8564:A241:BCA1
        Tunnel IPv6 Address: 2012:ABCD:ABCD:ABCD:ABCD:ABCD:ABCD:ABC3
        IPv6 Target Network: 2012:ABCD:ABCD:ABCD:ABCD:ABCD:ABCD:ABC3/128
        # Ent: 1, Status: UP, UpDn Time: 00:39:48, Cache Attrib: D

QUITO-GIRON#
```

Figura 36. Resultados del comando show dmvpn
Fuente: Ximena Bautista

En la Figura 37, se permitirá cargar la configuración del estado del túnel, entre esta información se describirá lo que es DMVPN HUB, es el hub central de la red piloto, así como también la MTU (unidad máxima de transferencia) con un valor de 1456 bytes, el protocolo del túnel es multipunto GRE/IPv6, el tiempo de vida (TTL) del túnel con un valor de 255, un ancho de banda transmisión y recepción de 8000 Kbps.

Resultados del comando show interface tunnel 10

```
QUITO-GIRON#show interfaces tunnel 10
Tunnel10 is up, line protocol is up
  Hardware is Tunnel
  Description: DMVPN HUB
  MTU 1456 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 2001:1111:AAAA:BBBB:5489:5647:AD12:54AC
  Tunnel protocol/transport multi-GRE/IPv6
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Tunnel transport MTU 1456 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input 00:00:08, output 00:00:08, output hang never
  Last clearing of "show interface" counters 00:43:53
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

Figura 37. Resultado del comando show interfaces túnel 10
Fuente: Ximena Bautista

Para la verificación de IPSec se realizará en el router Quito-Giro con los siguientes comandos igualmente estos comandos podrán ser utilizados en Cuenca y Guayaquil.

- show crypto isakmp sa //Permitirá conocer las sesiones que se encuentran en ISAKMP y sus asociaciones de seguridad dentro de IKE.
- show crypto engine conecction active //Permitirá conocer la información y configuración de encriptación.
- show crypto ipsec sa //Permitirá conocer las asociaciones de seguridad que están configuradas en el router.

En la Figura 38, se observará el estado de las negociaciones que se utilizó en ISAKMP, así como también el modo en el que se configuró IKE, en este caso se observa el estado

MM_KEY_EXCH describirá que ambos han intercambiado sus claves y han generado sus claves secretas, MM_NO_STATE especificará el proceso ISAKMP se ha iniciado, pero no está establecido, los modos anteriores pertenecen al modo principal de IKE, mientras que el modo rápido QM_IDLE establecerá que el ISAKMP SA está inactivo y se encuentra identificando.

Resultados del comando show crypto isakmp sa

```
QUITO-GIRON#show cry
QUITO-GIRON#show crypto is
QUITO-GIRON#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status

IPv6 Crypto ISAKMP SA

 dst: 2001:1111:AAAA:BBBB:5489:5647:AD12:54AC
 src: 2001:DCAD:DCAE:FACA:3654:8564:A241:BCA1
 state: MM_KEY_EXCH     conn-id:   1003 status: ACTIVE

 dst: 2001:1111:AAAA:BBBB:5489:5647:AD12:54AC
 src: 2001:DCAD:DCAE:FACA:3654:8564:A241:BCA1
 state: MM_NO_STATE     conn-id:   1002 status: ACTIVE (deleted)

 dst: 2001:1111:AAAA:BBBB:5489:5647:AD12:54AC
 src: 2001:DBAC:1234:1234:1234:ACAD:4512:5463
 state: QM_IDLE         conn-id:   1004 status: ACTIVE

QUITO-GIRON#
```

Figura 38. Resultados del comando show crypto isakmp sa
Fuente: Ximena Bautista

En la Figura 39, se observa la información y configuración de encriptación, así como también permitirá la verificación de que el túnel funcione correctamente, además se observará un ISAKMP SA, con MD5 como algoritmo de autentificación y 3DES utilizado para cifrar los mensajes de negociación IKE, los valores de cifrar y descifrar se encontraron en 0 debido a que no se ha establecido la negación, también se tiene dos IPSEC SA con MD5 que permitirá la comprobación de la integridad de los mensajes , así como también un cifrados 3DES para los paquetes ESP, los valores de cifrar y descifrar se encontrará en 17, demostrando así que la negociación se ha establecido.

Resultados del comando show crypto engine connections active

```
QUITO-GIRON#show crypto eng
QUITO-GIRON#show crypto engine co
QUITO-GIRON#show crypto engine cone
QUITO-GIRON#show crypto engine conne
QUITO-GIRON#show crypto engine connections a
QUITO-GIRON#show crypto engine connections active
Crypto Engine Connections

   ID  Type    Algorithm           Encrypt  Decrypt LastSeqN IP-Address
    1  IPsec   3DES+MD5                 0       17       17 2001:1111:AAAA:BBBB:5489:5647:AD12:54AC
    2  IPsec   3DES+MD5                17        0        0 2001:1111:AAAA:BBBB:5489:5647:AD12:54AC
 1004  IKE     MD5+3DES                 0        0        0 2001:1111:AAAA:BBBB:5489:5647:AD12:54AC

QUITO-GIRON#
```

Figura 39. Resultados del comando show crypto engine connections active en R5
Fuente: Ximena Bautista

En la Figura 40, se observa las asociaciones de seguridad que se encontrará configuradas en el router Quito, así como también los paquetes encriptados, desencriptados, verificados con un valor de 111.

Resultados del comando show crypto ipsec sa

```
QUITO-GIRON#
QUITO-GIRON#show crypto ipsec sa

interface: Tunnel10
    Crypto map tag: Tunnel10-head-0, local addr 2001:1111:AAAA:BBBB:5489:5647:AD12:54AC

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (2001:1111:AAAA:BBBB:5489:5647:AD12:54AC/128/47/0)
   remote ident (addr/mask/prot/port): (2001:DBAC:1234:1234:1234:ACAD:4512:5463/128/47/0)
   current_peer 2001:DBAC:1234:1234:1234:ACAD:4512:5463 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 111, #pkts encrypt: 111, #pkts digest: 111
    #pkts decaps: 111, #pkts decrypt: 111, #pkts verify: 111
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 2001:1111:AAAA:BBBB:5489:5647:AD12:54AC,
     remote crypto endpt.: 2001:DBAC:1234:1234:1234:ACAD:4512:5463
     path mtu 1456, ipv6 mtu 1456, ipv6 mtu idb (none)
     current outbound spi: 0xA984A733(2844043059)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x182CC545(405587269)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 3, flow_id: SW:3, sibling_flags 80004041, crypto map: Tunnel10-head-0
        sa timing: remaining key lifetime (k/sec): (4367578/3321)
        IV size: 8 bytes
 --More--
```

Figura 40. Resultados del comando show crypto ipsec sa
Fuente: Ximena Bautista

CAPÍTULO 3

3 Análisis y resultados

3.1 Prueba de servidores

Para la recopilación de los resultados, se deberá realizar el levantamiento de servicios para la red piloto, entre ellos se tendrá FTP y HTTP que se encontrarán en un Servidor Linux y para clientes se utilizará dos máquinas virtuales que serán Windows 7 como cliente de HTTP y Windows 8, dentro de esta última se tendrá instalado Filezilla para el tráfico de FTP.

Como se muestra en la Figura 41, se deshabilitará los servicios de ip-tables tanto para IPv4 como para IPv6.

Desactivación de los Servicios Iptables en Linux re

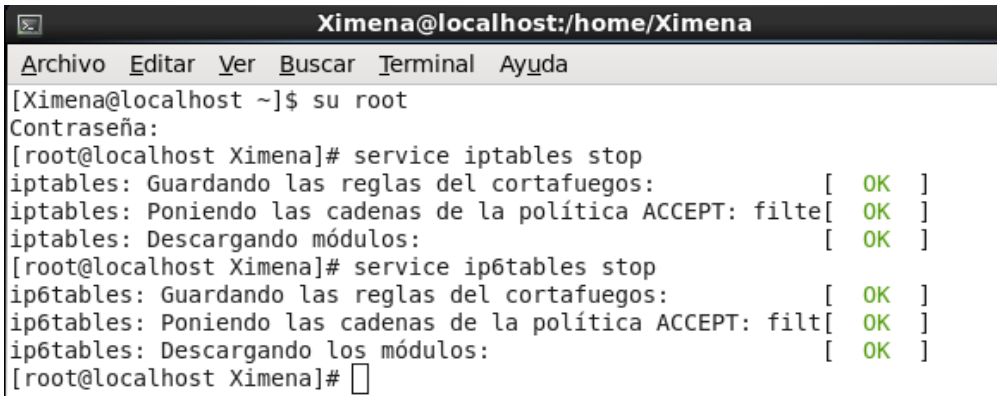

Figura 41. Desactivación de Servicios IP-Tables en Linux
Fuente: Ximena Bautista

Como se muestra en la Figura 42, se realizará la inicialización de los servicios que corresponden a httpd servicio Apache dentro de HTTP y vsftpd en Linux para la generar el tráfico respectivo.

Inicialización de los Servicios HTTPD Y VSFTPD en Linux

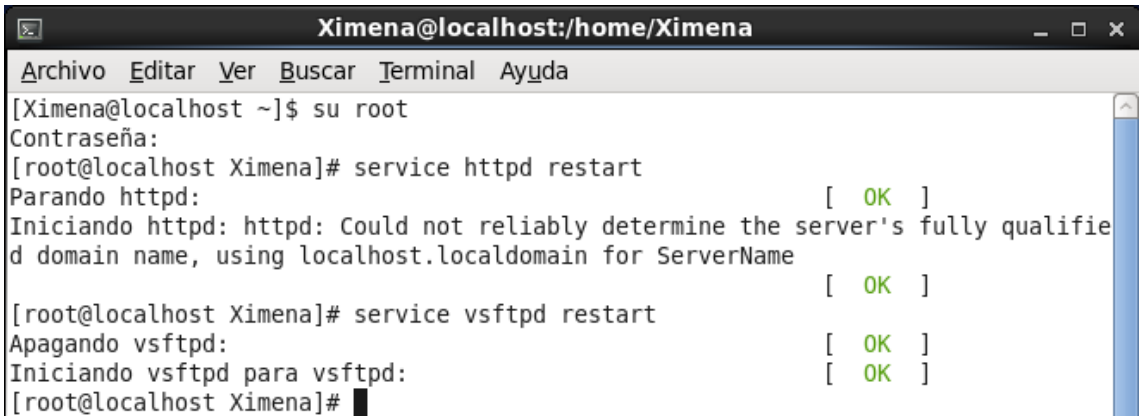

Figura 42. Inicialización de los Servicios HTTPD y VSFTPD en Linux
Fuente: Ximena Bautista

En la Figura 43, se mostrará la conexión al servidor de Linux mediante la aplicación de FileZilla que se encontrará instalada en Windows 8, cabe recalcar que para la conexión la dirección IPv6 del servidor deberá ir entre [] en la aplicación, así como también se deberá digitar el nombre del usuario, la contraseña y el puerto en el cual se encontrará ejecutando FTP que será el puerto 21 o el 22.

Conexión con el Servidor de Linux(FTP) mediante FileZilla en IPv6

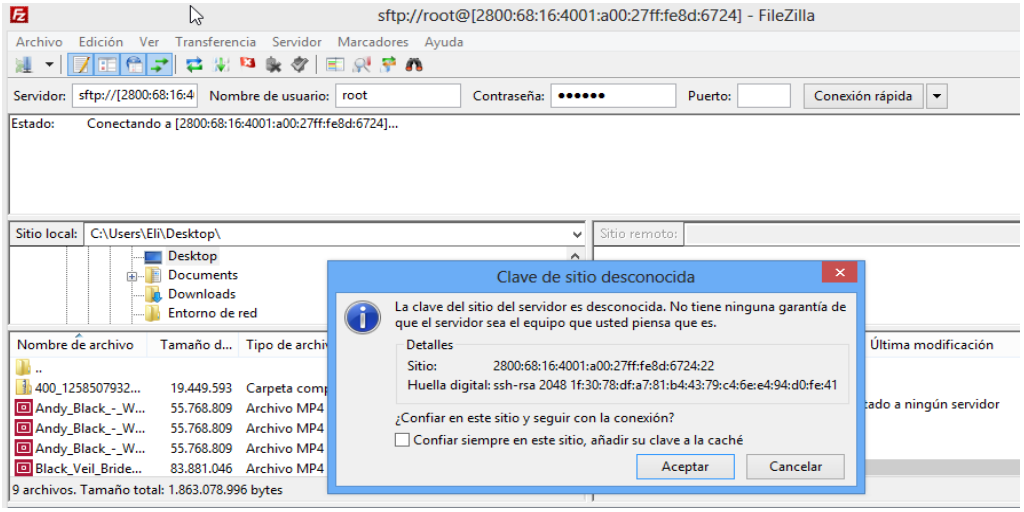

Figura 43. Conexión con el Servidor FTP en Linux con FileZilla en IPv6
Fuente: Ximena Bautista

Para la verificación de la HTTP en Linux, se deberá digitar la dirección del servidor Linux en el navegador, de igual manera dicha dirección se encontrará entre [] para que la conexión sea exitosa, como se muestra en la Figura 44.

De esta manera se podrá verificar que cada uno de los servicios que se levantaron en Linux, se encuentran funcionando de una manera óptima y estos servicios se podrán acceder desde cualquiera de las máquinas virtuales que trabajarán como clientes.

Verificación de HTTP en Linux con IPv6

Figura 44.Verificación de HTTP en Linux mediante navegador en IPv6
Fuente: Ximena Bautista

3.2 Análisis de Resultados

Se realizó un estudio comparativo utilizando dos escenarios, uno de los escenarios se encontrará estructurada por una Red IPv4 configurada con GRE punto a punto, mGRE multipunto e IPsec, de igual manera una Red IPv6 con GRE punto a punto, mGRE multipunto e IPsec, cada uno de estos escenarios con sus características específicas.

El objetivo de la implementación de estos dos escenarios, se realizó para conocer la variación de tiempo que tomaba cada uno de ellos al enviar diferentes paquetes con

distintos tamaños dentro de la red, para la captura de tráfico se ha tomado en cuenta el uso de Wireshark, esta herramienta permitirá el análisis e identificación del tráfico de la red en un momento específico y de una manera muy detallada.

La captura de los paquetes para la verificación de mGRE se realizó en el escenario IPv6 desde el router denominado QUITO-GIRON, se debe mencionar que dichas capturas fueron tomadas desde el inicio de los dispositivos de la red, hasta envió de paquetes de FTP, HTTP y la culminación del ping extendido que se realizará desde el servidor hasta los clientes.

Dentro del escenario de mGRE se podrá visualizar los paquetes NHRP que se encontrarán de color rojo, los paquetes ICMPv6, TCP de color verde, paquetes HELLO de OSPF de color ámbar, como se muestra en la Figura 45.

Captura de los Paquetes mGRE con Wireshark

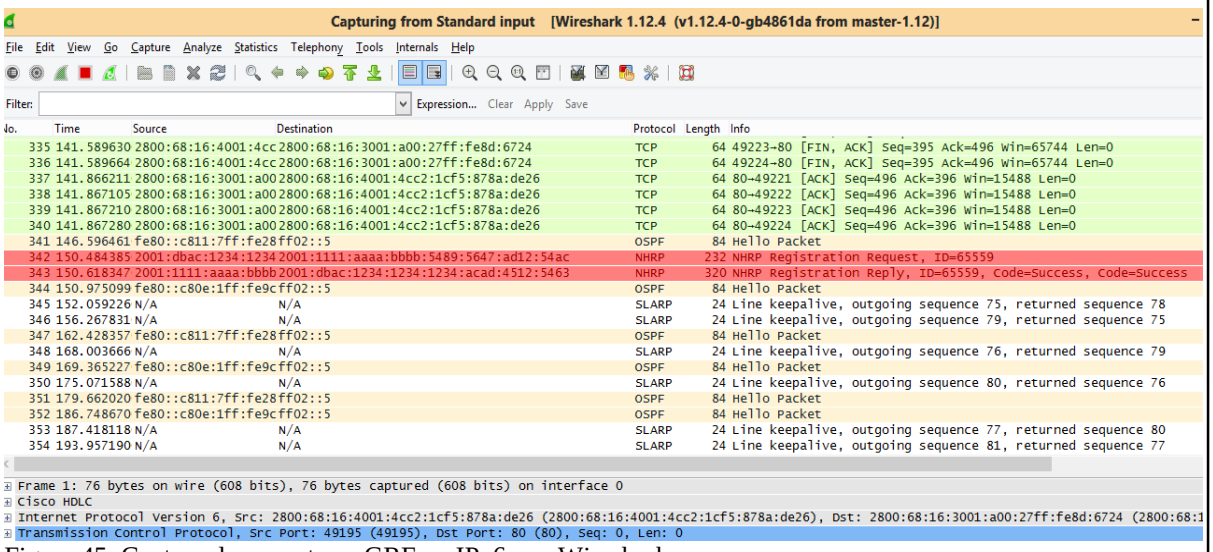

Figura 45. Captura de paquetes mGRE en IPv6 con Wireshark
Fuente: Ximena Bautista

Se debe mencionar que para proteger la información crítica al momento de ser solicitada por sucursales o sedes, debe ir encriptada y protegida, para lo cual se ha implementado la seguridad con IPsec.

Para la captura de paquetes IPSec con mGRE se realizó en el router QUITO-GIRON siendo este el router principal de la implementación de mGRE para Ipv6, dentro del escenario de implementación del protocolo IPSec se podrá visualizar paquetes ISAKMP de color azul, ESP de color blanco, así como también paquetes NHRP de color rojo, y los paquetes HELLO OSPF de color ámbar, como se muestra en la Figura 46.

Captura de los Paquetes IPSec + mGRE con Wireshark en IPv6

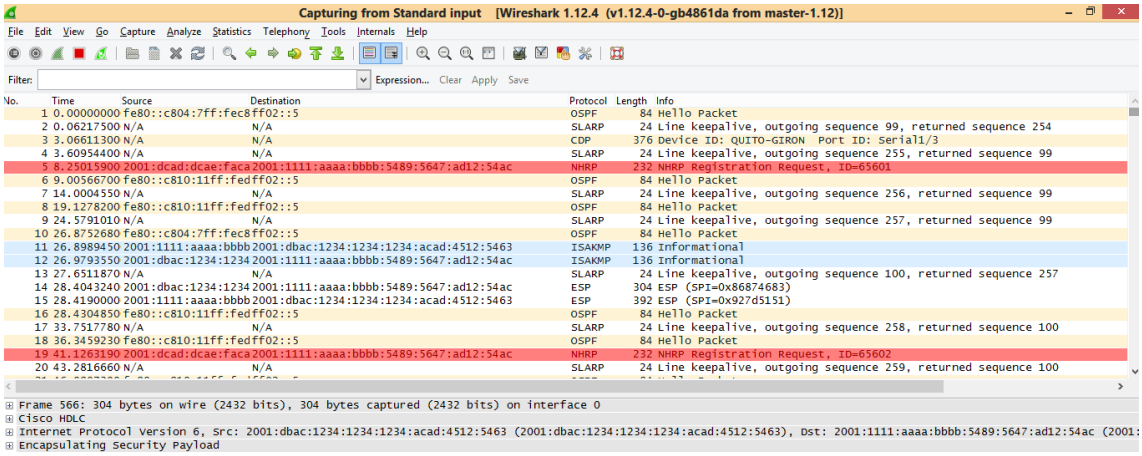

Figura 46. Captura de Paquetes IPsec+mGRE con Wireshark en IPv6
Fuente: Ximena Bautista

Para la captura de los tiempos dentro los dos escenarios IPv4 como IPv6, por la red se filtraron paquetes de diferentes tamaños que van desde los 10MB hasta los 70MB, se usó este rango como una muestra pequeña para analizar así el comportamiento de la red, con paquetes no mayores a 100 MB, determinando así la estabilidad de la red y como se seria su rendimiento con un flujo de paquetes más grandes.

En la Figura 47, se puede observar que en el escenario mGRe con IPv6 e IPsec el porcentaje de paquetes que se ha enviado es el 100% con un total de 79659 paquetes, dentro de ellos se incluye IPv6, ICMPv6, OSPF, ISAKMP, ESP.

El total de paquetes enviados para IPv6 es de 79553 que corresponde al 99,87%, que se encuentra conformado por ICMPv6 con un total de 1698 paquetes enviados que es

el 2,13%, paquetes OSPF con un total de 96 que corresponde al 0,12%, paquetes ISAKMP con un total de 112 que corresponde al 0,14%, paquetes ESP con un total de 16 que corresponde al 0,12%.

Dentro de los paquetes que corresponde a los servicios se tienen paquetes HTTP con un total de 374 que corresponde al 0,47% y paquetes TCP con un total de 77631 que corresponde al 97,64%.

Se debe recalcar que cuando se implementó el IPsec dentro de mGRE este es absorbido por el protocolo de IPsec, brindando de esta manera seguridad a la red.

Estadísticas de un paquete de 70MB en IPv6 con mGRE e IPSec

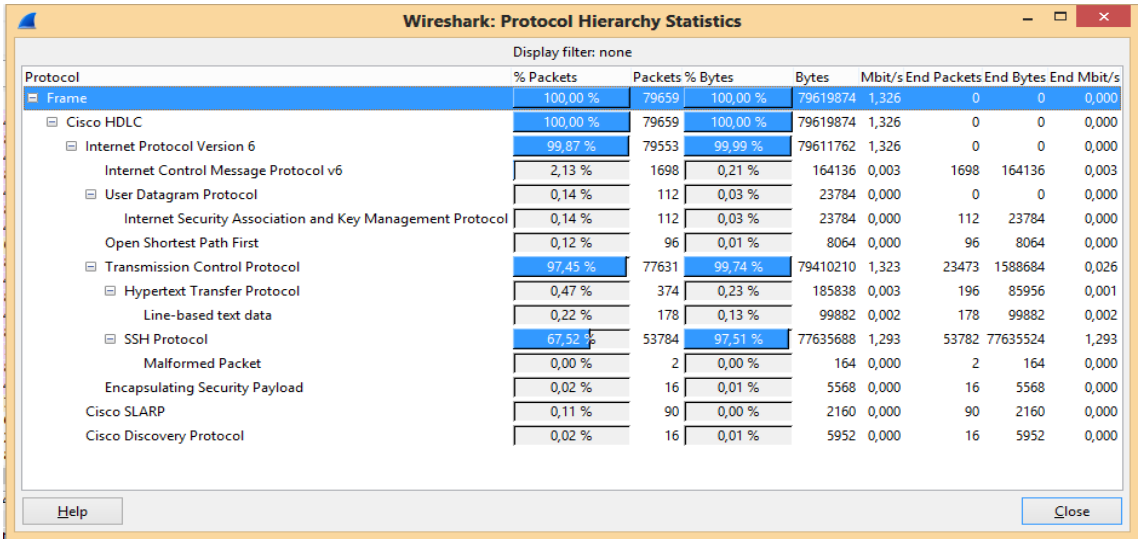

Figura 47. Estadísticas de 70MB en IPv6 con mGRE e IPSec
Fuente: Ximena Bautista

Como se observa en la Figura 48, se determinará las diferencias que existen entre el escenario IPv4 e Ipv6, al momento de transmitir un paquete de 10 MB en GRE IPv4 como en IPv6; se evidencia que el tiempo en que demorará es de 0,55s en comparación a IPv4 que su tiempo será de 1 min y 39s debido a que las cabeceras de IPv4 implementan un cheksum y esto hace que en IPv4 se demore 0,44s al momento

de transmitir la información, mientras que en IPv6 no se incorpora el cheksum con lo que hace que la información se traslade los paquetes a 0,55s.

Resultados del Tráfico de 10MB en mGRE en IPv4 e IPv6

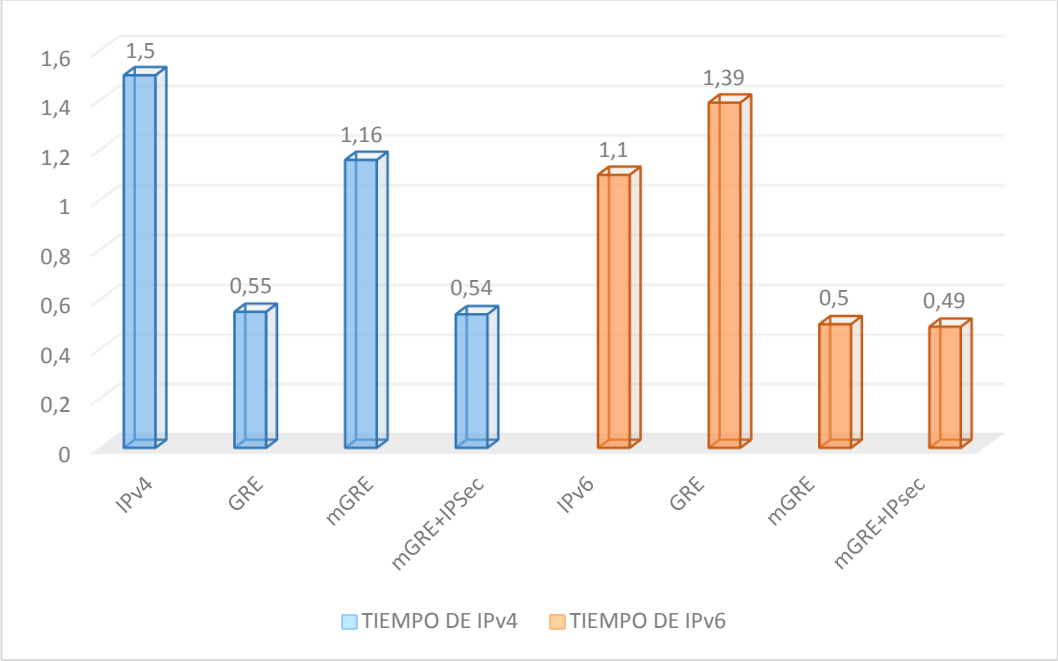

Figura 48. Resultados del Tráfico de 10MB en mGRE en IPv4 e IPv6
Fuente: Ximena Bautista

En la Figura 49, se observa un cambio notorio al momento de enviar un paquete de 30MB ya implementado IPSec,mGRE tanto en IPv4 como en IPv6 , en IPv4 al enviar los paquetes se tendrá un tiempo de 2 min y 28s, cabe recalcar que en IPv4 no es necesario la implementación de un protocolo de seguridad, pero en el escenario IPv6 con mGRE e IPsec, se tendrá una sobrecarga en la red al momento de enviar los paquetes con un tiempo de 3 min y 0,5 s el aumento será de 0,37 s esto se deberá a que se han introducido en la cabecera IPv6, cabecera de IPsec que son ESP y a su vez cabeceras de mGRE generando así el incremento mencionado anteriormete, que permitirá de esta manera pasar los paquetes cifrados y autentificados al destino, garantizando así seguridad en la red.

Resultados del Tráfico de 30 MB en IPv6, mGRE, IPSec en IPv4 e IPv6

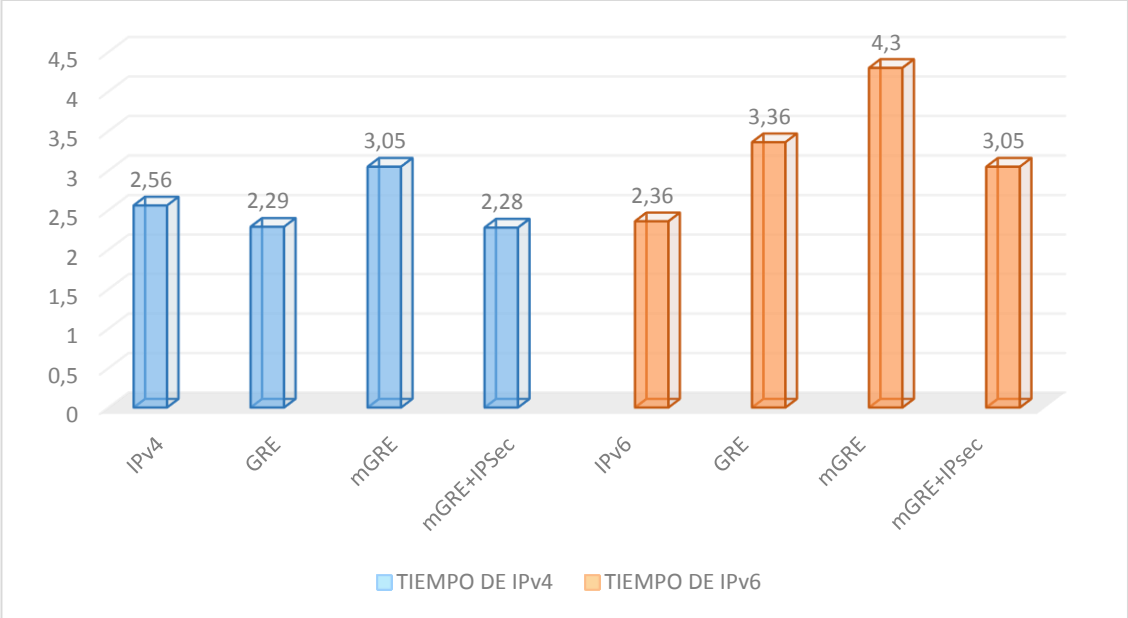

Figura 49. Resultados del Tráfico de 30 MB en IPv6, mGRE, IPSec en IPv4 e IPv6
Fuente: Ximena Bautista

En la Figura 50, se aprecia un comportamiento similar de los paquetes, es decir, el tiempo en que se demoró el tráfico de paquetes en IPv6, mGRE e IPSec en IPv6 se obtuvo un tiempo de 6 min y 0,4 s diferencia al tráfico de paquetes en mGRE, IPsec en IPv4 con un tiempo de 4 min y 0,1 s al momento de filtrar paquetes en la red con un tamaño de 50MB se puede observar claramente que el tiempo a crecido con una diferencia de 2 min y 0,3 s dicho aumento como se específico antes se deberá a las cabeceras de IPv6 , mGRE e IPsec que brindan protección a la red.

Resultados del Tráfico de 50 MB en IPv6, mGRE, IPSec en IPv4 e IPv6

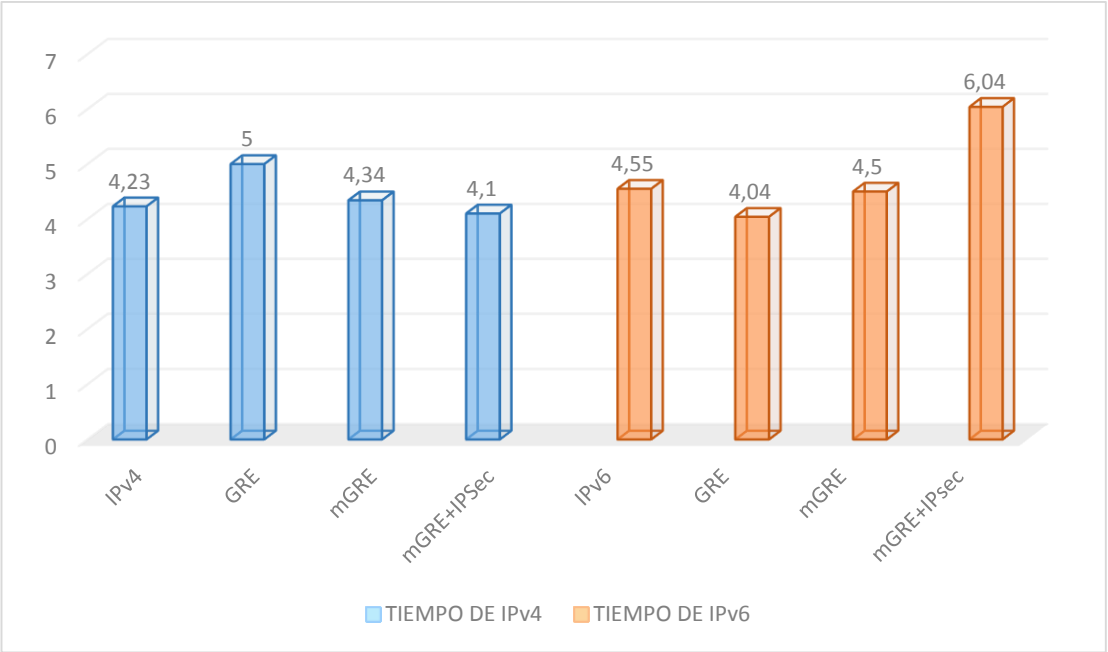

Figura 50.Resultados del Tráfico de 50 MB en IPv6, mGRE, IPSec en IPv4 e IPv6
Fuente: Ximena Bautista

En la Figura 51, se muestra el tiempo en que se demorará un paquete de 70 MB inyectado a la red IPv6 con mGRE, IPsec, al igual que en los escenarios anteriores, la tendencia tiende a ser similar.

Se observará que el tiempo obtenido en IPv4 será de 5 min y 27 s, mientras que el tiempo en IPv6 será de 6 min y 5s, deduciendo así que el aumento será de 0,82 s en el escenario IPv6.

Resultados del Tráfico de 70 MB en IPv6, mGRE, IPSec en IPv4 e IPv6

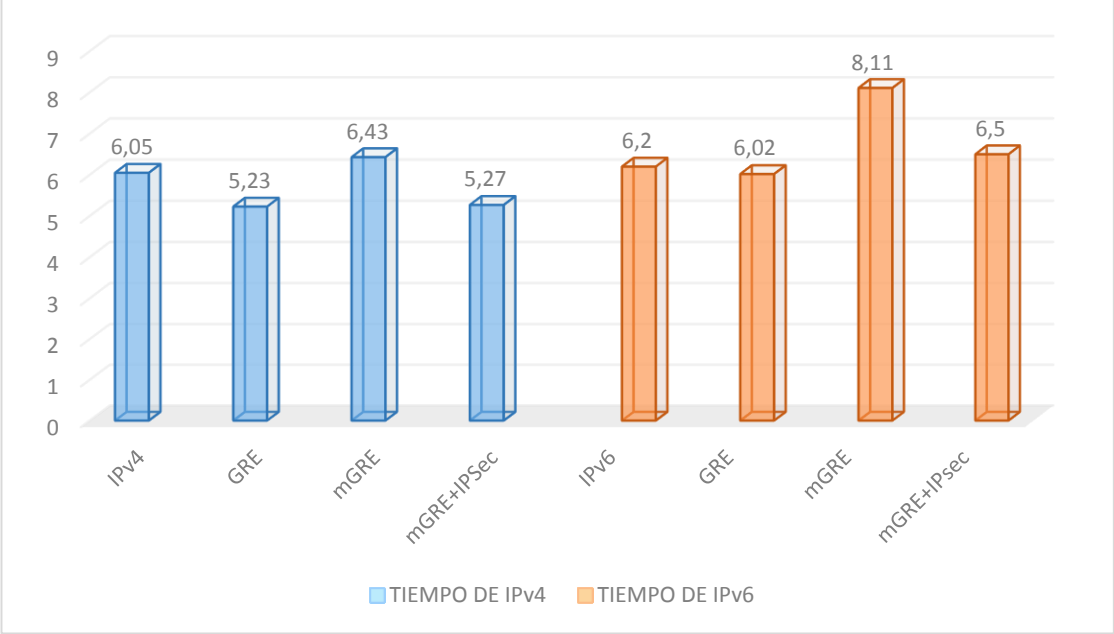

Figura 51.Resultados del Tráfico de 70 MB en IPv6, mGRE, IPSec en IPv4 e IPv6
Fuente: Ximena Bautista

CONCLUSIONES

- Que, mediante los resultados obtenidos de las configuraciones que se realizó en el capítulo 4 de la investigación, se demostró que es factible la implementación de mGRE con IPsec en IPv6, debido a que se encontró los recursos necesarios para su simulación, entre estos recursos se resaltará la IOS de Cisco 7200 que permitió la configuración de mGRE en un ambiente IPv6 e IPsec, con la finalidad de brindar la confidencialidad de los datos más críticos que entre ellos se encontrará, datos personales, transacciones de cualquier institución o empresa sea esta pública o privada.
- La implementación del protocolo mGRE se la podrá realizar siempre y cuando la infraestructura cumpla con los requisitos mínimos para su implementación, entre estos requisitos estará un router que soporte mGRE en IPv6 nativo.
- El uso de mGRE en IPv6 permite ventajas tales como una implementación fácil y sencilla tanto del Hub central como de los Spoke, así como también brindar seguridad a la información de la red, mediante algoritmos de encriptación y autentificación que proporciona IPSec.
- Dentro de la simulación de red mGRE e IPsec en el escenario IPv6, la transmisión de los paquetes de un extremo a otro se refleja un aumento del 36 % con referencia a la misma simulación en un escenario IPv4.

RECOMENDACIONES

Sabiendo que mGRE es un protocolo nuevo que no ha tenido la oportunidad de ser implementado en entornos IPv6, debido a la migración de entornos IPv4 a IPv6 no se ha demostrado aun sus ventajas y desventajas totalmente, existen algunas limitantes entre ellas la más importantes son que equipos en funcionamiento dentro de la red no son capaces de soportar el protocolo mGRE, la mayoría de los dispositivos soportan mGRE en IPv4 de provocando así una falta de experiencia y desconocimiento de las facultades del protocolo.

- Se recomienda en forma general la utilización de la IOS correcta que permita la implementación de mGRE en un ambiente IPv6.
- Se recomienda que la implementación de mGRE con IPSec en IPv6 se realice en escenarios de alto rendimiento, que necesiten enviar información crítica e indispensable a otros lugares o sucursales se lo pueda realizar mediante un tráfico seguro mediante cifrado.
- Realizar un futuro análisis para implementar calidad de servicio a mGRE con IPsec en Ipv6 mediante el protocolo MPLS, permitiendo así tener así un escenario con una alta velocidad de trasferencia orientado a calidad de servicio.
- Se recomienda realizar más investigaciones sobre mGRE, IPsec en IPv6 y, verificar si hay la posibilidad de que este protocolo sea implementado en IOS en versiones más bajas al 7200 de Cisco, para de esta manera empresas más pequeñas puedan beneficiarse de túneles multipuntos y seguridad mediante tráfico cifrado.

GLOSARIO DE TÉRMINOS

DMVPN: (Dynamic Multipoint VPN) protocolo que permite la implementación de túneles virtuales dinámicos atreves de una red virtual privada.

ESP: (Encapsulating Security Payload) protocolo perteneciente a IPSEC, que permite autentificación, integridad y protección a los paquetes que son enviados a trevés de la red.

IPSEC: (Internet Protocol Security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autentificando o cifrando cada paquete IP, incluyendo protocolos para el establecimiento de claves de cifrado (Grupo de Sistemas Operativos DATSI FI UPM, 2012).

IPV6: (Internet Protocol Version 6) es un conjunto de especificaciones que permite la identificación y ubicación de los equipos que se encuentran en la red.

mGRE: (Multiprotocol Generic Routing Encaptulation) es uno de los mecanismos de tunneling que utiliza IP como protocolo de transporte y puede ser usado para transportar distintos protocolos (CISCO, s.f.)

MTU: (Maximum Transmission Unit) palabra utilizada en redes para indicar el tamaño máximo en bytes de los paquetes de datos.

NHRP: (Next Hop Resolution Protocol) es un protocolo de consulta y respuesta permitiendo al remitente determinar una ruta con menor saltos posibles.

Ping: es un mecanismo que permite comprobar el estado de una o más conexiones entre equipos remotos.

LISTA DE REFERENCÍAS

Telnat . (2006). *Router Telnat Dynamic Multipoint VPN's*. Obtenido de Router Telnat Dynamic Multipoint VPN's: ftp://ftp.storm.hr/Upload/Teldat_privremeno/Teldat_dokumentacija/spa/..%5Cdocumentacion%5CManuales%2010.7%5CDm768%5CDm768v10-70_DMVPNs.pdf

Aguas, B. L. (2010). *Guía Practica para Crear Infraestructura de Red Segura utilizando IPSEC con Túneles GRE Y CET.* Quito.

Aimacaña Valladares, D. R. (2014). *Diseño y Evaluacion de Nivel de Seguirdad del Protocolo GETVN en una Redde Datos para un Entorno Multipunyo que utiliza MPLS para Comunicacion WAN .* Sangolqui.

Arguello Tello, J. B. (2013). *Análisis de Factibilidad para la Implementación del Protocolo IPSEC en el Nodo de Internet 2 de la Universidad Politécnica Salesiana Sede Quito, Campus Sur.* Quito.

Ariganello, E., & Sevilla Barriento , E. (2010). *CCNP A FONDO .* Mexico : Alfaomega.

Caprile R, S. (2009). *Desarrollo de Aplicaciones con Comunicación Remota basada en módulos Zig Bee y 802.15.4.* Buenos Aires: GAE.

CISCO. (s.f.). Obtenido de http://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-3/lxvpn/configuration/guide/vcasr9kv343/vcasr9kv3gre.pdf

CISCO . (1 de 8 de 2011). *Implementing IPSec in IPv6 Security* . Obtenido de Implementing IPSec in IPv6 Security : http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/xe-3s/ipv6-xe-3s-book/ip6-ipsec.pdf

CISCO . (23 de 11 de 2014). *mGRE Tunnel Support over IPv6*. Obtenido de mGRE Tunnel Support over IPv6: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book/ip6-mgre-tunls.html#GUID-D3EE0043-B731-4B99-9CF6-A30DCBE9F730

CISCO . (s.f.). *Extructura IPSec*. Obtenido de Extructura IPSec: http://ecovi.uagro.mx/ccna4/course/module7/7.3.2.2/7.3.2.2.html

CISCO . (s.f.). *Túneles GRE Site to Site* . Obtenido de Túneles GRE Site to Site : http://ecovi.uagro.mx/ccna4/course/module7/7.2.2.2/7.2.2.2.html

CISCO. (2008). *Introducción al Cifrado de la Seguridad IP(IPSEC)*. Obtenido de Introducción al Cifrado de la Seguridad IP(IPSEC): http://www.cisco.com/cisco/web/support/LA/7/75/75045_IPSECpart1.html

CISCO. (2012). *Dynamic Multipoint VPN Configuration Guide* . Obtenido de Dynamic Multipoint VPN Configuration Guide : http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-s/sec-conn-dmvpn-15-s-book/ip6-dmvpn.html

CISCO. (2 de 8 de 2013). *Dynamic Multipoint VPN (DMVPN)*. Obtenido de Dynamic Multipoint VPN (DMVPN):

http://www.cisco.com/cisco/web/support/LA/107/1074/1074085_sec_DMVPN_ps6922_TSD_Products_Configuration_Guide_Chapter.pdf

CISCO. (s.f.). *Configuracion de un Túnel VPN GRE punto a punto* . Obtenido de Configuracion de un Túnel VPN GRE punto a punto : http://ecovi.uagro.mx/ccna4/course/files/7.2.2.5%20Lab%20-%20Configuring%20a%20Point-to-Point%20GRE%20VPN%20Tunnel.pdf

CISCO. (s.f.). *Extructura IPSec*. Obtenido de Extructura IPSec: http://ecovi.uagro.mx/ccna4/course/module7/7.3.2.3/7.3.2.3.html

Configuracion de Túneles GRE con enrutadores Cisco . (s.f.). Obtenido de Configuracion de Túneles GRE con enrutadores Cisco : http://materias.fi.uba.ar/7543/download/conf_gre.pdf

Cortés, A. (2008). *Direccionamiento IP CISCO*. Obtenido de Direccionamiento IP CISCO: http://www.ie.itcr.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter8_Direccionamiento%20IP.pdf

Francisconi, H. A. (2009). *IPSec en Ambientes IPv4 e IPV6.*

Gobierno de España . (2015). *IPv6 Protocolo de Internet Version 6*. Obtenido de IPv6 Protocolo de Internet Version 6: http://www.ipv6.es/es-ES/Faqs/Paginas/tecnicas.aspx

Grupo de Sistemas Operativos DATSI FI UPM. (2012). *Protocolo IPSEC.* Obtenido de Protocolo IPSEC: http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec

Gumucio Torrico, J. R. (28 de Octubre de 2015). *CCNA BOLIVIA*. Obtenido de CCNA BOLIVIA: http://ccnabolivia.blogspot.com/2015/10/conociendo-dynamic-multipoint-vpn-dmvpn.html

López Logacho, J. E. (2014). *Factibilidad de IPSEC PARA IPV6 EN LA RED DE LA UNIVERSIDAD POLITÉNICA SALESIANA , SEDE QUITO.* QUITO.

Müller, L. (2011). *Seguridad en la Capa de Red -IPSec*. Obtenido de Seguridad en la Capa de Red -IPSec: http://www.laminfo.com/blog/archivos/__5_unidad_V_IP_sec.pdf

Networking. (19 de 3 de 2012). *Networking y Tecnología* . Obtenido de Networking y Tecnología : http://networkkings-es.blogspot.com/2012/06/mgre-tuneles-gre-multipunto.html

ORACLE. (2010). *Descripción General de las Direcciones IPv6* . Obtenido de Descripción General de las Direcciones IPv6 : https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-10/

Pérez Iglesias, S. (2001). *Análisis del Protocolo IPSec: El estándar de seguridad en IP .*

Ramirez Acuña, G. I. (s.f.). *Protocolo Seguro de Internet IPS*. Obtenido de Protocolo Seguro de Internet IPS: http://cdigital.uv.mx/bitstream/123456789/30995/1/RamirezAcuna.pdf

Samaniego Fuentes, R. A. (2013). *Túneles Manuales IPv6-IPv4*. Obtenido de Túneles Manuales IPv6-IPv4: http://ecovi.uagro.mx/ccna4/course/module7/7.2.2.2/7.2.2.2.html

Vozmediano, M. R., Montero, R. S., & Jiménez Fabero, J. (s.f.). *Protocolo IPV6: Direccionamiento*. Obtenido de Protocolo IPV6: Direccionamiento: http://www.fdi.ucm.es/profesor/rubensm/asor/Trasparencias/Tema%201-%20Protocolo%20IPv6.pdf

ANEXOS

Direcciones del IPS en IPv6

DIRECCIONAMIENTO IPV6 ISP						
REDES	***HOST***	***PREFIJO***	***REDES***	***HOST***	***PREFIJO***	***SERIAL***
2001:acad:1234:acde	aaaa:abcd:a1b1:abc1	/64	2001:acad:1234:acde	aaaa:abcd:a1b1:abc2	/64	ocupada R1-S1/1 vs R13-S1/1
2001:aaaa:bbbb:cccc	acad:cada:3421:dfe7	/64	2001:aaaa:bbbb:cccc	acad:cada:3421:dfe8	/64	ocupado R13-S1/0 vs R3-S1/0
2001:dbac:1234:acad	1234:5678:a123:cca7	/64	2001:dbac:1234:acad	1234:5678:a123:cca8	/64	ocupadoR3-S1/2 vsR11-S1/2
2001:dddd:4321:1234	1234:acad:bcda:ccca	/64	2001:dddd:4321:1234	1234:acad:bcda:cccb	/64	ocupado R11-S1/3 vs R4-S1/2
2001:aaaa:bbbb:adca	aaaa:abcd:a1b1:aa12	/64	2001:aaaa:bbbb:adca	aaaa:abcd:a1b1:aa13	/64	ocupado R4-S1/3 vs R12-S1/3
2001:afed:baca:7845	bbbb:acaa:a123:b12a	/64	2001:afed:baca:7845	bbbb:acaa:a123:b12b	/64	ocupadoR12-S1/2 vs R2-S1/2
2001:dbac:1234:bbcc	aaaa:abcd:a1b1:fde8	/64	2001:dbac:1234:bbcc	aaaa:abcd:a1b1:fde9	/64	ocupado R2-S1/1 vs R10-S1/1
2001:aaaa:fead:acda	bbbb:acaa:a123:cdea	/64	2001:aaaa:fead:acda	bbbb:acaa:a123:cdeb	/64	ocupado R10-S1/0 vs R1-S1/0
2001:dfea:faaa:fbac	8734:6237:9321:7839	/64	2001:dfea:faaa:fbac	8734:6237:9321:783a	/64	ocupado R1-S1/2 vs R4 S1/0
2001:afed:5478:2645	5874:4578:2145:1111	/64	2001:afed:5478:2645	5874:4578:2145:1112	/64	ocupado R1-S1/2 vs R3 S1/1
2001:dbac:1234:aab1	4521:4521:4521:4578	/64	2001:dbac:1234:aab1	4521:4521:4521:4579	/64	ocupado R3-S4/0 vs R12-S1/0
2001:aaaa:bbbb:8888	8734:6237:aaaa:5673	/64	2001:aaaa:bbbb:8888	8734:6237:aaaa:5674	/64	ocupado R3-S1/3 vs R2-S1/3
2001:1111:2222:3333	4444:5555:6666:7777	/64	2001:1111:2222:3333	4444:5555:6666:7778	/64	ocupado R2-S1/0 vs R11-S1/0
2001:fda1:4563:8756	2563:a254:bc45:bcb5	/64	2001:fda1:4563:8756	2563:a254:bc45:bcb6	/64	ocupado R13 -S1/2 vs R12-S1/1
2001:9999:8888:7777	6666:5555:4444:3333	/64	2001:9999:8888:7777	6666:5555:4444:3334	/64	ocupado R2-S4/0 vs R4 -S1/1
2001:aaaa:fead:dddd	546a:5687:ad21:564ª	/64	2001:aaaa:fead:dddd	546a:5687:ad21:564b	/64	ocupado R10 -S1/3 vs R13-S1/3
2001:acad:3333:6452	5478:aaaa:2365:aca1	/64	2001:acad:3333:6452	5478:aaaa:2365:aca2	/64	ocupado R10 -S1/2 vs R11-S1/1
2001:1111:aaaa:bbbb	5489:5647:ad12:54ac	/64	2001:1111:aaaa:bbbb	5489:5647:ad12:54ad	/64	ocupado R5 -S1/3 vs R13 -S4/0
2001:dbac:1234:1234	1234:acad:4512:5463	/64	2001:dbac:1234:1234	1234:acad:4512:5464	/64	ocupado R6 -S1/0 vs R3 -S4/1
2001:dcad:dcae:faca	3654:8564:a241:bca1	/64	2001:dcad:dcae:faca	3654:8564:a241:bca2	/64	ocupado R7 -S1/1 vs R11 -S4/0
2001:daca:1234:feca	ccca:abac:b123:dac1	/64	2001:daca:1234:feca	ccca:abac:b123:dac2	/64	ocupado R15 -S1/0 vs R14-S1/0

2001:2222:fbca:caed	abcd:7777:c345:afc1	/64	2001:2222:fbca:caed	abcd:7777:c345:afc2	/64	ocupado R15 -S1/1 vs R16-S1/1
2001:3333:aebc:cdef	fecc:1111:fba3:bcd1	/64	2001:3333:aebc:cdef	fecc:1111:fba3:bcd2	/64	ocupado R15-S1/2 vs R17-S1/1
2001:7abc:8888:bb31	5342:1245:3567:aaa1	/64	2001:7abc:8888:bb31	5342:1245:3567:aaa2	/64	ocupado R14-S1/3 vs R17-S1/3
2001:6135:a1b2:7c81	2238:72ea:dede:efc1	/64	2001:6135:a1b2:7c81	2238:72ea:dede:efc2	/64	ocupado R14-S1/1 vs R16-S1/0
2001:7777:3323:4566	dddd:351a:6abc:cda1	/64	2001:7777:3323:4566	dddd:351a:6abc:cda2	/64	ocupado R16-S1/2 vs R17-S1/2
2001:123a:4567:3aac	aaab:4441:6363:abd1	/64	2001:123a:4567:3aac	aaab:4441:6363:abd2	/64	ocupadoR14-S4/0 vs R10-S4/1
2001:6666:7777:3333	7321:243a:ac24:321ª	/64	2001:6666:7777:3333	7321:243a:ac24:321b	/64	ocupado R14-S4/1 vs R2-S4/3
2001:1111:2333:5367	1245:483a:3521:1bc2	/64	2001:1111:2333:5367	1245:483a:3521:1bc3	/64	ocupadoR14-S1/2 vs R12-S4/0
2001:2242:5571:aaaa	bbbc:125b:7341:dde1	/64	2001:2242:5571:aaaa	bbbc:125b:7341:dde2	/64	ocupado R15-S4/1 vs R10-S4/0
2001:5551:3311:5312	5555:3221:6344:aa32	/64	2001:5551:3311:5312	5555:3221:6344:aa32	/64	ocupado R15-S1/3 vs R1-S4/0
2001:aacd:feaa:dedd	aa21:1111:7773:243b	/64	2001:aacd:feaa:dedd	aa21:1111:7773:243b	/64	ocupado R15-S4/0 vs R13-S4/1
2001:2221:dbce:6666	7731:57ac:683b:3ff1	/64	2001:2221:dbce:6666	7731:57ac:683b:3ff2	/64	ocupado R15-S4/2 vs R3-S4/3
2001:daab:4561:4444	5ee2:5555:aaaa:7771	/64	2001:daab:4561:4444	5ee2:5555:aaaa:7772	/64	ocupado R16-S4/2 vs R12-S4/1
2001:3a3b:aefd:cccc	6611:faaf:bbcc:334ª	/64	2001:3a3b:aefd:cccc	6611:faaf:bbcc:334b	/64	ocupado R16-S4/1 vs R13-S4/2
2001:7aaa:6bcd:bbbe	5431:62bb:74cc:86ab	/64	2001:7aaa:6bcd:bbbe	5431:62bb:74cc:86ab	/64	ocupado R16-S4/0 vs R3-S4/2
2001:43ab:5eeb:55ae	eeee:dd11:cc22:bb12	/64	2001:43ab:5eeb:55ae	eeee:dd11:cc22:bb13	/64	ocupado R16-S4/3 vs R11-S4/2
2001:7372:1363:eeee	bbbb:fffe:aab2:edcb	/64	2001:7372:1363:eeee	bbbb:fffe:aab2:edcb	/64	ocupado R17-S4/2 vs R2-S4/2
2001:8822:7733:4422	1111:3332:6667:1134	/64	2001:8822:7733:4422	1111:3332:6667:1135	/64	ocupado R17-S4/0 vs R4-S4/0
2001:bcae:facd:1111	5662:8542:1381:dde6	/64	2001:bcae:facd:1111	5662:8542:1381:dde7	/64	ocupado R17-S4/1 vs R11-S4/1
2001:7aac:6bbb:5ccc	1abc:2ccb:3ded:4ffb	/64	2001:7aac:6bbb:5ccc	1abc:2ccb:3ded:4ffb	/64	ocupado R17-S4/3 vs R12-S4/3

Nota: Rango de Direcciones IPv6 para ISP
Fuente: Ximena Bautista

Direccionamiento para la Red LAN en IPv6

DIRECCIONAMIENTO IPV6 LAN						
Redes	***Host***	***Prefijo***	***Red***	***Host***	***Prefijo***	***Serial***
2008:0068:0016:1001	0A01:1200:0010:0001	/64	2008:0068:0016:1001	0A01:1200:0010:0002	/64	ocupadoR5 -S1/2 VS R8 -S1/2
2008:0068:0016:2001	0B01:1200:0020:0010	/64	2008:0068:0016:2001	0B01:1200:0020:0011	/64	ocupadoR5- S1/1 VS R9 -S1/1
2008:0068:0016:3001	0C01:1200:0030:0020	/64	2008:0068:0016:3001	--------	/64	ocupado F0/0 R5
2008:0068:0016:4001	0E01:1301:0010:0020	/64	2008:0068:0016:4001	--------	/64	ocupado F0/0 R6
2008:0068:0016:5001:	0D01:1510:0030:0010	/64	2008:0068:0016:5001	--------	/64	ocupado F0/0 R7
2800:0068:0016:6001:	0101:1610:0060:0010	/64	2008:0068:0016:6001	--------	/64	ocupado F0/0 R8
2800:0068:0016:7001:	0201:1710:0070:0010	/64	2008:0068:0016:7001	--------	/64	ocupado F0/0 R9

Nota: Rango de Direcciones IPv6 para LAN (Quito, Guayaquil, Cuenca)
Fuente: Ximena Bautista.

Direccionamiento en IPv6 para los túneles en mGRE

DIRECCIONAMIENTO PARA TUNEL MGRE			
Redes	***Host***	***Prefijo***	***Interfaz***
	ABCD:ABCD:ABCD:ABC1	/64	QUITO-HUB Túnel 10
	ABCD:ABCD:ABCD:ABC2	/64	CUENCA-SPOKE 1 Túnel 20
	ABCD:ABCD:ABCD:ABC3	/64	GUAYAQUIL-SPOKE 2 Túnel 30
2012:ABCD:ABCD:ABCD	ABCD:ABCD:ABCD:ABC4	/64	SUR-QUITO-SPOKE 3 Túnel 40
	ABCD:ABCD:ABCD:ABC5	/64	KENNEDY-QUITO-SPOKE 4 Túnel 50

Nota: Rango de Direcciones IPv6 para Túneles mGRE
Fuente: Ximena Bautista