DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

TEMA: ANÁLISIS DE UNA RED TRONCAL MULTISERVICIO PARA ENCRIPTACIÓN DE INFORMACIÓN SOBRE MPLS BASADA EN EL ESTÁNDAR IETF CON EL PROTOCOLO GETVPN

AUTOR: TORRES VILLAFUERTE, GABRIEL MESIAS

DIRECTOR: VEGA , CHRISTIAN

SANGOLQUÍ

2017

Certificado de tutoría
Certificado de tutoría

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERIA EN ELECTRÓNICA Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que el trabajo de titulación, " ***ANÁLISIS DE UNA RED TRONCAL MULTISERVICIO PARA ENCRIPTACIÓN DE INFORMACIÓN SOBRE MPLS BASADA EN EL ESTÁNDAR IETF CON EL PROTOCOLO GETVPN***" realizado por el señor ***GABRIEL MESIAS TORRES VILLAFUERTE***, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar al señor ***GABRIEL MESIAS TORRES VILLAFUERTE*** para que lo sustente públicamente.

Sangolquí, 19 de diciembre de 2016.

Atentamente,

Ing. Christian Vega.

DIRECTOR

Autoría de Responsabilidad

Autoría de Responsabilidad

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERIA EN ELECTRÓNICA Y TELECOMUNICACIONES

AUTORÍA DE RESPONSABILIDAD

Yo, GABRIEL MESIAS TORRES VILLAFUERTE con cédula de identidad N° 1804285938 declaro que este trabajo de titulación "ANÁLISIS DE UNA RED TRONCAL MULTISERVICIO PARA ENCRIPTACIÓN DE INFORMACIÓN SOBRE MPLS BASADA EN EL ESTÁNDAR IETF CON EL PROTOCOLO GETVPN", ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 19 diciembre de 2016.

Gabriel Mesías Torres Villafuerte

1804285938

Autorización de publicación

Autorización de publicación

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERIA EN ELECTRÓNICA Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, GABRIEL MESIAS TORRES VILLAFUERTE, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución la presente trabajo de titulación **"ANÁLISIS DE UNA RED TRONCAL MULTISERVICIO PARA ENCRIPTACIÓN DE INFORMACIÓN SOBRE MPLS BASADA EN EL ESTÁNDAR IETF CON EL PROTOCOLO GETVPN "** cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolquí, 19 de diciembre de 2016.

Gabriel Mesías Torres Villafuerte

1804285938

DEDICATORIA

La vida se encuentra plagada de retos, los cuales he podido superarlos gracias al apoyo incondicional de mis padres, quienes han fomentado en mi la perseverancia y superación, a la vez son mi motivación para seguir adelante y seguir superando los retos que se presenten en un futuro. Sus consejos van a servir como una enseñanza más de vida.

A mis hermanas por el apoyo incondicional, comprensión y confianza en los momentos indispensable de mi vida .

Gabo

AGRADECIMIENTO

Agradezco a Dios ser maravilloso que me dio fuerza y fé para terminar lo que parecía muy lejano. A mi familia por apoyarme y estar a mi lado siempre en todo momento de mi vida.

A mis maestros y compañeros quienes me apoyaron en mi permanencia en la universidad, en especial a mi Director Ing. Christian Vega, que gracias a su disposición y sus conocimientos han sabido guiarme como profesor y como amigo para la realización y culminación del presente trabajo.
Para todas estas personas gracias de todo corazón.

Gabo

ÍNDICE GENERAL

ÌNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente propuesta pretende observar el comportamiento de los diferentes mecanismos de seguridad que se pueden implementar a nivel de capa 3, los cuales puede ser adoptados por los proveedores de servicios y las diversas empresas que requieran este servicio, con la finalidad de que la información o los datos se transmitan de manera confiable y segura. Para estos mecanismos de seguridad se requiere que tengan una conexión de mallado completo, para que la transmisión de paquetes se desarrolle de manera óptima y adecuada, el mecanismo de seguridad tradicional IPSec es un mecanismo que funciona punto a punto, mientras que GETVPN es un mecanismo que realiza un trabajo multipunto multipunto. Mediante el software GNS3 que permite simular redes de esta magnitud, se realizó la experimentación con diferentes escenarios, identificando la seguridad y funcionamiento en una red MPLS con servicio de VPNs, además de una pequeña prueba de penetración o auditoría de red que permite saber que tan seguro se encuentra a un ataque de intrusión real. En la prueba de pentesting se ejecuta mediante una máquina virtual, que contienen el software Kali Linux, teniendo una conexión con GNS3, utilizando esta herramienta se realiza la prueba de penetración en la cual se observa la robustez y seguridad del sistema.
Palabras Claves:

PROTOCOLO DE ETIQUETAJE

SOFTWARE DE SIMULACIÓ REDES DE COMUNICACIÓN

PROTOCOLOS DE ENCRIPTACIÓN DE DATOS

REDES PUNTO - MULTIPUNTO

AUDITORÍA SEGURIDAD INFORMÁTICA

ABSTRACT

The present proposal aims to observe the behavior of the different security mechanisms that can be implemented at layer 3 level, which can be adopted by the service providers and the various companies that require this service, in order that the information . The data is transmitted reliably and safely. For these security mechanisms it is required that they have a full meshing connection, so that packet transmission is optimally and adequately developed, the traditional IPSec security mechanism is a point-to-point mechanism, where as GETVPN is a mechanism. Which performs a multipoint multipoint job. Using GNS3 software to simulate networks of this magnitude, experimentation with different scenarios was performed, identifying security and performance in MPLS network with VPN service, as well a small penetration test or network audit, Securely encountered a real intrusion attack. In the test of pentesting is executed by means of a virtual machine, that contains the software Kali Linux, having a connection with GNS3, using this tool the penetration test is realized in which the robustness and security of the system is realized.
Keywords:

LABEL PROTOCOL

SOFTWARE SIMULATION COMMUNICATION NETWORKS

DATA ENCRYPTION PROTOCOLS

POINT- MULTIPOINT NETWORKS

COMPUTER SECURITY PENTESTING

Siglas y Abreviaturas

ARP Address Resolution Protocol

AES Advanced Encryption Standard

BGP Border Gateway Protocol

CEF Cisco Express Forwarding

CR-LDP Constraint-based Label Distribution Protocol

CoS Class of Service

CE Customer Edge

DES Data Encryption Standard

EIGRP Enhanced Interior Gateway Routing Protocol

FR Frame Relay

FEC Forward Error Correction

GTSM Security Mechanism

GETVPN Group Encrypted Transport VPN

ISO International Organization for Standardization

ISP Internet Service Provider

ICMP Internet Control Message Protocol

IPSec Internet Protocol Security

IETF Internet Engineering Task Force

IGP Interior Gateway Protocol

MPLS Multiprotocol Label Switching

MD2 Message-Digest Algorithm 2

MD5 Message-Digest Algorithm 5

MP-BGP Multiprotocol BGP

LAN Local Area Network

LSR Label Switch Router

LSP Label-switched Paths

LDP Label Distribution Protocol

LER Label Edge Router

OSPF Open Shortest Path First

P Provider

PE Provider Edge

QoS Quality of Service

RIP Routing Information Protocol

RR Route reflectors

TTL Time To Live

TCP Transmission Control Protocol

TDP Tag Distribution Protocol

VPN Virtual Private Network

VRF Virtual Routing and Forwarding

CAPÍTULO 1

INTRODUCCION

1.1. Presentación

En el presente documento se desarrollará el diseño de una red de transporte virtual de datos, con el software GNS3 que permite la emulación de hardware de cisco, siendo una herramienta muy potente para la investigación y capacitación.

Está estructurado en 5 capítulos en los cuales se va a detallar todo el proceso investigativo y teórico, el primer capítulo consta de una breve introducción y antecedentes importantes de anteriores investigaciones, desarrolladas del tema propuesto, también se fijarán los objetivos tales como el principal y los específicos, así como la respectiva justificación e importancia además del alcance del proyecto.

El segundo capítulo consta de un marco teórico, que es una guía para la elaboración del proyecto, especificando las carácterísticas mas relevantes, así como las partes técnicas necesarias para un perfecto avance del proyecto.

El tercer capítulo se elabora un esquema del diseño de la red virtual de datos, utilizando la tecnología MPLS, con el diseño realizado se procede con las respectivas configuraciones en el backbone como asimismo en los otros dispositivos, configurando de igual manera los mecanismos de seguridad como el IPSec y GETVPN.

El cuarto capítulo una vez ya diseñado y configurado la red se procede a un análisis de los mecanismo de encriptación en la red virtual, asi como también se desarrollará

una prueba de pentesting para ver el grado de robustez y vulnerabilidad al momento de ser sometido a dicha prueba.

En el Quinto capítulo se recolecta la información, que se obtiene mediante el envió de paquetes en la red virtual con la configuración de los mecanismos de seguridad de acuerdo a dichos resultados se procederá a realizar las respectivas comparaciones para luego ser plasmadas en las recomendaciones y conclusiones.

1.2. Antecedentes

En el área de telecomunicaciones resulta elevado el costo al momento de implementar redes de comunicación de datos MPLS, por lo que se ha buscado diferentes alternativas tales como la emulación, la cuál es una herramienta muy importante para la capacitación e investigación. Se tiene un software como GNS3 que es un emulador de hardware de routers utilizados en las comunicaciones, como herramienta para configurar diseñar e implementar redes , el cuál se puede instalar en una Pc con cualquier sistema operativo, teniendo una interacción directa con cualquier tipo de estos dispositivos lo que permite configurar y diseñar topologías de comunicaciones grandes y complejas que soportan la emulación de un equipo real.(Nova,2012)

El backbone que es el principal enlace donde convergen todos los servicios, obliga el uso de una tecnología como MPLS (Multiprotocol Label Switching), las que han dado muchos beneficios, tales como : una mayor fiabilidad, la integración, una mayor eficiencia, una mejor forma de apoyar la multidifusión, clases de servicio directo, las capacidades de la aplicación de ingeniería de tráfico, más robusto (reduce la carga en la red de núcleos y de red privada), finalmente la virtualización (VPN) que ofrece escabilidad y capacidad de gestión. (Cisco MPLS,2006)

MPLS ofrece múltiples servicios en la comunicación, los clientes se conectan directamente sin pasar por una red de terceros porque utiliza un direccionamiento privado, seguridad de flujos de información internos y externos mediante la aplicación

de políticas de seguridad globales y/o específicas. Tomando en consideración que la información es lo más importante con que cuenta una entidad, lo que hace necesario garantizar la seguridad en el proceso de comunicación de datos. (Tomsu,2010)

El mecanismo de encriptación de datos IPSec es utilizado tradicionalmente en la seguridad de redes IP . Siendo una de las tecnologías mayormente consideradas, por su eficiencia que ha sido demostrada en el servicio con redes de seguridad IP, siendo una opcion prioritaria. IPSec es un mecanismo con mayor acogida, contituyendose en la más apropiada en el beneficio para garantizar seguridad en las comunicaciones. (Pérez, 2001)

GETVPN salió en el año 2015 como mejora del protocolo IPSec, es el más idóneo porque posee características óptimas para la configuración, implementación y administración de routers simplificando el cifrado mediante un servidor de claves, debido a que GETVPN permite realizar una encriptación en una red multipunto lo que debe ser considerado por los proveedores de servicio para la migración en corto o mediano plazo. (Haseeb Niazi, Nipul Shah , Biao Zhou, Varun Sethi, Marzo 2015)

Para comprobar el nivel de seguridad de la red bajo el protocolo de encriptación GETVPN, existe software especializado llamado Kali Linux que permite realizar pentesting que consiste en pruebas de penetración y auditorías de seguridad con fines educativos y éticos, con el que se puede explorar las debilidades en la seguridad de la red de comunicación, con la finalidad de hacerlas más robustas y seguras. (Engebretson, 2013).

1.3. Justificación e Importancia

Debido a que MPLS tiene la capacidad para integrar voz, video y datos con mejoras de rendimiento, permite un mejor manejo de las comunicaciones ya que ofrecen a sus clientes y operadores de telecomunicaciones, una alternativa de mucho mayor alcance, permitiendo por este motivo el utilizar esta tecnología para construir una red virtual considerando que hoy en día es necesario también implementar un

mecanismo de encriptación para una mayor seguridad, debido a intrusiones no permitidas en la red.

En una red MPLS por su robustez permite la creación de circuitos o túneles dentro de una red IP de comunicaciones para garantizar el aislamiento del tráfico y el acceso a la red, mejorando el rendimiento y haciendo posible la encriptación necesaria. En nuestro país la Superintendencia de Bancos y Seguros entidad que regula el sistema financiero nacional mediante resolución No.JB-2012-2148 del 26 de abril del 2012, dispuso a las instituciones del sistema financiero implememtentar suficientes medidas de seguridad para mitigar el riesgo de fraude mediante el uso de información y comunicaciones. (Superintendencia de Bancos y Seguros , 2012)

Por tal motivo en el Ecuador las entidades públicas como privadas deben prestar atención o importancia al tema de los mecanismos de encriptación de datos en la red de un Proveedor de Servicios . Con el protocolo GETVPN que permite su uso en circunstancias críticas tales como en transacciones de información entre diferentes entidades o empresas, con seguridades en el cifrado de la información , siendo esta una de las diversas soluciones para diferentes escenarios en donde se requiera los mecanismos de seguridad, independientemente de la aplicación que se utilice, de modo que se convierte esencialmente en la seguridad de las redes IP.

GETVPN es un protocolo que no requiere la configuración de túneles punto a punto, debido a que encapsula tramas, mediante el uso de un servidor de claves, el cuál proporciona seguridad de extremo a extremo por el tráfico de red, manteniendo la autonomía de la misma en conexiones full-mesh, utilizando la capacidad del núcleo de la red para el enrutamiento y réplica de paquetes entre diferentes sitios de una empresa.

El presente proyecto se justifica en base a lo explicado anteriormente, plenamente se encuentra enfocado a los mecanismos de encriptación GETVPN y IPSec en una red virtual MPLS de datos. Primeramente se diseñará una red virtual con el software GNS3 posteriormente se configurará los mecanismos de seguridad, adicionalmente se hara

la comparación con otro mecanismo de encriptación tradicional de preferencia IPSec para poder observar las mejoras referentes, para su aplicación .

Se realizará pruebas de pentesting, con el fin de evaluar la seguridad principalmente del mecanismo de encriptación GETVPN, comprobando la seguridad de este protocolo en routers , utilizando la herramienta de auditoría en redes de la comunicación llamada Kali Linux.

1.4. Alcance del Proyecto

El proyecto pretende diseñar una red de transporte virtual de datos con tecnología MPLS utilizando el software GNS3 para análisis de datos encriptados bajo el protocolo GETVPN perteneciente al estándar IETF a nivel de una red MAN y WAN basada en la conmutación de paquetes y proporciona un transporte de datos a través de la creación de circuitos virtuales VPN.

Para el desarrollo del proyecto en primer lugar se realizará el estudio del arte referente al protocolo GETVPN para encriptación de información en equipos para comunicación de datos, en segundo lugar se diseñara una red MPLS virtual que permita realizar la encriptación de datos bajo el protocolo GETVPN e IPSec, para luego analizar los parámetros tales como: la latencia, paquetes encriptados y paquetes desencriptados de esta manera comprobar el funcionamiento del protocolo de seguridad.

Se utilizará los resultados obtenidos de la red virtual para el análisis comparativo con respecto a los protocolos GETVPN e IPSec, además de realizar pruebas bajo dos escenarios, en primer escenario en una red con seguridad IPSec y en segundo escenario en una red que utilice el protocolo GETVPN para observar las mejoras presentes entre estos dos mecanismos de seguridad ; siendo el segundo escenario el que será sometido a ataques utilizando un software llamado Kali desarrollado por Linux que es especializado en penetración y auditorías de seguridad, de esta manera se podrá observar y constatar el grado de vulnerabilidad que presenta la red.

Por último se realizarán conclusiones y recomendaciones de los difetentes escenarios que son descritos anteriormente así como sugerencias para futuros trabajos.

1.5. Objetivos

1.5.1 Objetivo General

- Diseñar una red de transporte virtual de datos con tecnología MPLS utilizando el software GNS3, para análisis comparativo de los protocolos GETVPN e IPSec.

1.5.2 Objetivos específicos

- Realizar el estudio del arte referente al protocolo GETVPN para encriptación de datos en equipos para la comunicación.

- Diseñar una red MPLS virtual, configurar direccionamiento IP, enrutamientos, implementación VPN, que permita realizar la encriptación de datos bajo el protocolo GETVPN.

- Analizar los parámetros obtenidos en la red virtual para comprobar la calidad de servicio presente en la red.

- Utilizar los resultados obtenidos de la red virtual en un análisis comparativo con respecto a los protocolos GETVPN e IPSec.

- Realizar pruebas y comparación bajo dos escenarios, el primer escenario en una red con seguridad IPSec, el segundo escenario en una red que utilice el protocolo GETVPN, con la finalidad de observar las mejoras presentes entre dichos protocolos.

CAPÍTULO 2

Fundamentos Teóricos MPLS y VPNs

2.1 MPLS

Multiprotocol Label Switching MPLS, utiliza un método para el reenvío de paquetes mediante una red usando la información que contiene las etiquetas que se añaden a los paquetes IP, se puede considerar como un reemplazo de la tecnología IP sobre ATM ; este protocolo permite realizar túneles, su mejor función , es de hacer mucho más rápido el enrutamiento de paquetes en la red. (Barberá, 2007)

Los orígenes de MPLS suscitaron a mediados de los 90 , IP fue el que mejor se desempeñaba como protocolo de red por lo cuál fue implementado por los proveedores de servicios en los backbones IP, basando en la conexión de routers E1 y E3, con el incremento exponencial de internet se estaba produciendo un déficit de ancho de banda con lo que los proveedores aumentaban el número de enlaces y capacidad.

Por lo que se aumento la capacidad y mejoras de rendimiento en los diferentes routers que conforman la red de backbone , estas mejoras fueron concretadas con la combinación de distintas formas, como la eficiencia en las comutaciones ATM y la capacida de gestión de control de IP, se créo el modelo de Red IP sobre ATM pronto se acogió entre los proveedores de servicios, pero se gestionaba dos redes por separado.

Por 1997 y 1998 se generaron un conjunto de procedimientos reglas y protocolos que se dieron a conocer como conmutación IP o conmutación multinivel las cuales llevaron a concretar el presente estándar MPLS del IETF.

Un conmutador IP es un equipo de comunicaciones unificadas, diseñado para ofrecer servicios principalmente de voz a través de las redes de datos, la más clara aplicación es la voz sobre IP.

Un conmutador Multinivel es un equipo de comunicaciones que permite acoplar la capa de enlace con la capa de red ,permitiendo homogeneidad de servicios de un extremo a otro.

MPLS tiene dos componentes básicos en común que son la separación en funciones de control (routing) y de envió (forwarding), para la creación de circuitos virtuales como en ATM, se consideró en usar etiquetas añadidas a los paquetes, las cuales definen el circuito virtual en la red y están asociados con la calidad de servicio, por lo que inicialmente fue de dos maneras diferentes el etiquetamiento en la capa de enlace como en la capa de red.

2.1.1 Arquitectura

Mpls fue estructurado para admitir múltiples protocolos y aplicaciones:

- Unicast and Multicast IP Routing.
- VPN
- Qos
- Traficc Engineering
- AtoM

Por lo que combina Routing y Switching, ip routing es una tecnología de capa 3 mientras que ATM switching es tecnología de capa 2, por lo que fusiona capa3 y capa 2 obteniendo un resultado de alto nivel , la inteligencia del routing con la rapidez del switching.

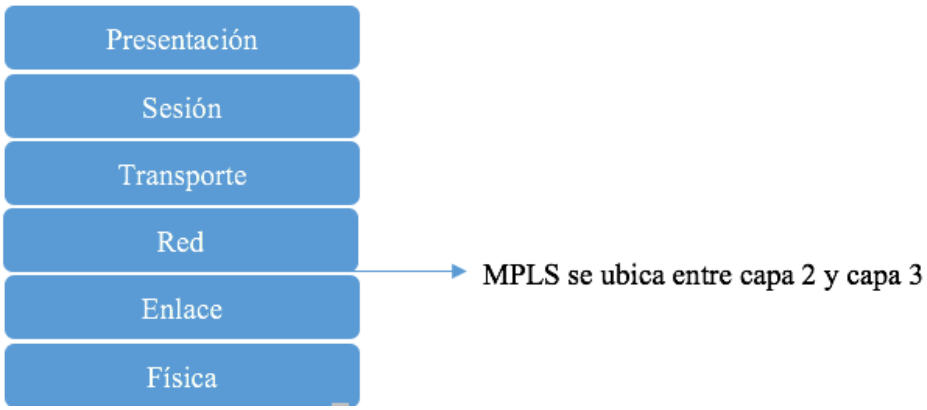

Figura 1 Modelo OSI y MPLS.

2.1.2 MPLS Conceptos

FEC (Forwarding Equivalence Class): “Corresponde a un grupo de paquetes que siguen el mismo camino a través de la red, con el mismo tratamiento el cuál puede incluir todos los paquetes con un determinado prefijo IP de destino, todos los paquetes con una IP destino y una IP origen” (Araujo, 2016). “De una FEC puede agrupar varios flujos, pero un mismo flujo no puede pertenecer a más de una FEC.” (Turmero, 2016)

LSP(Label Switched Path): “ es el nombre que toma la dirección del tráfico MPLS, semejante a una conexión de extremo a extremo MPLS . Siendo similar con la creación de un canal virtual punto a punto, punto a multipunto , multipunto a punto o multipunto a multipunto, pero es unidireccional ” . (Orozco, 2014, pág. 11)

LSR(Label Switching Router): es una etiqueta la cuál ayuda a mejorar la velocidad de enrutamiento en MPLS , dicha etiqueta proporciona un mejor enrutamiento al momento de utilizar protocolos IP, ejecutando una mejor trayectoria con el intercambio de etiquetas que se encuentran en el protocolo, Label Switching Router se categoriza por el direccionamiento del flujo de datos en la red, “ como enrutadores ascendentes (upstream, origen) o descendentes (downstream, destino) ”. (Orozco, 2014, pág. 11)

LDP(Label Distribution Protocol): es un protocolo que utiliza LSR para generar e intercambiar etiquetas de forma automática, cada router genera en forma local etiquetas con sus prefijos y luego anuncia los valores de esa etiqueta a sus vecinos.

LIB(Label Information Base): es una tabla de almacenamiento de LSR, que tienen información de las etiquetas con significado local, plano de control.

LFIB (Label Forwarding Information Base): se utiliza para el envió de paquetes MPLS basado en etiquetas relacionando la interfaz de entrada con la etiqueta de entrada con la interfaz de salida con la etiqueta de salida para un paquete etiquetado, plano de datos.

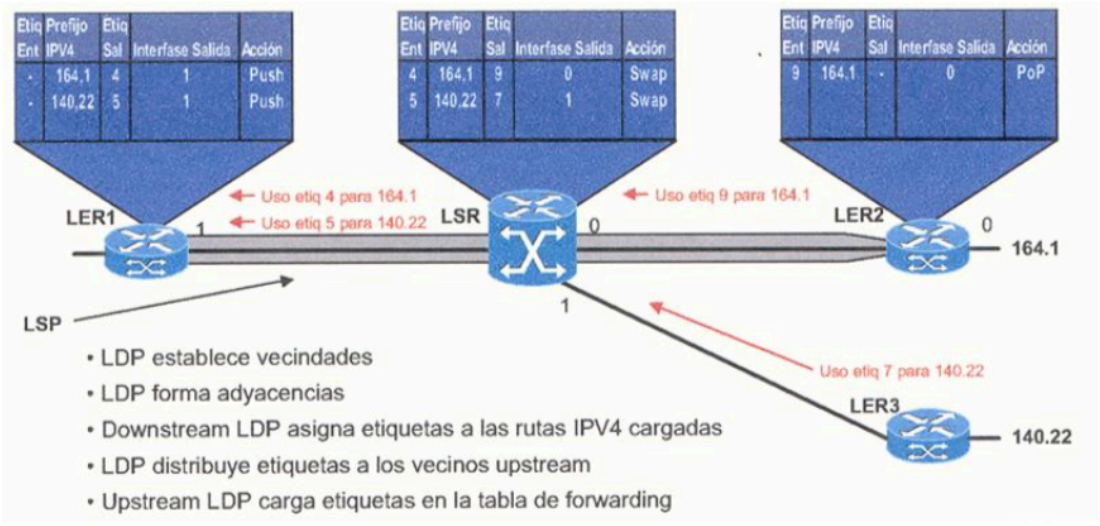

Figura 2 Asignación y Distribución en MPLS

Fuente: (Hirchoren, 2000)

La arquitectura MPLS está especificada con mayor detalle en RFC 3031 la que está adecuada principalmente por: plano de control y plano de datos.

Plano de Control: Responsable del intercambio de información de enrutamiento de capa 3 y etiquetas. Contiene mecanismos avanzados para el intercambio de información tales como OSPF , EIGRP, IS-IS, y BGP y para el intercambio de etiquetas tales como TDP, LDP, BGP y RSVP.

Protocolo de enrutamiento, se encarga del intercambio de información de enrutamiento el cuál prepara la tabla de enrutamiento IP, esta tabla hace el reenvió IP (FIB) en el plano de datos, LDP cambia las etiquetas entre los pares,después de intercambiar las etiquetas con LDP pares con LFIB se forma el plano de datos. (Uttam Kumar, 2010)

Plano de Datos: Responsable del envió de paquetes basados en etiquetas y cabecera IP, tiene un motor de reenvió simple que mantiene LFIB y FIB.

A medida que el paquete IP se enviá va hacer una búsqueda de enrutamento IP, y comprobar la etiqueta que está asociada en particular con FEC, si es así la etiqueta se

impone en el paquete y pasa al proceso de LFIB como paquete etiquetado. Si ninguna etiqueta esta asociada con paquetes IP, entonces se procesa como un paquete IP normal por el LFIB. (Uttam Kumar, 2010)

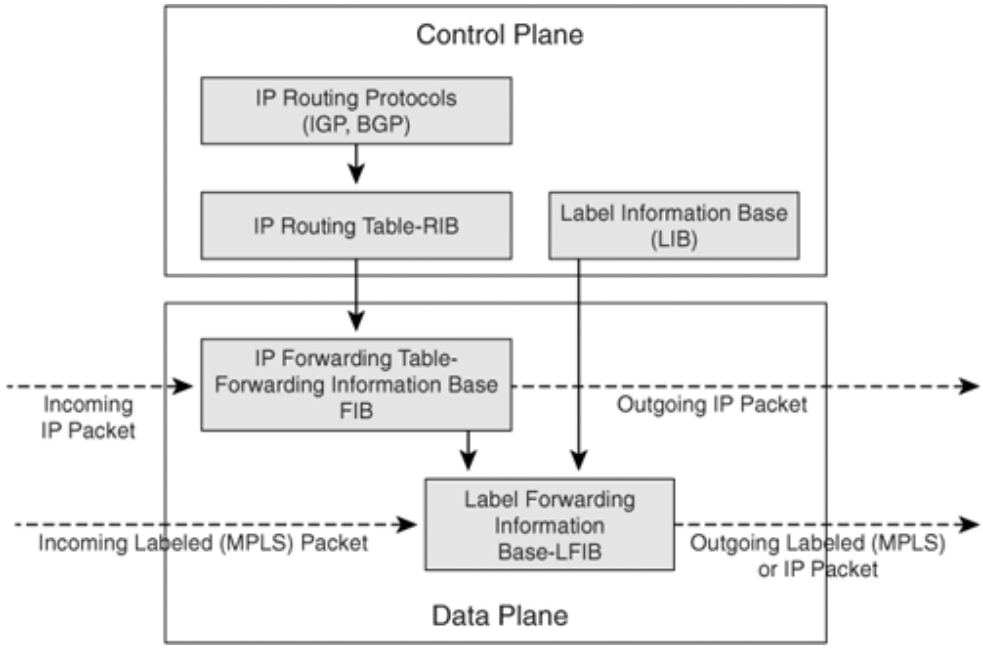

Figura 3 Plano de Control y Datos

Fuente: (Configuración MPLS de Cisco IOS software Lobo)

2.1.3 Dispositivos LSR

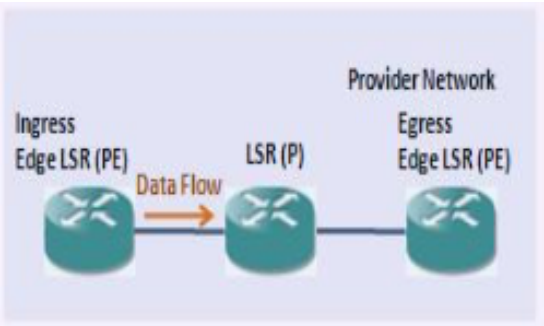

Figura 4 Dispositivos LSR.

Fuente: (Gokhankosem, 2011)

LSR interior que es el que encamina paquetes, su única función cambiar las etiquetas para cada FEC según la información de etiquetas con significado local .

LSR Edge Ingress de frontera de ingreso se ubica en la entrada del flujo de datos de la red MPLS clasifica los paquetes FECs con las correspondientes etiquetas.

LSR Edge Egress de frontera de egreso se ubica a la salida del flujo de datos de la red MPLS su función es eliminar la etiqueta del paquete dejándolo igual que al inicio.

La arquitectura del LSR interior se representa en la siguiente figura 5,

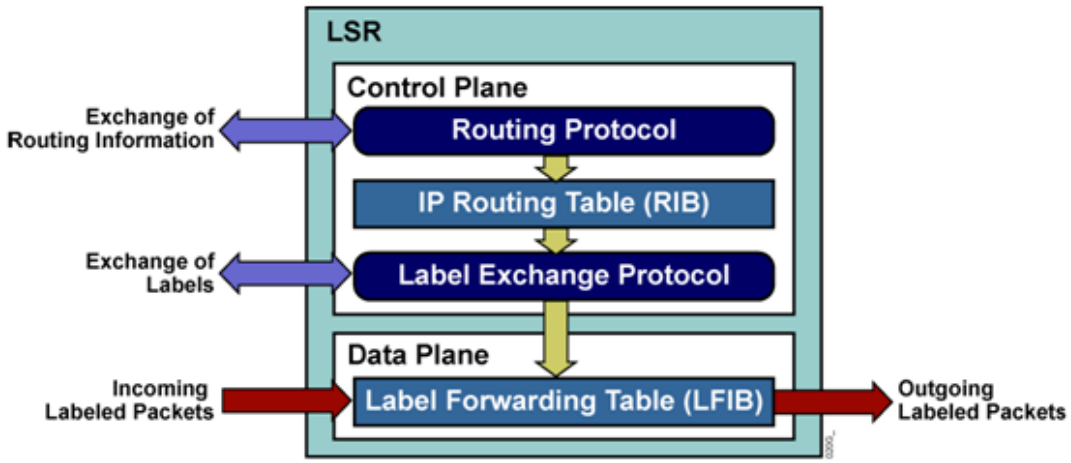

Figura 5 LSR Dispositivo

Fuente: (Faizal, 2010)

Un LSR tiene estas tres funciones:

Pop: remueve la etiqueta superior, el paquete se envía con la pila de etiquetas o como un paquete sin etiquetar.

Swap: la etiqueta superior es eliminada y reemplazada con una nueva etiqueta, cambiando el paquete de enlace de salida.

Push: la etiqueta superior se sustituye con una nueva y se añaden más etiquetas empujando las etiquetas en el paquete recibido.

Por lo que convergen entre los diferentes protocolos de enrutamiento con los protocolos de intercambio de etiquetas;en estos dispositivos no se realiza el reenvió de paquetes que no esten respectivamente etiquetados.

La arquitectura LSR Edge se representa en la siguiente figura 6,

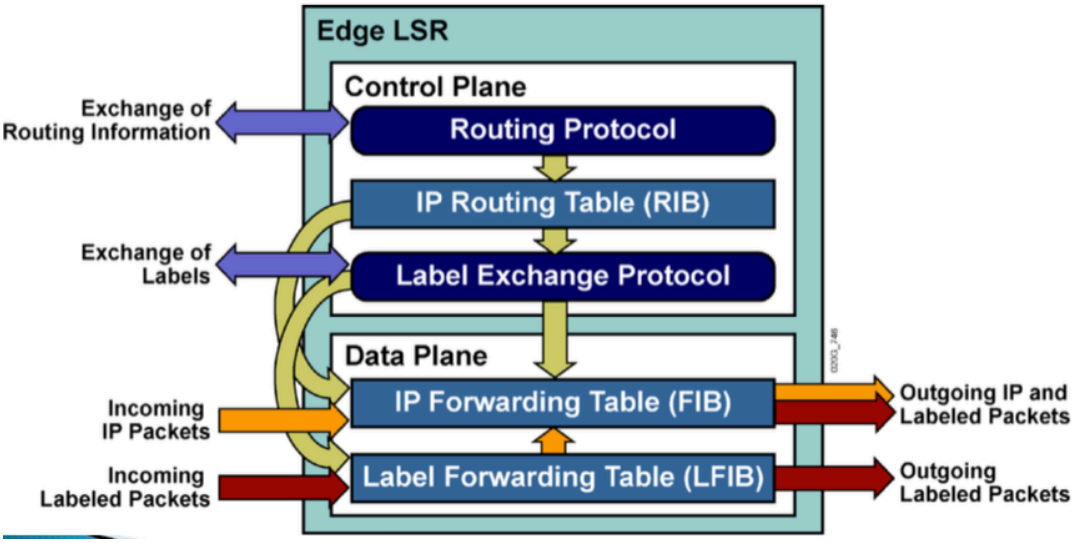

Figura 6 Dispositivo Edge LSR

Fuente: (Rahman, 2013)

Por lo general los Edge LSR se encuentran localizados en el borde de la red MPLS y aplica una pila de etiquetas a los paquetes, realizan una acción de etiqueta pop salida que consiste en la eliminación de la etiqueta superior en el punto del dominio MPLS, basandose en la dirección IP de destino. Tiene por función implantar, repartir, extraer las etiquetas de los paquetes de la red MPLS.

2.1.4 MPLS Label

La etiqueta MPLS se ajusta entre las cabeceras de capa 2 y capa3 del modelo OSI, los campos usados en la cabecera ATM son usados como etiquetas, la etiqueta MPLS tiene 32 bits los cuales se describe a continuación:

Figura 7 Dispositivo Edge LSR

Fuente: (Faizal, 2010)

“

- Los primeros 20 bits son el valor de la etiqueta. Este valor puede estar entre 0 y 2^{20} – 1 o 1.048.575. Sin embargo los valores del 0 al 15 son reservados.
- Los bits del 20 al 22 son bits experimentales, se utiliza únicamente para la calidad de servicio(Qos).
- El bit 23 es el inferior de la pila de bits. Es 0 , cuando es la inferior etiqueta en la pila. Si es así, el inferior de la pila de bits se pone a 1.La pila es un grupo de etiquetas que se encuentran en la parte superior del paquete. La pila puede tener una sola etiqueta o muchas más. El número de etiquetas(es decir, el campo de 32bits) que se puede encontrar en la pila es ilimitada, aunque muy raras veces se observa una pila que consta de cuatro o mas etiquetas.
- Los bits del 24 al 31 son utilizados para el time to live (TTL), su función principal es evitar que un paquete quede atrapado en un bucle de enrutamiento, es decir elimina bucles en la región del MPLS. ” (Faizal, 2010)

2.1.5 MPLS Pila de etiquetas

MPLS puede tener la necesidad de que se ejecuten mas de una etiqueta en su parte superior , se realiza este proceso para el empaquetamiento de todos los paquetes en una pila. La cual la primera se llama etiqueta superior y la última obtiene el nombre de etiqueta inferior, por lo que entre la superior e inferior se tiene cualquier número de etiquetas . (Ghein, 2007, pág. 26)

Figura 8 MPLS Stack
Fuente: (Vidal, 2008)

Por lo general una etiqueta es colocada en un paquete, pero se puede colocar una pila de etiquetas, por lo que es estos escenarios se pueden producir más de una etiqueta.

2.1.6 MPLS LDP

Proporciona los medios para que los LSR pidan, distribuyan y liberen la información obligatoria del prefijo de escritura de la etiqueta para mirar routers en la Red. El LDP permite a los LSR descubrir los pares potenciales y establecer las sesiones entre LSR con el fin de intercambiar información de las etiquetas. Permite a un LSR informar a otro las vinculaciones de las etiquetas que ha hecho , una vez que un par de routers comunican los parámetros LDP, establece una trayectoria conmutada de Etiquetas (LSP). El MPLS LDP permite a los LSR distribuir la escritura de la etiqueta a lo largo del trayecto ruteado, este método de distribución se llama salto por el salto, con reenvió, cuando un paquete llega a un router el router mira la dirección destino del encabezado IP, realiza las operaciones de búsqueda de la ruta y adelante el paquete al salto siguiente, con MPLS cuando un paquete llega un router el router mira la etiqueta entrante, mira la etiqueta en la tabla y entonces el paquete da el salto siguiente, lo que es muy útil para MPLS VPNs. (Cisco, MPLS Label Distribution Protocol (LDP), 2013)

2.1.7 Sesión LDP Establecimiento

Luego de que las etiquetas son asignadas en el enrutador, a su vez son repartidas entre Label Switching Router los cuales permanecen conectadas cuando las interfaces entre ellos esten activadas haciendo posible el envió de paquetes en el entorno de MPLS , se ejecuta con el protocolo de distribución LDP, exisen 4 categorias LDP:

- Discovery Messages (Mensajes de Descubrimiento): Son aquellos mensajes que comunican y ayudan con la aparición de LSR.
- Session Messages (Mensajes de Sesión) : establecen, mantienen y eliminan las sesiones entre LSR.
- Advertisement Messages (Mensaje de Advertencia): anuncian la correspondencia de etiquetas al FECs, este grupo es utilizado para crear, modificar y borrar las asignaciones de estiquetas a los FEC.

- Notification Menssages (Mensajes de Notificación): este grupo de mensajes es usado para transportar información correspondiente a señales de error.

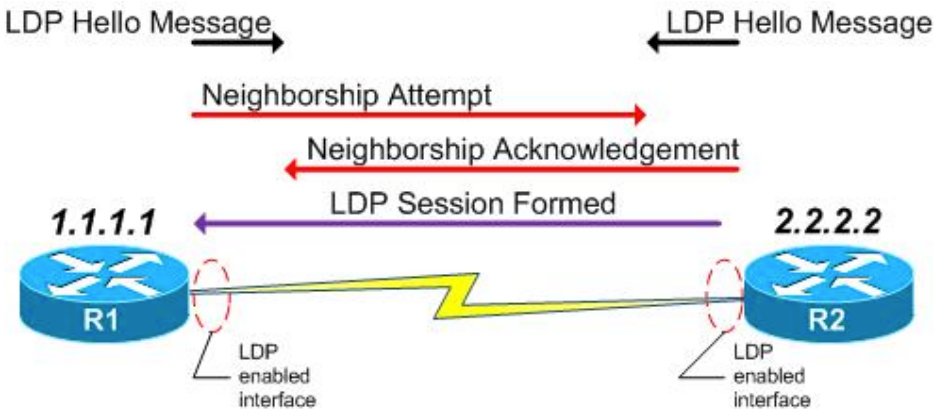

Figura 9 Estableciendo Sesión LDP

Fuente: (Cisco, 2005)

Todos los mensajes LDP, siguen un formato de valo (TVL), LDP utiliza el puerto 646 de TCP, para implementar la conexión LDP se explica de la siguiente manera:

Los establecimientos de conexión LDP empiezan al momento que LSR transmite paquetes repetidamente sobre las interfaces que permiten el envió, si LSR se encuentra en conexión con la misma interfaz y se encuentra habilitado MPLS, LSR establece una conexión directa con la fuente de origen del LDP .

LSR transmite un mensaje que inicia la transmisión la cuál contienen información similar como se transmite las etiquetas en el modo de distribución, además del tiempo en que tarda en establecer la conexión, la mayor longitud PDU, así como la identificación de LDP receptor.

LSR que se mantiene activo transmite paquetes de time of life al LDP el cual se mantiene activo estableciendo la conexión con LSR, por lo que en esos instantes las etiquetas que se encuentran en FEC pueden realizar una transición con LSR. (Lobo, 2005)

2.1.8 Técnicas de Distribución de Etiquetas

El método de distribución de etiquetas que se utiliza en MPLS son dos que indican la dirección como se produce:

- Distribución de Etiquetas bajo demanda downstream: la arquitectura MPLS permite a un LSR que requiera explícitamente una etiqueta relacionada con un FEC en particular.
- Distribución de Etiquetas no solicitada downstream:la arquitectura MPLS permite a un LSR distribuir uan etiqueta a otro LSR que no lo requiera explícitamente

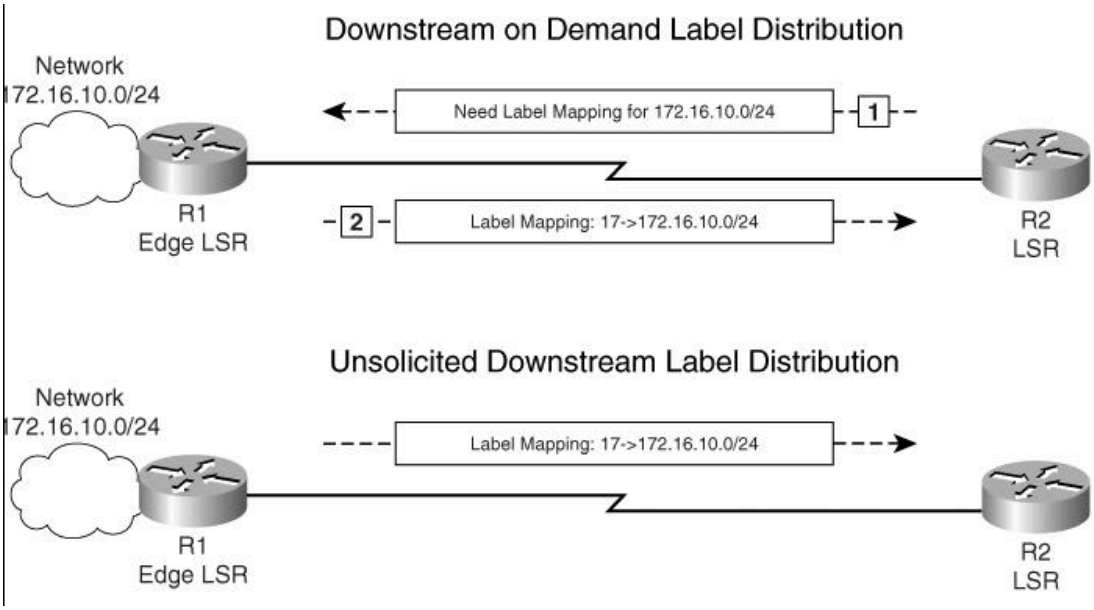

Figura 10 Distribución de Etiquetas

Fuente: (Kumar C. , 2010)

2.1.9 Funcionamiento MPLS

El funcionamiento de una red MPLS, según lo establecido en el IETF, con el transporte de datos es más fácil administrar este tipo de arquitectura, que consiste en un grupo de enrutadores de etiquetas que se añade a cada paquete. Los router MPLS

no investigan el encabezado IP tampoco lo procesan, examinan el paquete observando la información y valor de la etiqueta. Su proceso es el siguiente:

1. Se establece entre los routers la creación y asignación de las etiquetas utilizando estos dos protocolos FEC y LDP.
2. Al terminar la asignación se crea tablas de información en cada router , está contiene par de etiquetas correspondientes a cada interfaz.
3. Se crea los LSR borrando la etiqueta de entrada y añadiendo la nueva etiqueta de salida y se envía al siguiente LSR dentro del LSP.
4. Lee la etiqueta y la envía a su destino.

El funcionamiento de esta tecnología se basa en el cambio de etiquetas de un paquete que se encuentra ya etiquetado. Al momento de transmitir el mensaje de un host A a un host B , siguiendo una misma trayectoria

El paquete que se transmite desde el host debe llegar a su detino que es un enrutador IP luego este toma otro trayecto con la finalidad del llegar al enrutador que contiene la tecnología MPLS el cuál acoge el nombre de router de ingreso.

FEC tiene un camino o trayectoria específica por el cuál realiza su recorrido en la red MPLS con diferente calidad de servicio, el cual depende de las necesidades que se requiera. La calidad de servicio tiene un papel fundamental en la transmisión de paquetes, utilizando de mejor manera los recursos en la red, optimizando de una manera más rápida los recursos, mediante el protocolo de enrutamiento OSPF (Open Short Path First) siendo este un protocolo confiable y viable al momento de realizar un envió de paquetes con calidad de servicio. Este protocolo permite utilizar las vías más rápidas por la cuales se pueden transmitir el paquete, por lo que no quiere decir que en algún momento estas vías no puedan lleguar a ser saturadas.

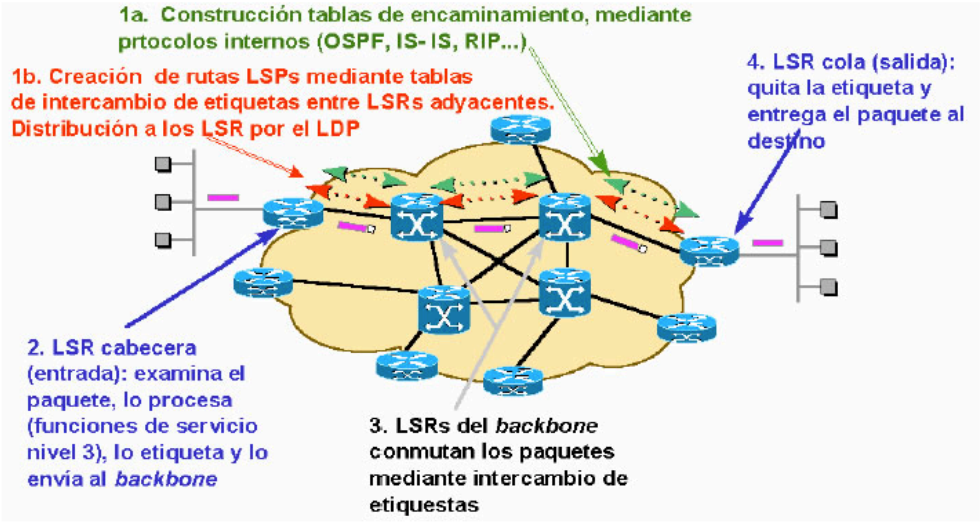

Figura 11 Funcionamiento MPLS

Fuente:

(http://ldc.usb.ve/~poc/RedesII/Grupos/G5/funcionamiento_esquema.htm, s.f.)

Para saber que etiqueta asignarle al paquete se tiene que comparar con las etiquetas ubicadas en las tablas de enrutamiento que se van dando desde la dirección destino a la dirección fuente por medio de pequeños mensajes entre conmutadores y/o enrutadores. Normalmente el camino es decidido antes de que se mande la información; el camino se forma en las tablas de enrutamiento cuando los dispositivos son conectados a la red.

Una vez que ya se tienen las tablas de enrutamiento al paquete se le asigna una etiqueta la cuál va cambiando en cada conmutador o enrutador en la red MPLS al que llega simplemente revisando esa etiqueta. El paquete va saltando hasta que llega al enrutador extremo de egreso(Egress Label Edge Router) en el cuál se le eliminan todas las etiquetas que tenían y llega al computador de destino o simplemente sale de la red MPLS. (catarian.udlap)

2.1.10 Aplicaciones MPLS

Básicamente las aplicaciones de MPLS se diferencian por las funciones que realizan en el control plane, estás aplicaciones utilizan un mismo data plane para la conmutación de etiquetas y forwarding. Generalmente una etiqueta es asignada a un FEC que es usado para la descripción de paquetes que tienen características comunes de forwarding (dirección de destino, QoS), MPLS tiene algunas aplicaciones tales como :

- Funciones de Ingeniería de tráfico (MPLS TE)
- Ruteo por Políticas (Policy Routing)
- Unicast IP Routing
- Multicast IP Routing
- Servicios de redes privadas virtuales (VPN:Virtual Private Network)
- Servicios que requieren calidad de servicio (QoS:Quality of Service)
- Diferenciación de niveles de servicio mediante clases (CoS)
- Integración de diversas redes o red de transporte universal (Any Transport over MPLS - AToM)

Acontinuación vamos a explicar las más utilizadas y de tener mayor consideración para los administradores y usuarios de estas redes:

Unicast Ip Routing: La configuración requiere de dos componentes,

- Un protocolo de enrutamiento IP (OSPF, IS-IS, EIGRP, etc)
- Un protocolo de distribución de etiquetas (LDP o TDP)

Los protocolos de enrutamiento brinda información sobre la conexión entre las redes. Mientras que los protocolos de distribución de etiquetas une las etiquetas a las redes a travéz del protocolo de enrutamiento. FEC es igual a una red de destino que se encuentra almacenada en una tabla de enrutamiento IP, esto intensifica la eficacia de los dispositivos en el núcleo de una red, debido a que la asignación de etiquetas disminuye el procesamiento del equipo.

Multicast Ip Routing: Utiliza un protocolo independiente que sirve para propagar la información de enrutamiento y las etiquetas PIM v2 (Protocol Independent Multicast) versión 2, el FEC es igual a la dirección multicast de destino.

MPLS TE: Resiste enrutamiento con restricciones, siempre que la ruta para el tráfico de red sea el camino más corto, reduciendo la congestión de red, los siguientes requerimientos son escenciales:

Cada uno de los LSR deben ver la topología de red mediante OSPF y IS-IS estos dos protocolos mantienen en la base de datos la topología completa de la red.

LSR también necesita una información extra de los enlaces de red, esa información incorpora medios disponibles y restricciones, los protocolos OSPF y IS-IS ayudan a la transmisión de la información adicional.

RSVP o CR-LDP (Constrain-based routing LDP) son usados para establecer túneles TE y propagar las etiquetas.

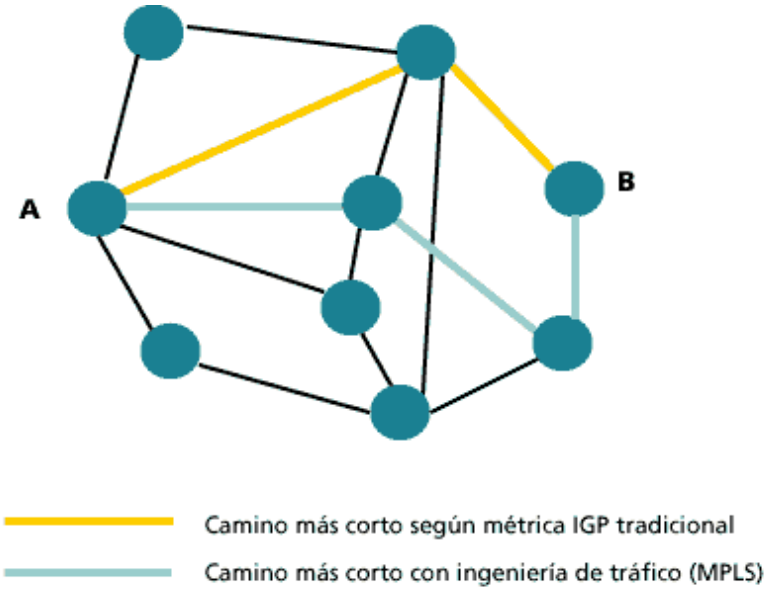

Figura 12 Ingeniería de Tráfico

Fuente: (Barberá, 2007)

La trayectoria con mayor posibilidad de tener una baja métrica entre A y B según lo recomendado por IGP es la que realiza dos saltos, teniendo en cuenta que puede

mostrarse otra opción, ya sea por un mayor tráfico en la red o en los routers, se hace el uso o la utilización de un salto más en la red sin tener inconvenientes en la transmisión de paquetes de datos . (Barberá, 2007)

QoS (Calidad de Servicio): Tiene beneficios para los administradores de red, evitando la congestión del tráfico en la red, mejorando la interacción del usuario con el sistema, en la actualidad no hay la necesidad de aumentar el ancho de banda no es la solución correcta, con la red MPLS se utiliza mejor los recursos reduciendo los costos mejorando el control sobre la latencia y el jitter, garantizando un transporte de datos más confiable ya que no toman un camino específico a través de la red, lo cual mejora el servicio asegurando una transmisión sin interrupciones.

2.2 Seguridades VPN con MPLS

VPN: Red privada Virtual que utiliza una red pública o no controlada como el internet, ofreciendo un bajo costo al momento de implementar la red a larga distancia al basarse sobre internet, además de ofrecer autentificación de usuarios o equipos a través de cifrados, firmas digitales o claves de acceso para una identificación inequívoca; ofrece también integridad, garantizando que los datos enviados por el emisor sean exactos a los que reciben, y confencialidad, el cifrado hace posible que nada de lo transmitido sea interceptado o interpretado por nadie más que emisor y destino. (Virtuales, 2014).

Las Redes Privadas Virtuales está basada en estandares preestablecidos, la tecnología de túneles (Tunneling) es un modo de transferir datos entre dos redes similares sobre una red inmediata. Denominado también encapsulación, a la tecnología de túneles que encierra un tipo de paquetes de datos dentro del paquete de otro protocolo, que en este caso sería TCP/IP. La tecnologí de túneles VPN, añade otra dimensión al proceso de túneles antes nombrado encapsulación, ya que los paquetes están encriptados de forma que los datos son ilegibles para los extraños. Los paquetes encapsulados viajan a través de internet hasta que alcanza su destino, entonces, los paquetes se separan y vuelven a su formato original. La tecnología de autentificación

se emplea para asegurar que el cliente tiene autorización para contactar con el servidor. (Tecnico, 2011)

Hay dos tipos comunes de VPN:

- **Acceso Remoto:** Se denomina como una virtual private dialup network (VPDN), que se encuentra en una conexión LAN de una compañía o identidad, utilizada por empleados que requieren una conexión a la red privada de los distintos lugares remotos. Los VPN de acceso remoto permiten seguridad, las conexiones encriptadas entre la red privada de una compañía y a los usuarios remotos a través de un proveedor del servicio de otras compañías.
- **Punto a Punto:** VPN de punto a punto se encuentara en la categoria de los intranets o extranets, una VPN de punto a punto construido entre las oficinas de la misma compañía es una intranet, mientras que una VPN construido para conectar a la compañía con su partner o cliente se refiere como extranet. (Cisco, 2008)

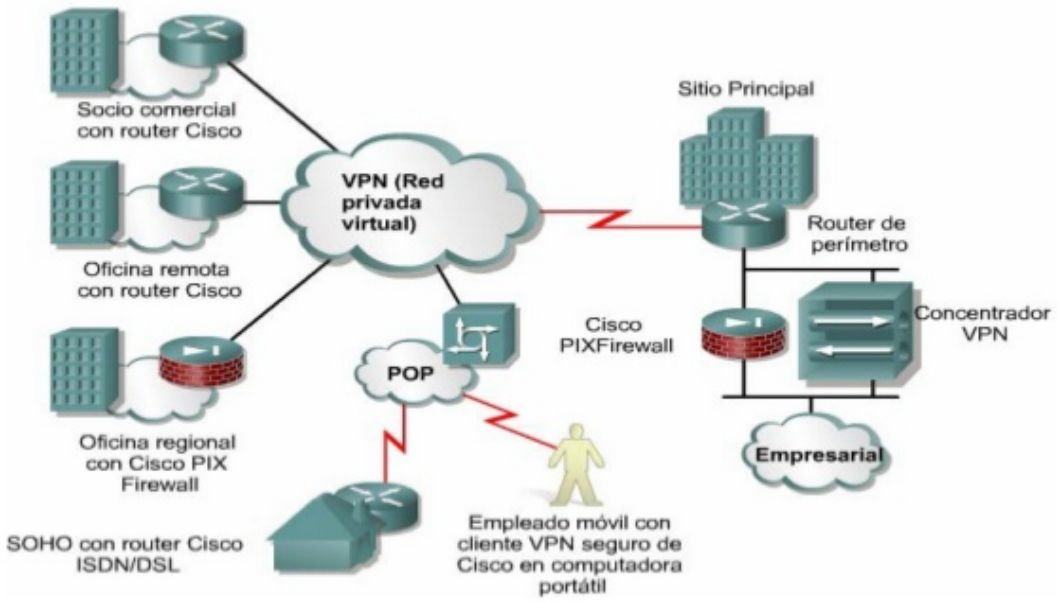

Figura 13 Red Privada Virtual

Fuente: (Jonathan, 2009)

2.2.1 MPLS VPN

Una MPLS VPN es una red privada virtual construida sobre la parte superior de una proveedor de servicio para ofrecer conectividad entre las diferentes ubicaciones de la empresa. Que se encuentra disponible en la capa 2 o capa 3 , la VPN aprovecha las capacidades multiprotocolo y etiquetado de MPLS para ofrecer una red peer - to - peer y enlazar todo los sitios remotos de la empresa en una red común. En la mayoría de los casos los servicios MPLS VPN se venden sin encriptación, normalmente basándose en el hecho de que cada cliente está aislado de los otros en su propia red privada. Sin embargo para aquellos clientes que lo requieran, el esquema de encriptación como IPSec se lo puede añadir en la configuración de la VPN.

MPLS VPN combina los beneficios de MPLS y el BGP(Border Gateway Protocol) que es un protocolo de enrutamiento. MPLS se utiliza para reenviar paquetes a través de la red troncal del proveedor y BGP se utiliza para la distribución de las rutas sobre el backbone. En MPLS VPN se encuentra los siguientes equipos:

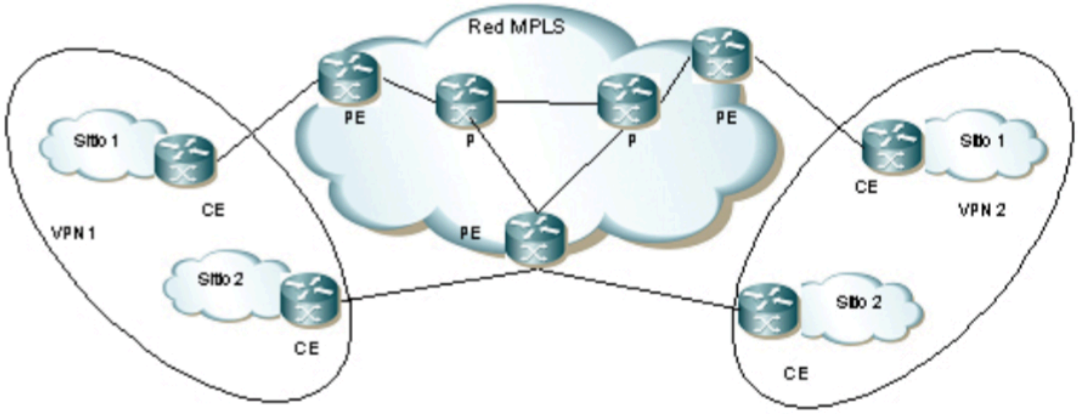

Figura 14 MPLS VPN
Fuente: (Rodriguez D. , 2008)

Customer Edge (CE): Se encuentran por lo general en la propiedad del cliente, algunos proveedores de servicio pueden suministrar el equipo.

Provider Edge (PE): Son los routers de borde del proveedor de servicios al que se conectan los CE. Los routers PE son propiedad del proveedor de servicios.

Provider (P): Estos son routers de tránsito y se encuentran en la red central del proveedor de servicios.

La información de enrutamiento es pasada del CE router al PE router mediante cualquiera de las rutas estáticas o con un protocolo de enrutamiento BGP. El PE mantiene una tabla de reenvió por sitio también conocido como virtual routing and forwarding (VRF) enrutamiento virtual y reenvió, es una tecnología que se incluye en los enrutadores de red IP que permite múltiples instancias en una tabla de enrutamiento, esto aumenta la funcionalidad, VRF aumenta la seguridad de la red.

Cada router PE está configurado por el proveedor de servicios con su propio VRF que es único, los routers dentro de la red MPLS VPN no comparten directamente la información VRF.

2.2.2 MPLS L3 VPN

Estas redes privadas virtuales son la mejor opción para los proveedores de servicio, ya que la arquitectura de MPLS L3 VPN es diferente a las tradicionales soportando el overlapping del espacio de direcciones IP, las rutas de intercambio en el router CE con el router PE que forman el núcleo de la red troncal de servicio, este utiliza siempre BGP como protocolo de enrutamiento el cuál expande los prefijos marcando con un identificador de 64 bits llamado RD(Route Distinguisher) es un valor único asignado por un proveedor para cada VPN haciendo una ruta única para que los clientes no vean las rutas de los demás.

La dirección de un cliente llegará a tener 96 bits en IPv4 a esto se lo llama VPNv4 que es la suma de los prefijos RD+VPN IP y son intercambiadas entre los routers PE mediante el protocolo MP-BGP, este es un multiprotocolo BGP que soporta unicast y multidifusión tanto en IPv4 como en IPv6, facilitando el uso de VPNv4.

"RD existe para hacer los prefijos en las VPNs de MPLS único, solucionando el problema de múltiples clientes con el mismo direccionamiento interno. Adicionalmente nos permite obtener balanceo de carga entre diferentes PEs conectados al mismo sitio." (Rodriguez D. , 2013)

Los RT(Route Target) se encuentran en la arquitectura de MPLS L3 VPN, es una comunidad de 64 bits en BGP utilizada para marcar los prefijos exportados en una VPN. Marcar los prefijos con un RT nos permite tener mayor flexibilidad en ambientes de VPNs complejas, escogiendo que prefijos queremos importar basándonos en este valor. (Rodriguez D. , 2013)

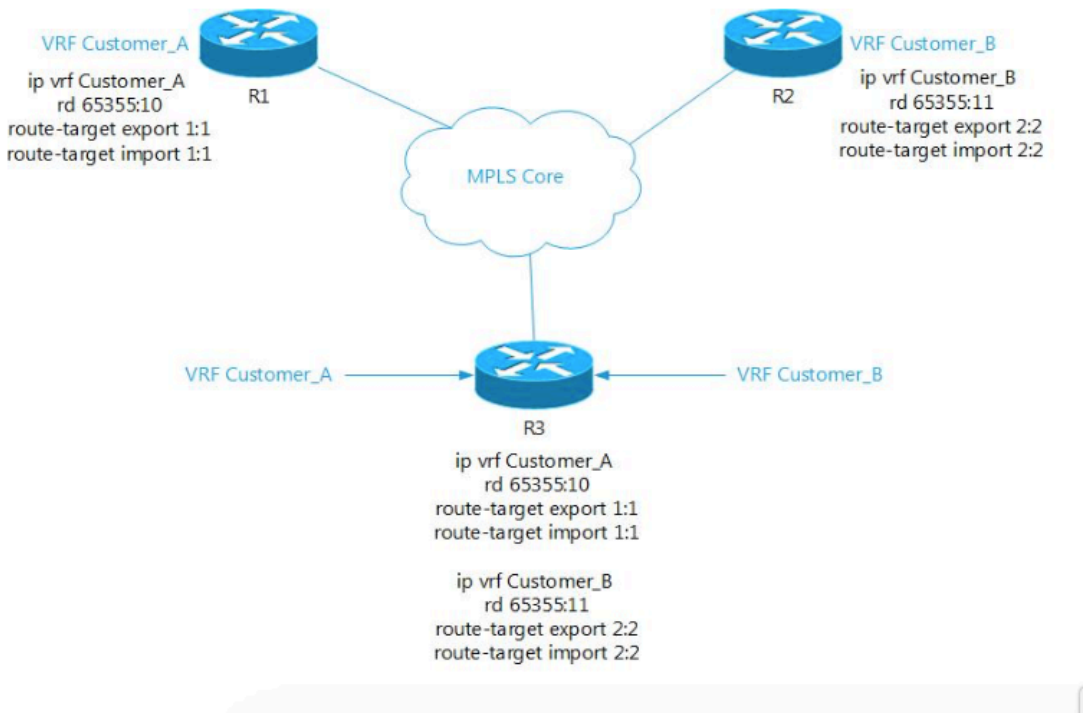

Figura 15 Esquema RD y RT

Fuente: (Perkin, 2013)

2.2.3 MPLS L2 VPN

La VPNs de la capa de enlace en MPLS se asemejan a un servicio de tipo de circuito virtual y es utilizado de manera eficaz por los proveedores de servicio que asegura la

conectividad en la capa de enlace sin llegar a la capa de red LAN extendida. Siendo esto posible para usar la red MPLS para el transporte de datos en capa dos encapsulando tramas de ethernet en paquetes MPLS y enviándolas a través de la red, cada trama es llevada como un solo paquete y los routers PE conectados al backbone eliminan o agrega etiquetas según el requerimiento.

2.2.4 Tipos de VPN

Las VPNs más utilizadas tenemos las siguientes:

Tunneling: Esta se basa en hacer el establecimiento de conexiones, entre dos host por medio de un mecanismo de seguridad , una opción es SSH (Secure SHell), con esta opción todo el envío de paquetes o datos que son inseguros pasan a transformarse en paquetes en modo seguro. Está conexión de túnel es segura entre los dos hosts por los cuales se encuentra transmitiendo los paquetes de datos, por lo general se encuentra en los extremos de las entidades . La tecnología utilizada en el túnel requiere una cuenta de acceso segura y confiable, para la realización imprescindible comunicación de datos. (Alejandro, 2007)

VPN sitio a sitio: Esta topología se utiliza en la conexión de oficinas remotas con el lugar central de las empresas. El terminal que se encuentra en la central VPN debe tener un enlace con un proveedor de internet, la cuál adopta todas las conexiones de internet de todos los sitios con la finalidad de establecer un túnel VPN. Los servidores que se localizan en las sedes deben estar conectadas a internet por el proveedor de servicios , asegurándose que la conexión del proveedor sea de un ancho de banda aceptable . Con la finalidad de eliminar los enlaces punto a punto tradicionales, teniendo en cuenta la comunicación con entidades internacionales. (Alejandro, 2007)

Figura 16 VPN sitio a sitio.
Fuente: (nethumans, 2013)

VPN de acceso remoto : Consta de una implementación prácticamente sencilla en la cual los usuarios puedan establecer una conexión entre los mismo sitios que se encuentren en la empresa o fuera de ella siendo esta una conexión remota, utilizando internet como el medio local de acceso. (Alejandro, 2007)

Figura 17 VPN de acceso remoto.
Fuente: (nethumans, 2013)

VPN Interna : Este tipo de VPN no es muy conocida pero resulta ser muy útil en el ámbito de redes privadas virtuales funcionan con la condición de que se encuentren perteneciendo a la misma red local . Esta VPN se creó con el motivo de poder aislar o fragmentar la red y los servicios que contiene, con la finalidad de hacerla más segura.

Esta tecnología se utiliza en especial en redes inalámbricas aumentando la seguridad , lo que separa de la red interna de la empresa evitando fuga de información y el acceso a usuarios no autorizados . (Alejandro, 2007)

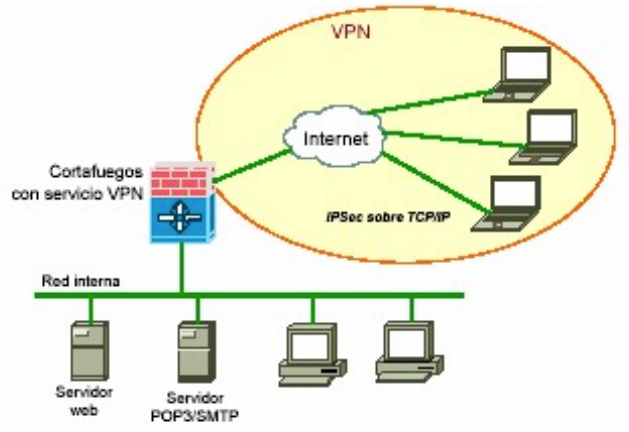

Figura 18 VPN Interna.
Fuente: (wikispaces, s.f.)

Los protocolos que incluyen VPN son :

PPTP: Point – to – point tunneling protocol , este protocolo acepta redes privadas virtuales bajo demanda y multiprotocolo a través de redes públicas, como la internet, agregando un nuevo nivel de seguridad ya que encapsula los protocolos IP o IPX en los datagramas PPP, haciendo posible la ejecución de forma remota las aplicaciones que dependen de protocolos de red específicos. Sin embargo, es más que una conexión de host a host segura, en lugar de una LAN a LAN.

IPSec: Es el mecanismo de seguridad más utilizado a nivel de capa 3. Es un protocolo que proporciona seguridad en la transmisión de paquetes, funciona en el puerto TCP como para UDP.

Con el mecanismo de seguridad en mención hace posible la comunicación entre hosts o routers que se encuentren conectados a una misma red de una manera segura, que es una de las soluciones mayormente implementada en los entornos corporativos donde la seguridad es la parte primordial en la capa 3 del modelo OSI, proporcionando

varios servicios necesarios para que la comunicación sea segura, en estos servicios los cuales constan: confidencialidad, integridad y autentificación, utilizando dos protocolos Authentication Protocol y Encapsulated Security Payload. (redeszone, 2014)

L2TP: Layer 2 Tunneling Protocol es un protocolo que facilita la transmisión de paquetes de una forma clara, con los usuarios que se encuentren en los extremos de un túnel. Utilizando mensajes de control y mensajes de datos. El primero que son los mensajes de control se utiliza para establecer la conexión. El segundo mensajes de datos cumple la función de encriptar los paquetes y enviarlos mediante el túnel. (Alejandro, 2007)

2.2.5 Protocolo GRE

El protocolo GRE (Generic Routing Encapsulation) este protocolo encapsula paquetes con fin de enrutar otros protocolos sobre la red IP, GRE está definido por RFC 2784 del IETF.

GRE fue desarrollado como una herramienta de túneles destinado para llevar los protocolos de capa 3 del modelo OSI a través de la red IP, en esencia crea una conexión privada de punto a punto como una red privada virtual.

GRE funciona mediante la encapsulación de una carga útil, es decir que un paquete interno necesita ser entregado a una red de destino en el interior de un paquete IP externo, en los extremos del túnel GRE se envía cargas útiles a través de este túnel mediante el enrutamiento de paquetes encapsulados en las redes IP involucradas. Otros routers IP no analizan la carga útil es decir el paquete interno, solo analizan el paquete IP externo ya que lo envían hacia el final del túnel GRE, al alcanzar el punto final del túnel la encapsulación GRE se elimina y la carga útil se transmite a lo largo de su destino final.

A diferencia de los túneles IP a IP, GRE puede transportar multicast y IPv6 entre el tráfico de redes. Las ventajas de los túneles GRE están los siguientes:

- Encierra múltiples protocolos sobre un único protocolo en el backbone.
- Proporciona soluciones para redes con saltos limitados.
- Conectan subredes discontinuas.
- Permiten VPNs a través de la WAN.

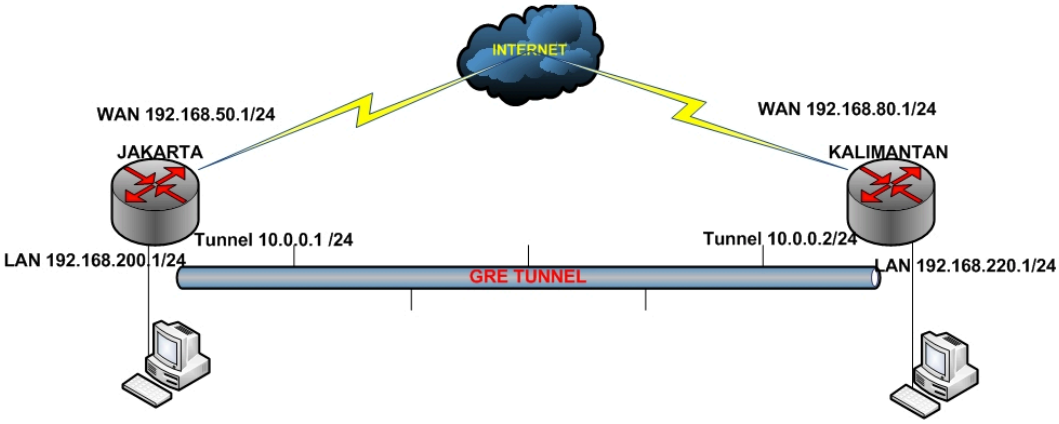

Figura 19 Túnel GRE.

Fuente: (junaedi, 2008)

2.3 GETVPN con el protocolo GDOI

2.3.1 GETVPN

Group Encrypted Transport VPN es una tecnología que no utiliza túneles, la cuál proporciona seguridad de extremo a extremo para el tráfico de red en un modo nativo y manteniendo la inteligencia de la red como conexiones full – mesh, routing y QoS. Por lo que es implementado principalmente en redes privadas MPLS, está basada en el estándar IETF (RFC 3547), utiliza el mecanismo GDOI (Dominio del Grupo de Interpretación) con el cifrado de seguridad IP (IPSec) ofreciendo al usuario un método eficaz en la protección del tráfico IP multicast o unicast. Todos los miembros del grupo (GMS) comparten una asociación de seguridad común (SA) . Esto permite encriptar el tráfico del grupo (GMS) que se cifró por cualquier otro (GM). En IPSec el router CE actúa como si fuera un GM.

Al momento de implementar Group Encrypted Transport VPN, se debe hacerse responsable que existe una red basada en VPNs la cual debe estar funcionando en perfectas condiciones con la respectiva activación de cifrado por seguridad en la capa de red.

2.3.2 Principales Beneficios GETVPN

Los beneficios de GETVPN son los siguientes:

- Es altamente escalable proporciona una VPN a cualquier tipo de topología de red utilizando la seguridad IPSec.
- Se aprovecha de la infraestructura subyacente del enrutamiento IP VPN y no requiere en el plano de control de una superposición de enrutamiento.
- Se integra perfectamente con la infraestructura multicast sin problemas de replicación de multicast, que suele verse en las soluciones tradicionales basadas en túneles IPSec.
- Conserva la IP de origen y destino durante la encriptación y encapsulación IPSec. Por lo tanto GETVPN se integra muy bien con las características como la calidad de servicio y la ingeniería de tráfico.
- Baja latencia y jitter en la comunicación con el tráfico directo entre los sitios.
- El ancho de banda utiliza de manera más eficiente mediante la habilitación de multicast.

2.3.3 Arquitectura GETVPN

GETVPN abarca Multicast Rekeying, una manera de activar el cifrado de paquetes multicast ¨nativos¨ y unicast Rekeying a través de una WAN privada . Multicast Rekeying y GETVPN se basa en GDOI como se define en Internet Engineering Task Force (IETF) RFC 3547. Además hay similitudes con IPSec en el área de la cabecera de preservación y SA de búsqueda. La distribución dinámica de IPSec SA es añadida y las propiedades de superposición del túnel IPSec se han eliminado. (Cisco, Techexams, 2016, pág. 4)

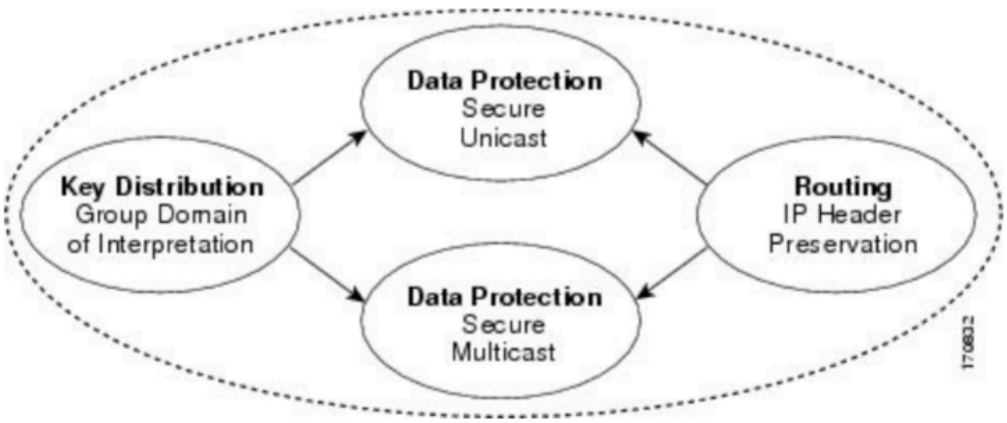

Figura 20 GETVPN Relación de Conceptos.

Fuente: (Cisco, Techexams, 2016, pág. 4)

2.3.4 GDOI

Group Domain of Interpretation se basa en Internet Key Exchange (IKE), para proteger la distribución de las claves . A igual que el método tradicional IPSec puede utilizar claves compartidas (PSK) o claves públicas (PKI) son compatibles con la autentificación inicial. Después que los VPNs se autentifican el protocolo GDOI es implementado para actualizar los GM de una manera eficiente.

GDOI introduce dos claves de cifrado diferentes. La clave de cifrado de claves (KEK) se utiliza para asegurar el plano de control, mientras que la clave utilizada para el cifrado de datos es la clave de cifrado de tráfico (TEK).

Los miembros del grupo de GETVPN son los routers IOS responsables de su cifrado y descifrado del tráfico de datos.

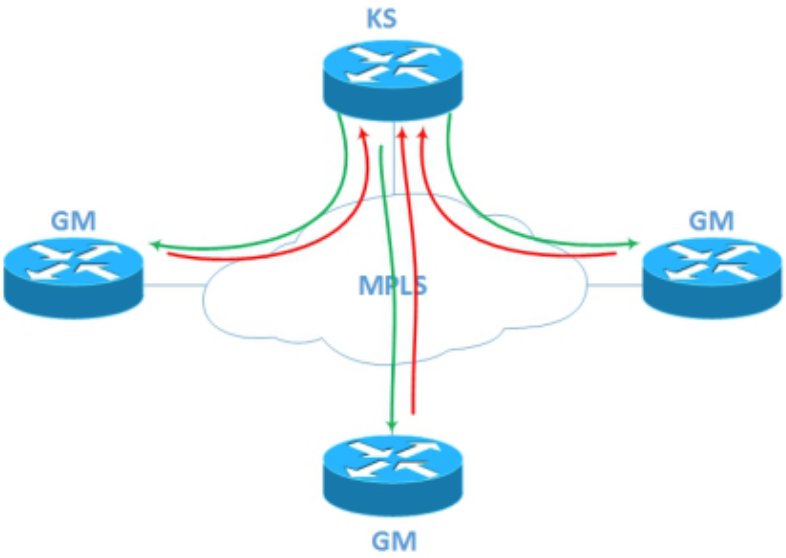

Figura 21 Autentificación y Distribución GDOI.
Fuente: (Gentil, 2014)

En la figura 21 podemos observar la autentificación y distribución de las políticas de trabajo. Las flechas rojas representan la autentificación y registro de GMs y el KS con flechas verdes representa la distribución de las políticas.

GDOI actualiza periódicamente la información de claves criptográficas y las distribuye a los miembros del grupo, ya que tiene la capacidad de enviar mensajes de cambio de claves como multicast o unicast en la infraestructura de la red.

El protocolo GDOI además está protegido por un intercambio de ISAKMP fase 1.Tanto el servidor de claves como el miembro del grupo GDOI deben tener la misma política de ISAKMP. El ISAKMP fase 1 debe ser lo suficientemente robusto para proteger el protocolo, el intercambio de mensajes puede ocurrir en dos modos el modo principal y el modo agresivo . La siguiente figura como se produce el intercambio ISAKMP fase 1:

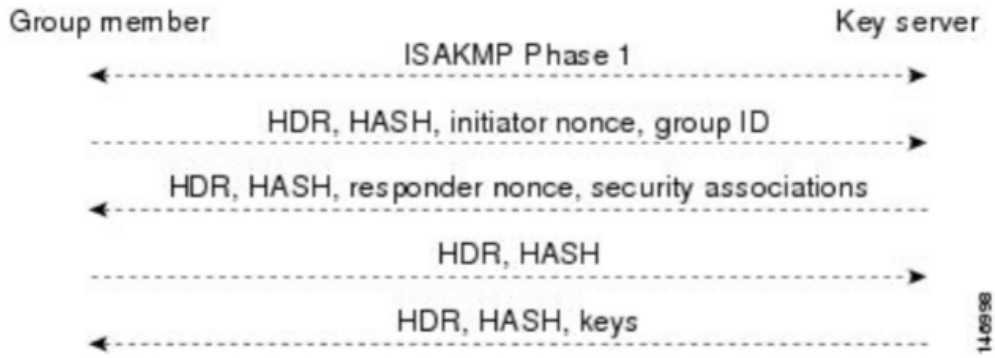

Figura 22 Autentificación y Distribución GDOI.

Fuente: (Cisco, Techexams, 2016, pág. 4)

Los mensajes ISAKMP fase 1 y los cuatro mensajes del protocolo GDOI se conoce como el registro GDOI, y el intercambio de todo los que se muestra en el unicast entre el miembro del grupo y el servidor de claves. Durante el registro, el mecanismo de cambio de clave es multicast, el miembro del grupo recibe la dirección multicast del grupo y se registra en este grupo el cuál recibe la regeneración de las claves multicast. El protocolo GDOI utiliza UDP con el puerto 848 con traducción de direcciones de redes transversales NAT-T.

2.3.5 KSs

Un servidor de claves o key server (KS), es el responsable de crear y mantener el plano de control GETVPN. Todas las políticas de encriptación como el tráfico, los protocolos de encriptación, la asociación de seguridad, cambio de claves , etc. Están definidas en el KS , cuando un miembro del grupo se registra descargar las claves para el GM.

El key server tiene dos responsabilidades : revisar las solicitudes de registro y él envió de cambio de claves.

Un miembro del grupo puede registrase en cualquier momento y recibir las políticas y claves actuales. Cuando un miembro del grupo se registra en el servidor de claves

comprueba la ID del grupo el cual está tratando de unirse , si este ID es válido el servidor de claves envía las políticas de asociación segura a los miembros del grupo.

Hay dos tipos de claves que el key server puede descargar: la clave de cifrado de clave (KEK), está encripta el mensaje de cambio de clave, la clave de cifrado de tráfico (TEK) realiza la función de IPSec SA con lo que los miembros del grupo se comunican entre ellos.

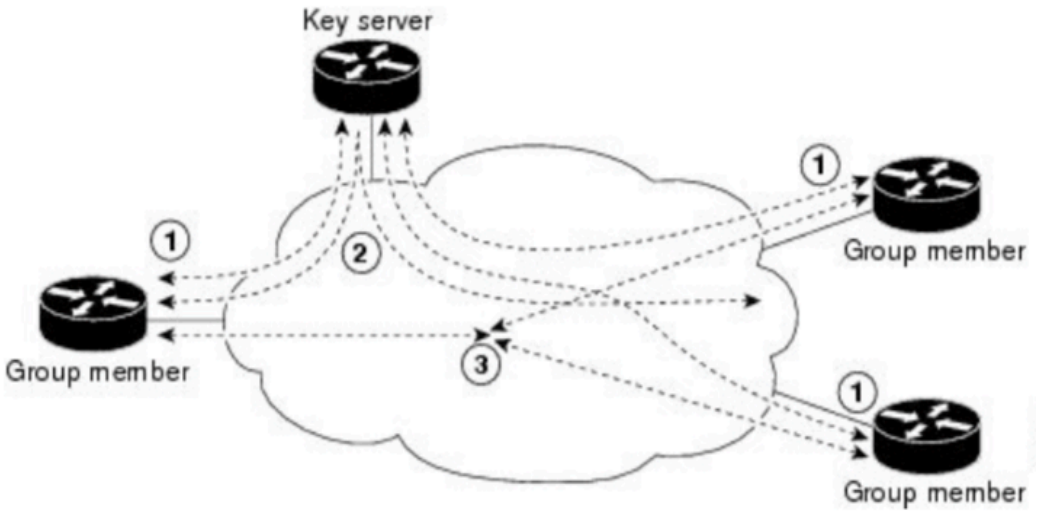

Figura 23 Funcionamiento Key Server .
Fuente: (cisco, 2016, pág. 6)

1. Los miembros del grupo se registran en el servidor de claves. El servidor de claves autentifica y autoriza a los mienbros del grupo descargar las políticas y las claves necesarias para la encriptación y desencriptación de los paquetes multicast IP.
2. Según sea necesario, el servidor de claves envía un mensaje de cambio de clave a los miembros del grupo. El mensaje de cambio de clave contiene una nueva política IPSec y las claves para utilizar cuando las antiguas expiren. Los mensajes de cambio de claves son enviados antes de que expiren, para asegurar que las claves del grupo siempre esten disponibles.
3. Los miembros del grupo son autenticados por el servidor de claves, que se encuentran en el mismo grupo usando IPSec SAs. (Haseeb Niazi, Group Encrypted Transport VPN (Get VPN), 2015)

2.3.6 GMs

Miembros del grupo es un enrutador responsable de la encriptación y desencriptación de paquetes un dispositivo encargado de manejar el plano de datos VPN. Las políticas de cifrado se define principalmente en el KS y se descargan en el GM en el momento de la inscripción. GM decide si el tráfico tiene que estar cifrado o descifrado y que claves usar. En una red GETVPN, las políticas del miembro del grupo GM son dictadas por el key server, pero en algunos casos un GM puede anular una de estas políticas.

Cualquier política global (incluyendo tanto el permiso como la negación de entradas) definido en el key server, afecta a todos los miembros del grupo, por lo que algunas políticas tienen más sentido cuando se definen a nivel local. Como ejemplo, si un grupo de GMs ejecuta un protocolo de enrutamiento diferente, una entrada local puede ser añadido a estos. (Haseeb Niazi, Group Encrypted Transport VPN (Get VPN), 2015, pág. 6)

2.3.7 Group SA

A diferencia de las soluciones tradicionales de cifrado IPSec, GETVPN utiliza el concepto de grupo SA. Todos los miembros del grupo GETVPN pueden comunicarse entre sí utilizando una política de cifrado común y una SA compartida, no hay la necesidad de negociar IPSec entre GMs, esto reduce la carga de recursos en los enrutadores IPSec. (Haseeb Niazi, Group Encrypted Transport VPN (Get VPN), 2015, pág. 6)

2.3.8 Rekey Process

Es un proceso de envió de claves cuando las existentes están a punto de expirar, se genera un único cambio de claves para un grupo particular en el servidor de claves. GETVPN tiene dos tipos de cambios de claves : unicast y multicast.

Unicast rekeying: Es el proceso de generación de claves, el servidor de claves genera un mensaje de cambio de claves y envía varias copias del mensaje una copia a cada GM. Al recibir el mensaje de cambio de clave, un GM envía un ACK al servidor de claves. Este mecanismo ACK no solo asegura que la lista del grupo de miembros activos esta sobre el servidor de claves, sino que también asegura que el mensaje de cambio de clave se envía solo a los miembros del grupo activos.

Un servidor de claves puede ser configurado para retransmitir un paquete de regeneración de claves para superar los efectos transitorios de la red. Si un miembro del grupo no reconoce tres generaciones de claves enviadas consecutivamente, el servidor de claves elimina el mensaje del miembro de grupo activo y deja de enviar mensajes de cambio de clave.

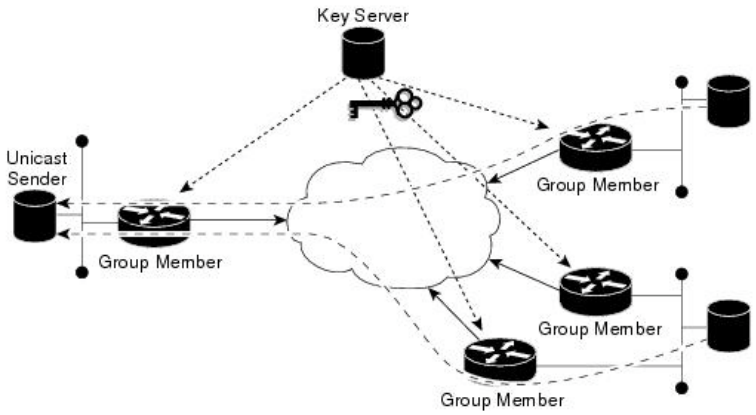

Figura 24 Multicast ReKey .
Fuente: (Cisco, Cisco Group Encrypted Transport VPN , 2016)

Multicast rekeying: Es el proceso de generación de claves multicast muy eficiente, todos los miembros del grupo que están registrados en el grupo recibe este cambio de claves multicast, estas se envía periódicamente sobre la anterior antes que expiren en el servidor de claves. A diferencia de la generación de claves unicast, multicast no posee un mecanismo de ACK, por lo que el servidor de claves no mantiene una lista de miembros de grupo activa.

Tabla 1

Unicast vs Multicas Rekeying

Unicast	Multicast
Su uso es en infraestructura competente a unicast	Debe tener una infraestructura competente a multicast
Reconocimiento de generación de claves	Retransmite la clave varias veces sin acuso de recibo
Podría requerir ajustes en los routers si hay un gran número de usuarios en cola	Es el método más rápido y escalable

2.3.9 Preservación Tunnel Header

En IPSec tradicional, las direcciones del extremo del túnel se utilizan con un nuevo paquete de origen y destino, el paquete es enrutado sobre la infraestructura IP, utilizando la dirección de origen del router encriptado y la dirección del router de destino desencriptado. En el caso de GETVPN, los paquetes de datos protegidos en IPSec encapsulan los paquetes de origen como de destino de las direcciones originales del host en la cabecera IP externa preservando la dirección.

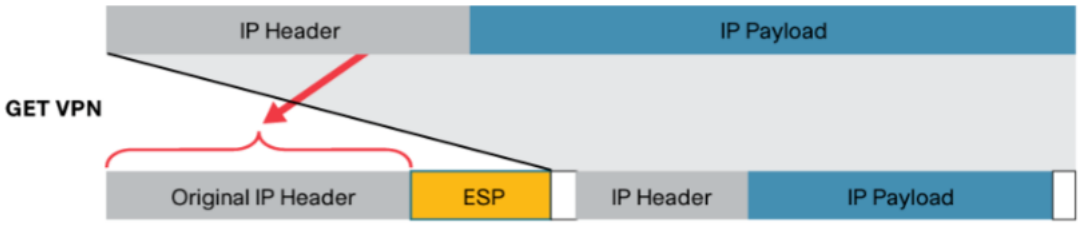

Figura 25 Tunnel Header.

Fuente: (Haseeb Niazi, Group Encrypted Transport VPN (Get VPN) , 2015)

La mayor ventaja de la preservación del tunnel header es la capacidad de enrutar los paquetes encriptados utilizando la infraestructura de enrutamiento de red

subyacente. La alta disponibilidad de derivación (HA) proporcionada por una infraestructura MPLS VPN (dobles radio , dobles enlaces, etc.) se integra perfectamente con GETVPN. No hay necesidad de proporcionar HA en el nivel de IPSec.

Debido a la preservación del túnel de cabecera se combina con el grupo de las SA, la replicación de multicast es más eficiente en el backbone de los proveedores. Porque cada GM comparte la misma SA, el enrutador IPSec más cercano a la fuente de multicast, no tiene que replicar paquetes a todos los miembros del grupo, y ya no está sujeto a problemas de replicación de multicast que existe en el tradicional IPSec.

Vale la pena señalar que la preservación del túnel de cabecera parece muy similar al modo de transporte IPSec. Sin embargo, el modo subyacente opera en el modo del túnel IPSec, mientras que el modo de transporte IPSec, reutiliza la cabecera IP original, y por lo tanto añade menos perdida en la cabecera de un paquete IP. (Haseeb Niazi, Group Encrypted Transport VPN (Get VPN) , 2015, pág. 5)

2.5 Kali Linux

Es una distribución de Linux , la que nos permite hacer el uso de esta herramienta al momento de efectuar pruebas de penetración y auditorías de seguridad, es de código abierto y de distribución libre, fue desarrollada por Offensive Security a partir de la reescritura de BackTrack, esta versión trae preinstalados numerosos programas entre los más importantes esta un sniffer como lo es Wireshark, además de un crackeador de passwords y la suite Aircrack-ng que nos sirve para pruebas de seguridad de redes inalámbricas, la distribución se lo hace a través de imágenes ISO o puede ser usada desde un Live CD o Live – USB e instalada como un sistema operativo.

2.5.1 Características para la Instalación

En la instalación Kali Linux puede descargado de la siguiente página: https://www.kali.org/downloads/ (Caballero, 2015, pág. 9)

- Mínimo de 8 GB de espacio libre en el disco duro, recomendable 25 GB.

- Mínimo de 512 MB de Ram.

2.4.2 Top 10 Security Tools Kali Linux

Una lista con las 10 herramientas más utilizadas, con mayor demanda y utilidad del mercado. Para ello Offensive Security ha realizado diferentes estudios basado en estadísticas de uso, encuestas de popularidad y resultados basados en el mundo de la seguridad informática siendo la lista de herramientas la siguiente:

Figura 26 Top 10 Kali Linux.

Fuente: (sanchez, 2013)

- **Aircrack-ng:** Se trata de un conjunto de software de seguridad inalámbrica que incluye un analizador de paquetes de redes, un crackeador de redes WEP y WAP/WPA2-PSK y otro conjunto de auditoría inalámbrica.
- **Burp Suite:** Es una herramienta escrita integramente en Java que permite realizar test de intrusión de aplicaciones web, permitiendo combinar técnicas manuales y automáticas para analizar, detectar y explotar aplicaciones web. Incluye elementos tales como un Spider web, un Intruder, un repetidor de llamadas con lo que las peticiones pueden ser automatizadas.
- **Hydra:** Es un crackeador de contraseñas multihilo por fuerza bruta en base a diccionarios. Puede crackear practicamente cualquier servicio (Telnet, POP3,SMTP, IMAP,SMB, SSH V1, y 2 etc) usando una conexión directa o proxys, con o sin SSL. Esta herramienta a tenido una gran reputación gracias a poder ser ejecutada desde consola tanto en sistemas Linux como Windows.
- **John:** Hace referencia, como no, a John The Ripper, una herramienta muy popular, ya que permite comprobar que las contraseñas de los usuarios son lo suficientemente seguras. Aplica fuerza bruta para descifrar contraseñas, siendo capaz de romper varios algoritmos de cifrado o hash, como DES, SHA-1 entre otros.

- **Maltego:** Es una aplicación de minería y recolección de información utilizada durante la fase de Data Gathering, proceso en el cuál se trata de obtener el mayor número de información posible para su posterior ataque. La información la obtiene de internet y la representa de forma gráfica, para que sea más sencillo de analizar. Es un herramienta muy potente llena de opciones que pueden ser útilies para investigar empresas, sitios, personas y mucho más. Permite iniciar busquedas a partir de dominios, Ips, ubicaciones geográficas, correos, nombres, teléfonos e incluso frases. (Gonzalez Perez, Sanchez Garces, & Soriano de la Camara, Pentesting con Kali, 2013, pág. 34)
- **Metasploit:** Una forma sencilla de definir Metasploit Framework es que se trata de una herramienta para desarrollar y ejecutar exploits contra un equipo remoto. Sin embargo está herramienta dispone de gran cantidad de funcionalidades las cuales son muy utilizadas en el día a día por los auditores de seguridad para llevar a cabo su test de intrusión, pudiendo realizar con Metasploit Framework no solamente la explotación y post explotación del sistema, sino también los pasos previos a ellos.
- **Nmap:** Es un programa por consola de comandos que sirve para efectuar rastreo de puertos y se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.
- **Sqlmap:**Es una herramienta muy útil en los test de intrusión que automatiza el proceso de detección y explotación de fallos de tipo SQL Injection y de está forma obtener toda la información contenida dentro de los servidores de la base de datos. Indispensable en auditorias web
- **Wireshark:** Esta aplicación es un analizador de paquetes que permite examinar datos de una red viva o de un archivo de captura salvado en disco. Analiza la información capturada a través de los detalles y sumarios por cada paquete. Aunque su uso docente esta muy extendido, wireshark no solamente se emnarca en el área educativa, ya que en la actualidad se ha convertido en una herramienta imprescindible para los auditores informáticos.
- **Zaproxy:** Es una herramienta fácil de usar y que forma parte de las aplicaciones de uso habitual en el proceso de pentesting para encontrar vulnerabilidades en aplicaciones web. Está diseñado para ser utilizado por usuarios con diferente nivel en seguridad, y como tal , es ideal para desarrolladores y probadores funcionales que son nuevos en el hacking ético, además de ser una herramienta útil en el pentesters de nivel avanzado. (Gonzalez Perez, Sanchez Garces, & Soriano de la Camara, Pentesting con Kali, 2013, pág. 35)

2.4.3 Diferentes entornos de Kali Linux

Entorno de una auditoría Interna: Se desarrolla en el entorno de una entidad u organización, pueden ser un esquema complejo y vulnerabilidades que aunque no son detectadas existen, cada entidad u organización debe realizar una prueba de auditoría interna para verificar el estado en el que se encuentra su organización.

A esto se lo conoce con el nombre de Prueba de Caja Blanca ,asume el rol de un usuario que tienen acceso para evaluar las redes, con información de diagramas de red,

detalles del hardware, sistemas operativos, aplicaciones entre diferente información que le puede ayudar a la realización de las pruebas.

Elevando así el nivel de seguridad investigando al máximo las vulnerabilidades que puede presentar los servidores internos, fallos en configuraciones, sistemas e aplicaciones desactualizados, comunicaciones no seguras en la red corporativa, además de redes Wireless no deseadas, con el fin de potenciar la seguridad y no ser víctima de un ataque que provocaría el robo de información valiosa en una entidad.

Entorno de una auditoría Externa: Debido a que las entidades tienen una gran cantidad de servicios públicos está más sometida a fallos o pérdidas sensibles en la información.

Se lo conoce como auditoría de Caja Negra, es cuando se realiza una prueba un atacante externo a la entidad o hacker solo con el conocimiento de una dirección IP o una dirección web, con el fin de obtener información importante de la organización comprometiendo y poniendo a prueba las barreras de seguridad que tiene la entidad en su red corporativa.

También sirve para evaluar el nivel de seguridad de la red externa de una entidad, con la finalidad de descubrir las vulnerabilidades y fallos de seguridad, tomando esto como una manera de mejorar y fortalecer la red con planes de mejora continua, obteniendo informes completos de estas actividades con el fin de aumentar la seguridad.

Entorno de una auditoría Web: En la actualidad los servicios web son muy susceptibles a un grupo de ataques independientes de la plataforma o tecnología utilizada que por lo general tienen defectos en los diseños así como también en descuidos en la programación, por lo que ocasionan grandes pérdidas a nivel económico en una empresa que se ve afectada dejando una mala imagen hacia nuevos clientes o asociados.

Entorno de un análisis Forense : Consiste en la recuperación de información después de que haya ocurrido algún tipo de accidente, cuando esto ocurre hay que actuar de la manera más rápida posible y ser precavido al momento de recoger datos o información que pueden ser relevantes al momento de realizar la investigación.

Pueden suceder fallos en los sistemas operativos que corrompan las pruebas, un fallo eléctrico o cualquier situación que ocasione pérdidas de información al momento de la recolección de evidencias.

2.5 Calidad de Servicio QoS

Los parámetros en la medición de calidad de servicio según la ITU-T son los siguientes : Latencia, Jitter, Pérdida de Paquetes, los mismos que sirven para el análisis de una red.

Estos pueden variar dependiendo de los requerimientos del cliente y lo que puede ofrecer el proveedor de servicios , garantizando un excelente servicio. Para definir la transferencia de datos en la red que se basa en los parámetros tales como :

Latencia: Se lo conoce también como Delay, es el tiempo que tarda un paquete en hacer el recorrido desde su origen hasta su destino en la red, estos retardos se da dependiendo del número de nodos, los protocolos de enrutamiento entre otros.

En el caso de una red MPLS, utiliza una conmutación por etiquetas escogiendo los caminos cortos, permitiendo en cada flujo de datos una etiqueta haciendo una conmutación rápida entre nodos (toma en consideración la etiqueta y no el destino).

Jitter: Es una variación de retardo de los paquetes en los nodos, los cuales pueden variar según el tráfico de información, el estado del dispositivo , es un parámetro aleatorio por lo que varía impredeciblemente a lo largo de la trayectoria entre el emisor y el receptor. Este parámetro afecta en su mayoría en paquetes de audio y video disminuyendo la calidad en la transferencia en la red.

Pérdida de Paquetes: Se refiere a la pérdida o descarte de la información en la red, esto es provocado debido a fallas en los dispositivos, exceso de tráfico, también al protocolo en la capa de transporte donde los cuales pueden ser TCP o UDP, TCP asegura que los paquetes lleguen a su destino sin importar el tiempo que lleva en la transmisión, UDP más utilizado en servicio de video y voz.

Ancho de Banda: Es definido como la cantidad de información que fluye a través de enlaces de red en un determinado tiempo. Mientras más ancho de banda exista, más datos pueden transmitirse.

2.5.1 Clasificación de Tráfico

Las herramientas de clasificación de tráfico son las ACL (lista de control de acceso) y NBAR (Network Based Application Recognition).

ACL: La lista de control de acceso es una forma para determinar los permisos de acceso apropiados, permitiendo controlar el flujo del tráfico, cuya función principal es filtrar el tráfico entrante o saliente. Al momento del ingreso de un paquete este es verificado para luego posteriormente ser entregado cumpliendo las condiciones de las lista de acceso permitiendo seguir con el proceso.

En QoS se las utiliza para dar prioridad a un determinado tipo de tráfico, siempre que cumpla con la sentencia caso contrario será negada.

NBAR : Reconocimiento de aplicaciones basadas en la red, proporciona una aplicación inteligente con QoS, soporta una amplia gama de protocolos, que proporciona flexibilidad y permite soportar nuevas aplicaciones que se encuentren en la red, agregando protocolos adicionales que no se encuentran en la lista.

Es capaz de identificar de forma inteligente el tipo de cada paquete y proporcionar las características de la red adecuado, permitiendo combinar multiservicio en datos, voz y video en una red unificada.

2.5.2 Marcaje de Tráfico.

El marcado de tráfico es el proceso por el que se identifica cada paquete de acuerdo a una clase o categoría de modo que los dispositivos de la red puedan reconocer a que clase pertenece para poder operar en consecuencia. El marcado de tráfico también se involucra en la configuración de algunos bits dentro del encabezado de la capa de red, con el objetivo de dejar a los otros dispositivos con calidad de servicio basado en valores de marcaje.

Entre los métodos de marcado de tráfico se encuentran el DSCP, IP Precedence y CoS.

DSCP: Se considera una de las técnicas más extendidas y estandarizadas , asegurando un trato preferente, pero sin fijar garantías , basada en el RFC 2474 , utiliza un campo de la cabecera IP para definir la prioridad o tipo de servicio.

IP Precedence : Es un modelo en el cual el tráfico es procesado a través de sistemas intermedios con prioridades relativas en base al campo del tipo de servicio, reemplaza la especificación original para definir la prioridad del paquete, aumentando el número de niveles de prioridad definibles al momento de reasignar los bits de una paquete IP para hacer una marcación prioritaria.

CoS: Clase de servicio es el esquema de prioridad 802.1p, esta proporciona un método de asignación de etiquetas a los paquetes con información sobre la prioridad.

El valor de la clase de servicio está dado entre 0 y 7, este valor es agregado al encabezado de la capa 2 de los paquetes, donde el 0 es la prioridad más baja y el 7 la prioridad más alta.

Valor de CoS	Valores de las colas de reenvío
0	Q2
1	Q1(prioridad más baja)
2	Q1(prioridad más baja)
3	Q2
4	Q3
5	Q3
6	Q4(prioridad más alta)
7	Q4(prioridad más alta)

Figura 27 Prioridad CoS.
Fuente: (sanchez, 2013)

2.5.3 Modelos de Calidad de Servicio.

Son empleados para ofrecer calidad de servicio a los usuarios de la red los cuales garantizan la entrega de paquetes , entre ellos tenemos el modelo Best Effort, Int-Serv y DiffServ.

Best Effort: Es el modelo más básico que existe, es el que se emplea por defecto, este tipo de redes todos los usuarios reciben el mejor servicio que se pueda proporcionar , por lo que tiene diferentes tiempos esto se debe de acuerdo al número de paquetes que se está, se utiliza en páginas web, correos electrónicos y otros servicios similares, sin garantía de efectividad en la transmisión.

Int-Serv: Este modelo es empleado en redes WAN, debido a que cuenta con una arquitectura propia de los protocolos garantizando la eficiencia en la red. Este modelo cuenta también con el servicio del modelo Best Effort en tiempo real y compartición controlada con los medios de transmisión mediante la reserva de los recursos en cada sesión, dando un nivel garantizado en el servicio, la ventaja que presenta es la facilidad de integrarse con las políticas de red, siendo conveniente para las llamadas de voz.

DiffServ: Este es un modelo el cual garantiza la calidad de servicio en redes WAN, empleando políticas, asignando prioridad a los paquetes según la clase respectiva.

Debido que es un conjunto de tecnologías en donde los proveedores de servicio ofrecen calidad de servicio a distintos niveles, sin necesidad de ser implementados en todos los nodos.

DiffServ se encuentra involucrado con los comportamientos específicos para cada clase de tráfico llamado PHB que define la cantidad de tráfico que corresponde a un paquete, especificando la prioridad de la ruta, también permite ofrecer servicios basados en un conjunto de reglas de salto definidas en los dispositivos que componen la red mediante DSCP.

Las ventajas que posee este mecanismo se encuentra la escalabilidad, debido a que soporta voz y datos sobre la misma infraestructura, reduce los requerimientos en el funcionamiento, es flexible con muchos tipos de tráfico, maneja las cabeceras de los protocolos IPv4 e IPv6, es una de los mejores modelos que existe en la actualidad en QoS.

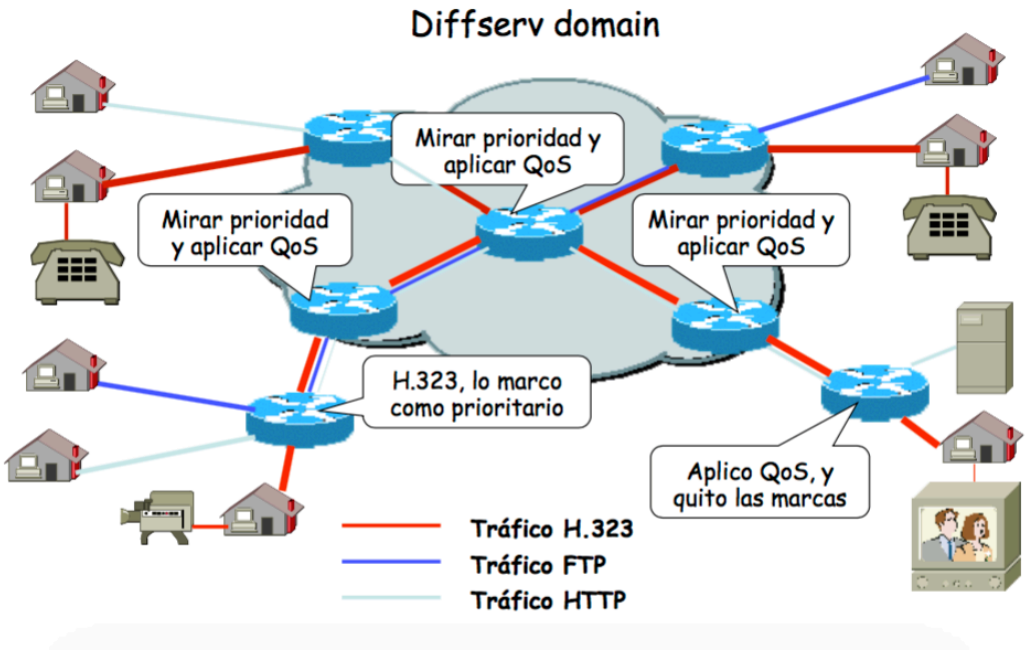

Figura 28 Modelo DiffServ.

Fuente: (unavarra, 2014)

CAPÍTULO 3

Diseño de la Red

3.1 Requerimientos de la Red Multiservicio

En el capítulo se desarrollará el diseño de una red MPLS con los requerimientos necesarios que la conforman, además de la arquitectura que se utiliza en los backbones de una red corporativa, de esta manera podemos entender las variables necesarias así como los estándares que se utiliza además de los procedimientos a seguir en las diferentes configuraciones que se realicen.

El principal motivo para el diseño de un backbone con tecnología MPLS, es por sus beneficios que se encuentra sobre las demás tecnologías, la tecnología MPLS es una de las más utilizadas en la actualidad en todo proveedor de servicios, por lo que resulta muy fundamental e indispensable disponer mecanismos que ayuden en la encriptación de datos para solventar problemas con el control de seguridades aplicando los nuevos recursos que los investigadores descubren a diario.

Mediante la plataforma GNS3, que es una herramienta muy eficaz y confiable en el ámbito investigativo, se establece una emulación del backbone MPLS con todas las configuraciones necesarias, que garantice el funcionamiento y el resultado esperado, con el objetivo de que la red sea confiable, eficaz, escalable y segura.

3.1.1 Consideraciones de Requerimiento de Red

En cuando al diseño de una red hay algunas consideraciones que un proveedor de servicio debe asegurarse que el diseño que se va a elegir soporte el manejo de grandes cantidades de información y pueda ofrecer seguridad en el transporte de la misma.

Una de esas consideraciones es el de poseer una red que su núcleo se encuentre una topología netamente mallada, esto es que cada nodo o dispositivos están conectados entre todos los nodos o dispositivos obteniendo enlaces entre ellos , porque la

información que se encuentra en el backbone debe tener muchas opciones para realizar el transporte y lograr su destino final, se lo realiza por si algún nodo o enlace entre ellos puede fallar, el transporte de la información puede utilizar una dirección distinta como una ruta de respaldo cumpliendo con el traslado de la información.

También en el diseño se debe considerar los dispositivos que se llegan a utilizar, ya que estos dispositivos son los encargados del soporte de la información y encriptación los cuales deben ser equipos que sean robustos, de manera que tengan gran capacidad, eficiencia a igual que un perfecto procesamiento sin causar pérdidas, de esta manera la red se mostrara fiable y con la capacidad de entregar la información con garantías que se requiere en el transporte.

Se debe tener una topología lógica para enviar información a través de la red MPLS, de tal manera al momento del envió se lo realice de una manera transparente, con enlaces dedicados y también alcanzar el destino por diferentes caminos por lo que este método hace una red más confiable y segura al momento del transporte de la información de datos.

Se dice que una red es netamente funcional cuando crece el número de nodos sin tener el cambio o modificación de su diseño. Con el fin de permitir la interconexión con la mayor cantidad de clientes, siempre garantizando la prestación de servicios de extremo a extremo.

- Backbone o Core: En el core de MPLS es donde se transporta grandes cantidades de información de manera confiable y rápida, por lo que los equipos deben tener alta capacidad que permitan el intercambio de tráfico a velocidades superiores a los 100Gbps, por esta razón es de gran importancia considerar latencia y velocidad. Con la agrupación de varios equipos se logra alcanzar una mayor capacidad.
- Acceso: Proveen el enrutamiento con el filtrado de paquetes permitiendo aquellos paquetes que lleguen al núcleo o core, deben tener alto rendimiento

que soporten velocidades de 10Gbps, 1Gbps, 100Gbps, E1, T1, E3, T3, ubicandos entre el core y los clientes.

- Clientes: Son equipos que se utiliza para la conexión de red con el proveedor de servicio por lo general son de velocidad moderada.

3.1.2 Arquitectura de Backbone con Seguridades.

De acuerdo a la arquitectura que se encuentran en las industrias, se debe diseñar un backbone que sirva para disminuir problemas de seguridad en el plano de control y de gestión, por lo que la arquitectura se debe diseñar en un ámbito flexible, escalable, dinámico, operable y sobre todo seguro.

Es deseable contar con un mallado completo, para que no sea posible la desconexión y sea tolerante a fallas. Contar con jerarquías que tengan niveles en la red es de suma importancia al momento de la transferencia de tráfico, igual en la información de enrutamiento, podemos considerar que los niveles jerárquicos en nuestra red son de acceso y backbone.

El uso compartido de la red de acceso, así como el QoS para cada servicio tiene diferentes grados de calidad, en algunos casos no puede ser viable , en cambio la integración del plano de control y del plano de gestión permite aprovechar de mejor manera los beneficios de la convergencia de la red.

Para alcanzar los niveles de seguridad, flexibilidad, escalabilidad y QoS, es necesario utilizar mecanismos como la Ingeniería de Tráfico, para una mayor organización sobre los flujos de información y mejor control en la QoS.

En la arquitectura de seguridad se debe tener las siguientes consideraciones basadas en la ITU X.805 que proporcionan seguridad de red de extremo a extremo, corrigiendo los problemas de seguridad en gestión, control e infraestructura.

3.1.2.1 Dimensiones de Seguridad

Las medidas de seguridad sirven para tratar de mejorar el esquema en el que se desarrolla la seguridad en la red . Este grupo consta de 8 tipos de seguridad que protegen de las diferentes amenazas a las que está expuesta, sin limitaciones de red sino en conjunto con los usuarios, los proveedores de servicio ofrecen una gama de seguridad a sus clientes las cuales son:

Tabla 2

Dimensiones de Seguridad

Dimensión de Seguridad	Descripción	Ejemplo
Control de Acceso	Límites y control en al acceso a los elementos de red, servicios y aplicaciones.	Password, listas de acceso, firewall, etc
Autenticación	Garantía de la procedencia de la información	Password compartido, firmas digitales, certificados digitales, etc
No - Repudio	Garantía de que no se pueda negar cualquier tipo de actividad en la red.	Bitácoras, sistemas de registros de eventos, firmas digitales, etc.
Confidencialidad de los Datos	Garantía de que la información solo es accesible por las entidades, sistemas o personas autorizadas.	DES, AES, RSA, etc.
Comunicación segura	Garantía de que la información fluye desde la fuente al destino.	Frame Relay, MPLS, IPsec, etc.
Integridad de los Datos	Garantía de que la información no ha sido modificada o corrompida de manera alguna, desde su transmisión hasta su recepción.	MD5, firmas digitales, software antivirus, etc.
Disponibilidad	Garantía de que los elementos de red, servicios y aplicaciones, se mantengan disponibles para los usuarios legítimos.	IDS, IPS, redundancia en la red, etc.
Privacidad	Garantía de que la información que fluye en la red se mantenga privada.	NAT, DES, AES, RSA, etc.

Fuente: (UNAD, 2011)

3.1.2.2 Capas de Seguridad

La capa de seguridad es una serie de trabajadores que dan soluciones a la red. Por lo que se define tres niveles de seguridad: capa de infraestructura , de servicios y

aplicaciones. La capa de infraestructura trabaja sobre la capa de servicios y esta capa a su vez trabaja sobre la de aplicaciones, corrigiendo las vulnerabilidades de seguridad capa por capa ofreciendo flexibilidad en la lucha contra las amenazas potenciales que puedan infringir la seguridad.

Las tres capas se pueden aplicar al modelo OSI, las cuales se complementan mutuamente las describiremos en la siguiente tabla.

Tabla 3

Capas de Seguridad

Capa	Descripción	Ejemplo
Seguridad de infraestructura	La capa de seguridad de infraestructura, comprende los dispositivos de transmisión y los elementos de red. Esta capa constituye la base fundamental de las redes, sus servicios y aplicaciones.	Enrutadores, centros de conmutación, servidores, enlaces de comunicación, etc.
Seguridad de Servicios	La capa de seguridad de servicios, tiene que ver con la seguridad de los servicios que los proveedores prestan a sus clientes.	Servicios básicos de transporte y conectividad, plataformas auxiliares para el acceso a Internet (servicios AAA, DHCP DNS, etc.), o servicios de valor añadido como QoS, mensajería instantánea, etc
Seguridad de Aplicaciones	La capa de seguridad aplicaciones tiene que ver con la seguridad de las aplicaciones de la red a las que acceden los clientes de proveedores de servicios. Son aplicaciones soportadas por servicios de red.	Aplicaciones básicas como FTP o HTTP, aplicaciones como mensajería en red y correo electrónico y aplicaciones más elaboradas, como comercio electrónico o móvil, colaboración en vídeo, etc.

Fuente: (UNAD, 2011)

3.1.2.3 Planos de Seguridad

El plano de seguridad cumple una labor primordial en una red protegida . Los 3 tipos de actividades en la red se pone en consideración en la siguiente Tabla 4.

Tabla 4

Planos de Seguridad

Capa	Descripción
Gestión	Este plano tiene que ver con la protección de las funciones de operación, administración, mantenimiento y configuración de los elementos de red, dispositivos de transmisión, sistemas administrativos y centros de datos. El tráfico para estas actividades puede transportarse en la red dentro o fuera de la banda, con respecto al tráfico de usuario del proveedor de servicio. La capa de seguridad de infraestructura, comprende los dispositivos de transmisión y los elementos de red. Esta capa constituye la base fundamental de las redes, sus servicios y aplicaciones.
Control	Este plano tiene que ver con la protección de las actividades que permiten una distribución eficiente de información, servicios y aplicaciones en la red. Generalmente consiste en la comunicación que permite determinar la mejor forma de enrutar o conmutar el tráfico en la red de transporte. Se habla de información de control o información de señalización. Estos mensajes se pueden transportar en la red dentro o fuera de la banda, con respecto al tráfico de usuario del proveedor de servicio. Los protocolos de enrutamiento, DNS, SIP, SS7, Megaco/H.248, etc., son ejemplos de este tráfico. La capa de seguridad de servicios, tiene que ver con la seguridad de los servicios que los proveedores prestan a sus clientes.
Usuario de Extremo	Este plano tiene que ver con la seguridad cuando los clientes acceden y utilizan la red del proveedor de servicio. En este plano también se incluyen flujos de datos efectivos del usuario de extremo. El usuario de extremo puede utilizar una red que sólo proporciona conectividad, puede utilizar redes para servicios de valor añadido como las RPV, o redes para acceder a aplicaciones de red.

Fuente: (UNAD, 2011)

En la siguiente figura se puede observar la arquitectura de seguridad con cada actividad de red con los distintos elementos y algunas amenazas mencionadas anteriormente.

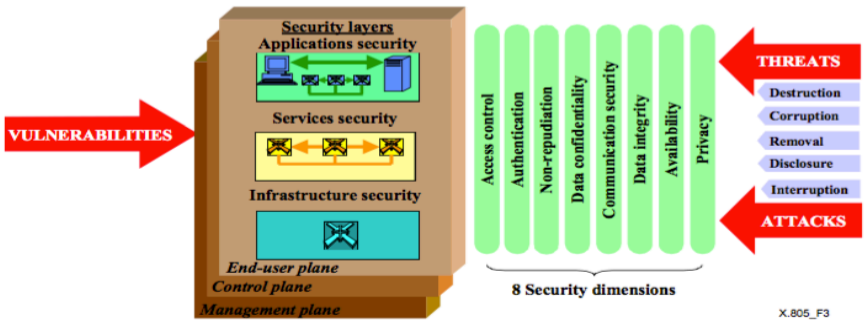

Figura 29 Arquitectura de Seguridad.

Fuente: (X.805(ITU), 2003)

3.1.3 Criptografía en Redes

La herramienta más importante para la seguridad de redes y comunicaciones es el cifrado , por lo que habitualmente se usa dos tipos de cifrado los cuales son el cifrado convencional o simétrico, y cifrado de clave pública o asimétrico, un nuevo tipo de cifrado es el híbrido que es la unión de las mejores características de los dos anteriores, resaltando las técnicas de cifrado que más son utilizadas el DES (Data Encryption Standard) y sus sucesores la versión triple clave de DES y al AES (Advanced Encryption Standard).

Cifrado Simétrico: Es la técnica más antigua y de mayor uso. Una clave secreta que puede ser un número, una palabra o una simple cadena de letras aleatorias, esta se puede aplicar al texto de un mensaje para cambiar su contenido, esto es tan simple como cambiar cada letra por un número en diferentes lugares del alfabeto, el remitente y destinatario conocen la clave secreta los cuales pueden cifrar y descifrar los mensajes.

Cifrado Asimétrico: El principal problema de la clave es el intercambio en internet o una red grande, en la distribución de la clave los distintos usuarios pueden cifrar y descifra el mensaje, por lo tanto si cae en manos equivocadas la comunicación ya no es segura y se debe generar una nueva, es más lento que el cifrado simétrico ya que requiere de más recursos en procesamiento para cifrar y descifrar el mensaje.

Cifrado Híbrido: Es la unión del cifrado simétrico con el asimétrico, generando una clave pública y otra privada en el receptor, cifra el archivo de forma síncrona de manera rápida y eficiente.

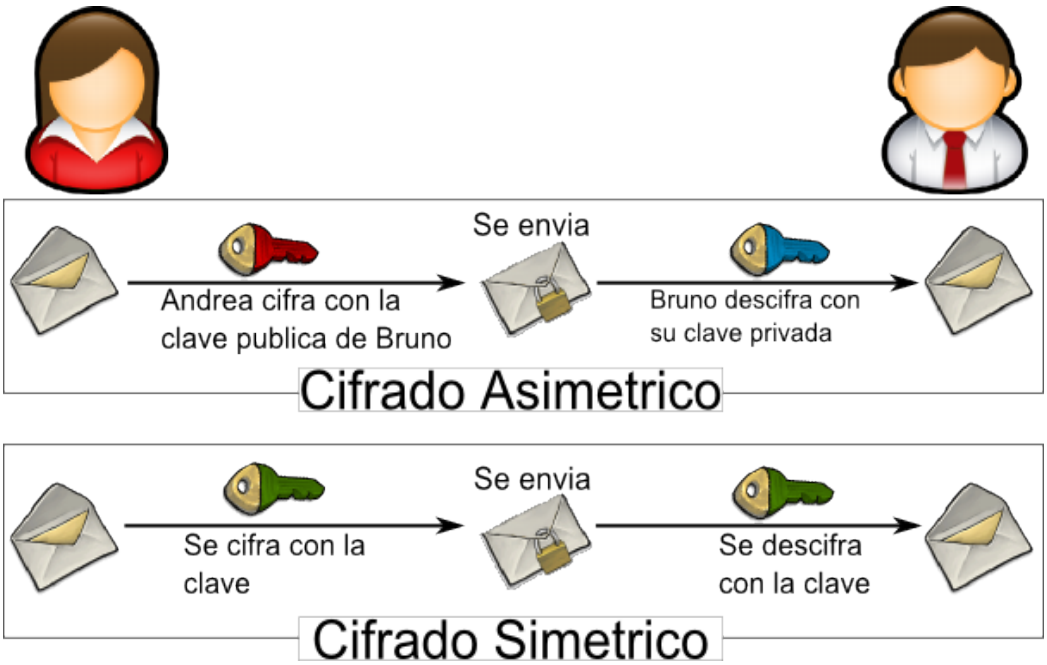

Figura 30 Tipos de Cifrado.

Fuente: (Sanchez, 2014)

Tenemos otros tipos de cifrado los cuáles se encuentran en la capa 2 y capa 7 del modelo OSI.

Cifrado de Enlace: Se encuentra en la capa 2 del modelo OSI, cifra el mensaje incluyendo las cabeceras de niveles superiores, tiene un nodo intermedio con capacidades de cifrado/descifrado, por lo que la información está protegida entre cada par de nodos consecutivos, es importante descifrar parcialmente, para procesos de encaminamiento y control de errores.

Cifrado de Extremo a Extremo: Se encuentra en la capa 7 del modelo OSI, en las cuales se cifran los datos, las cabeceras se añaden y se transmiten sin cifrar manteniendo el cifrado de origen a destino.

3.1.4 Servicios de Seguridad

Un servicio de seguridad tiene por objetivo realizar auditorías y analizar los continuos ataques o cambios, siempre mejorando el sistema de información de una

identidad u organización. Estos servicios sirven para la detección y prevención de ataques, realizando un buen servicio de protección de la información. Encontramos algunas clases de servicios de seguridad las cuales se mencionaran a continuación:

Confidencialidad: La confidencialidad es no difundir información a personas, entidades que no estén autorizadas, permitiendo la protección de información con la finalidad de prevenir ataques.

Autentificación: Confirma la identidad de un usuario que desea acceder a la red, verificando si es el correcto con un método distribuido en la autentificación.

Integridad: Advierte de posibles cambios o modificaciones en la información por personas que no están autorizadas a realizarlos.

No Repudio: Son pruebas que se llevan a cabo entre un emisor y receptor, el receptor puede comprobar que ese mensaje fue enviado por el emisor y de manera viceversa.

Control de acceso: Es el servicio que controla quienes están autorizados para acceder a la información y evitar el uso no autorizado de recursos de la red.

3.1.5 Seguridad a Nivel de Red

El protocolo de IPSec es el que proporciona el nivel de seguridad en capa 3, pertenece al RFC 2401, estándar IETF desde el año de 1999, proporcionando seguridad IP y los protocolos de capas superiores.

3.1.5.1 IPSec

Fue desarrollado por la IETF con la finalidad de crear un túnel seguro en la capa de red, protegiendo y autentificando los paquetes IP entre los dispositivos que contengan el protocolo. Por lo tanto provee: control de acceso, integridad no orientada a la

conexión, autenticación del origen de datos, rechazo o reenvió de paquetes, confidencialidad, negociación de compresión IP.

IPSec de acuerdo a sus características es obligatorio la implementación para IPv6 y opcional para IPv4, en ambos casos las características se implementan como cabeceras de extensión, que siguen a las cabeceras principal IP. La cabecera de autentificación (AH, Authentication Header) , para la encriptación se encuentra la cabecera de carga útil de seguridad (ESP, Encapsulating Security Payload header).

3.1.5.2 Arquitectura IPSec

En la arquitectura del protocolo IPSec se cubren los conceptos generales, de igual manera los requisitos y definiciones de esta tecnología.

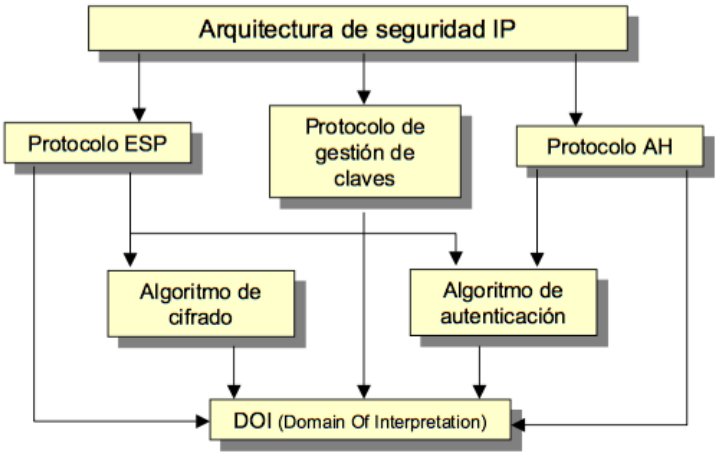

Figura 31 Arquitectura IPSec.
Fuente: (Ternero, 2003, pág. 75)

Cabecera de autentificación (AH): Cubre el formato del paquete y los aspectos generales relacionados con el uso del AH para la autentificación de paquetes. Funciona con el protocolo 51 en IPv4 y Next header en IPv6, compatible con los algoritmos HMAC-MD5 y HMAC-SHA-1, se lo puede implementar solo o en combinación con ESP o en el modo túnel del IPSec, pero si se utiliza solo garantiza una protección débil.

El proceso del AH ocurre en el siguiente orden:

- La cabecera IP y la carga útil de datos, se realiza un hash (algoritmo que transforma una entrada de datos grande en una de longitud fija) utilizando la clave secreta compartida.
- El hash construye una nueva cabecera AH, que se inserta en el paquete original.
- El nuevo paquete se transmite al router del IPSec del mismo nivel.
- El router del mismo nivel codifica la cabecera IP y los datos de carga útil utilizando la clave secreta compartida, extrayendo el hash de la cabecera AH, comparando los valores del hash.

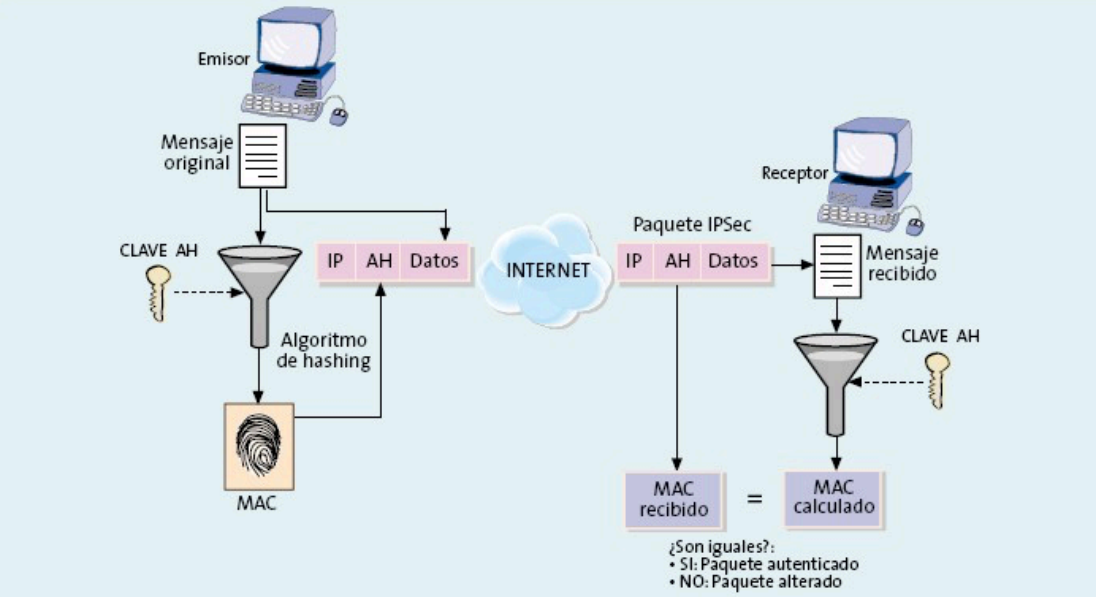

Figura 32 AH.

Fuente: (Burton, 2014)

Encapsulado de carga útil de seguridad(ESP):cubre un formato del paquete y los aspectos generales relacionados con el uso de ESP para el cifrado de paquete y de manera opcional, para la autentificación. Ofreciendo los mismos servicios de seguridad que AH (autentificación e integridad) con el cifrado encapsulando los datos que se van a proteger, opera con el protocolo 50 en IPv4 y Next Header en IPv6.

En primer lugar la carga útil es cifrada mediante DES, 3DES, AES, luego la carga útil es cifrada es ordenada para proporcionar la autentificación e integridad de los datos con HMAC-MD5 o HMAC-SHA-1, garantizando el contenido de los paquetes no pueda ser revisado por otras personas, opcionalmente se puede incluir AH.

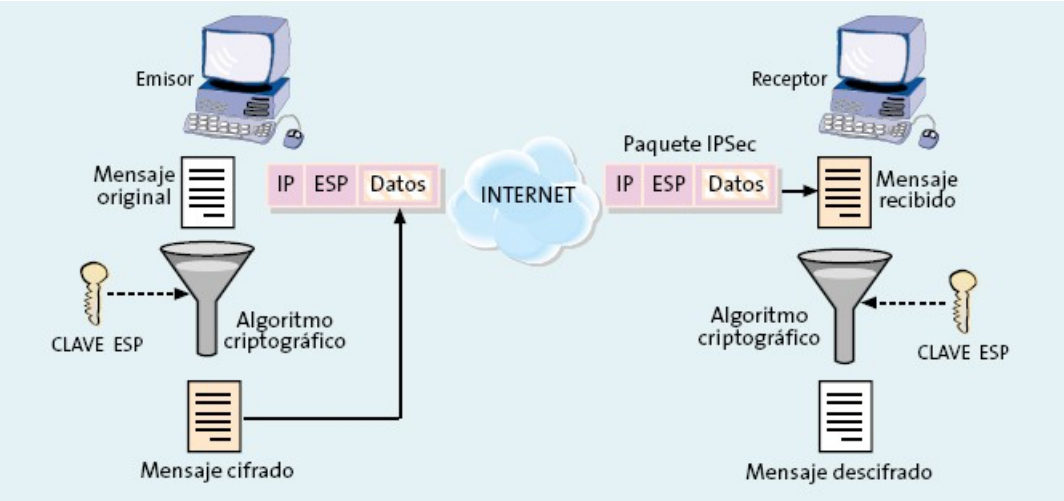

Figura 33 ESP.

Fuente: (Burton, 2014)

Algoritmo de Cifrado: es un conjunto de documentos que describen como se utilizan distintos algoritmos de cifrado para ESP.

Algoritmo de Autentificación: un conjunto de documentos que describen como se utilizan distintos algoritmos de autentificación para AH y para la opción de autentificación ESP.

Gestión de Claves: realizan la gestión con documentos que se encuentran en los esquemas.

Dominio de Interpretación (GDOI) : contiene los valores necesarios para que los demás documentos se relacionen entre sí. Incluyendo identificadores para algoritmos de cifrado y de autentificación, así como parámetros operativos con el tiempo de vida de las claves.

3.1.6 Servicios IPSec

IPSec proporciona servicios de seguridad en la capa IP, permitiendo que un sistema elija los protocolos de seguridad necesarios, determinen los algoritmos que va a usar para el servicio o servicios y ubique las claves criptográficas necesarias para proporcionar los servicios solicitados. Por lo tanto se usan dos protocolos para

proporcionar seguridad: un protocolo de autentificación designado por la cabecera del protocolo, AH, y un protocolo combinado de cifrado/autentificación designado por el formato del paquete para ese protocolo, ESP. Los servicios son los siguientes:

- Control de Acceso
- Integridad sin conexión
- Autentificación del origen de los datos
- Rechazo de paquetes reenviados
- Confidencialidad
- Confidencialidad limitada del flujo del tráfico .

3.1.6.1 Asociaciones de Seguridad

Lo fundamental que aparece en los mecanismos de autentificación y confidencialidad en IP es la Asociación de Seguridad (SA, Security Association), es un componente básico de IPSec. Una asociación es una relación unidireccional entre un emisor y receptor que ofrece servicios de seguridad en los paquetes que transporta, los servicios de seguridad que usa una SA es AH o ESP, pero no los dos.

Las asociaciones de seguridad se mantienen dentro de una base de datos, que se establece en cada dispositivo, una VPN tiene entradas de SA que definen los parámetros de cifrado IPSec, así como también las entrada SA definen los parámetros de intercambio de claves, estos contienen todos los parámetros de seguridad necesarios para transportar de forma segura los paquetes entre los host y definiendo las políticas de seguridad al momento de utilizar IPSec.

Una asociación de seguridad se la identifica por tres parámetros:

Índice de parámetro de Seguridad(SPI): Security Parameters Index es un conjunto de bits asignada a SA y que tiene solo significado local. El SPI se transporta en cabeceras AH y ESP para permitir que el sistema receptor elija la SA con la cual se procesará un paquete recibido.

Dirección IP Destino: Es la dirección del destino final del SA, puede ser un sistema de un usuario final o un sistema de red, por ejemplo un cortafuegos o router.

Identificador del protocolo de seguridad: identifica si la asociación es una asociación de seguridad AH o ESP.

3.1.6.2 Tipos de SA

Existen dos tipos de SA:

Modo de transporte: Este modo trata de una asociación de seguridad entre dos hosts, también se le conoce como IP seguro, protege la carga útil es decir el payload en la capa de transporte, produciendo una comunicación segura de extremo a extremo, por lo que requiere la implementación de IPSec en los dos hosts.

Proporciona protección principalmente a los protocolos de capas superiores, por ejemplo cuando un host ejecuta AH o ESP sobre IPv4, la carga útil consiste en los datos que habitualmente siguen a la cabecera IP y a cualquier cabecera de extensión de IPv6 que esté presente, con la posible excepción de la cabecera de opciones de destino, que se puede incluir en la protección.

Modo Túnel: Proporciona protección al paquete IP completo, después de que se han añadido los campos AH y ESP al paquete IP, el paquete completo más los campos de seguridad se tratan como carga útil de un paquete IP exterior nuevo con una nueva cabecera IP exterior, este paquete viaja a través de un túnel desde un punto de la red IP a otro, ningún router a lo largo del camino puede examinar la cabecera IP interior.

Este modo se usa cuando uno o los dos extremos de una SA es un camino de seguridad, como podría ser un cortafuegos o un router que implementa IPSec. Con el modo túnel, una serie de host en redes, detrás de cortafuegos pueden estar implicados en comunicaciones seguras sin implementar IPSec. Los paquetes no protegidos

generados por dichos host se transmiten por un túnel a través de redes externas por medio de las asociaciones de seguridad en modo túnel.

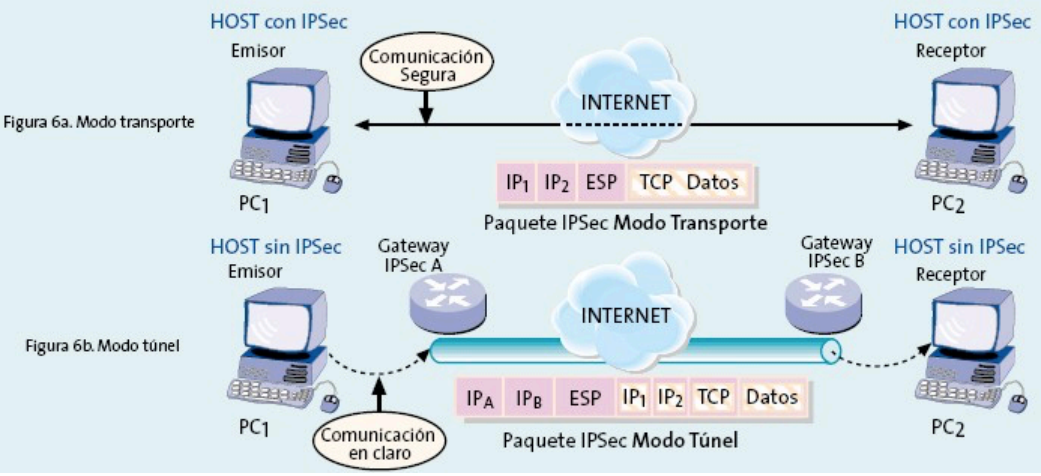

Figura 34 Modo de Transporte y Modo Túnel.

Fuente: (Burton, 2014)

3.1.6.3 Combinación de Asociaciones de Seguridad

Una SA individual puede implementar el protocolo AH o ESP pero no los dos. En ocasiones, un flujo de tráfico particular pedirá los servicios proporcionados por AH y ESP. En este caso , se deben emplear varias SA por el mismo flujo de tráfico con el objetivo de conseguir los servicios IPSec deseados. El grupo de asociaciones de seguridad se refiere a una secuencia de asociaciones a través de las cuáles se debe procesar el tráfico para proporcionar un conjunto de servicios IPSec. Las SA en un grupo puede finalizar en distintos extremos o los mismos. Las asociaciones de seguridad se pueden combinar de dos formas:

Transporte adyacente: Se refiere a la aplicación de más de un protocolo de seguridad al mismo paquete IP, sin invocar el modo túnel. Este enfoque para la combinación de AH y ESP permite un solo nivel de combinación; un mayor grado de anidamiento no produce beneficios adicionales, ya que el procedimiento se realiza en una instancia IPSec: el destino.

Anidamiento de Túneles: se refiere a la aplicación de varias capas de protocolos de seguridad mediante modo túnel IP. Este enfoque permite múltiples niveles de anidamiento, ya que cada túnel puede originarse o terminar en un sitio IPSec diferente a lo largo del recorrido.

Un aspecto interesante que surge al considerar los grupos SA es el orden en el que se pueden aplicar la autentificación o cifrado entre un par dado de los extremos finales y las formas de hacerlo.

3.1.6.4 Gestión de Claves

La gestión de claves en IPSec implica la determinación y distribución de claves secretas. Consta de cuatro claves para la comunicación entre dos aplicaciones: en parejas de transmisión y recepción tanto para AH como para ESP. En la arquitectura de IPSec se asigna soporte para dos tipos de gestión de claves:

Manual: un administrador de sistema configura manualmente cada sistema con sus propias claves y con las claves de otros sistemas que se comunican. Esto es práctico para entornos relativamente pequeños estáticos.

Automática: un sistema automático permite la creación bajo demanda de claves para asociaciones de seguridad y facilita el uso de claves en un sistema distribuido grande con una configuración cambiante.

El protocolo de gestión de claves automático predeterminado para IPSec se conoce como ISAKMP, el cuál especificaremos a continuación:

3.1.7 ISAKMP

Define los formatos y procedimientos de los paquetes para establecer, negociar, modificar y eliminar asociaciones de seguridad, ISAKMP define las cargas útiles para intercambiar la generación de claves y los datos de autentificación, los formatos de las cargas útiles proporciona un marco de trabajo consistente independiente del protocolo

específico de intercambio de claves, del algoritmo de cifrado y del mecanismo de autentificación. (RFC2408, 1998)

ISAKMP tiene dos fases la primera consiste en establecer un canal seguro y autentificado(SA) y el segundo el de negociar parámetros de seguridad (KMP).

En la actualidad existen dos métodos para configurar ISAKMP: el primero es la utilización de las claves previamente compartidas, que son fáciles de configurar. El segundo es la utilización de CA, que es escalable por toda organización.

A continuación una breve explicación de algunos términos en el vocabulario del cifrado.

Advanced Encryption Standard (AES, Norma de cifrado avanzado): es un algoritmo de criptografía que tuvo su autorización de funcionamiento con la finalidad de proteger y perseverar la seguridad en la información de datos informáticos. AES tiene influencia del algoritmo Rijndael, que es un algoritmo que permite utilizar claves que contienen una longitud de bits de 128, 192 o 256. (Cisco, cisco, 2013)

Autenticación: realiza la función desde la parte interna del protocolo IPSec. Estableciendo en la conexión integridad en los datos, los cuales están seguros dando una veracidad que no van hacer manipulados durante la transmisión de los mismos. Proporcionando un acuse de recibo de parte del origen de datos. (Cisco, cisco, 2013)

Certification Authority (CA, Autoridad de certificación): esta entidad cumple una función que es la de emitir los certificados de autoridad. Cada uno de los dispositivos emiten un certificado propio de ellos que los identifica con la CA. (Cisco, cisco, 2013)

Data Encryption Standard (DES , Estándar de cifrado de datos): es un estándar emitido en el año de 1977, diseñado exclusivamente para la tecnología de cifrado de claves el cuál se basa en un algoritmo denominado lucifer de IBM. En los routers de

Cisco es mayormente utilizada este tipo de cifrado que se lo considera como un cifrado clásico con longitudes de 40 y 56 bits. . (Cisco, cisco, 2013)

Hash: esta función es acogida por routers Cisco principalmente al momento de implementar el mecanismo de seguridad IPSec.

3.2 Diseño de la Red.

En este ítem se detallará el diseño de la red mediante la plataforma GNS3, la cual se basa en la implementación de una red IP/MPLS utilizando los IOS de Cisco más apropiados y tomando en consideración que el backbone principal de las telecomunicaciones en el ecuador está implementado con la tecnología MPLS, por lo tanto deben tener las respectivas seguridades garantizando la integridad de las entidades como la de sus usuarios.

Por medio de la simulación se aspira tener un correcto funcionamiento de la red, de tal manera que se pueda evidenciar el respectivo comportamiento de las seguridades, antes que sea implementado en un equipo real. El diseño se fundamenta en los proveedores de servicio que quieran optar por la tecnología de encriptación de datos con sus clientes, con el fin de resguardar la información, manteniendo a salvo de posibles ataques que pueden perjudicar a las entidades.

3.2.1 Cisco IOS a usar en la Red

El IOS (Internetwork Operating System) es un sistema que se utiliza en los dispositivos cisco routers, switches para la implementación de redes y la selección adecuada de cada versión se da de acuerdo a las características que ofrecen cada uno de los equipos, entre ellas IPv6, MPLS , DiffSer, Seguridad, VPNs.

La imágenes de Cisco IOS consta de una parte en donde indica las características y otra que corresponde a la versión, por ejemplo en la siguiente tabla de imágenes Cisco ISO en donde se puede observar la manera de nombrar de acuerdo al grupo de

características, que tiene por finalidad aclarar y simplificar la selección de una de estas imágenes , cada vez que una nueva características es agregada está es heredada por los niveles superiores, podemos ver a continuación algunos de los nombres que se usan :

Tabla 5

Nombres Imágenes Cisco IOS

Nombre	Características
c3700-ipbase-mz	IP Base
c3700-ipvoice-mz	IP Voice
c3700-advsecurity-mz	Advanced Security
c3700-spservices-mz	Service Provider Services
c3700-entbase-mz	Enterprise Base
c3700-advipservices-mz	Advanced IP Services
c3700-entservices-mz	Enterprise Services
c3700-adventerprise-mz	Advanced Enterprise Services

De acuerdo al nombramiento de la imágenes Cisco IOS para nuestra propuesta vamos a utilizar Advanced IP Services por el grupo de características que esta posee.

El número de serie o equipos a utilizar son los siguientes de acuerdo a las características y plataformas que soportan los mismos que se destacan a nivel de capa 2 y de capa 3, el diseño se basa en la configuración de los equipos routers Cisco de Core y Distribución, para esta emulación se tomara en cuenta cinco routers 3725 y dos routers 7200, siendo este un modelo escalable para una red en crecimiento.

3.2.1.1 3725 Imagen Cisco IOS.

El router de la serie 3700 proveen de interfaces de red LAN y WAN, proporcionando puertos de fastEthernet, esta serie permite realizar la encriptación de datos con algoritmos de cifrado, soportando el sistema de gestión de claves, además facilita el despliegue de aplicaciones convergente, proporcionando flexibilidad en la configuración y adaptándose al cambio del entorno.

Otras características importantes del router 3725 son :

- Soporta los principales protocolos de enrutamiento en una red WAN y medios de comunicación.
- Tarjetas de interface WAN.
- Funcionalidades en capa 2 y capa 3.
- Enrutamiento Ipv6

3.2.1.2 7200 Imagen Cisco IOS.

El router de la serie 7200 tienen un gran rendimiento en la QoS, lo que es una opción principal para el despliegue para un proveedor de servicio de última generación. Los servicios WAN gestiona los equipos, transporte y de costos administrativos, con un elevado rendimiento y protección, escalable con una amplia gama de opciones con gran capacidad de gestión en el campo de las comunicaciones.

Características importantes del ruteador 7200 son:

- WAN edge por su alto rendimiento en la calidad de servicio.
- MPLS de última generación.
- Seguridad VPN escalable.
- Flexibilidad soporta fast ethernet , gigabit ethernet, paquetes sobre SONET y más.
- Servicios de hasta 2 Mpps.

3.2.2 Protocolos y configuraciones que se utiliza

Tomando en consideración la plataforma de cisco soporta tres tipos de mecanismos de IP switching:

- Routing table driven switching - process switching: que es una búsqueda completa para cada paquete.
- Cache driven switching – fast switching: Los destinos más recientes se almacenan en cache, el primer paquete se maneja como process switching.
- Topology driven switching : CEF cache (tabla FIB), que soporta la carga por paquete oigen o destino .

3.2.2.1 CEF (Cisco Express Forwarding)

Para que MPLS funcione de manera correcta se debe habilitar primero la conmutación CEF, es una plataforma de los procesos de la conmutación de paquetes transportados por la red a su destino basados en la tabla de enrutamiento. Se basa en la tabla FIB que contiene una completa información de conmutación IP, el ruteador usa la información de esta tabla para los envíos de paquetes, en algunas versiones de cisco IOS CEF ya viene habilitado por defecto.

Para la configuración de CEF se utiliza el siguiente comando:

ip cef [distributed] , este comando inicia el CEF switching y crea la tabla FIB, la palabra distributed es opcional, debido a que esta opción distribuye información a las tarjetas de línea.

3.2.2.2 Configuración MPLS

Para habilitar MPLS, se debe activar obligatoriamente la conmutación CEF, esta depende de la versión de Cisco IOS, dependiendo de las versiones algunas vienen activado por defecto. El protocolo de distribución de etiquetas LDP sobre la interface en la que se utilice para la conmutación.

Opcionalmente, hay varias configuraciones entre las cuales tenemos: MPLS ID, MTU que es el tamaño para paquetes etiquetados, TTL que por defecto se copia en la cabecera IP y se coloca en la etiquetas MPLS cuando el paquete entra en la red, el anuncio condicional de etiquetas. (Cisco, Cisco Systems, 2013)

Para la configuración de MPLS sobre un router es la siguiente:

mpls ldp router-id interface [force]: se especifica en la interface preferida para determinar el LDP router ID.

Tabla 6

MPLS ID

Parámetro	Descripción
interface	Causa que la dirección IP de la interfaz especificada sea usada como ID del router
force	Forzar la utilización de la interfaz como ID del router

mpls ip: habilita label switching en la interface, también inicia LDP en direcciones IPv4.

mpls label protocol [tdp | ldp | both]: selecciona el protocolo de distribución de labels en la interfaz especificada

Tabla 7

MPLS Label Protocol

Parámetro	Descripción
tdp	Habilita el protocolo de distribución tag en la interfaz
ldp	Habilita ldp en la interfaz
both	Habilita tdp y ldp en la interfaz

mpls mtu bytes: la conmutación de etiquetas incrementa el mtu en la interfaz por la cabecera de la etiqueta, el mtu se incrementa automáticamente en las interfaz de la red WAN y se reduce en la redes LAN.

no mpls ip propagate-ttl: por defecto la ip ttl se copia en la etiqueta mpls, el comando deshabilita el comportamiento por defecto e inserta un valor de 255 en la etiqueta, la propagación del campo ttl debe ser deshabilitada en los routers de entrada y salida de los bordes LSRs.

3.2.2.3 Monitoreo MPLS

Se describirá los comandos con las diferentes sintaxis para la verificación de las interfaces, nodos vecinos, las tablas, etiquetas de envío con el propósito de tener un

correcto funcionamiento de la red MPLS, corrigiendo problemas que se encuentre en las interfaces de la red.

En monitoreo de la red MPLS se utiliza los siguientes comandos:

show mpls ldp parameters: muestra los parámetros ldp del router local.

show mpls interfaces : muestra el estado mpls de las interfaces.

show mpls ldp discovery: muestra los vecinos ldp descubiertos.

show mpls ldp neighbor : muestra los vecinos individuales ldp.

show mpls ldp neighbor detail : muestra con mayor detalle sobre los vecinos ldp.

show mpls ldp bindings: muestra la tabla LIB.

show mpls forwarding - table: muestra la tabla LFIB.

show ip cef detail: muestra la etiqueta o etiquetas impuestas a cada paquete durante el proceso de etiquetamiento.

3.2.2.4 Implementación VPNs

La implementación de VPNs se puede ofrecer en base a dos modelos principales:

Overlay VPNs: usa la tecnología X.25, frame relay , atm para el caso de overlay VPNs en capa 2, y generic routing encapsulation (GRE), IPSec y Getvpn para overlay VPNs en capa 3. El proveedor de servicio entrega una conexión punto a punto entre los sites del cliente a través de una infraestructura de red compartida. No interviene en el enrutamiento de la red del cliente en capa 3.

Peer- to-peer VPNs: implementadas con ruteadores y los filtros específicos, con ruteadores independientes por cliente, o con tecnología VPNs de mpls. El proveedor de servicios si interviene en el enrutamiento de la red del cliente.

Las VPNs reemplazan a los circuitos dedicados punto a punto con emulación de enlaces dedicados que comparte una infraestructura común. Los clientes de un proveedor de servicios usan las VPNs para reducir costos.

Unas de las formas de propagación de la información de VPNs es el protocolo dedicado al transporte de rutas del cliente entre los PE routers es BGP, debido a que puede manejar un amplio número de rutas. Evitando la duplicidad de direcciones de subred de los clientes expandiendo los prefijos IP del cliente, obteniendo un único prefijo que haga única a las direcciones IP de los clientes.

Este prefijo es de 64 bits y se llama RD, permite convertir una dirección del cliente de 32 bits en una única dirección del cliente de 96 bits que puede ser transportada entre los PE routers.

RD (Route Distinguishers): es un prefijo de 64 bits usado para hacer la dirección ip única, la dirección ip resultante es la dirección VPNv4 estas direcciones son intercambiadas entre los routers mediante BGP.

El protocolo BGP soporta otras familias de direcciones adicionales a las IPv4 es llamado multiprotocolo IBGP (MP - BGP). Generalmente MPLS VPN es usado dentro de un mismo sistema autónomo por lo que la sesión BGP entre los routers PE es siempre la sesión IBGP.

RT (Route Targets): cuando tienen que participar en algunos sitios más de una VPN el RD no puede identificar esta participación de varias VPNs, por lo que RTs permiten soportar topologías de VPNs complejas, siendo estos atributos adicionales adjuntos a las rutas BGP VPNv4 para indicar la participación de una VPN.

Dentro de BGP se utiliza las comunidades extendidas para codificar estos atributos, cualquier número de RTs puede ser añadidos a una simple ruta.

Export RTs: Identifican la participación en la VPN, añadiendo a la ruta del cliente cuando se convierten en prefijos VPNv4.

Import RTs: Asociados a cada tabla de enrutamiento virtual, selecciona las rutas que se va a insertar dentro de la tabla de enrutamiento virtual.

3.2.2.5 MP- BGP update

Un update de MP – BGP contiene lo siguiente:

- VPNv4 address
- Extended communities (route targets, opcional SOO)
- Etiqueta utilizada para VPN packet forwarding
- Cualquier otro atributo BGP (AS path, local preference, MED, standar community, etc.)

3.2.2.6 Tabla de enrutamiento virtual

Una VRF (Virtual Routing and Forwarding Table) es utilizada para el enrutamiento y envió de información de un grupo de lugares con idénticos requerimientos de seguridad, está asociado con el Route Distinguisher y con los import y export route targets.

Las interfaces VPN pueden ser físicas, subinterfaces e interfaces lógicas que son asignadas a las VRFs, también pueden existir muchas interfaces por VRF, una interfaz puede no pertenecer a VRF alguna sin embargo puede recibir y enviar tráfico correspondiente a múltiples VPNs por la misma interfaz.

3.2.2.7 Configuración VRF

Para la configuración de las VRFs se utiliza los siguientes pasos:

- Crear VRF
- Asignar RD a la VRF
- Especificar export e import route targets
- Configurar el VPN ID (opcional)
- Asignar interfaces a las VRFs
- Configurar enrutamiento estático o dinámico para cada VRF

En la configuración de VRFs se utiliza los siguientes comandos:

ip vrf name : este comando crea un nuevo vrf o entra en la configuración de una vrf ya existente, solo tiene significado local, no está operacional si no se configura RD.

rd route – distinguisher : asigna dentro de la vrf un ruta distinguisher, utilizando estos formatos ASN:nn o A.B.C.D:nn para el RD. Cada VRF en un PE debe tener un RD único.

Detallando export y import RTs:

route-target export RT : especifica un RT que se adjunta a cada ruta exportada desde VRF para MP-BGP.

route-target import RT : especifica un RT para ser utilizado como un filtro de rutas importados desde la VRF .

route-target both RT: en los casos que la exportación coincide con la importación, se puede utilizar la ruta de destino para simplificar la configuración.

3.2.2.8 VPN ID

Permite identificar a la VPN con un número, pero no es utilizado para la distribución de información de ruteo. Tiene los siguientes elementos:

OUI (3 octetos en hexadecimal)

VPN index (4 octetos en hexadecimal)

Debe ser único

3.2.2.9 Configuración VPN IDs

ip vrf vrf – name: este comando crea una tabla de enrutamiento VRF y una tabla de reenvió CEF, y entra en el modo de configuración VRF.

vpn id oui:vpn-index: asigna el identificador de VPN a la VRF.

Asignando una tabla VRF a una interfaz

La asignación se lo realiza con los siguientes comandos:

ip vrf forwarding vrf-name: asocia una interfaz con el vrf especificado, la conmutación CEF debe estar habilitado en la interfaz.

Para en ruteo estático en la vpn se utiliza el siguiente comando:
ip route vrf gabo 10.0.0.0 255.255.255.252 fastethernet0/0 1.1.1.1 name cliente.

3.2.2.10 Configuración BGP

Se trata de observar el proceso de BGP en una red MPLS, habilitando una VPN, con los pasos y comandos que se utilizan con sus respectivas descripciones, debido a que la mayor parte de la configuración de una MPLS VPN depende de cómo se realiza la configuración en los routers de borde del proveedor.

El proceso BGP en un router implementado MPLS VPN realiza tres tareas independientes:

- Global BGP routers (enrutamiento de internet) son intercambiadas de acuerdo al funcionamiento tradicional de BGP.
- Los prefijos VPNv4 son intercambiados a través de MP- BGP.
- Las rutas de cada VPN pueden ser intercambiadas con los routers de los clientes CE a través de EBGP (External Border Gateway Protocol), pero puedn usarse otros protocolos de enrutamiento hacia el cliente y realizar distribución hacia BGP dentro de la vrf y viceversa.

Comandos para BGP address families:

router bgp as-number: habilita el proceso global de BGP identificando su sistemas autónomo.
address-family vpnv4: configura el intercambio de prefijos VPNv4 en las sesiones de MP-BGP.
address-family ipv4 vrf vrf-name: configura los parámetros de ruteo EBGP para cada VRF

Tabla 8

BGP Address Families

Parámetro	Descripción
as-number	Muestra el número de sistema autónomo que identifica al router o a otros routers BGP etiqueta la información de enrutamiento.
ipv4	Configura las sesiones que llevan los prefijos de las direcciones ipv4 estándar.
vpnv4	Configura los prefijos VPNv4 de clientes, mediante la adición de una RD de 8 bytes.
unicast	Opcional especifica los prefijos unicast
vrf vrf-name	Especifica el nombre de una VPN VRF asociada al submodo de comando.

3.2.2.11 Configuración BGP vecinos y MP-BGP

Los vecinos MP-BGP se configuran bajo el proceso de enrutamiento BGP, los vecinos necesitan estar activados por cada familia de direcciones globales que ellos apoyan, los parámetros de la familia pueden ser configurados para los vecinos.

Para la configuración de MP-IBGP tenemos:

router bgp as-number

neighbor ip-address remote-as as-number

neighbor ip-address update-source interface-type

interface number

Se deben configurar todos los vecinos MP-BGP (PE routers o route-reflectors), estableciendo las sesiones MP-IBGP entre las direcciones de las interfaces de loopback.

address-family vpnv4: el comando inicia la configuración de enrutamiento MP-BGP para el intercambio de la ruta VPNv4.

neighbor ip-address activate: el vecino bgp debe ser activado dentro del address family para el intercambio de prefijos VPNv4.

neighbor ip-address next-hop-self : es recomendable si se está usando EBGP hacia el cliente.

neighbor ip-address send-community [standard | extended | both]: este comando con la opción extendida está activado de forma predeterminada por el

software Cisco IOS después de que los vecinos BGP tengan activado el cambio de rutas VPNv4.

no bgp default ipv4-unicast: el intercambio de rutas IPv4 entre vecinos BGP está habilitado por defecto, todos los vecinos configurados también recibirán rutas IPv4, este comando desactiva el intercambio predeterminado de IPv4, trabaja en conjunto con la opción activate para cada vecino dentro de los address-family ipv4 y vpnv4.

3.2.2.12 Monitoreo VRFs

Se describirá los comandos con las diferentes sintaxis para la verificación del enrutamiento virtual VRF, para asegurarse el correcto funcionamiento de la red y si hay problemas solucionarlo de una manera eficaz.

Comandos que supervisan la información VRF:

show ip vrf : muestra la lista de todas las VRFs configuradas en el router.

show ip vrf detail : muestra una configuración detallada de las VRFs.

show ip vrf interfaces : muestra las interfaces asociadas a las VRFs.

3.2.2.13 Monitoreo VRF routing

Comandos que supervisan la información VRF routing :

show ip protocols vrf vrf-name : muestra los protocolos de enrutamiento configurados en una VRF.

show ip route vrf vrf-name : muestra la tabla de enrutamiento VRF.

show ip bgp vpnv4 vrf : muestra la tabla VRF de BGP.

3.2.2.14 Monitoreo MP-BGP

Comandos que supervisan la información MP-BGP de sus vecinos :

show ip bgp neighbors: el comando muestra los vecinos BGP globales y los protocolos que existen entre los vecinos, también se utiliza para las sesiones BGP con los routers PE.

show ip bgp vpnv4 all : muestra toda la tabla VPNv4

show ip bgp vpnv4 vrf vrf-name : muestra los parámetros BGP asociados con la VRF especificada, cualquier comando show bgp puede ser utilizado con estos parámetros.

show ip bgp vpnv4 rd route-distinguisher : muestra los parámetros BGP asociados con la RD especificado.

3.2.2.15 Configuración de OSPF

Esta configuración del protocolo de enrutamiento se da entre los routers PE y CE, que son necesarios cuando se está ejecutando Open Shortest Path Firts (OSPF), este protocolo de enrutamiento no solo se puede utilizar entre el proveedor y el acceso de los clientes, también cuando se está desarrollando bajo el entorno de conmutación de etiquetas multiprotocolo (MPLS) con VPNs.

OSPF divide a la red en áreas, que pueden corresponder a los sitios individuales desde la perspectiva MPLS VPN.

Para la configuración de OSPF primero se necesita tener configurado VRF con copia de OSPF con la redistribución en MP-BGP, antes de iniciar el proceso es necesario un OSPF separado para cada enrutamiento virtual.

router ospf process-id vrf vrf-name: este comando inicia el proceso de enrutamiento OSPF per-VRF, el número limitado de proceso de enrutamiento es 32 por enrutador.

redistribute bgp as-number subnets: realiza la distribución de las rutas MP-BGP en OSPF mientras que la palabra subnets es obligatoria para el correcto funcionamiento.

router bgp as-number

address-family ipv4 vrf vrf-name

redistribute ospf process-id

La ruta de distribución se debe configurar con el comando redistribute bajo al comando adecuado de address-family.

3.2.2.16 Configuración de RIP

Esta configuración del protocolo de enrutamiento se da entre los routers PE y CE, los parámetros de RIP tienen que ser especificados en la VRF, solo existe la versión 2 del protocolo de enrutamiento.

router rip

version 2

address-family ipv4 vrf vrf-name

redistribute bgp as-number metric transparent

Las rutas BGP deben ser redistribuidas en RIP, las métricas deben ajustarse manualmente cuando el protocolo RIP se lo utiliza con otros protocolos.

3.2.2.17 Características de Advanced VRF

Es muy importante como ajustar con precisión de la conmutación de etiquetas en la red privada virtual que mejorarán el funcionamiento de la red, para esto VRF tiene las siguientes funciones.

Selective import : permite especificar que rutas son importadas dentro de la VRF, para la configuración se utiliza el siguiente comando

import map route-map : este comando se conecta con el mapa de la ruta realizando el proceso de importación de VRF.

Selective export: permite añadir RT a rutas exportadas.

export map name : este comando se conecta con el mapa de la ruta realizando el proceso de exportación de VRF, todas las rutas exportadas siempre reciben RT configuradas con el comando route-target export.

VRF route limit : permite limitar el número máximo de rutas importadas en una VRF previniendo el consumo de memoria o evitar un ataque DOS.

3.2.3 MPLS con IPv6

Los proveedores de servicios que ya han implementado MPLS en su red o que quieren hacerlo pueden tener los siguientes beneficios con la implementación de 6PE:

- Mínimo costo de operación y riesgo.
- Sin impactos sobre los servicios existentes en IPv4 con MPLS.
- Tienen la necesidad de hacer mejoras solo en los ruteadores de borde.
- Un ruteador 6PE puede ser un router existente PE o uno nuevo dedicado para tráfico IPv6 y se puede agregar en cualquier momento a la red.
- Sin necesidad de cambios en los routers de borde para IPv6.
- El ISP puede conectarse hacia el cliente con ruteo estático o dinámico.

El plano de envió en MPLS se da cuando un paquete IPv6 llega al router PE de ingreso, el cuál realiza una observación en su FIB de IPv6 y se encuentra que se debe agregar dos etiquetas que ayude atravesar la nube MPLS y llegar al destino. Siendo la etiqueta externa la etiqueta de IPv4 que identifica al router 6PE de salida, mientras que la etiqueta interna es la Aggregate IPv6.

En el router 6PE de salida la etiqueta Aggregate IPv6 es usada para hacer una inspección en la LFIB que instruye al router que haga un POP de la etiqueta y la tabla FIB de IPv6.

3.2.3.1 Comandos IPv6 en MPLS-6PE

Estos son algunos de los comando utilizados en IPv6, tienen el mismo significado que en IPv4 estos son utilizados en MPLS, así como también en los diferentes protocolos de enrutamiento, IPv6 también se puede configurar las diferentes VPNs con las respectivas VRFs.

Los comandos serán mostrados en la siguiente figura:

```
ipv6 unicast-routing
ipv6 cef
!
interface Loopback60
 no ip address
 ipv6 address 2001:60::1/48
!
!
interface FastEthernet0/1.60
 encapsulation dot1Q 60
 no snmp trap link-status
 ipv6 address 2001:1::2/64
!
!
address-family ipv6
 neighbor 2001:1::1 activate
 neighbor 2001:1::1 send-community both
 neighbor 2001:1::1 soft-reconfiguration inbound
 network 2001:60::/48
 network 2001:61::/48
 no synchronization
 exit-address-family
!
!
ipv6 route 2001:6::/64 2001:7::1
ipv6 route 2001:66::/48 2001:7::1
```

Figura 35 Comandos IPv6.
Fuente: Autor

3.2.4 Implementaciones de Seguridad.

En la actualidad las implementaciones de seguridad son de suma importancia en las empresas u organizaciones, la información es lo más importante que debe salvaguardar de sus usuarios, para lo cual las VPNs son una manera de realizar esta comunicación

segura , tenemos mecanismos que nos permiten realizar estas conexiones, entre las cuales tenemos:

- GRE (Generic Routing Encapsulation)
- IPSec (IP Security)
- GETVPN (Group Encrypted Transport VPN)

En este ítem se trata de describir de una manera generalizada la configuración o los pasos a seguir para la implementación de las seguridades basadas en VPNs para luego hacer una comparación entre dos de ellas.

3.2.4.1 Implementación de GRE

La creación de túneles VPN GRE es considerado como uno de los principales mecanismo de transición, siendo este un protocolo que permite encapsular una variada cantidad de protocolos diferentes dentro de túneles IP, originando una red entre dos puntos está definido por RFC 1701, 1702 y 2784.

GRE puede encapsular cualquier tipo de paquete, utilizando IP para crear un enlace virtual punto a punto entre los routers Cisco, soportando multiprotocolo y un túnel de multidifusión IP, siendo el más adecuado para redes VPN multiprotocolo de sitio a sitio.

GRE funciona tomado un paquete existente con el encabezado en capa de red y agrega un segundo encabezado en la misma capa de red, lo que significa que el paquete que se envía por el túnel es de mayor longitud por lo que puede generar un problema excediendo su longitud, provocando una eliminación del paquete, la forma de superar este inconveniente es la aplicación del comando ip tcp adjust-mss 1436 en la interfaz del túnel. Otro percance que puede producirse es que un extremo del túnel esta up y el otro down, para que esto no suceda se habilita la opción de keepalive en cada extremo del túnel.

Configuración GRE

A continuación se detalla los comando para la configuración de GRE:

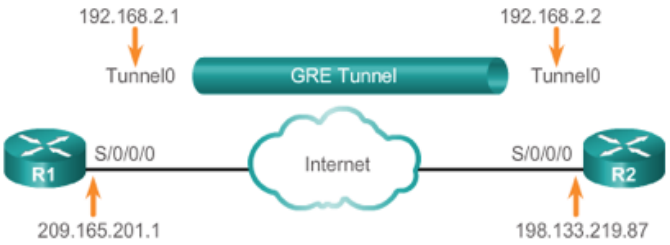

Figura 36 GRE Túnel.

Fuente: (Cisco, Cisco systems, 2009)

- Primero se crea la interface del túnel.
- Asigna el túnel de una dirección IP.
- Identificar la fuente del interfaz del túnel.
- Identificar el destino del túnel.
- Opcional identificar el protocolo para encapsular en el túnel GRE.

CE1:

```
CE1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CE1(config)#interface Tunnel0
CE1(config-if)# ip address 172.16.100.2 255.255.255.252
CE1(config-if)# tunnel source 10.200.200.2
CE1(config-if)# tunnel destination 10.200.200.10
```

Figura 37 Comandos Túnel CE1.

CE2:

```
CE2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CE2(config)#interface Tunnel0
CE2(config-if)# ip address 172.16.100.1 255.255.255.252
CE2(config-if)# tunnel source 10.200.200.10
CE2(config-if)# tunnel destination 10.200.200.2
```

Figura 38 Comandos Túnel CE2.

Monitoreo GRE

A continuación se detalla los comando para la verificación del túnel :

show ip interface brief | include tunnel: nos permite ver la interfaz del túnel si se encuentra en up.

show interface Tunnel 0: podemos observar la dirección ip fuente y de destino.

show ip ospf neighbor: verifica la adyacencia de OSPF del túnel GRE.

3.2.4.2 Implementación de IPSec

Una IPSec VPN puede asegurar la protección de todo el tráfico IP unicast dentro de ella. No puede reenviar el tráfico de difusión o multidifusión, por lo tanto se compone de varios elementos de configuración entre las cuales tenemos:

- Crear una política de ISAKMP(IKE) identificando las características específicas para el intercambio de claves y parámetros de seguridad inicial.
- Los detalles que posee IPSec definen como se encapsula el paquete IP.
- La información del túnel VPN se identifica en un mapa criptográfico llamado crypto map que combina las políticas ISAKMP, con IPSec detail, las direcciones y el crypto ACL.
- El crypto ACL identifica el tráfico que activara el túnel, este componente a veces se debe ajustar cuando se implementa en conjunto con otros servicios como NAT y GRE .
- El crypto map se aplica a la interfaz del túnel.

Esta implementación utiliza con un security Gateway, mediante este proporciona protección en el tráfico de paquetes IP. La protección que ofrece es de acuerdo a requerimientos definidos en una base de datos de políticas de seguridad, mantenidas por el administrador o usuario del sistema.

En la siguiente figura observaremos la configuración de IPSec VPN.

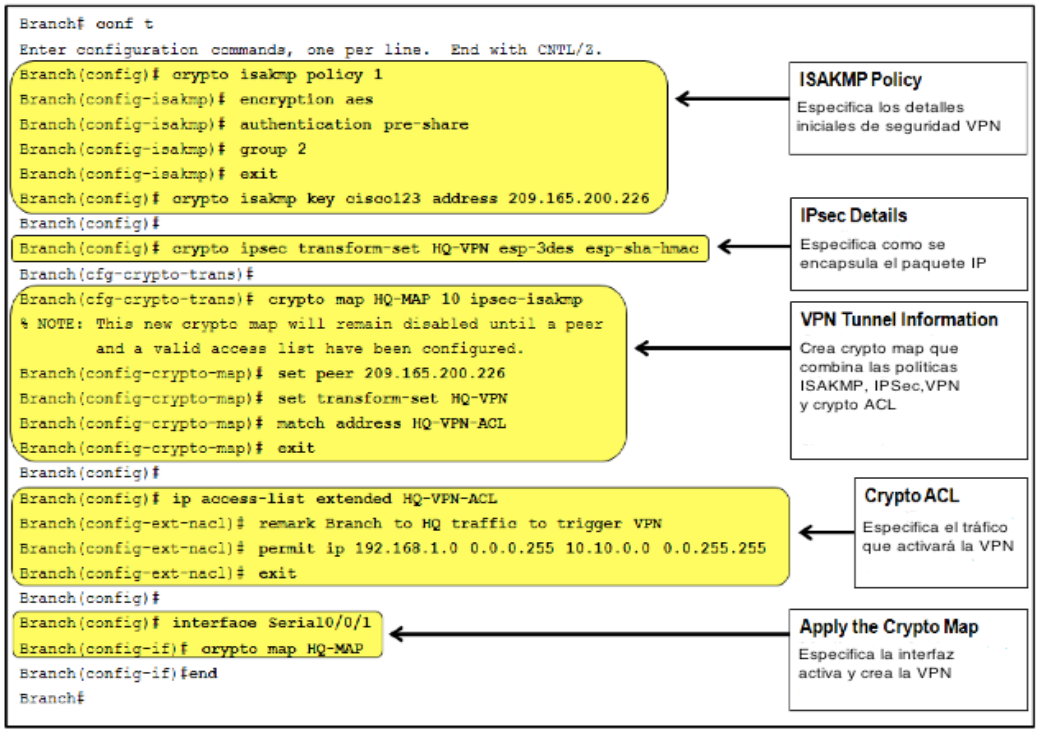

Figura 39 Comandos IPSec.

Algunos de los comando para verificación de IPSec son:

show crypto sesión detail: el cual permite observar si la sesión esta up, con la dirección IP con la que se realizó el IPSec.

3.2.4.3 Implementación de GETVPN

Es un modelo de seguridad basado en estándares, basada en los miembros de confianza, utilizando la metodología de seguridad común que es independiente de cualquier relación de túnel punto a punto, por lo que es altamente escalable manteniendo las características de la red. Se describirá la configuración básica y la verificación de los componentes que posee GETVPN.

- Los Key servers (KSs) y los miembros del grupo (GMs)
- Una pre llave compartida (PSK) y la infraestructura de clave pública (PKI)
- Unicast y Multicast rekey
- Cooperative (COOP) KSS

Configuración KS: Para la configuración de KS se debe tener toda la conectividad, las rutas por defecto con los protocolos de enrutamiento respectivos con una red funcional para proceder con la configuración.

Para la configuración básica de un KS debe incluir lo siguiente :

- IKE Policy: IKE es un mecanismo de autentificación cuando GM es registrado
- IPSec Policies : Se define las políticas utilizadas para asegurar el tráfico de datos (algoritmo de cifrado, paquetes de autentificación, etc).
- Clasificación del Tráfico ACL: determina que tráfico debe ser cifrado ¨ permit any any ¨ en GETVPN, teniendo cuidado en excluir el tráfico crítico.

IKE Policy

La configuración es la siguiente:

```
crypto isakmp policy 5
 encr aes 256
 authentication pre-share
 group 14
 lifetime 8000
crypto isakmp key gabocisco address 10.200.200.10
crypto isakmp key gabocisco address 10.200.200.2
```

Figura 40 IKE Policy.

IPSec Policies

```
crypto ipsec transform-set GABO esp-aes esp-sha-hmac
 mode tunnel
!
crypto ipsec profile VPNProfile
 set security-association lifetime seconds 7200
 set transform-set GABO
```

Figura 41 IPSec Policies.

GDOI Group: Antes de esta configuración KS, generan las claves RSA que se usan durante las rekeys.

crypto key generate rsa general-keys label getvpn-export-general modulus 1024 exportable

Unicast rekey : Se establece una entidad para el grupo de getvpn 1234, también se define las políticas para ser distribuidas utilizando la lista de acceso 199, otra generación de claves se envían a través del mecanismo de transporte con retransmisiones con intervalos de 10 segundos .

```
crypto gdoi group Secure
 identity number 50
 server local
  ! Incomplete unicast rekey configuration
  ! Rekey authentication is not configured
  rekey retransmit 40 number 2
  rekey transport unicast
  sa ipsec 1
   ! Incomplete
   ! Match address is not configured
   profile VPNProfile
   match address ipv4 Secure
   replay counter window-size 64
  address ipv4 10.0.1.2
```

Figura 42 Unicast Rekey .

Acces list policies

Getvpn es compatible con las claves simétricas como también asimétricas.

De manera simétrica :

permit ip any any

permit ip 10/8 10/8

De manera asimétrica :

permit ip 10/8 any

access-list 199 permit ip 10.1.0.0 0.0.255.255

Cooperative (COOPS) KSS: Antes de la implementación se debe tener en consideración la generación de claves RSA en los KS y exportar las claves privadas y públicas para toda la COOPS, keepalive periódica en ISAKMP para realizar un seguimiento todas estas configuraciones se las realiza de forma manual.

Los comando son:

crypto key export rsa getvpn-export-general pem terminal 3des passphrase

crypto key import rsa getvpn-export-general exportable terminal passphrase

3.3 Emulación y diseño de la Solución Propuesta.

Con lo mencionado y descrito anteriormente, desarrollada la implementación que se basa en la configuración de routers cisco de Core y distribución, haciendo énfasis en la seguridad a nivel de capa 3, dando a conocer el nivel de seguridad que cada cliente puede exigir a su proveedor de servicios. En vista que los ataques a la red son más comunes, obteniendo información sumamente importante y causando un desajuste en el funcionamiento de toda empresa.

Siempre tomando en consideración que una red IP/MPLS es la más utilizada en los proveedores de servicio y en la cual se puede hacer uso de la implementación de VPNs, además de ser una red que se adapta muy bien al constante crecimiento, sin perder las características y beneficios que esta posee.

En la siguiente figura se representa el diagrama general en la cual se desarrollara el análisis de seguridad, dando a conocer el respectivo funcionamiento con los protocolos utilizados, así como las configuraciones que se realizaron en cada uno de los routers con las respectivas direcciones IP.

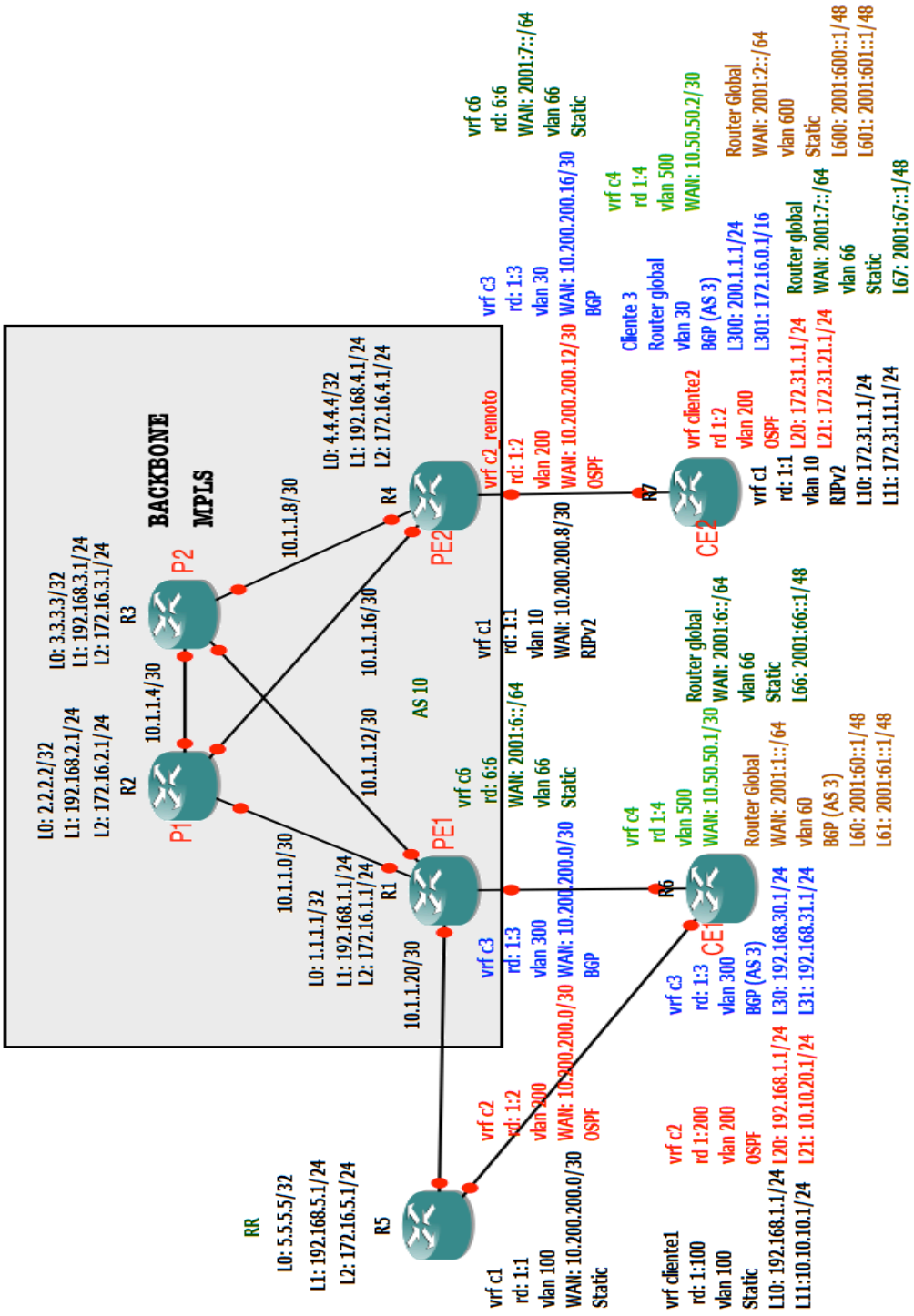

Figura 43 Solución Propuesta.

En la siguiente tabla se detalla la distribución de cada uno de los equipos

Tabla 9

Distribución MPLS.

Nivel	Equipos
Core	R1 = PE1 R2 = P1 R3 = P2 R4 = PE2
Distribución	R6 = CE1 R7 = CE2
Reflector	R5 = RR

Los componentes del proyecto fueron escogidos de acuerdo a consultas realizadas y características de proveedores de servicio, tomando en cuenta una mínima muestra del diseño de red de un proveedor de servicio de internet que es muy semejante a la realidad, por lo que se consideró los siguientes componentes:

3.3.1 Backbone MPLS implementado

En el backbone MPLS está compuesto por equipos activos que soportan gran cantidad de tráfico, los cuales son cuatro routers de Core, tres de ellos son Cisco de la serie 3725 y uno de la serie 7200, que se encuentran conectados entre sí de una manera mallada para que puedan escoger varios caminos al momento de la transmisión de información. Siendo estos también agregadores de rutas MPLS para todas las conexiones que se encuentran dentro del backbone esta infraestructura dependerá del proveedor de servicio.

Estos routers son los encargados de recoger el tráfico que se transportará a todos los lugares, siendo una jerarquía de primer nivel al mismo tiempo siendo quienes transfieran a una jerarquía de segundo nivel en donde se encuentran todas las rutas y equipos a otros equipos.

Debido a estos equipos que son agregadores de rutas, que cumplen su función agregando el tráfico que llega a los diferentes nodos de acceso en la red en el primer nivel y enviando a los demás equipos con jerarquías superiores. También efectúan trabajos de conmutación de diferentes servicios y escenarios utilizando VLANS.

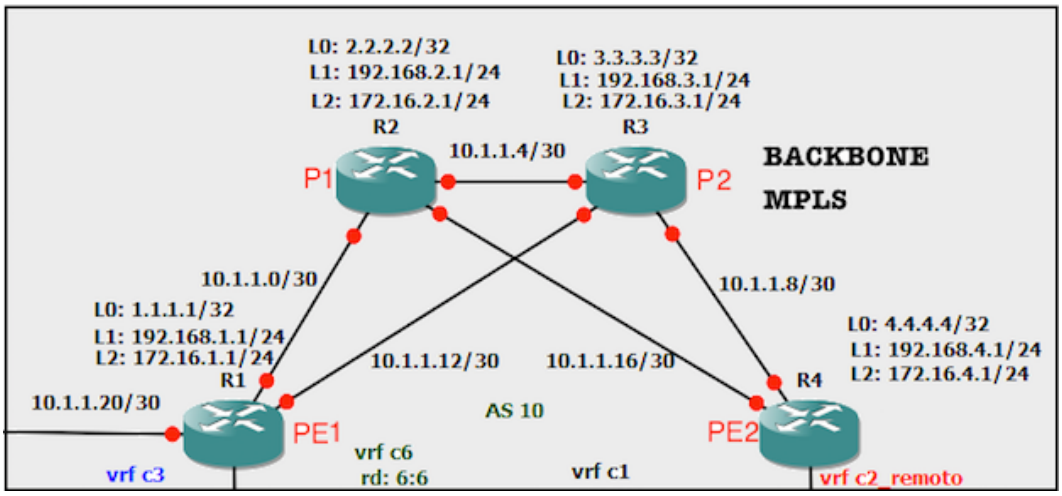

Figura 44 Backbone MPLS.

Fuente: Autor

Lo que se utilizó en el procedimiento para la implementación del backbone MPLS se describe a continuación:

1 Paso : Diseño del backbone

2 Paso : Loopbacks globales

3 Paso : Direcciones WAN

4 Paso : Conexión Lógica

5 Paso : Comprobación de la conexión

6 Paso : Configuración de MPLS

7 Paso : Monitoreo de MPLS

8 Paso : Configuración de enrutamiento OSPF

9 Paso: Configuración MP-BGP

10 Paso : Configuración VRFs

11 Paso : Configuración de VLANS en PE

12 Paso : Configuración de enrutamiento entre PE y CE

13 Paso : Configuración del protocolo RIPv2 en PE

14 Paso : Monitoreo de verificación

3.3.2 CE y RR implementado

Está compuesto por los equipos activos, que soportan gran cantidad de tráfico, como CE tenemos dos routers de la serie 3725 y el Route Reflector es un router de la serie 7200, los cuales se encuentran conectados al backbone MPLS, los CE se encuentran intercambiando rutas con las VRFs correspondientes , encargada de recibir el tráfico, se utiliza en la creación de VLANS.

Ya que las direcciones de las interfaces loopback hacen exportaciones hacia la VPN del servidor, el route reflector se utiliza para ver las actualizaciones compartiendo información con sus vecinos, haciendo un intercambio de rutas con los otros clientes, ayuda al ahorro de recursos en la red.

Una característica del route reflector es que pueden reenviar mensajes recibidos por BGP a otros vecinos BGP, mientras que para los routers de los clientes no lo pueden hacer.

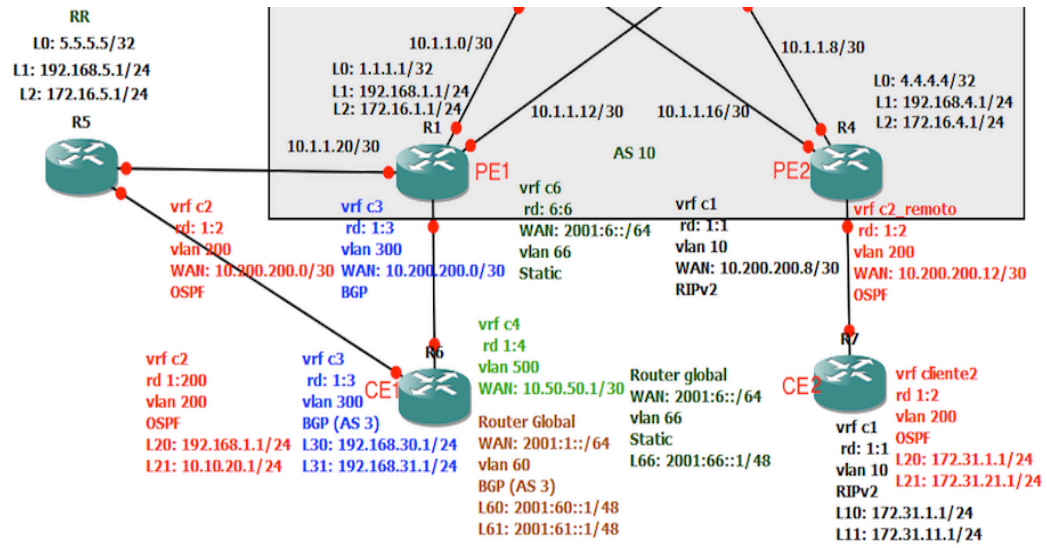

Figura 45 CE Y RR.

Lo que se produjo en la implementación de los routers CE y RR se describe a continuación:

1 Paso : Loopbacks globales

2 Paso : Configuración VRFs

3 Paso : Direcciones WAN

4 Paso : Configuración de enrutamiento OSPF

5 Paso : Configuración MP-BGP

6 Paso : Configuración de VLANS

7 Paso : Configuración del protocolo RIPv2 en CE

8 Paso : Monitoreo de verificación

9 Paso : Configuración de MPLS en RR

10 Paso : Monitoreo de MPLS en RR

Una vez terminado la configuración e implementación del Backbone MPLS con los respetivos routers CE y RR, verificada la conectividad entre todos los enlaces, se procederá con la evaluación de seguridad descritas en el proyecto las cuales son las siguientes:

- Implementación de IPSec.
- Implementación de GETVPN.
- Pruebas de Pentesting con Kali.

CAPÍTULO 4

PRUEBAS Y RESULTADOS

4.1 Análisis de la Red MPLS

4.1.1 Análisis Backbone MPLS

Las pruebas se las realizó utilizando el ping extendido, debido a sus ventajas las cuales son: fragmentación, IP de destino, número de paquetes, tamaño de paquetes, tiempo de respuesta, obteniendo un control avanzado de alcance y conectividad con la red, este da como resultado la medición de la latencia.

El backbone MPLS que está compuesto por los routers P1,P2 ,PE1 y PE2 en este escenario se va a desarrollar pruebas de conexión recolectando datos de la latencia en esta topología, y por qué es una de las más utilizadas en la actualidad a continuación se muestra los elementos involucrados en los cuales se procederá a realizar dicha prueba además de una tabla en donde se encuentra el direccionamiento de la red WAN.

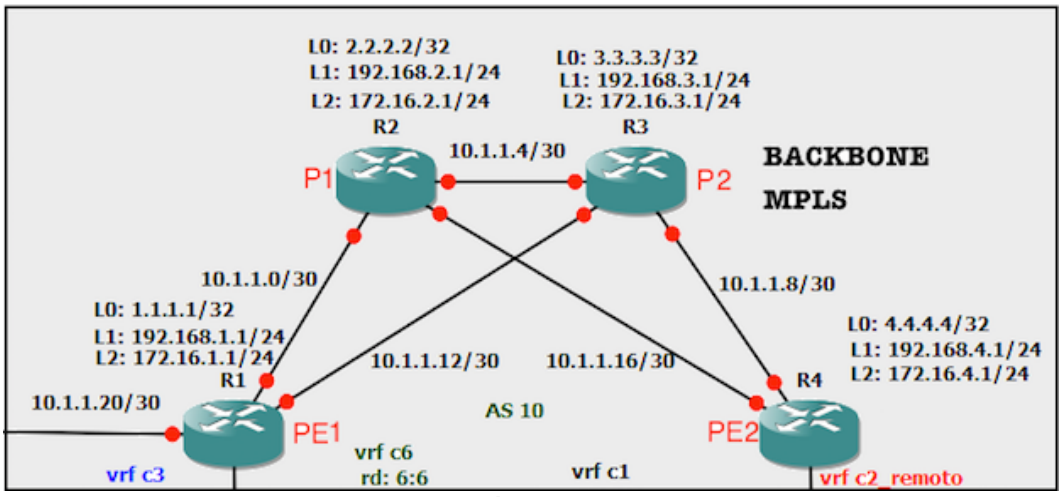

Figura 46 Topología Backbone para pruebas.

Fuente: Autor

En la siguiente tabla se puede observar el planteamiento IP, asignado a cada uno de los routers de la red IP/MPLS, correspondiente a la clase A que es privada, con una

máscara de 30 debido a que se realizó el subnetting de tamaño variable VLSM, está máscara es muy utilizada en el levantamiento de pares de equipos , también se crearon loopbacks que son muy útiles al momento de monitorear o administrar el dispositivo, normalmente usadas para levantar adyacencias, utilizando máscara de 24 sirve para realizar modificaciones mientras que la máscara de 32 son utilizadas en monitoreo punto a punto , siempre y cuando esta sea única sin ser utilizada o configurada en otra interfaz.

Tabla 10

Distribución IP MPLS.

Router	Interface	Red WAN	IP Origen	Loopback
R1=PE1	F0/0 F1/0	10.1.1.0/30 10.1.1.14/30	10.1.1.2/30 10.1.1.12/30	L0:1.1.1.1/32 L1:192.168.1.1/24 L2:172.16.1.1/24
R2=P1	F0/0 F0/1 F1/0	10.1.1.0/30 10.1.1.4/30 10.1.1.16/30	10.1.1.1/30 10.1.1.5/30 10.1.1.17/30	L0:2.2.2.2/32 L1:192.168.2.1/24 L2:172.16.2.1/24
R3=P2	F0/0 F0/1 F1/0	10.1.1.4/30 10.1.1.8/30 10.1.1.12/30	10.1.1.6/30 10.1.1.9/30 10.1.1.13/30	L0:3.3.3.3/32 L1:192.168.3.1/24 L2:172.16.3.1/24
R4=PE2	F0/0 F1/0	10.1.1.8/30 10.1.1.16/30	10.1.1.10/30 10.1.1.18/30	L0:4.4.4.4/32 L1:192.168.4.1/24 L2:172.16.4.1/24

Para medir la eficacia de la red realizaremos las siguientes pruebas que constan: la primera es la constatación de una red robusta y eficaz que todos los paquetes enviados atreves de ella lleguen sin pérdidas, la segunda trata de ver las tramas de transmisión con capturas de tráfico, y los protocolos que se utiliza en dicha red.

Se tomarán las muestras, enviando diferentes tamaños de archivos o paquetes, con el fin de ver la latencia que existe, siendo este un valor de suma importancia para el rendimiento con la taza de transferencia de datos, comprobando también la calidad de servicio al observar que en ningún momento se perdió la conexión por lo tanto todos los paquetes enviados fueron satisfactorios.

En la topología de la figura 39 que es el backbone las pruebas se las realizará en los extremos de los routers, los cuales son PE1 y PE2, el modo en el que se realiza la prueba es con el fin de constatar el perfecto funcionamiento de la red MPLS

especialmente en el área del core de comunicaciones que es la emulación de una red WAN IP/MPLS.

En la siguiente tabla se observa resultados de la emulación realizada con diferente cantidad de archivos y el tiempo en que tarda en generar dicha acción:

Tabla 11

Datos de Latencia Red MPLS.

Cantidad Archivos	Latencia(ms) mínima	media	máxima	Tiempo
1MB	6	34	148	00:00:16
3MB	4	35	180	00:00:49
5MB	4	35	188	00:01:20
7MB	4	35	228	00:01:51
10MB	4	36	244	00:02:37

La Latencia que suele darse en redes WAN son variadas, el correcto funcionamiento sin que se produzca problemas es de máximo 380 ms, como podemos mirar en la siguiente gráfica los rangos de las pruebas realizadas se encuentran en un rango aceptable. Al momento del realizar las pruebas toda la cantidad de paquetes enviados, no tuvieron pérdidas en la transmisión.

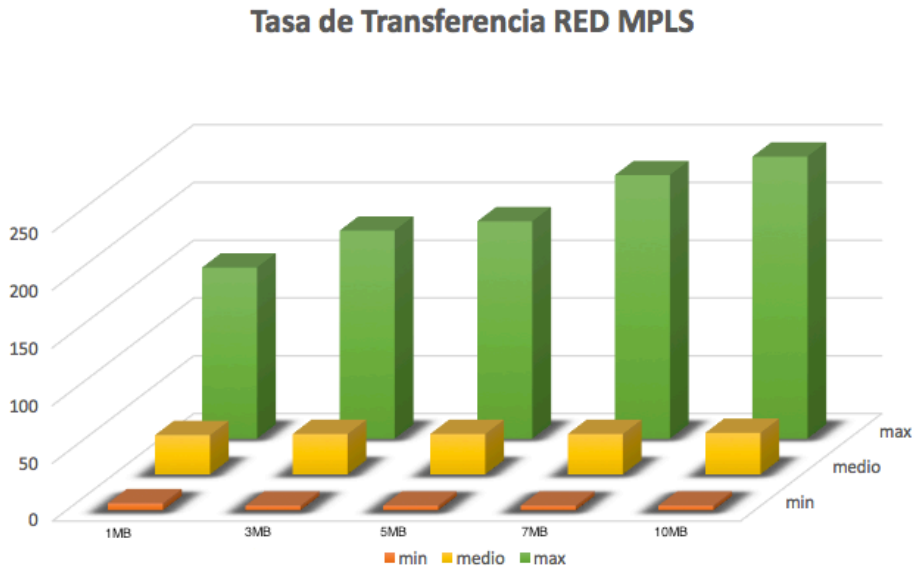

Figura 47 Tasa de Transferencia Red Mpls.

Utilizando la capacidad para la captura de tramas en GNS3, que atraviesan de un router a otro, se muestra una captura de tráfico realizado con Wireshark en donde se observará como los paquetes fueron enviados desde la dirección de origen hasta la dirección de destino, observando la transmisión y recepción de paquetes ICMP.

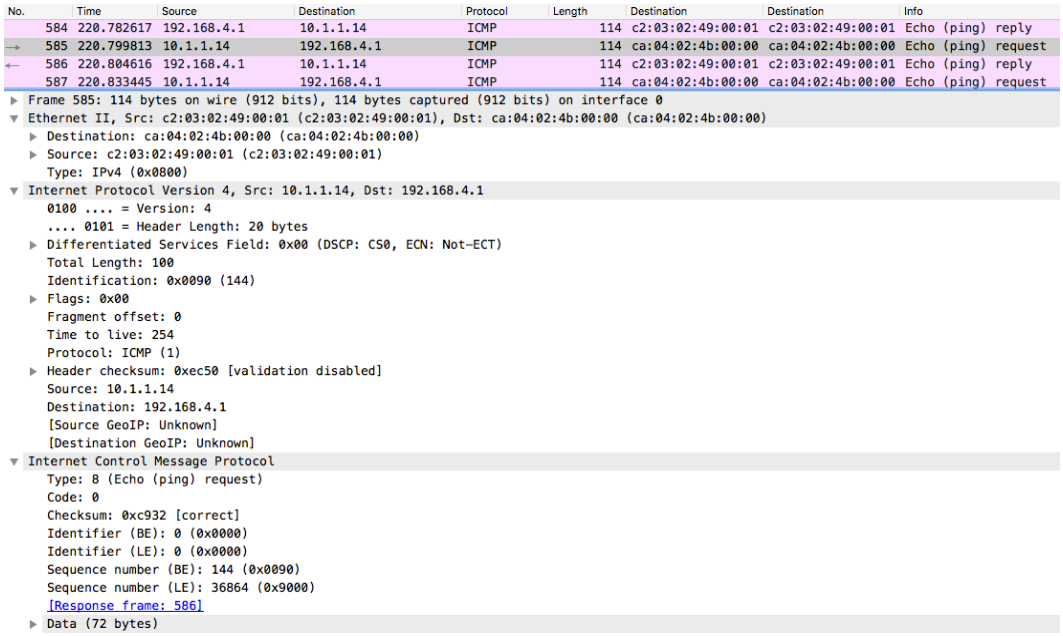

Figura 48 Captura de Tráfico MPLS .

A modo de autentificación de las configuraciones realizadas en la propuesta implementada, se visualizará la comunicación entre los protocolos de enrutamiento utilizados, así también se puede observar que ruta tomo al momento del envío de paquetes, escogiendo siempre el camino más óptimo y adecuado.

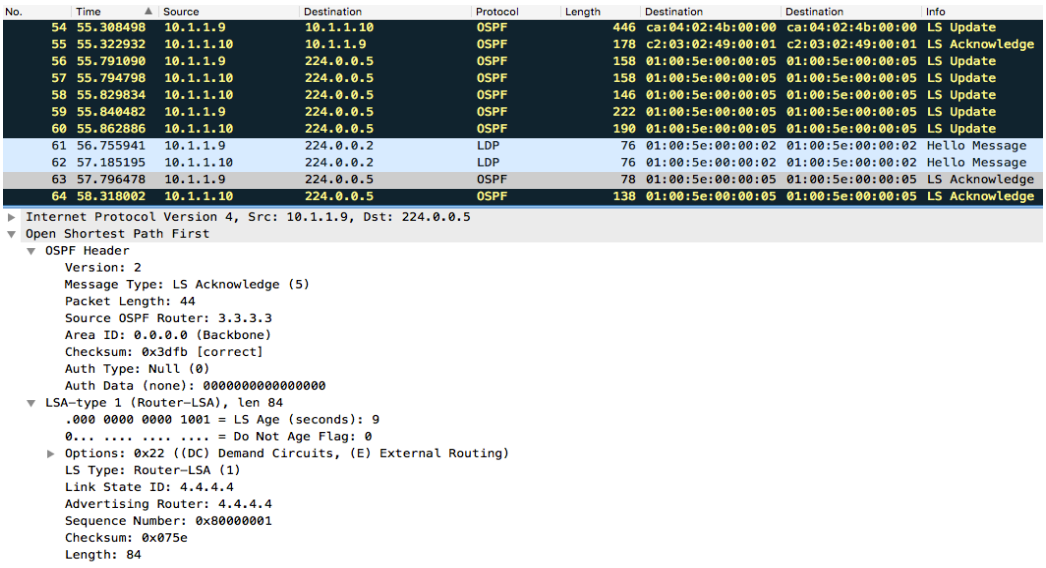

Figura 49 Captura de Tráfico del Protocolo .

Con la captura del tráfico realizado se confirma la ruta por la cual los paquetes fueron enviados, en vista que se envió un ping a una de las loopbacks del router PE2, específicamente a la dirección 192.168.4.1, en la siguiente figura se puede observar la ruta que tomo para llegar a su destino y la importancia que es tener los dispositivos con una red mallada.

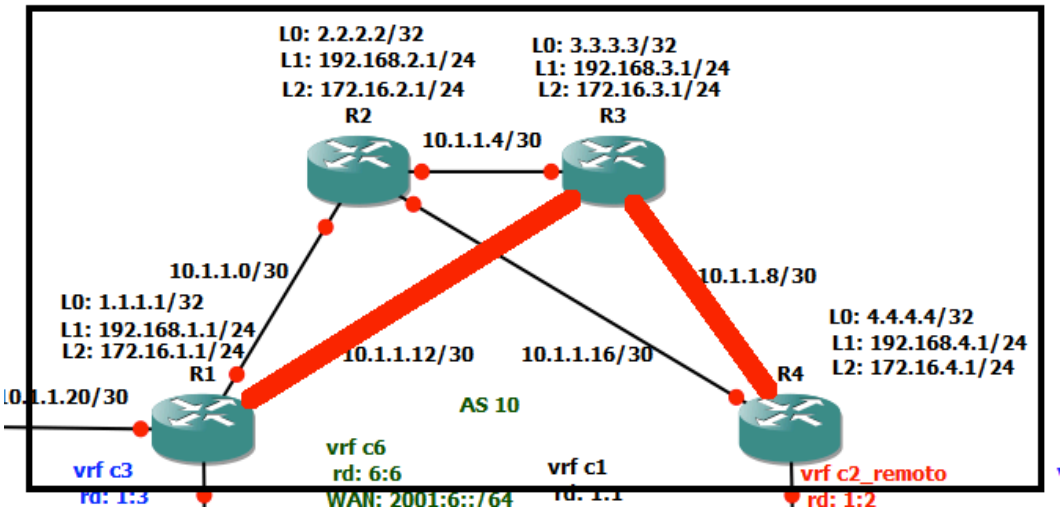

Figura 50 Captura de Tráfico Ruta MPLS.

4.1.2 Análisis de Cliente a Cliente.

En este análisis cliente a cliente que son los routers CE1 y CE2, se va a desarrollar pruebas de conexión constatando el correcto funcionamiento entre dichos routers, con la finalidad de poder observar el comportamiento antes de la aplicación de las seguridades correspondientes en la red WAN.

Para esto en la configuración de los routers se implementó la configuración de VRFs con vlans para poder simular una pequeña red virtual, con las cuales se va a implementar la creación de los túneles de seguridad, que posteriormente será sometidos a pruebas sobre la infraestructura WAN, así como la comprobación del rendimiento sin sufrir degradación en la transmisión de los datos.

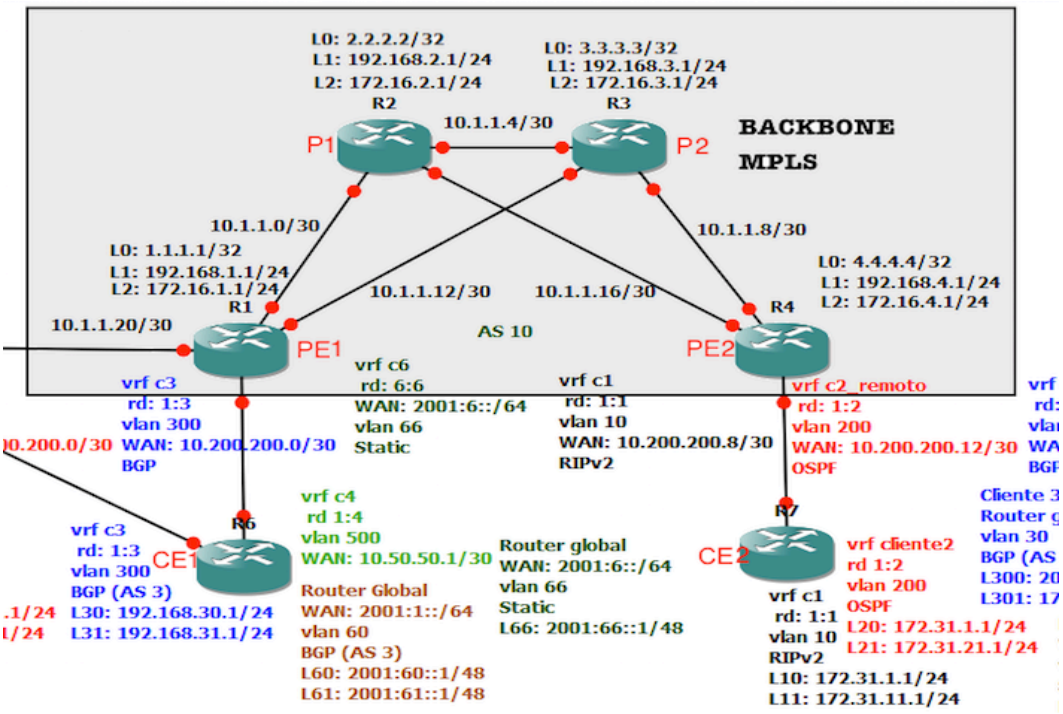

Figura 51 Topología Pruebas CE.

En la tabla 12 se puede observar el planteamiento de las vrfs con sus respectivas vlans además de las Loopbacks de cada vrf así como también a la red WAN que pertenece, se asignó a los routers PE direcciones IP correspondiente a la clase A que es privada, con una máscara de 30, mientras que a los routers CE se les asigno las loopbacks con direcciones IP correspondientes a la clase A, también con clase C, con máscara de 24.

Tabla 12

Distribución IP en CE y PE.

Router	Vlan	Red WAN	IP Origen	Loopback
R1=PE1	100 200 300	10.200.200.0/30	10.200.200.1	L0:1.1.1.1/32 L1:192.168.1.1/24 L2:172.16.1.1/24
R6=CE1	100 200 300	10.200.200.0/30	10.200.200.2	L10:192.168.1.1/24 L11:10.10.10.1/24 L20:192.168.1.1/24 L21:10.10.20.1/24 L30:192.168.30.1/24 L31:192.168.31.1/24
R4=PE2	10 200 30	10.200.200.8/30 10.200.200.12/30 10.200.200.16/30	10.200.200.9 10.200.200.13 10.200.200.17	L0:4.4.4.4/32 L1:192.168.4.1/24 L2:172.16.4.1/24

Continua ⟶

R7=CE2	10	10.200.200.8/30	10. 200.200.10	L10:172.31.1.1/24 L11:172.31.11.1/24
	200	10.200.200.12/30	10.200.200.14	L20:172.31.1.1/24 L21:172.31.21.1/24
	30	10.200.200.16/30	10.200.200.18	L300:200.1.1.1/24 L301:172.16.0.1/24

Para medir la eficacia de la red cliente a cliente al igual que las pruebas realizadas anteriormente estas constan : la primera es la verificación de la red robusta y eficaz que todos los paquetes enviados atreves de ella lleguen sin pérdidas, la segunda trata de ver las tramas de transmisión con capturas de tráfico, y los protocolos que se utiliza en dicha red.

En estas pruebas también se realizará la toma de muestras enviando diferentes cantidades de archivos o paquetes, con el fin de ver la latencia que existe entre los routers de los clientes siendo este un valor primordial para el rendimiento con la taza de transferencia de datos, comprobando también la calidad de servicio al observar que en ningún momento se perdió la conexión por lo tanto todos los paquetes enviados fueron satisfactorios.

En la topología de la figura 44, las pruebas se las realizará en los extremos de los routers, los cuales son CE1 y CE2, con el fin de constatar el perfecto funcionamiento de la red entre clientes, especialmente con la posterior implementación de seguridades, las cuales van a garantizar la privacidad entre archivos.

En la tabla 13 se observa resultados de la emulación realizada con diferente cantidad de archivos y el tiempo en que tarda en generar dicha acción entre clientes :

Tabla 13

Datos de Latencia CE - CE

Cantidad Archivos	Latencia(ms) mínima	media	máxima	Tiempo
1MB	4	68	140	00:00:16
3MB	4	68	148	00:00:49
5MB	12	71	160	00:01:20
7MB	12	73	188	00:01:51
10MB	16	74	188	00:02:37

La Latencia recolectada fue sumamente aceptable , se encuentran valores mucho menores a los 380 ms, en la figura 45 es evidente que los tiempos en milisegundos, no sobrepasan los 200 ms por lo que la red es bastante robusta e eficaz . Al momento del realizar las pruebas toda la cantidad de paquetes enviados, no tuvieron pérdidas en la transmisión.

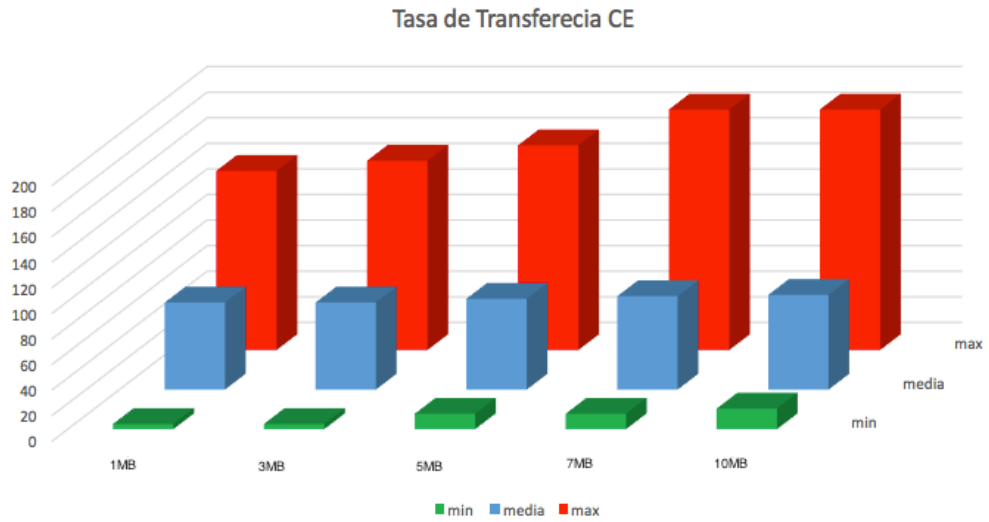

Figura 52 Tasa de Transferencia CE.

A su vez utilizando la captura de tramas en GNS3, se puede demostrar la captura del tráfico, en la cual se corrobora la transmisión de los mismos en donde se fijarán como los paquetes fueron enviados desde la dirección de origen hasta la dirección de destino con su vrf creada , observando la transmisión y recepción de paquetes ICMP.

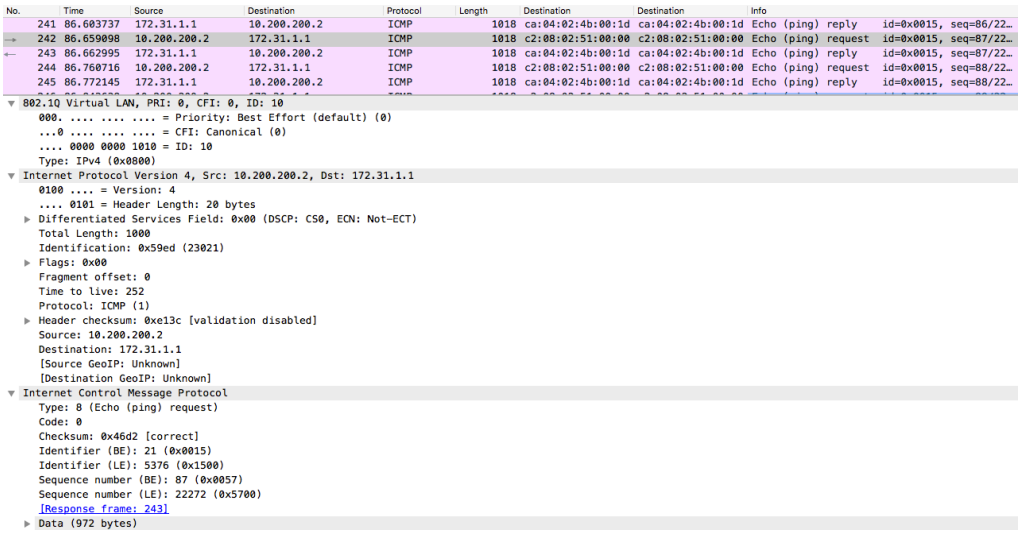

Figura 53 Captura de Tráfico CE.

A igual manera el modo de autentificación de las configuraciones realizadas en la propuesta implementada, se visualizará la comunicación entre los protocolos de enrutamiento utilizados con las vrfs implementadas.

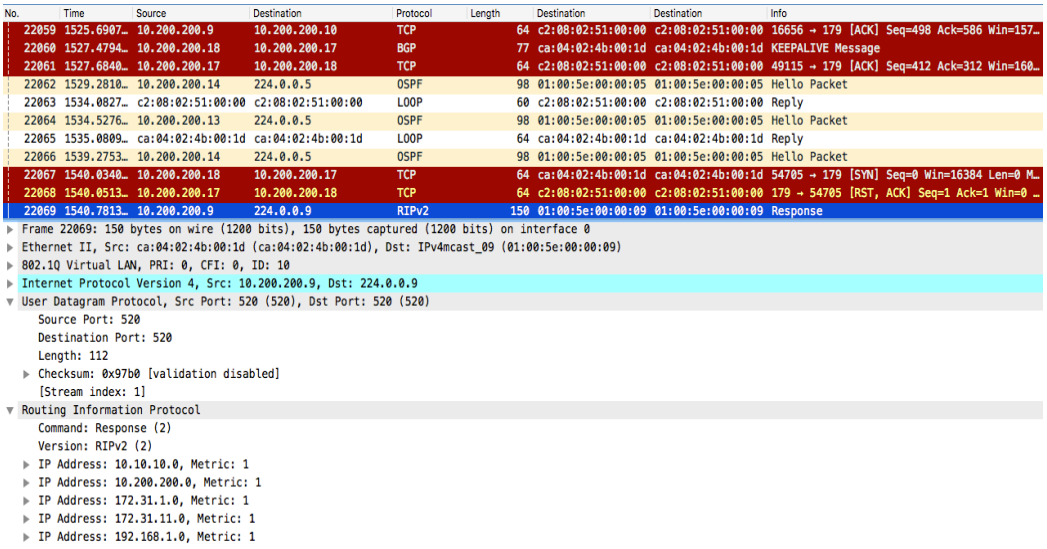

Figura 54 Captura de Tráfico CE Protocolos.

La ruta por la cual los paquetes fueron enviados, fue la que se mostrara en la figura 48, se realizó un ping específicamente a la dirección 172.31.1.1 que es la dirección loopback asignada a la vrf c1, en la siguiente figura se puede observar la ruta que tomo para llegar a su destino.

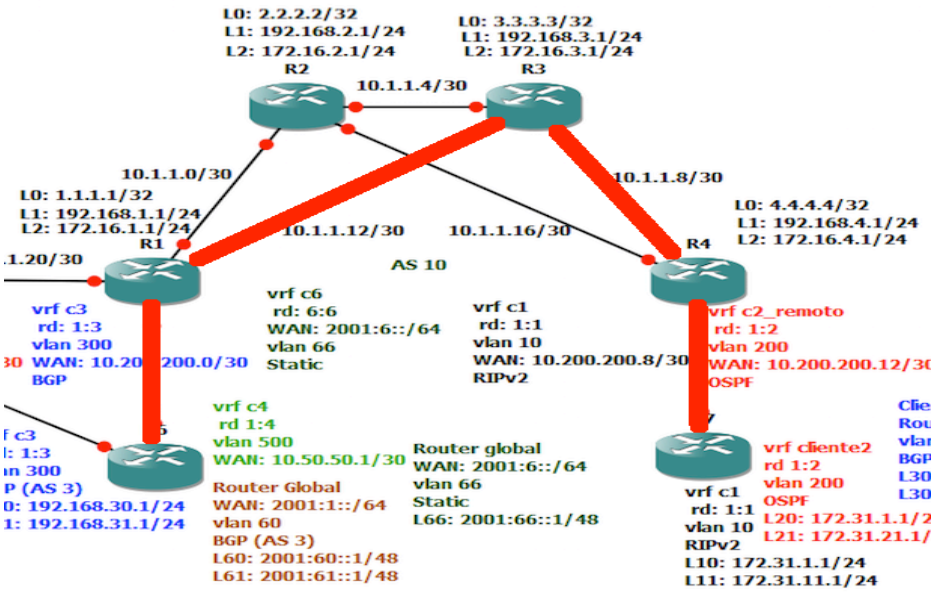

Figura 55 Captura de Tráfico Ruta CE.

4.2 Análisis de la Red con Seguridades.

4.2.1 Análisis Implementado IPSec.

Se realizó la configuración del protocolo de encriptación IPSec, en el escenario 1 en los routers de los clientes, los cuales son CE1 y CE2, pasando por la red MPLS/IP para la recolección de datos con diferentes archivos enviados, también se observará los respectivos protocolos de transmisión utilizados además de realizar capturas con wireshark para verificar la encriptación.

En el siguiente escenario se tiene en consideración las configuraciones en los routers PE1, PE2, CE1 y CE2, en los cuales se realizaron las configuraciones pertinentes para el correcto funcionamiento del protocolo de encriptación.

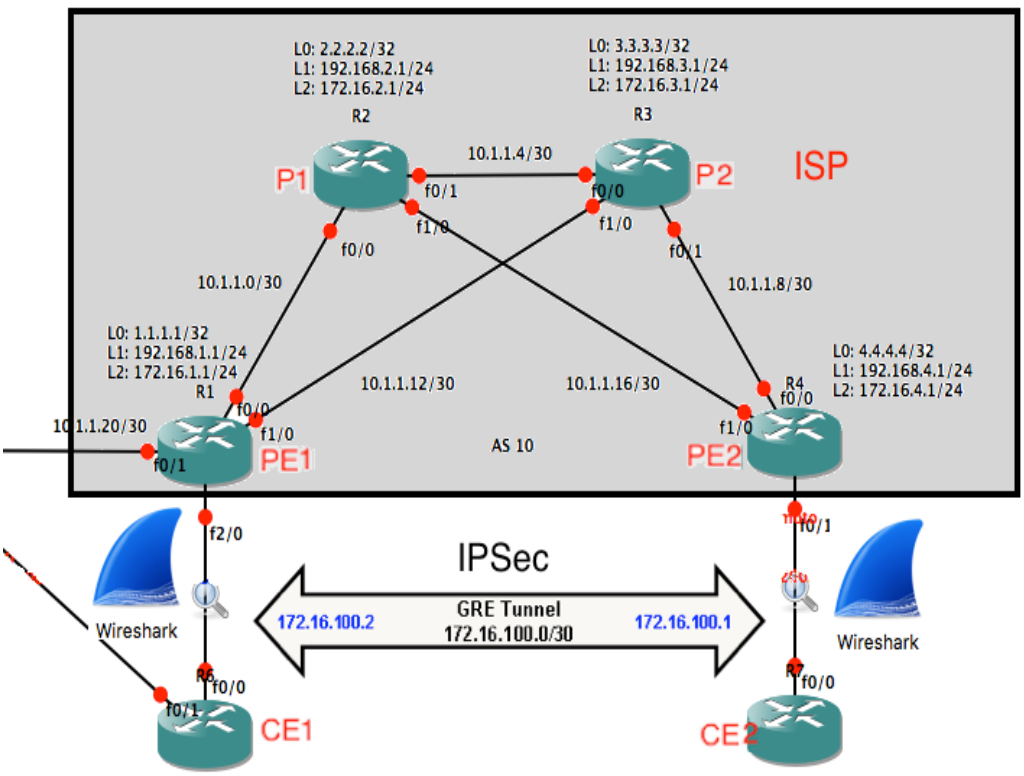

Figura 56 Configuración de IPSec Escenario 1.

En la tabla 14 se puede observar el planteamiento de la IP asignada al túnel GRE, también se utilizó la red WAN para el protocolo de encriptación IPSec, se asignó a los routers CE direcciones IP correspondiente a la clase A que es privada, con una máscara de 30, mientras que el túnel GRE tiene una IP de clase B con máscara de 30.

Tabla 14

Distribución IP en CE y Túnel GRE.

Router	Red WAN	IP Origen	Loopback
R1=PE1	10.200.200.0/30	10.200.200.1	L0:1.1.1.1/32 L1:192.168.1.1/24 L2:172.16.1.1/24
R6=CE1	10.200.200.0/30	10.200.200.2	L10:192.168.1.1/24 L11:10.10.10.1/24
R4=PE2	10.200.200.8/30	10.200.200.9	L0:4.4.4.4/32 L1:192.168.4.1/24 L2:172.16.4.1/24
R6=CE2	10.200.200.8/30	10.200.200.10	L10:172.31.1.1/24 L11:172.31.11.1/24
		Túnel GRE	
CE1	172.16.100.0/30	172.16.100.2	Sin loopback
CE2	172.16.100.0/30	172.16.100.1	Sin loopback

Para el análisis de encriptación de paquetes en la red cliente a cliente al igual que las pruebas realizadas anteriormente, se realiza envió de paquetes para verificación de la red mediante la cual se comprobará la llegada de paquetes sin pérdidas, se verifica mediante comandos el funcionamiento del protocolo y se realiza capturas en wireshark para observar la encriptación de paquetes a igual que los diferentes protocolos de enrutamiento utilizados en la red.

Para asegurar y proteger todo el tráfico de la red, comprobando que la sesión de encriptación este siempre habilitada se utiliza el siguiente comando: **show crypto session detail,** las zonas resaltadas con color amarillo demuestran el estado de la sesión con el flujo de IPSec.

CE1#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication

Interface: FastEthernet0/0
Session status: DOWN
Peer: 10.200.200.10 port 500 fvrf: (none) ivrf: (none)
      Desc: (none)
      Phase1_id: (none)
  IPSEC FLOW: permit ip 10.200.200.0/255.255.255.252
10.200.200.8/255.255.255.252
        Active SAs: 0, origin: crypto map
        Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
           Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0

La sesión está actualmente deshabilitada, porque el tráfico IPSec aún no ha sido procesado, para hacer una prueba del enlace VPN se utiliza un ping desde la interfaz del cliente 2 con la interfaz desde la fuente que es el cliente 1 de la siguiente manera :

```
CE1#ping 10.200.200.10 source 10.200.200.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.200.200.10, timeout is 2 seconds:
Packet sent with a source address of 10.200.200.2
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 76/87/92 ms
```

Figura 57 Ping IPSec up.

En donde el 80 % del ping tuvo éxito, esto se realiza para que el túnel VPN sea habilitado, necesita tiempo para la negociación de los parámetros de seguridad específicas en el mapa criptográfico.

Nuevamente utiliza el siguiente comando: **show crypto session detail,** las zonas resaltadas con color amarillo van a cambiar de estado a igual que el número de paquetes encriptados y desencriptados.

CE1#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication

Interface: FastEthernet0/0
Session status: UP-ACTIVE

Peer: 10.200.200.10 port 500 fvrf: (none) ivrf: (none)
Phase1_id: 10.200.200.10
Desc: (none)
IKE SA: local 10.200.200.2/500 remote 10.200.200.10/500 Active
Capabilities:(none) connid:1001 lifetime:23:59:27
IPSEC FLOW: permit ip 10.200.200.0/255.255.255.252
10.200.200.8/255.255.255.252
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 4 drop 0 life (KB/Sec) 4577547/3567
Outbound: #pkts enc'ed 4 drop 1 life (KB/Sec) 4577547/3567

Para la verificación del Túnel GRE se encuentre activo se utiliza el siguiente comando: **show interfaces tunnel 0,** en donde se muestra el funcionamiento del túnel GRE.

```
CE2#show interface tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 172.16.100.1/30
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.200.200.10, destination 10.200.200.2
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Figura 58 show interface tunnel .

En la tabla 15 los resultados de la emulación realizada con diferente cantidad de archivos encriptados :

Tabla 15

Datos de Latencia encriptación IPSec.

Cantidad Archivos	Latencia(ms) mínima	media	máxima	Tiempo
1MB	44	80	140	00:00:28
3MB	24	81	172	00:01:06
5MB	12	82	204	00:01:58
7MB	4	82	192	00:02:36
10MB	20	85	200	00:03:17

La Latencia recogida mantuvo su nivel aceptable en la red WAN, a pesar de la encriptación y desencriptación de paquetes, al igual que las anteriores pruebas no hubo pérdidas de paquetes durante la transmisión de archivos, a pesar de la utilización del protocolo de encriptación IPSec, los tiempos de transmisión incrementaron debido a que se utiliza Seguridad a nivel de Capa 3.

Utilizando la captura de tráfico en GNS3 mediante wireshark se confirma la validez de los datos concernientes al cifrado y descifrado, en la figura 50 se detalla los paquetes encriptados.

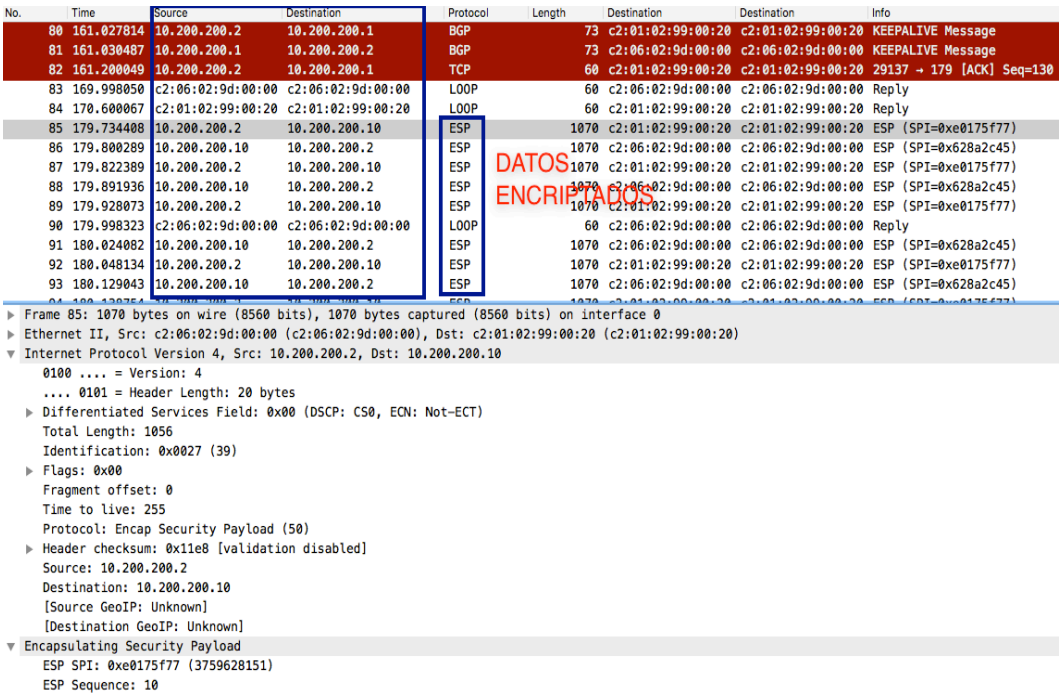

Figura 59 Verificación de encriptación IPSec.

En la figura 51 se corrobora los datos de cifrado y descifrado mediante el uso del comando: **show crypto ipsec sa**, nos da una muestra de los paquetes encriptados además del algoritmo de encriptación utilizado en IPSec.

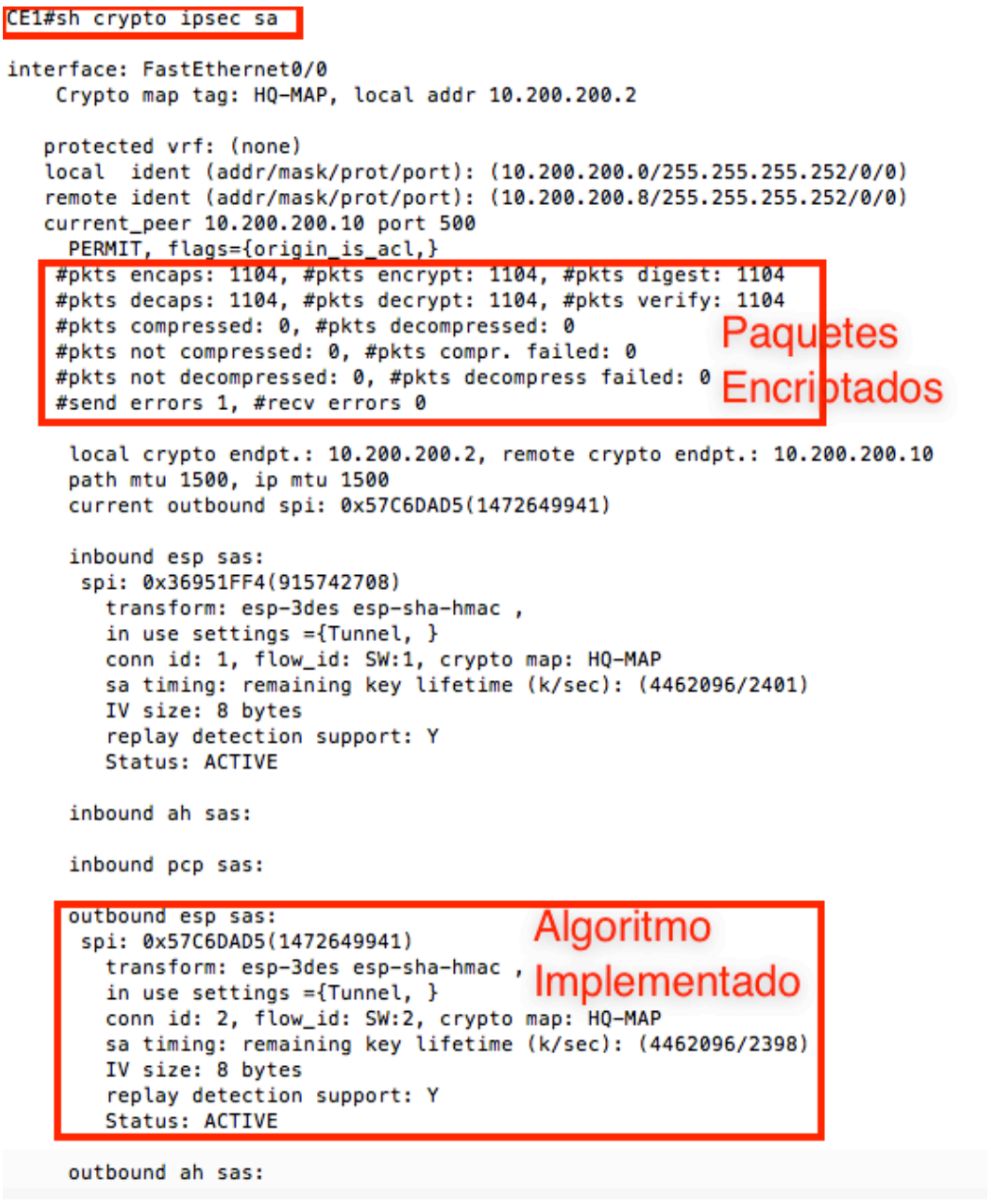

Figura 60 Comando de Verificación IPSec.

4.2.2 Análisis Implementado GETVPN.

Para la configuración del protocolo GETVPN los routers de los clientes pasan a llamarse miembros del grupo, los cuales realizan la encriptación y desencriptación del tráfico, por tal motivo se aumentará un router en la topología el cuál realiza la función de un servidor de claves , de igual manera el tráfico será enviado por la red MPLS/IP realizando la recolección de datos con diferente tamaño de archivos, se corrobora los diferentes protocolos que se utilizan en la transmisión capturada por wireshark , a su vez se observara el funcionamiento de encriptación del protocolo.

El escenario 2 que se muestra en la figura 52 se tiene en consideración el aumento del router KS que es el servidor de claves para los GM1 y GM2, donde serán implementadas las configuraciones para el funcionamiento del protocolo de encriptación GETVPN .

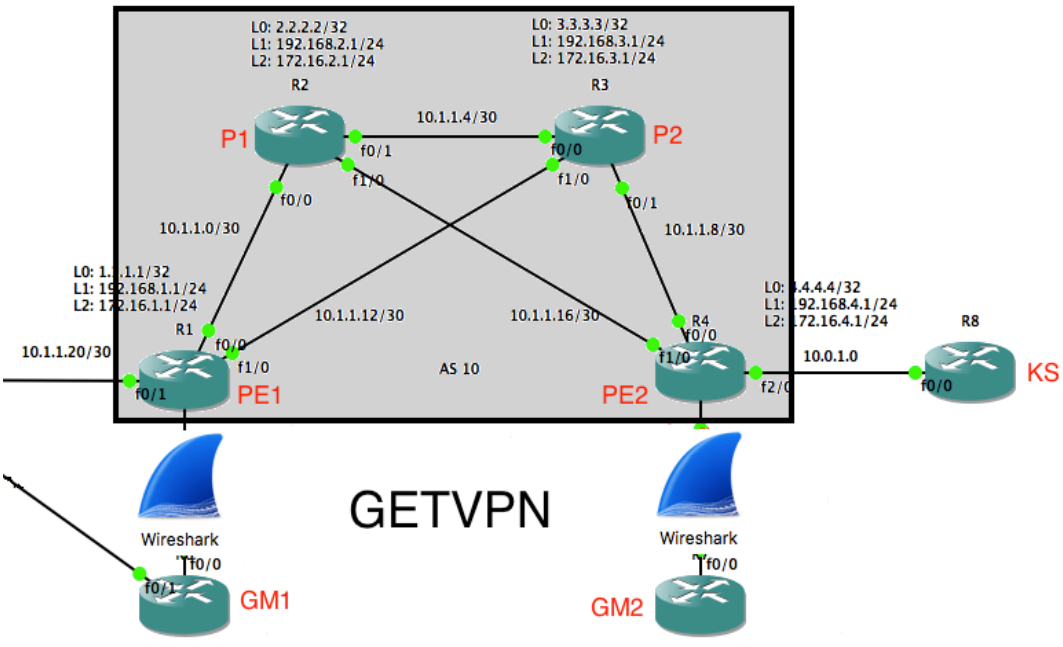

Figura 61 Configuración de GETVPN Escenario 2 .

En la tabla 16 se plantea el direccionamiento IP al servidor de claves, igual que las direcciones de la red WAN para el protocolo de encriptación GETVPN, se asignó una red al router PE2 como al KS una dirección IP correspondiente a la clase A que es

privada, con una máscara de 30, mientras que para los GMs seguirá siendo la misma de la red WAN anteriormente utilizada.

Tabla 16

Distribución IP en KS y GMs.

Router	Red WAN	IP Origen	Loopback
R4=PE2	10.0.1.0/30	10.0.1.0	L0:4.4.4.4/32 L1:192.168.4.1/24 L2:172.16.4.1/24
R6=GM1	10.200.200.0/30	10.200.200.2	L10:192.168.1.1/24 L11:10.10.10.1/24
R8=KS	10.0.1.0/30	10.0.1.2	Sin loopback
R6=GM2	10.200.200.8/30	10.200.200.10	L10:172.31.1.1/24 L11:172.31.11.1/24

En el análisis de encriptación de los paquetes en la red, se concede en realizar las mismas pruebas que en el protocolo IPSec, por esta razón se ejecuta él envió de paquetes de diversos tamaños obteniendo los parámetros deseados en el funcionamiento de la red , se corrobora mediante capturas en wireshark la encriptación de paquetes a igual de los diferentes protocolos de enrutamiento utilizados en la red.

En la verificación de este protocolo se utiliza comandos tanto en el servidor de claves como en los miembros de grupo con la finalidad de que las asociaciones de seguridad estén funcionando correctamente, el siguiente comando: **show crypto gdoi group GDOI ,** es aplicado en el KS permitiendo verificar la información de los GMs.

```
KS#show crypto gdoi group GDOI
    Group Name               : GDOI (Unicast)
    Group Identity           : 1234
    Crypto Path              : ipv4
    Key Management Path      : ipv4
    Group Members            : 2
    IPSec SA Direction       : Both
    Group Rekey Lifetime     : 3600 secs
    Group Rekey
        Remaining Lifetime   : 3044 secs
    Rekey Retransmit Period  : 10 secs
    Rekey Retransmit Attempts: 2
    Group Retransmit
        Remaining Lifetime   : 0 secs

      IPSec SA Number        : 10
      IPSec SA Rekey Lifetime: 3600 secs
      Profile Name           : IPSEC
      Replay method          : Count Based
      Replay Window Size     : 64
      SA Rekey
         Remaining Lifetime  : 3045 secs
      ACL Configured         : access-list GETVPN-ACL

     Group Server list       : Local
```

Figura 62 show crypto gdoi group GDOI .

Otro comando utilizado es: **show crypto gdoi ks,** en el cuál se puede observar los miembros del grupo que se encuentran registrados en el servidor de claves.

```
KS#show crypto gdoi ks
Total group members registered to this box: 2

Key Server Information For Group GDOI:
   Group Name              : GDOI
   Group Identity          : 1234
   Group Members           : 2
   IPSec SA Direction      : Both
   ACL Configured:
         access-list GETVPN-ACL
```

En la tabla 17 se detallan los resultados obtenidos mediante la emulación con los diferentes tamaños de archivos :

Tabla 17

Datos de Latencia encriptación GETVPN.

Cantidad Archivos	Latencia(ms) mínima	media	máxima	Tiempo
1MB	8	76	196	00:00:28
3MB	16	77	240	00:01:06
5MB	8	77	276	00:01:58
7MB	12	78	272	00:02:36
10MB	4	80	308	00:03:17

La Latencia se mantiene el niveles muy aceptables sin pérdida de paquetes , a pesar del uso de este mecanismo de encriptación, los tiempos de transmisión incrementaron paulatinamente con referencia al anterior protocolo debido a que se utiliza Seguridad a nivel de Capa 3.

La captura de tráfico mediante la herramienta wireshark en donde se corrobora los datos concernientes al encriptado y desencriptado , en la figura 53 se observa el tipo de encriptación.

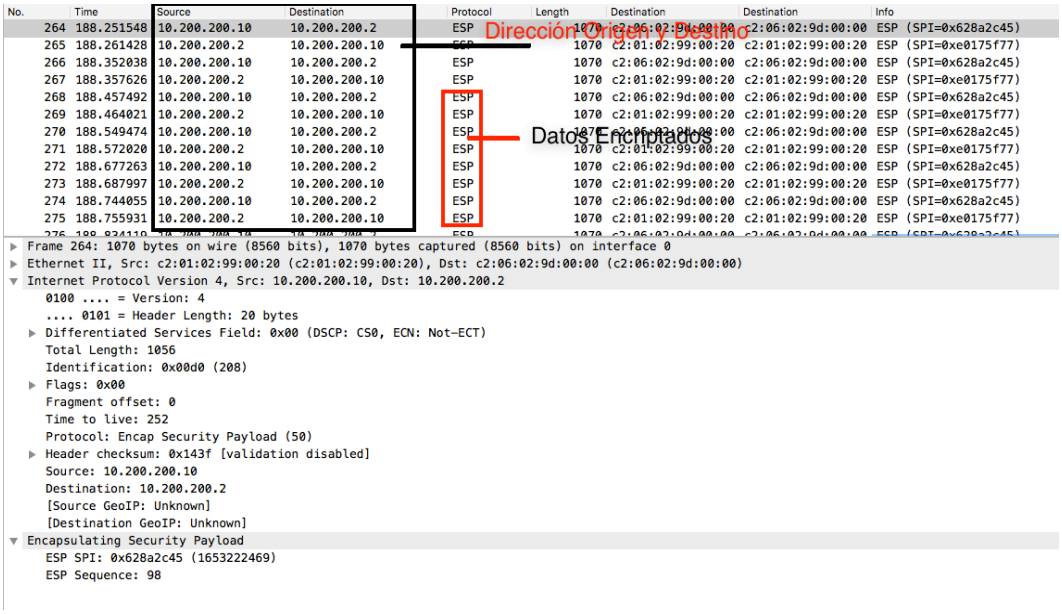

Figura 63 Verificación GETVPN .

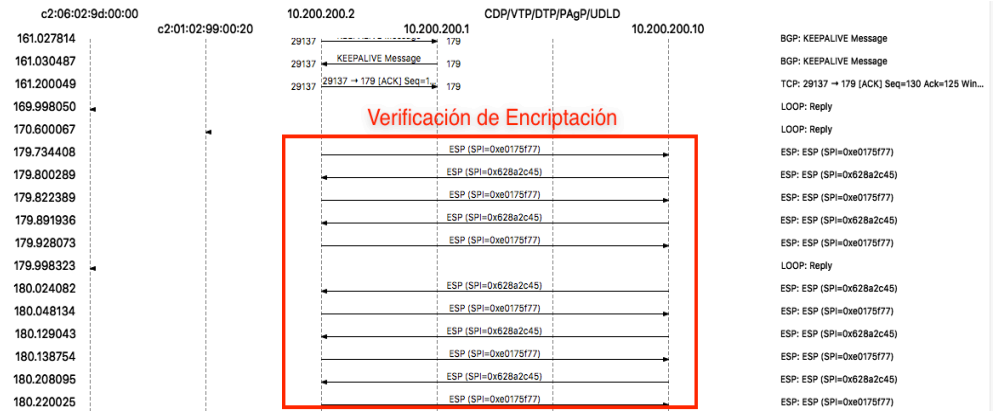

Figura 64 Registro de GETVPN .

En la figura 54 consta el proceso que realiza al momento de encriptar los paquetes, con el tráfico de red, además del protocolo utilizado en el transporte de paquetes con los respectivos mensajes de conexión, además se verifica el registro en el servidor de claves y las direcciones IP de origen y destino.

4.2.3 Comparación de Resultados entre IPSec y GETVPN .

Los mecanismo de seguridad propuestos en este documento ayuda a examinar el nivel de seguridad en una red de servicios, haciendo práctica la encriptación a nivel de capa 3 entre IPSec y GETVPN, con los resultandos obtenidos en las pruebas anteriores las cuales constan de paquetes encriptados, la latencia obtenida al momento de transmitir paquetes y la estabilidad en la red MPLS/IP.

En la tabla 18 se realiza una comparación de la latencia, luego de realizar la configuración de seguridades a nivel de capa 3, constatando la capacidad de resolución para envió de paquetes al momento de encriptarlos y desencriptarlos .

Con esto podemos constatar el funcionamiento de las seguridades sobre una red MPLS que es mayormente utilizada en la actualidad por los servidores de internet en el país, y las cuales servirán como referencia para comprobar y corroborar con la finalidad que el proveedor no sufran degradaciones en su servicio.

Tabla 18

Comparación de Latencia

	Latencia(ms)						
	IPSEC			GETVPN			
Cantidad Archivos	mínima	media	máxima	mínima	media	máxima	Tiempo
1MB	44	80	140	8	76	196	00:00:28
3MB	24	81	172	16	77	240	00:01:06
5MB	12	82	204	8	77	276	00:01:58
7MB	4	82	192	12	78	272	00:02:36
10MB	20	85	200	4	80	308	00:03:17

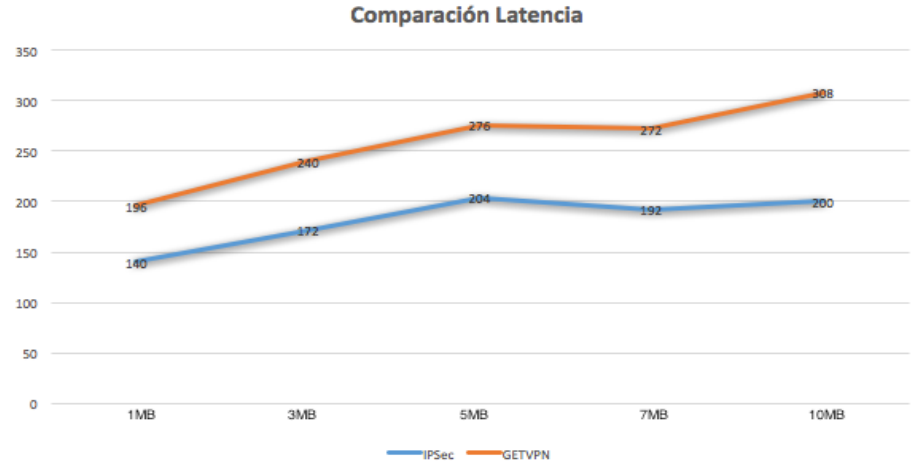

Figura 65 Comparación Latencia .

Tabla 19

Paquetes Encriptados

	Paquetes Encriptados						
	IPSEC			GETVPN			
Cantidad Archivos	encapsulado	desencapsulado	verificado	encapsulado	desencapsulado	verificado	Tiempo
1MB	500	500	500	500	400	400	00:00:28
3MB	850	850	850	850	816	816	00:01:06
5MB	970	970	970	970	905	905	00:01:58
7MB	1110	1110	1110	1110	1000	1000	00:02:36
10MB	1200	1200	1200	1200	1099	1099	00:03:17

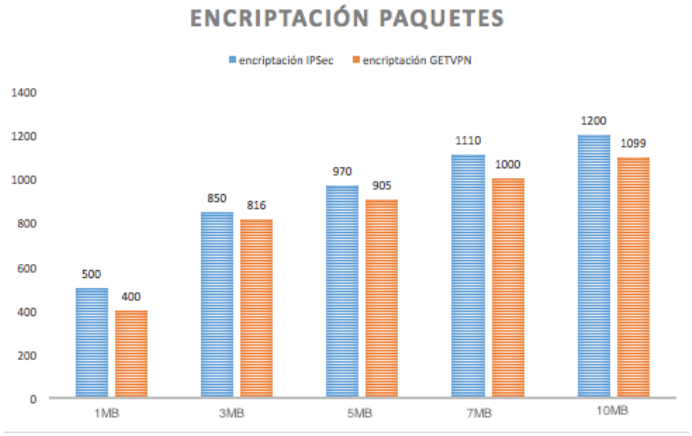

Figura 66 Comparación Encriptación de Paquetes .

Tabla 20

Características entre IPSec - GETVPN

Características	IPSEC	GETVPN
Beneficios del cliente	• Proporciona cifrado entre sitios. • Soporta Calidad de servicio.	• Simplificación de cifrado en las redes WAN y de conmutación en las etiquetas MPLS. • Simplifica la administración de cifrado, mediante el uso del servidor de claves de grupo, en lugar de claves punto a punto. • Permite escabilidad y manejabilidad de uno a uno entre estos sitios. • Soporta calidad de servicio, multicast y enrutamiento.
Cuando Usar	• Se utiliza cuando se requiere interoperabilidad de varios proveedores	• Añade cifrado a MPLS o redes WAN IP, preservando la conectividad any-to-any, con sus funciones de red. • Ofrece escabilidad a tiempo completo en el mallado en IPSec VPN. • Permite la participación de pequeños enrutadores, para una red mallada. • Simplifica la administración de claves, mientras soporta enrutamiento, calidad de servicio y multicast.
Interoperabilidad	• Diferentes	• Solo routers CISCO
Topología	• Mallado a pequeña escala	• Hub and Spoke, any to any
Ruteo	• No soporta	• Conectividad any to any, punto multipunto,multipunto multipunto
QoS	• Soporta	• Soporta
Multicast	• No soporta	• Soporte nativo en MPLS y redes privadas
Alta disponibilidad	• Genera conmutación por error	• Enrutamiento

Fuente: (Cisco, Cisco, 2006)

Con la realización de las pruebas de cifrado tanto para IPSec como GETVPN, la recolección de datos obtenidos, nos demuestra el funcionamiento de los dos mecanismo de seguridad a nivel de capa 3, por lo tanto el mecanismo de seguridad que contiene mayor latencia es GETVPN.

Esto se debe a que GETVPN al momento de enviar paquetes, tiene un límite de registro en el servidor de claves , lo que lleva a un mayor procesamiento en los paquetes al momento de encriptar y desencriptar, por ende tiene mayor latencia.

Mientras tanto con el protocolo de encriptación IPSec, la latencia es menor debido a su funcionamiento interactuando directamente entre los routers , haciendo de esta combinación una manera de transmisión más eficiente en la encriptación y desencriptación de paquetes.

GETVPN elimina túneles y desarrolla la encriptación entre los extremos de manera nativa, mejorando la capacidad para comunicarse entre más miembros de grupo con una IP de origen y destino, enrutando de mejor manera los paquetes, logrando que esta transmisión se realice entre diferentes miembros de grupo.

4.3 Prueba de Pentesting.

Para esta prueba se utiliza la herramienta Kali Linux en conjunto con GNS3, con los cuáles vamos a emular, un ataque de intrusión a un router Cisco, para esto tenemos que agregar a nuestra topología la conexión de una máquina virtual en donde se encuentre presente el software Kali Linux, se lo realiza incluyendo una nube en GNS3 en conexión con el router del cliente, siendo este uno de los más opcionados al momento de realizar una intrusión indebida.

La topología luego de la inclusión de la máquina virtual, se puede observar en la figura 55, esta máquina virtual aparece como una nube en GNS3.

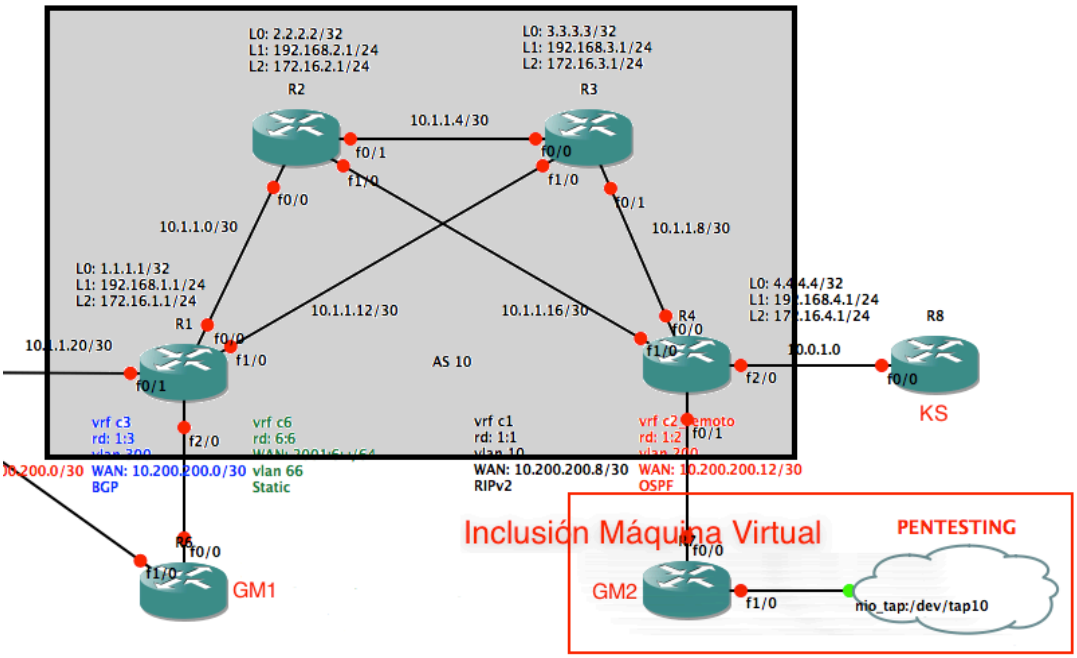

Figura 67 Inclusión Máquina Virtual .

Con la inclusión de la nube se procede a configurar, para que la máquina virtual encuentre el router, añadiendo una interfaz que hace posible la comunicación entre ambos dispositivos.

En vista que se añadió una nueva interfaz al router se lo procede a configurar, vamos a asignarle una IP que va hacer la local host y así poderlo conectar. En la figura 56 nos muestra el adaptador de red, la cual nos muestra la que podemos utilizar.

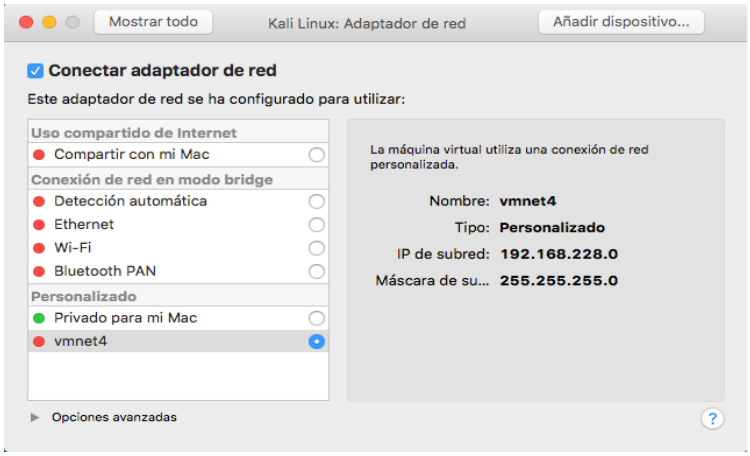

Figura 68 Adaptador de Red .

La tabla 21 muestra la distribución de IP de acuerdo al adaptador de red, en este caso es una IP de clase C con máscara de 24, en la interfaz del router asignamos una IP que se encuentre en ese rango.

Tabla 21

Distribución IP del adaptador de Red.

Router	Red WAN	IP Origen
R7=GM2	192.168.228.0/24	192.168.228.128
Pentesting	192.168.228.0/24	192.168.228.127

Una vez terminadas las configuraciones, con el respectico nivel de seguridad en el router, se ejecuta la máquina virtual con Kali Linux, en este caso se utiliza la herramienta cisco-auditing-tool que es una de las muchas herramientas que ofrece Kali Linux, esta herramienta se aplica debido al uso de routers cisco en la propuesta planteada.

Ya ejecutado la máquina virtual se procede con cisco-auditing-tools, se abre un terminal en donde se procede a realizar la prueba, para realizar la prueba se debe saber la IP del router el que va hacer atacado.

Se utiliza el siguiente comando: CAT –h 192.168.228.127 –a , las letras CAT es la herramienta que se va utilizar cisco-auditing-tool (CAT), seguido de –h que indica la dirección del host al que se va a realizar el ataque, por último se agregar –a que es un buscador de listas de contraseñas por defecto.

En la figura 57 se detalla como la herramienta realiza su trabajo, ejecutando una búsqueda del password de una lista que tiene por defecto, como también la lista de comunidad las cuales pueden ser públicas o privadas , depende de la configuración que se realizó.

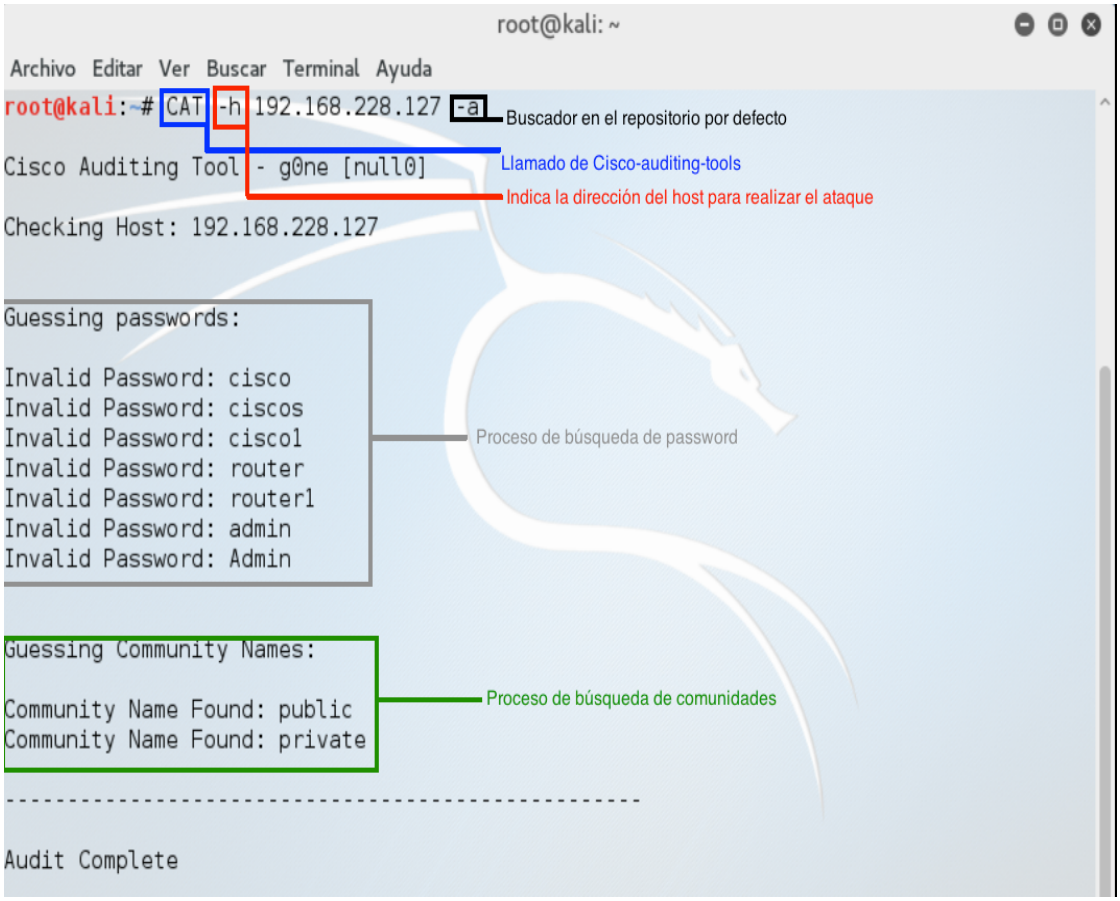

Figura 69 Pentesting .

En este caso se observa la búsqueda de los password de una lista, esta lista se encuentra conformada por 7 passwords posibles. Ninguno de estos passwords resultan ser válidos, caso contrario sucede con las listas de comunidades en las cuales fueron encontradas como válidas tanto las públicas como privadas.

Kali Linux tiene algunos archivos, en los que se puede configurar, como quiere el usuario, que funcione esta herramienta, en este caso se debe ingresar a los archivos del sistema o disco local en la carpeta de usuario, para luego ir a la carpeta con el nombre de share en donde buscamos la herramienta que este caso es cisco-auditing-tool, en donde se hallan tres carpetas más, escoger la carpeta lists.

En esta carpeta se encuentran la lista de nombres de contraseñas y servidores comunitarios los cuales pueden ser modificados, agregando muchas contraseñas en su repositorio.

La dirección en donde se encuentra este repositorio es: /usr/share/cisco-auditing-tool/lists .

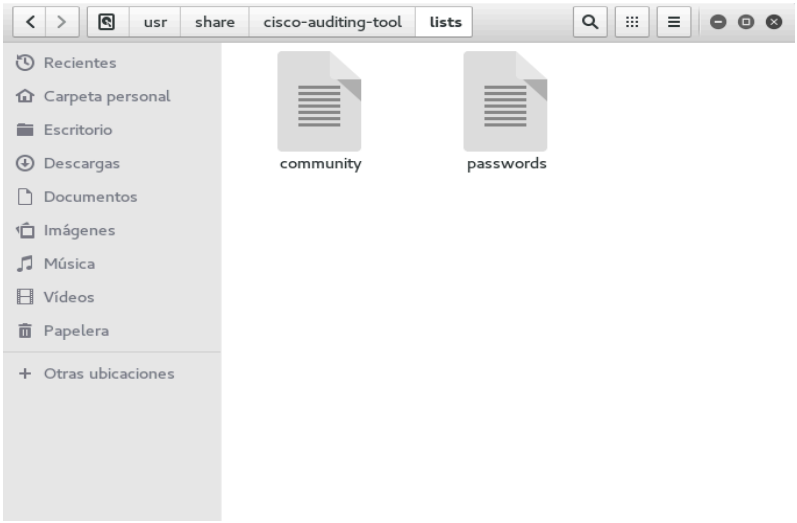

Figura 70 Repositorio cisco-auditing-tool .

En la figura 59 se encuentra los posibles passwords, esta lista puede ser modificada.

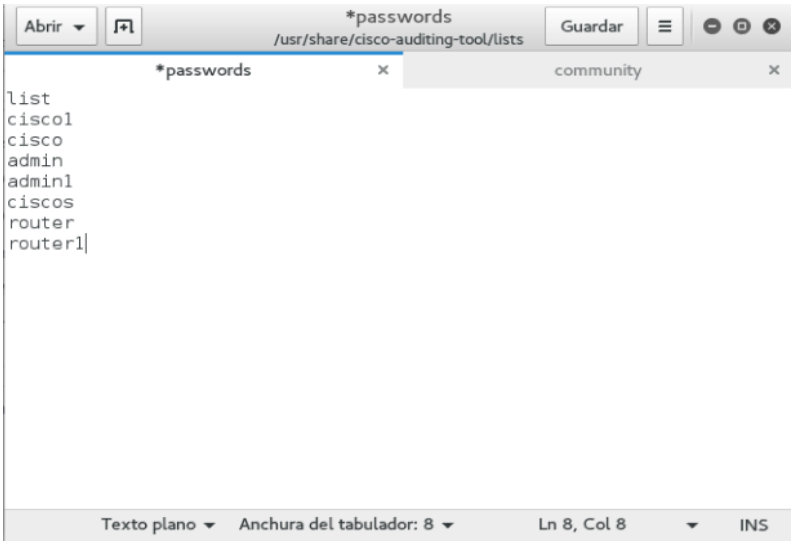

Figura 71 Lista cisco-auditing-tool.

4.4 Calidad de Servicio en la Red.

Para observar la calidad de servicio en la red de datos, se configura en el emulador GNS3 el escenario descrito en la siguiente Figura 70 , en el cual se aumenta dos hosts los cuales pertenecen a dos máquinas virtuales, en las que se instaló la herramienta de inyección de tráfico (D-ITG), mediante las cuales se realiza la inyección de tráfico de datos con calidad de servicio y sin ella.

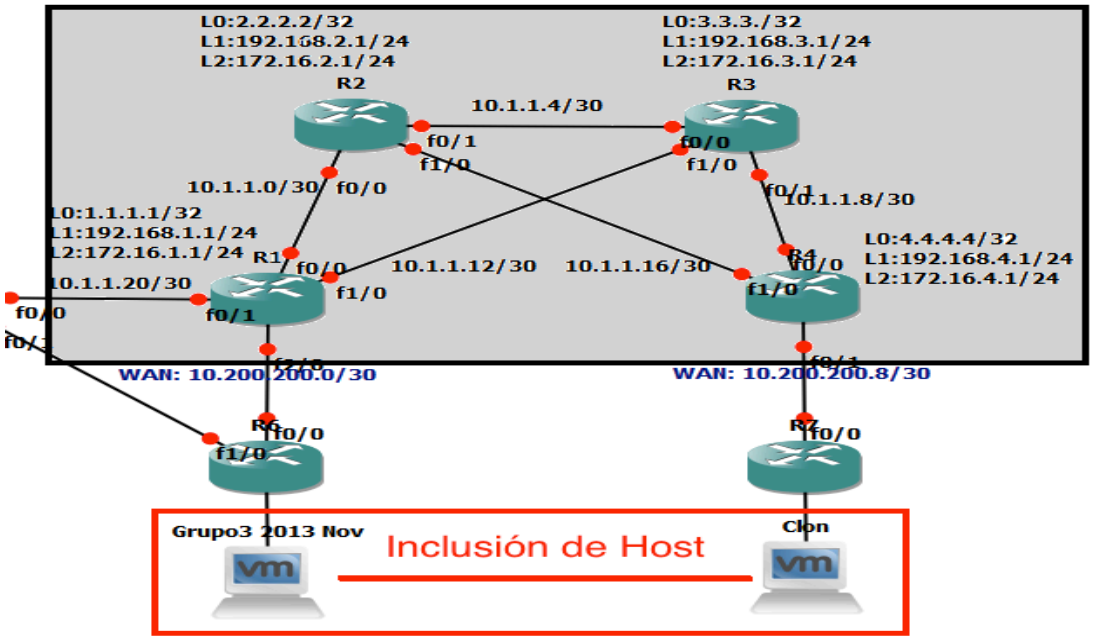

Figura 72 Inclusión Host VM.

A continuación se explica la manera de configurar las máquinas virtuales con las PCs emuladas en el escenario anterior.

- En gns3 click en la pestaña Preferencias.
- Seleccionar la opción VMware VMs en donde se muestra una ventana con la máquina virtual que vamos a enlazar (Figura 71).
- Pulsar Ok.
- Arrastramos la máquina virtual al escenario, damos click derecho en la PC.

- Escoger la opción Configure.
- En la siguiente ventana click en Network y escoger las dos opciones (Figura 72).
- Pulsar OK.

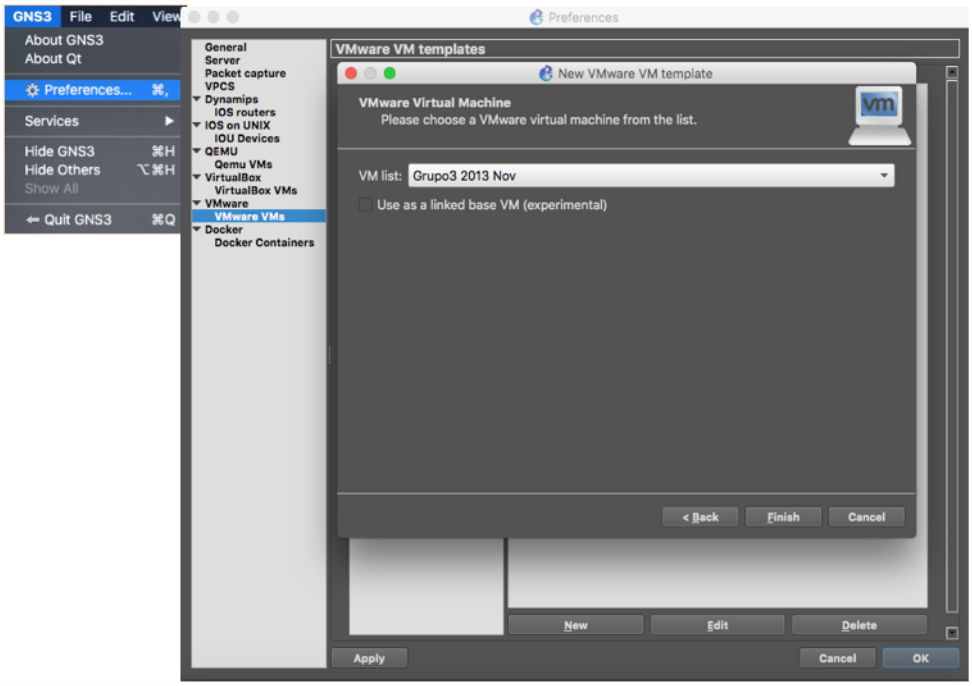

Figura 73 Configuración VMware.

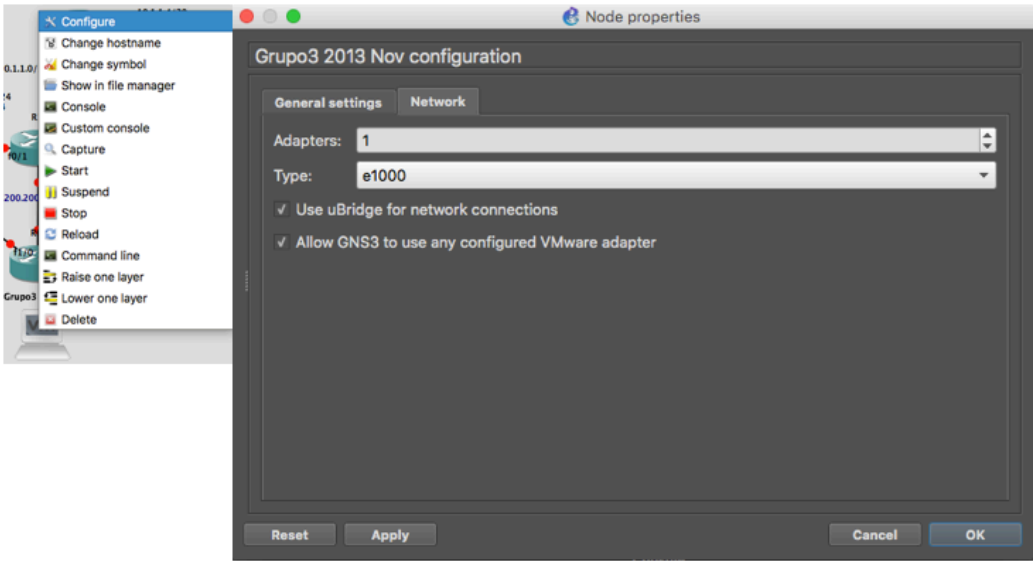

Figura 74 Configuración Network.

Para verificar la conexión entre máquinas virtuales y la física, con los respectivos adaptadores de red, se procede abrir el cmd en donde se procede a escribir el comando ipconfig en donde aparece la lista de los adaptadores de red en VMware , para verificar la conexión se hace ping entre las direcciones ip de VMware ver figura 73.

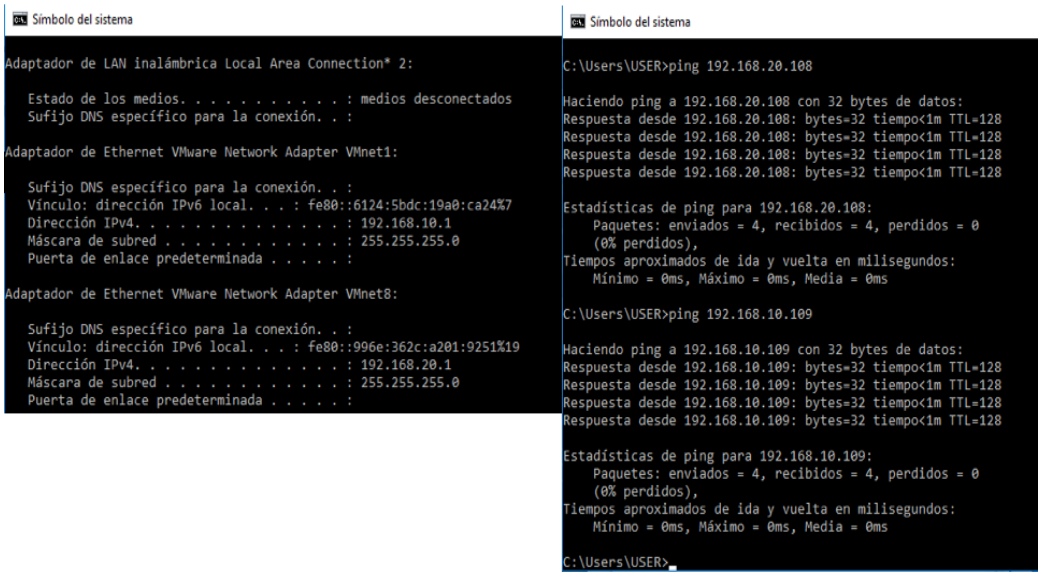

Figura 75 Física y VMware.

Una vez ya puesto en marcha el software de emulación GNS3, con las máquinas virtuales, se realiza el siguiente procedimiento, se verifica la conexión entre las máquinas virtuales, se abre el terminal de la máquina virtual y se ejecuta el comando ifconfig en donde se observa la dirección IP de cada una de ellas, para verificar la conexión se realiza un ping entre máquinas virtuales Figura 74.

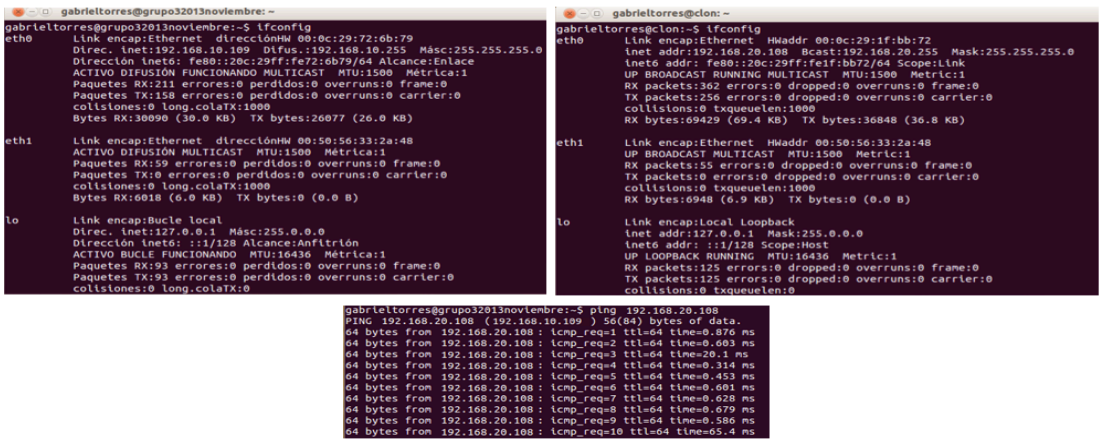

Figura 76 Máquinas Virtuales ping.

4.4.1. Inyección y configuración D-ITG

En este ítem se detalla configuración e inyección de tráfico mediante la herramienta D-ITG con la red emulada. Se realiza dos tipos de configuraciones primero con la red sin mecanismo de calidad y el segundo aplicando este mecanismo. Primeramente se detalla los pasos a seguir para la ejecución del inyector de tráfico en la máquina virtual.

- Abrir el terminal
- Ejecutar el comando cd root seguido de la tecla enter
- Una vez dentro presionamos cd itggui-092
- Por último java -jar ITGGUI.jar (Figura 75).

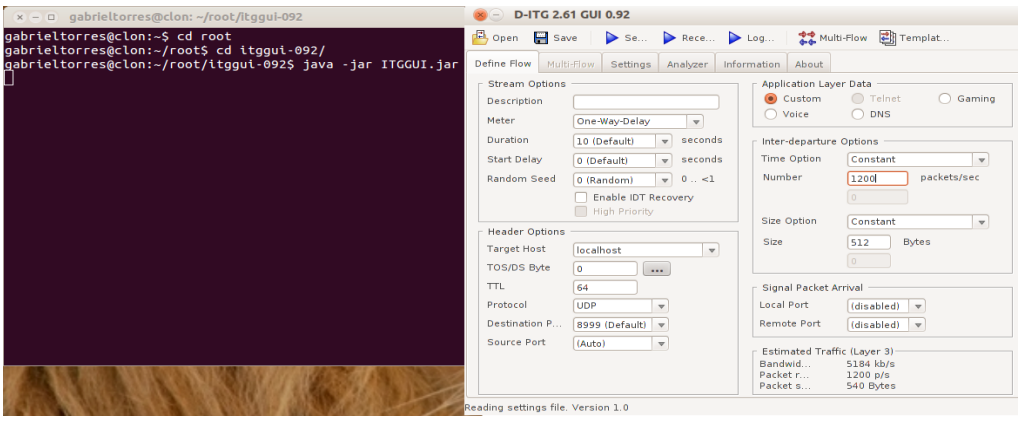

Figura 77 Ejecución D-ITG Linux.

Configuración D-ITG emisor sin calidad de servicio:

- Pestaña definición de flujo.

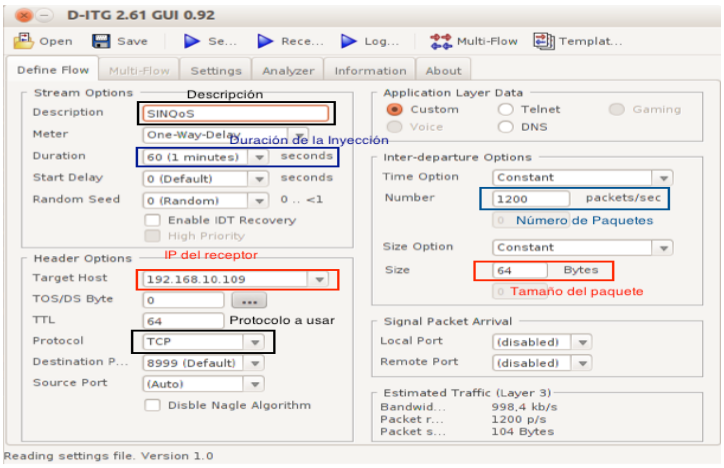

Figura 78 Definición Flujo Emisor.

- Pestaña Ajustes

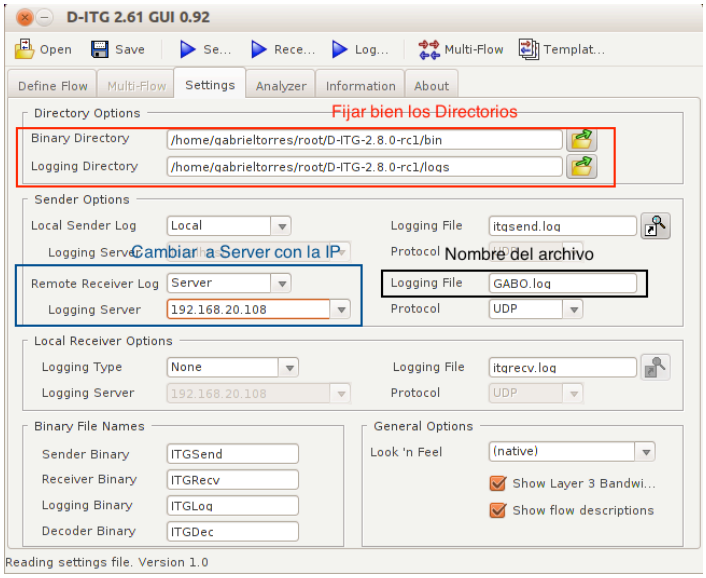

Figura 79 Ajustes Emisor.

Configuración D-ITG sin calidad de servicio:

- Pestaña definición de flujo

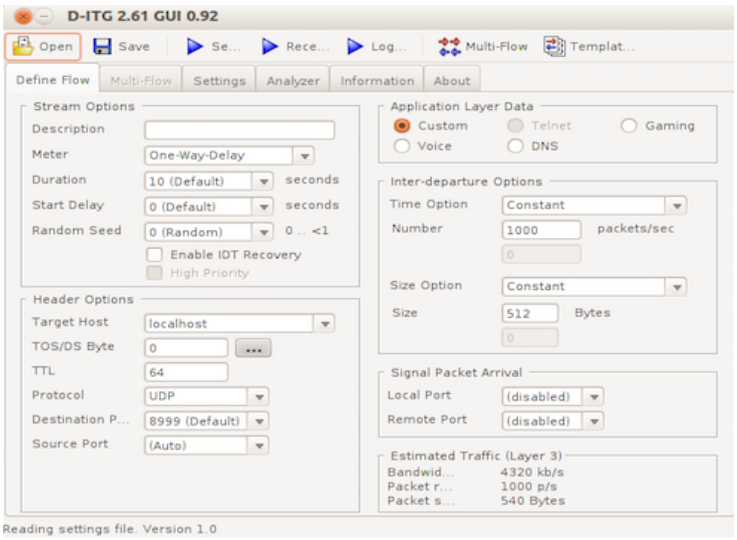

Figura 80 Definición de flujo receptor.

- Pestaña Analizador
- Escogemos el archivo a ser analizado
- Click en Run Analyzer

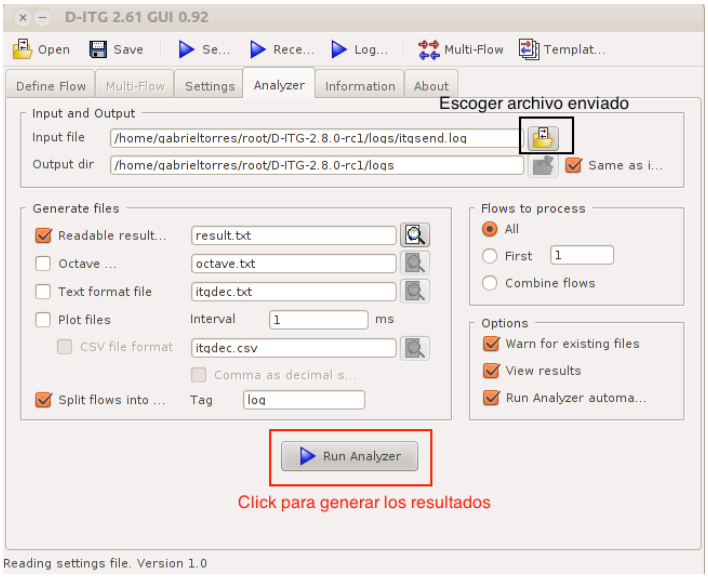

Figura 81 Analizador receptor.

- Resultados del Receptor.

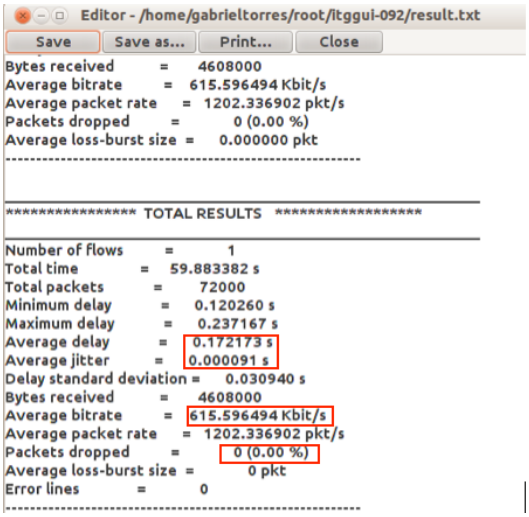

Figura 82 Resultados receptor.

Configuración D-ITG emisor y receptor con calidad de servicio:

La configuración tanto en el emisor como en el receptor es la misma presentada anteriormente desde la Figura 76 hasta la Figura 80 , pero tenemos una pequeña variante, tanto en el receptor como en el emisor vamos activar la Pestaña TOS/DS .

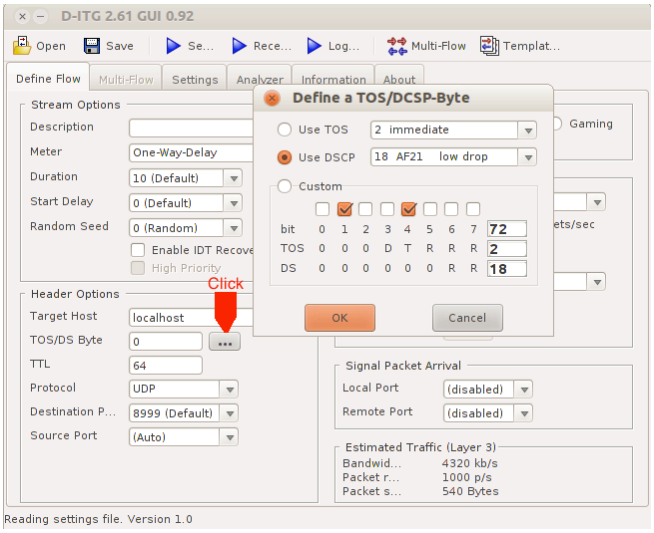

Figura 83 Ventana TOS/DS emisor y receptor.

Es un método que garantiza la calidad de servicio en redes, utilizando la pila TOS dando prioridad a cada paquete enviado.

Proceso de captura de datos con DITG:

- Activar el Logger del receptor para almacenar la información
- Activar el Receiver del receptor para recibir la captura de tráfico.
- Activar el Sender del Emisor para que comience a inyectar el tráfico.
- El emisor se detiene automáticamente según lo configurado.
- Detener la captura de tráfico en el receptor click en Receiver.
- Detener dando click en Logger del receptor.
- En la pestaña Analyzer pulsar el botón Run Analyzer para obtener los parámetros de calidad de servicio.

4.4.2. Resultados

Se debe tomar en cuenta que los valores de los diferentes parámetros pueden tener un margen de variación por la utilización de un emulador, debido a que estos emuladores basados en software cuentan con un margen mínimo de error, por lo tanto la latencia y

los demás valores pueden variar, ya que los factores incidentes son varios, entre ellos es la prioridad que da los procesos en el sistema operativo antes que el emulador, de la misma manera esta la memoria ram del computador así como la velocidad de procesamiento, entre otras.

En las pruebas de inyección de tráfico, se las realizó manteniendo el mismo número de paquetes con diferente tamaño de acuerdo a la Tabla 22, trabajando con la capa de transporte específicamente el protocolo TCP, debido a que es un protocolo orientado a la conexión procurando que todos los paquetes lleguen a su destino sin importar el tiempo.

Tabla 22

Dimensiones de Inyección.

	Dimensiones		
Número	1200 packets/s	1200 packets/s	1200 packets/s
Tamaño	1024 bytes	512 bytes	64 bytes

En la Tabla 23 se pondrá los valores que han sido obtenidos con la inyección de tráfico.

Tabla 23

Valores de Inyección.

Parámetros	Red Sin Qos			Red con QoS		
	1024	512	64	1024	512	64
Delay (ms)	255,72	213,94	172,17	230,28	171,15	154,95
Jitter (ms)	55,6	39,16	23,38	45,05	33,45	21,05
Bitrate (Kbit/s)	9827,44	4886,24	615,59	9829,87	4915,11	614,40
Packets dropped	0%	0%	0%	0%	0%	0%

Tabla 24

Valores de Qos Datos.

Parámetros	Servicio Datos Bueno	Muy Bueno	Excelente
Latencia	> 300 ms	> 250 ms y < 300 ms	< 250 ms
Jitter	> 70 ms	> 55 ms y < 70 ms	< 55 ms
Pérdida Paquetes	> 5 %	> 3 % y < 5%	< 3%

Valores obtenidos en las inyecciones de Tráfico con el software D-ITG.

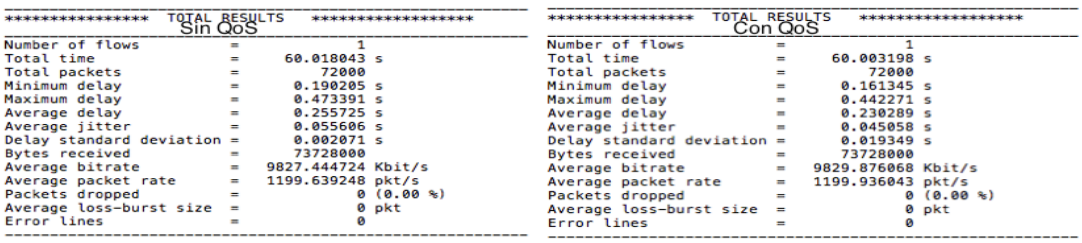

Figura 84 Valores Obtenidos.

En la Tabla 24 es una donde se puede observar diferentes valoraciones de QoS para datos según las recomendaciones de UIT- T G.1010, Y1541 y la IEEE.

De acuerdo a la Tabla 23 y Tabla 24 solo se toma en cuenta el resultado obtenido con el tamaño de paquete de 1024 bytes, la Latencia en el servicio de datos, con la inyección de tráfico en el escenario de pruebas, es muy bueno sin calidad de servicio, esto se debe al uso del protocolo TCP tratando que los paquetes enviados lleguen a su destino por lo tanto toma mayor tiempo en el proceso de transmisión de la información provocando retardo. Es excelente la latencia aplicando el mecanismo DiffServ, que agrupa los paquetes con prioridad, reenviando principalmente aquellos que tengan prioridad.

Con respecto al Jitter, de acuerdo al target de QoS están en un estado muy bueno sin Qos , de acuerdo al tamaño hace que la variación sea muy baja y se encuentre en un estado excelente con Qos, esto se debe a que además de utilizar un tamaño fijo de

paquete, el mecanismo DiffServ asigna sus prioridades lo que permite llegar en menor tiempo los datos.

No se encuentran pérdidas de paquetes esto hace que ambas inyecciones de tráfico se encuentren en un estado excelente, el protocolo TCP tiene por función principal asegurar que todos los paquetes lleguen a su destino; el mecanismo DiffServ no produce mayor efecto debido al protocolo TCP.

Tomando como referencia estos resultados, en donde se determinó que la QoS se encuentran en un rango aceptable, se establece una tabla de valoraciones.

Tabla 25

Tabla de Valoraciones.

Parámetros	Valor Cuantitativo	Porcentaje	Valor Cualitativo
Jitter Latencia	2	80 %	Muy Bueno
Paquetes Pérdidos	3	100 %	Excelente

En la Tabla 25 los porcentajes se los tomo de acuerdo a los datos obtenidos en las inyecciones, respecto al cuadro de valoraciones de QoS en donde se puede evidenciar los diferentes rangos los valores de la latencia y Jitter, en esta tabla da un valor con un porcentaje cuantitativo.

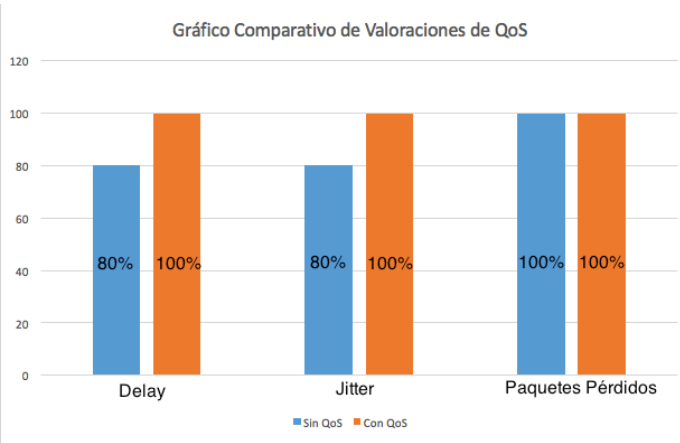

Figura 85 Gráfica Comparativa de mejora con QoS.

En la figura 85, se puede observar que la latencia o delay pasa de un 80% a un 100% mejorando con la aplicación del mecanismo DiffServ, debido a que usa las prioridades de paquetes de datos. El jitter se encuentra en 80 % y mejora al 100 % , pero la variación entre estas no es muy significante. La pérdida de paquetes en la red es mínima, se encuentra en el 100 % por el protocolo TCP que aseguran que todos los paquetes llegue a su destino. Mediante estos datos obtenidos se llega a comprobar la calidad de servicio en la red, observando claramente que es útil utilizar el mecanismo DiffServ para ofrecer un mejor servicio.

CAPÍTULO 5

CONCLUSIONES ,RECOMENDACIONES Y TRABAJOS FUTUROS

5.1 Conclusiones

Los resultados obtenidos en la aplicación de los mecanismos de seguridad, tanto para IPSec como GETVPN, son opciones sumamente viables, para la transmisión de datos seguros en un entorno de una red MPLS, manteniendo siempre niveles óptimos con una buena respuesta en calidad de servicio.

El protocolo IPSec es el que mejor maneja los paquetes encriptados en una red MPLS, manteniendo siempre sus políticas de seguridad, siendo eficiente en la calidad de servicio, lo cual es sumamente importante que las organizaciones o empresa requieran su implementación para el intercambio de información segura.

GETVPN es una buena alternativa, para integrar seguridad a nivel de capa 3, aunque su latencia aumente considerablemente, permanece en el target adecuado y considerado normal en una red WAN. Siendo una de las razones más considerables para una posible migración de esta tecnología siempre y cuando el cliente lo requiera .

Al realizar las pruebas, se pudo observar el comportamiento de los diferentes mecanismos de encriptación sobre la infraestructura MPLS, se constató que el mecanismo de seguridad GETVPN tiende a perder paquetes, esto se debe al límite de tiempo para registrase en el servidor de claves.

La encriptación GETVPN se la configuró de una forma entendible considerando que cada lector la tome de una manera educativa e investigativa , con la finalidad de que cada persona tenga la posibilidad de entender el funcionamiento y administración de este mecanismo de seguridad, que se implementa a nivel de capa 3.

Se cumplió con los objetivos, así como también la propuesta realizada, la cual se hizo de acuerdo al funcionamiento y estructura de un proveedor de servicios que se asemeja a la realidad, para su posible implementación, siendo este un mecanismo que da seguridad a nivel de capa 3.

Se realizó un análisis de los parámetros obtenidos en la red virtual utilizando inyecciones de tráfico con D-ITG, comprobando una mejora de estos al ser configurada la red con QoS. No se profundizó en este análisis debido a que no es parte fundamental de este trabajo de titulación.

5.2 Recomendaciones

Se recomienda para la configuración de los mecanismos de seguridad en capa 3 utilizar las imágenes cisco IOS versión 12.2 en adelante, debido a que en versiones anteriores los comandos a utilizar no existen, con estas funciones actualizadas se procede a un mejor desarrollo del proyecto de investigación.

Se recomienda agregar en la topología del escenario 2 un mayor número de miembros de grupo, para observar el funcionamiento del servidor de claves a medida que aumenta los mismo en la red MPLS/IP.

Antes de realizar las pruebas hay que verificar que todos los protocolos de enrutamiento estén activados , debido a que las adyacencias tardan un poco en activarse, para un correcto funcionamiento por lo que es necesario esperar que estén todos activos.

Es recomendable descargar el software utilizado en este proyecto de páginas oficiales para no tener inconvenientes en su computador.

Cuando se utiliza el software de auditorías en la red se debe realizar una pequeña investigación previa, debido a que se utiliza el terminal para las configuraciones sin causar daño a terceros.

Para evitar el acceso a los routers de manera indebida o no autorizada, se recomienda utilizar claves que no sean fáciles de descifrar, y la información no esté en manos equivocadas que pueden hacer mal uso de ella.

Para este proyecto de investigación se recomienda utilizar software actualizado, para un correcto funcionamiento de las políticas de información y comunicación.

5.3 Trabajos Futuros

Como trabajos futuros, se podría realizar pruebas más exhaustivas , con el software de auditoría en seguridad, buscando siempre mejorar la seguridad de una empresa, mediante mecanismos que nos permitan asegurar una mejor confiabilidad en los datos internos de una empresa.

GETVPN implementado sobre el protocolo de comunicaciones IPV6, realizando un análisis de su comportamiento y funcionamiento mediante una red que contenga su backbone y usuarios netamente funcional en IPV6.

Un análisis de los diferentes algoritmos de cifrado que se pueden implementar a nivel de capa 3, en una red MPLS.

Bibliografía

Uttam Kumar, 2. (s.f.).

Blog Networking. (2010). Recuperado el 19 de julio de 2016, de http://www.startnetworks.info/2010/08/mpls-control-plane-and-data-plane.html

Uttam Kumar. (2010). Recuperado el 19 de julio de 2016, de Uttam Kumar: http://www.startnetworks.info/2010/08/mpls-control-plane-and-data-plane.html

Configuración MPLS de Cisco IOS software Lobo, L. (s.f.). Configuración MPLS de Cisco IOS software. En L. Lancy (Ed.). Cisco. Obtenido de http://flylib.com/books/en/2.686.1.19/1/

Autor. (s.f.).

Araujo, G. (21 de julio de 2016). *academica.edu*. Obtenido de academia: https://www.academia.edu/7660657/MPLS_Multiprotocol_Label_Switching

Turmero, P. (21 de julio de 2016). *monografias*. Recuperado el 21 de julio de 2016, de monografias.com: http://www.monografias.com/trabajos108/pos-packet-over-sonet-y-mplsa-multiprotocol-label-switching/pos-packet-over-sonet-y-mplsa-multiprotocol-label-switching2.shtml

Orozco, F. (3 de septiembre de 2014). Diseño de una red privada virtual con tecnología MPLS para la Carrera de Ingeniería de Networking de la Universidad de Guayaquil. *tesis de maestria*, 11. guayaquil.

Hirchoren, G. (20 de enero de 2000). *slide*. Recuperado el 21 de julio de 2016, de slide player: http://slideplayer.es/slide/1641927/

Gokhankosem. (23 de mayo de 2011). *challenge Ip Networking*. Recuperado el 22 de julio de 2016, de http://ipcisco.com/mpls-overview-part-1/

Faizal, R. (24 de june de 2010). *the knowledge is power*. Recuperado el 22 de julio de 2016, de mpls: https://faizalrahimi.wordpress.com

Rahman, M. (31 de julio de 2013). *belajar jaringan komputer*. Recuperado el 22 de julio de 2016, de (Go)-Blog: https://belajarcomputernetwork.com/tag/data-plane/

Ghein, L. d. (2007). *MPLS Fundamentals.* indianapolis, usa: cisco press.

Vidal, O. (29 de noviembre de 2008). *wordpress*. Recuperado el 22 de julio de 2016, de administrador de redes: https://omar1985.wordpress.com

Cisco. (2013). *MPLS Label Distribution Protocol (LDP).* San Jose, usa : Cisco Systems.

Cisco. (3 de noviembre de 2005). Obtenido de http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t2/ftldp41.html

Lobo, L. (2005). *Configuración MPLS de Cisco IOS Software.* indianapolis: cisco.

Kumar, C. (5 de agosto de 2010). *Mpls : the core*. Obtenido de blogspot: http://chetanress.blogspot.com/2010/08/mpls-label-distribution-modes.html

http://ldc.usb.ve/~poc/RedesII/Grupos/G5/funcionamiento_esquema.htm. (s.f.). Recuperado el 26 de julio de 2016, de http://ldc.usb.ve/~poc/RedesII/Grupos/G5/funcionamiento_esquema.htm

catarian.udlap. (s.f.). Recuperado el 26 de julio de 2016, de http://catarina.udlap.mx/u_dl_a/tales/documentos/lep/rubio_s_d/capitulo2.pdf

Barberá, J. (22 de noviembre de 2007). Recuperado el 26 de julio de 2016, de http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.9.gif

Barberá, J. (22 de noviembre de 2007). Recuperado el 26 de julio de 2016, de http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html

Virtuales, R. P. (28 de julio de 2014). *Universidad Tecnica Federico Santa Maria.* Recuperado el 27 de julio de 2016, de http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G20/Redes%20Privadas%20Virtuales%20(VPN).pdf

Tecnico, I. S. (30 de noviembre de 2011). Recuperado el 27 de julio de 2016, de http://comp.ist.utl.pt/aaa/Prog/Manual%20-%20Curso%20Redes%20Privadas%20Virtuales.pdf

Cisco. (23 de junio de 2008). Recuperado el 27 de julio de 2016, de http://www.cisco.com/cisco/web/support/LA/7/74/74718_how_vpn_works.pdf

Jonathan. (23 de septiembre de 2009). *Computo Practico*. Recuperado el 27 de julio de 2016, de http://computopractico.blogspot.com/2009_09_01_archive.html

Rodriguez, D. (noviembre de 2008). Recuperado el 27 de julio de 2016, de http://www.ub.edu.ar/investigaciones/tesinas/259_rodriguez.pdf

Rodriguez, D. (2 de enero de 2013). *networkfaculty*. Recuperado el 28 de julio de 2016, de http://blog.networkfaculty.com/es/mpls/mpls-vpn-route-distinguisher-y-route-target/

Perkin, R. (9 de mayo de 2013). Recuperado el 28 de julio de 2016, de http://www.rogerperkin.co.uk/ccie/mpls/route-distinguisher-vs-route-target/

Alejandro. (20 de octubre de 2007). Recuperado el 29 de julio de 2016, de http://enredajo.blogspot.com/2009/03/que-es-una-vpn-y-tipos-de-vpn.html

nethumans. (2013). *empresa*. Recuperado el 29 de julio de 2016, de https://www.nethumans.com/solutions/itSecurity/VPN.aspx

wikispaces. (s.f.). Obtenido de http://redprivadavirtualiut.wikispaces.com/Tipos+de+VPN

redeszone. (17 de marzo de 2014). *redeszone.net*. Recuperado el 29 de julio de 2016, de http://www.redeszone.net/ipsec-todo-lo-que-debes-saber-sobre-ipsec-recopilacion-de-articulos/

junaedi, f. (12 de agosto de 2008). Recuperado el 29 de julio de 2016, de https://feryjunaedi.wordpress.com/2008/08/12/simple-configuration-gre-tunnel/

Cisco. (2016). Cisco Group Encrypted Transport VPN Configuration Guide, Cisco IOS XE Release 3S. En cisco, *Cisco Group Encrypted Transport VPN Configuration Guide.* san jose, california, USA.

Gentil, R. (21 de agosto de 2014). *Network bits* . Recuperado el 2 de agosto de 2016, de A group conversation. Getting started with GETVPN and crypto GDOI.: https://rsnetworkingbits.wordpress.com/2014/08/21/a-group-conversation-getting-started-with-getvpn-and-crypto-gdoi/

Haseeb Niazi, N. S. (2015). Group Encrypted Transport VPN (Get VPN) . En U. b. Sastry, *Group Encrypted Transport VPN (Get VPN) Design and Implementation Guide.* cisco systems.

Haseeb Niazi, N. S. (2015). Group Encrypted Transport VPN (Get VPN) . En S. Sastry, *Group Encrypted Transport VPN (Get VPN) Design and Implementation Guide.* cisco systems.

cisco. (2016). Cisco Group Encrypted Transport VPN Configuration Guide. En cisco, *Cisco Group Encrypted Transport VPN Configuration Guide, Cisco IOS XE Release 3S.* san jose , california, usa: cisco systems.

Haseeb Niazi, N. S. (2015). Group Encrypted Transport VPN (Get VPN). En S. Sastry, *Group Encrypted Transport VPN (Get VPN) Design and Implementation Guide.* san jose, california, usa: cisco systems.

Haseeb Niazi, N. S. (2015). Group Encrypted Transport VPN (Get VPN). En cisco, *Group Encrypted Transport VPN (Get VPN) Design and Implementation Guide.* san jose, california, usa: cisco systems.

Cisco. (2016). Cisco Group Encrypted Transport VPN . En Cisco, *Cisco Group Encrypted Transport VPN Configuration Guide, Cisco IOS XE Release 3S.* san jose, california, usa: cisco systems.

Tides, B. (4 de agosto de 2013). Recuperado el 10 de agosto de 2016, de http://www.binarytides.com/kali-linux-security-distro/

Gonzalez Perez, P., Sanchez Garces, G., & Soriano de la Camara, J. M. (2013). *Pentesting con Kali.* Mostoles, Madrid, España: 0xWORD Computing.

Caballero, Q. A. (2015). *reydes.* Recuperado el 10 de agosto de 2016, de reydes.com: http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf

Gonzalez Perez, P., Sanchez Garces, G., & Soriano de la Camara, J. M. (2013). *Pentesting con Kali.* Mostoles, Madrid, España: 0xWORD Computing.

X.805(ITU), I. (29 de octubre de 2003). *ITU*. Recuperado el 16 de agosto de 2016, de Security architecture for systems providing end-to-end communications: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.805-200310-I!!PDF-E&type=items

Sanchez, R. (11 de marzo de 2014). *Seguridad Informatic1 1314*. Recuperado el 18 de agosto de 2016, de blogspot: http://rsanchezgsi1314.blogspot.com/2014_03_01_archive.html

Ternero, M. R. (2003). *Seguridad en redes y protocolos asociados*. Recuperado el 24 de agosto de 2016, de http://www.dte.us.es/personal/mcromero/docs/ip/tema-seguridad-IP.pdf

Burton, L. (26 de junio de 2014). *penflip*. Recuperado el 24 de agosto de 2016, de implementación VPN: https://www.penflip.com/Joan/implementacion-vpn/blob/master/chapter1.txt

RFC2408. (NOVIEMBRE de 1998). *IETF.* Recuperado el 25 de AGOSTO de 2016, de http://www.ietf.org/rfc/rfc2408.txt

Cisco. (2 de agosto de 2013). *Cisco Systems.* Recuperado el 7 de septiembre de 2016, de mpls ldp: http://www.cisco.com/cisco/web/support/LA/107/1073/1073692_mp_ldp_autoconfig_ps6922_TSD_Products_Configuration_Guide_Chapter.html?bid=0900e4b182096539

Cisco. (29 de junio de 2009). *Cisco systems*. Recuperado el 11 de septiembre de 2016, de https://supportforums.cisco.com/document/13576/how-configure-gre-tunnel

Cisco. (4 de 11 de 2006). *Cisco*. Recuperado el 4 de 11 de 2016, de http://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/enterprise-class-teleworker-ect-solution/prod_brochure0900aecd80582078.pdf

Pérez, S. (19 de Noviembre de 2001). *frlp*. Recuperado el 19 de marzo de 2016, de Análisis del protocolo IPSec: http://www.frlp.utn.edu.ar/materias/internetworking/apuntes/IPSec/ipsec.pdf

Barberá, J. (5 de febrero de 2000). *rediris.es*. Recuperado el 21 de noviembre de 2016, de http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html

Cisco. (2 de junio de 2016). *Techexams*. Obtenido de www.techexams.net: http://www.techexams.net/forums/ccie/115361-cisco-group-encrypted-transport-vpn-get-vpn.html

UNAD. (9 de agosto de 2011). *datateca.unad*. Recuperado el 16 de agosto de 2016, de arquitectura de seguridad en redes: http://datateca.unad.edu.co/contenidos/233015/233015Exe/leccin_19_arquitectura_de_seguridad_en_redes.html

Cisco. (31 de julio de 2013). *cisco*. Obtenido de cisco.com: http://www.cisco.com/cisco/web/support/LA/7/75/75045_IPSECpart1.html