DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

MAESTRÍA EN REDES DE INFORMACIÓN Y CONECTIVIDAD
PROMOCIÓN I

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER

TEMA: "ESTUDIO COMPARATIVO ENTRE IPSEC Y MPLS PARA REDES PRIVADAS VIRTUALES (VPN)"

AUTOR: BRITO AYALA JUAN CARLOS

DIRECTOR: CHAFLA JUAN FRANCISCO

SANGOLQUÍ

2015

DEPARTAMENTO DE ELECTRICA Y ELECTRÓNICA

MAESTRÍA EN REDES DE INFORMACIÓN Y CONECTIVIDAD
PROMOCIÓN I

CERTIFICACIÓN

Certifico que el trabajo de titulación, "ESTUDIO COMPARATIVO ENTRE IPSEC Y MPLS PARA REDES PRIVADAS VIRTUALES (VPN).**",** realizado por el señor BRITO AYALA JUAN CARLOS, 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 BRITO AYALA JUAN CARLOS para que lo sustente públicamente.

Quito, abril del 2015

Atentamente,

Msc Juan Francisco Chafla
DIRECTOR

DEPARTAMENTO DE ELECTRICA Y ELECTRÓNICA

MAESTRÍA EN REDES DE INFORMACIÓN Y CONECTIVIDAD
PROMOCIÓN I

AUTORÍA DE RESPONSABILIDAD

Yo, JUAN CARLOS BRITO AYALA, con cédula de identidad N° 1714222682 declaro que este trabajo de titulación "ESTUDIO COMPARATIVO ENTRE IPSEC Y MPLS PARA REDES PRIVADAS VIRTUALES (VPN).**",** 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.

Quito, Abril de 2015

_____

Ing. Juan Carlos Brito Ayala
C.C. 171422268-2

DEPARTAMENTO DE ELECTRICA Y ELECTRÓNICA

MAESTRÍA EN REDES DE INFORMACIÓN Y CONECTIVIDAD
PROMOCIÓN I

AUTORIZACIÓN

Yo, Juan Carlos Brito Ayala, autorizo a la Universidad de las Fuerzas Armadas " ESPE" a publicar en la biblioteca Virtual de la institución el presente trabajo "ESTUDIO COMPARATIVO ENTRE IPSEC Y MPLS PARA REDES PRIVADAS VIRTUALES (VPN).**",** cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Quito, Abril de 2015

_____

Ing. Juan Carlos Brito Ayala
C.C. 171422268-2

DEDICATORIA

Principalmente dedico este trabajo a mi esposa Rossana y a mi hija Isabella, pues son el motivo primordial y la razón para todos los proyectos que tengo en la vida, me dieron la fortaleza y el empuje para terminar este escalón más en mi preparación académica. A mis padres por inculcarme siempre los estudios, los valores y principios que marcan mi vida profesional.

AGRADECIMIENTO

Un agradecimiento a todos los que de una u otra forma han participado en la culminación de este proyecto, Coordinador, Director, Oponente, a Enrique Erazo y a Level3 por el apoyo con los equipamientos de prueba y a Edgar Sanchez compañero de la Maestría por su guía y ánimos brindados.

ÍNDICES DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El documento constituye una guía para la evaluación del diseño e implementación de una red de area extendida Wan basada en los principales tipos de redes privadas virtuales o VPN. Se analizó en base a pruebas de laboratorio el comportamiento de este tipo de VPN frente a diferentes tipos de tráfico y/o protocolos orientados y no orientados a conexión como son TCP y UDP respectivamente, y evaluando el desempeño que cada sistema posee frente a los diferentes tipo y tamaños de paquetes que posee la transmisión de información. El manejo del paquete IP original que realiza cada tecnología VPN o sistema a evaluar, así como el procesamiento que usan los equipos para transmitir esta información son los decisorios para la elección de una tecnología de red Wan. El desarrollo de aplicaciones de evaluación o desempeño de redes tales como JPERF y analizadores de protocolos como Wireshark han hecho posible bajo un escenario o maqueta de pruebas de laboratorio obtener resultados comparativos de tres sistemas VPNs.

.

PALABRAS CLAVE

- RED PRIVADA VIRTUAL-VPN.
- PROTOCOLO DE INTERNET–IP
- MULTIPROTOCOLO DE SWITCHEO DE ETIQUETAS–MPLS
- PROTOCOLO DE INTERNET SEGURO–IPSEC
- PROTOCOLO DE CONTROL DE TRANSPORTE–TCP

ABSTRACT.

The document is a guide for the evaluation of the design and implementation of a Wide Area network, based on the main types of virtual private network or VPN. Analyzes was made through laboratory tests the behavior of this type of VPN against different types of traffic and / or oriented and connectionless such as protocols TCP and UDP respectively, and evaluating the performance that each system has against different types and sizes of packets about transmission of information. The handling of the original IP packet that carries each VPN technology or system to be evaluated, as well as the processing equipment used to transmit this information for decision-making are choosing a network technology Wan. The development of applications or network performance tools for evaluation like JPerf and protocol analyzers such as Wireshark made possible under a scenario or model of laboratory tests to obtain comparative results of three VPNs systems.

KEY WORDS

- VIRTUAL PRIVATE NETWORK-VPN.
- INTERNET PROTOCOL–IP
- MULTIPROTOCOL LABEL SWITCHING–MPLS
- INTERNET PROTOCOL SECURITY–IPSEC
- TRANSPORT CONTROL PROTOCOL–TCP

CAPITULO I

CONTEXTO DEL PROYECTO

1.1 Introducción

En lo que respecta a las redes de Telecomunicaciones la industria y desarrolladores de tecnología en la actualidad se encuentran en pleno crecimiento a nivel mundial, refiriéndonos a los estudios de las tendencias del mercado, hacia las comunicaciones unificadas de servicios en donde se convergen la voz, video y datos, estos representados por las aplicaciones sobre una única plataforma de red segura y confiable, en base a esta premisa existen dos principales tecnologías de redes privadas virtuales como soluciones a nivel Wan; IPSEC y MPLS sobre las que se puede implementar esta convergencia de servicios.

Una red privada virtual es un grupo de dos o más sistemas de computadoras conectadas en condiciones seguras a través una red pública o una red externa a la las fuentes de información. Las condiciones de seguridad en un VPN son definidas de una tecnología a otra, implementadas en diferentes capas del modelo OSI sin embargo la mayoría de expertos en seguridad coinciden que en las VPN deberían estar dotadas de encriptación y una autenticación solida entre los equipos que la forman para ocultar o enmascarar la información frente a posibles atacantes desde la red pública.

MPLS (siglas de Multiprotocol Label Switching) es un mecanismo de transporte de datos estándar creado por la IETF y definido por el RFC 3031, opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes; ofrece una plataforma en donde las primordiales características son el ser full-mesh, aplicabilidad de calidad de servicio la misma que se mantiene a nivel de todo el transporte por el Backbone IPv4 del proveedor, la diferenciación y tratamiento especial de las diferentes tecnologías que son manejadas por las TICS (Tecnologías de la

información y comunicación), la convergencia de datos, voz y video sobre una plataforma única hace que MPLS sea la mejor opción tecnológicamente.

IPsec (abreviatura de Internet Protocol Security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el protocolo de Internet IPv4, autenticando y/o encriptado cada paquete IPv4 en el flujo de datos, es un protocolo de seguridad de extremo a extremo; toda la funcionalidad e inteligencia de la conexión VPN la mantienen los equipos externos sobre la cual está configurada la misma; la red pública o del proveedor no es consciente de la existencia de la VPN ya que IPsec crea túneles que aseguran el transporte de datos de aplicación mediante encapsulación, las direcciones fuente y destino de los paquetes IP son las direcciones de los puntos extremos del túnel.

1.2 Objetivo General

Determinar el desempeño, mediante simulaciones con pruebas reales de laboratorio el desempeño de una red IPVPN-MPLS versus una red IPsec sobre un red de Internet y de igual manera versus una tecnología DMVPN sobre MPLS.

1.3 Objetivo Específico

- Determinar con pruebas y simulaciones el desempeño de una plataforma IPVPN-MPLS para tráfico TCP, UDP, voz y video.
- Determinar con pruebas y simulaciones el desempeño de una plataforma IPsec sobre Internet para tráfico TCP, UDP, voz y video.
- Determinar con pruebas y simulaciones el desempeño de una plataforma DMVPN sobre MPLS para tráfico TCP, UDP, voz y video.
- Determinar el porcentaje y variables de desempeño comparativo en base a las pruebas realizadas en los tres escenarios.

1.4 Justificación e importancia

En base a una investigación y análisis de desempeño de las tecnologías de redes IPsec y MPLS se quiere desarrollar un marco comparativo en ventajas, desventajas,

pruebas y simulaciones que nos permitan tener una visión más puntual de cada una al momento de desarrollar un proyecto de redes de datos y telecomunicaciones.

Actualmente sobre MPLS se maneja el transporte de IPv4 inseguro, refiriéndonos a la palabra inseguro como susceptible de ser copiado y en IPsec se maneja transporte IPv4 seguro sobre una plataforma insegura; el desempeño de los servicios depende de las tecnologías de red de acceso que ofrecen los proveedores a nivel WAN, existe una sola desventaja en cuanto la seguridad de las redes MPLS puesto que; a pesar que en una red de este tipo la seguridad a nivel de backbone es similar a la que presenta las redes Frame – relay; la integridad y la privacidad del tráfico IPv4 que pasa por las infraestructura, redes y equipos externos están siempre ligadas a los convenios y acuerdos de confidencialidad que ofrecen los ISP.

Sin embargo a nivel técnico sigue existiendo la manera de que la información pueda ser vulnerable en cuanto a la privacidad debido a que no existe ningún tipo de encriptación en el transporte de la información, teniéndose para las empresas teóricamente un hueco de seguridad; en cambio con IPsec por lo general se encuentra montada sobre Internet en esquema VPN punto a punto, teniendo muchas desventajas como son la dificultad implementar un ambiente mallado, la susceptibilidad a ataques de denegación de servicio por estar montada sobre una red pública y deficiencia en el funcionamiento de calidad de servicio.

En un esquema mixto usando DMVPN sobre MPLS se resuelve el tema de esta vulnerabilidad manteniéndose las características primordiales de las dos tecnologías. Efectuando el análisis por medio de pruebas y simulaciones en un ambiente de laboratorio, se obtendrá parámetros medibles del desempeño de las aplicaciones en comparación con IPsec, MPLS manejadas independientemente

CAPITULO II

MARCO TEORICO

2.1. Modos de Transporte de Datos.

Para enfocarse en los modos de transporte que tiene la información en las redes de datos se debe tener claro con una breve perspectiva el modelo OSI en el cual se basan todos los sistemas de telecomunicaciones y redes de datos.

2.2. Modelo OSI.

El modelo de interconexión de sistemas abiertos, también llamado OSI (en inglés open system interconnection) es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización en el año 1984. Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones. El núcleo de este Estándar es el modelo de referencia OSI, una normativa formada por siete capas que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones. Siguiendo el esquema de este modelo se crearon numerosos protocolos. El advenimiento de protocolos más flexibles donde las capas no están tan desmarcadas y la correspondencia con los niveles no era tan clara puso a este esquema en un segundo plano. Sin embargo es muy usado en la enseñanza como una manera de mostrar cómo puede estructurarse una "pila" de protocolos de comunicaciones.

El modelo especifica el protocolo que debe ser usado en cada capa, y suele hablarse de modelo de referencia ya que es usado como una gran herramienta para la enseñanza de comunicación de redes. Se trata de una normativa estandarizada útil debido a la existencia de muchas tecnologías, fabricantes y compañías dentro del mundo de las comunicaciones, y al estar en continua expansión, se tuvo que crear un método para que todos pudieran entenderse de algún modo, incluso cuando las tecnologías no coincidieran. De este modo, no importa la localización geográfica o el lenguaje utilizado. Todo el mundo debe atenerse a unas normas mínimas para poder

comunicarse entre sí. Esto es sobre todo importante cuando hablamos de la red de redes, es decir, Internet. Este modelo está dividido en siete capas:

2.2.1 Capa 1 – Capa Física.

Es la que se encarga de las conexiones globales de la computadora hacia la red, tanto en lo que se refiere al medio físico como a la forma en la que se transmite la información. Sus principales funciones se pueden resumir como definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados (o no, como en RS232/EIA232), coaxial, guías de onda, aire, fibra óptica.

2.2.2 Capa 2 – Capa de Enlace de Datos.

Esta capa se ocupa del direccionamiento físico, de la topología de la red, del acceso al medio, de la detección de errores, de la distribución ordenada de tramas y del control del flujo. Por lo cual es uno de los aspectos más importantes a revisar en el momento de conectar dos ordenadores, ya que está entre la capa 1 y 3 como parte esencial para la creación de sus protocolos básicos (MAC, IP), para regular la forma de la conexión entre computadoras así determinando el paso de tramas (trama = unidad de medida de la información en esta capa, que no es más que la segmentación de los datos trasladándolos por medio de paquetes), verificando su integridad, y corrigiendo errores.

2.2.3 Capa 3 – Capa de Red.

Se encarga de identificar el enrutamiento existente entre una o más redes. Las unidades de información se denominan paquetes, y se pueden clasificar en protocolos enrutables y protocolos de enrutamiento.

Enrutables: viajan con los paquetes (IP, IPX, APPLETALK).

Enrutamiento: permiten seleccionar las rutas (RIP,IGRP,EIGRP,OSPF,BGP).

El objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino, aun cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea se denominan encaminadores, aunque es más frecuente encontrarlo con el

nombre en inglés routers. Los routers trabajan en esta capa, aunque pueden actuar como switch de nivel 2 en determinados casos, dependiendo de la función que se le asigne. Los firewalls actúan sobre esta capa principalmente, para descartar direcciones de máquinas. En este nivel se realiza el direccionamiento lógico y la determinación de la ruta de los datos hasta su receptor final.

2.2.4 Capa 4 – Capa de Transporte.

Capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la de destino, independizándolo del tipo de red física que se esté utilizando. La PDU de la capa 4 se llama Segmento o Datagrama, dependiendo de si corresponde a TCP o UDP. Sus protocolos son TCP y UDP; el primero orientado a conexión y el otro sin conexión. Trabajan, por lo tanto, con puertos lógicos y junto con la capa red dan forma a los conocidos como Sockets IP: Puerto (191.16.200.54:80).

2.2.5 Capa 5 - Capa de Sesión.

Esta capa es la que se encarga de mantener y controlar el enlace establecido entre dos computadores que están transmitiendo datos de cualquier índole. Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción. En muchos casos, los servicios de la capa de sesión son parcial o totalmente prescindibles.

2.2.6 Capa 6 - Capa de Presentación.

El objetivo es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres los datos lleguen de manera reconocible. Esta capa es la primera en trabajar más el contenido de la comunicación que el cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas. Esta capa también permite cifrar los datos y comprimirlos. Por lo tanto, podría decirse que esta capa actúa como un traductor.

2.2.7 Capa 7- Capa de Aplicación.

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (Post Office Protocol y SMTP), gestores de bases de datos y servidor de ficheros (FTP), por UDP pueden viajar (DNS y Routing Information Protocol). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar. Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente.

2.2.8 Paquetes de la Arquitectura TCP/IP.

Para cada capa del modelo OSI y/o modelo TCP/IP existen las unidades de datos de protocolo, también llamadas PDU, se utilizan para el intercambio de información entre capas disparejas dentro de cada capa del modelo OSI. Cada capa del modelo OSI en el origen debe comunicarse con capa igual en el lugar destino. Esta forma de comunicación se conoce como comunicación de par-a-par. Durante este proceso, cada protocolo de capa intercambia información en lo que se conoce como unidades de datos de protocolo, entre capas iguales. Cada capa de comunicación, en el computador origen, se comunica con un PDU específico de capa y con su capa igual en el computador destino. En el contexto del Modelo OSI tenemos los siguientes PDU más importantes.

2.2.8.1 PDU de Capa 1 – Bit.

El PDU correspondiente a la capa 1 es el bit, representación digital de 1 o 0 binario, consiste en una secuencia de bits de preámbulo, una cabecera y de un PDU de capa superior conocido como PDU de capa 2 llamados trama.

2.2.8.2 PDU de Capa 2 – Trama.

El PDU correspondiente a la capa 2 es la trama, al igual que en la capa 1 consta de una cabecera o header seguida de un PDU de capa 3 llamado paquete y un valor de secuencia de corrección de errores o checksum.

2.2.8.3 PDU de Capa 3 – Paquete.

El PDU correspondiente a la capa 3 es el paquete, al igual que en las anteriores capas consta de una cabecera o header seguida de un PDU de capa 4 llamado segmento.

2.2.8.4 PDU de Capa 4 – Segmento.

El PDU correspondiente a la capa 4 es el segmento, al igual que en las capas anteriores consta de una cabecera o header seguida de un PDU de capa superior. Como se puede observar en la figura 1 desde la capa 1 hasta la capa 7 existe la misma operación o funcionalidad de cabecera de capa seguida del PDU de capa superior.

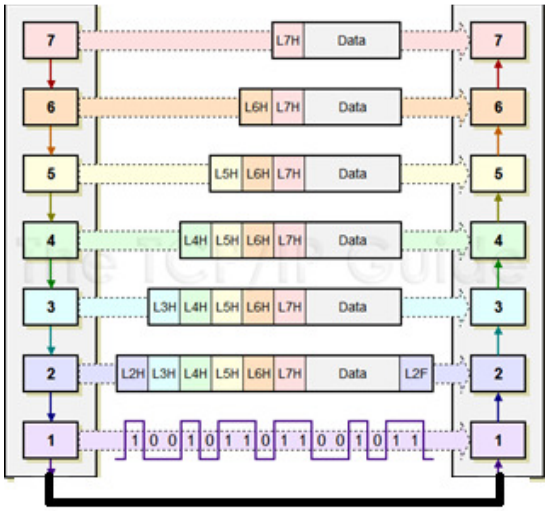

Figura 1. Paquetes de la arquitectura TCP/IP

Fuente: (Elaborado por el Autor)

2.3. Protocolos de la Familia TCP/IP.

Un protocolo es un método estándar que permite la comunicación entre procesos (que potencialmente se ejecutan en diferentes equipos) y un conjunto de reglas y procedimientos que deben respetarse para el envío y la recepción de datos a través de una red. En Internet existen diversos protocolos de acuerdo a la comunicación y que pertenecen a una sucesión o a un conjunto de protocolos relacionados entre sí (familias de protocolos de Internet).

La familia de protocolos de Internet es un conjunto de protocolos de reden la que se basa Internet y que permiten la transmisión de datos entre redes de computadoras. En ocasiones se le denomina conjunto de protocolos TCP/IP, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse, y que son los más utilizados de la familia. Existen tantos protocolos en este conjunto que llegan a ser más de 100 diferentes, entre ellos se destacan los siguientes:

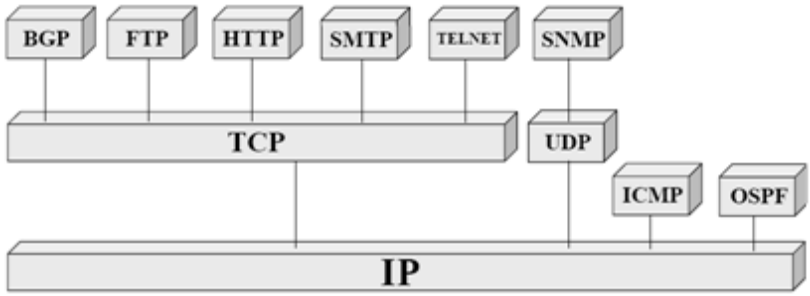

Figura 2. Protocolos TCP/IP

Fuente: (Elaborado por el Autor)

2.3.1 TCP - Protocolo de Control de Transmisión.

El Protocolo de Control de Transmisiones uno de los protocolos fundamentales en la comunicación IP .Muchos programas dentro de una red de datos compuesta por computadoras pueden usar TCP para crear conexiones entre ellos a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron.

También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto. Este es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, posibilita la administración de datos que vienen del nivel más bajo del modelo. Cuando se proporcionan los datos al protocolo IP, los agrupa en datagramas IP, fijando el campo del protocolo en 6 para que sepa con anticipación que el protocolo es TCP.

Como es un protocolo orientado a conexión permite que dos máquinas que están comunicadas controlen el estado de la transmisión. Las principales características del protocolo TCP son las siguientes: Da soporte a muchas de las aplicaciones más populares de Internet, incluidas HTTP, SMTP, SSH y FTP. Permite colocar los datagramas nuevamente en orden cuando vienen del protocolo IP. También permite el monitoreo del flujo de los datos y así evita la saturación de la red.

Permite que los datos se formen en segmentos de longitud variada para "entregarlos" al protocolo IP. Permite multiplexar los datos, es decir, que la información que viene de diferentes fuentes por ejemplo, aplicaciones en la misma línea pueda circular simultáneamente. Por último, permite comenzar y finalizar la comunicación amablemente.

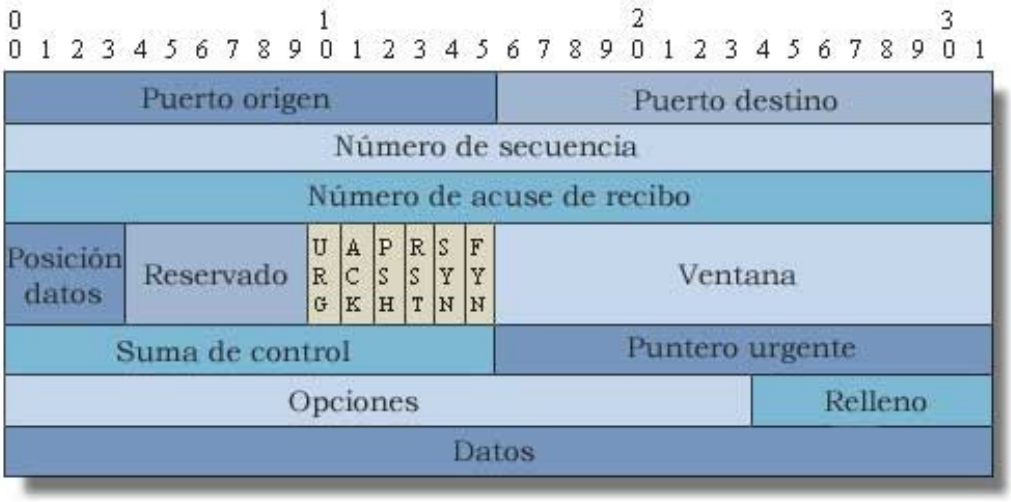

Figura 3. Segmento TCP/IP

Fuente: www.openredes.com

2.3.2 UDP – Protocolo de Datagramas de Usuario.

Es un protocolo del nivel de transporte basado en el intercambio de datagramas RFC 768. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni

control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción. Su uso principal es para protocolos como DHCP, BOOTP, DNS, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

2.3.3 IP - Protocolo de Internet.

El Protocolo de Internet es un protocolo de capa 3 no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados. Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas. En particular, en IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes.

El Protocolo de Internet provee un servicio de datagramas no fiable, también llamado del mejor esfuerzo; IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad mediante sumas de comprobación de sus cabeceras y no de los datos transmitidos.

Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP.

Si los datagramas a transmitir supera el tamaño máximo negociado en el tramo de red por el que van a circular podrá ser dividida en paquetes más pequeños, y reensamblada luego cuando sea necesario. Estos fragmentos podrán ir cada uno por un camino diferente dependiendo de cómo estén congestionadas las rutas en cada momento. Las cabeceras IP contienen las direcciones de las máquinas de origen y destino (direcciones IP), direcciones que serán usadas por los conmutadores de paquetes y los enrutadores para decidir el tramo de red por el que renviarán los paquetes.

Las direcciones IP son direcciones numéricas compuestas por cuatro números enteros (4 bytes) entre 0 y 255, y escritos en el formato xxx.xxx.xxx.xxx. Por ejemplo, 194.153.205.26 es una dirección IP en formato técnico.

Los equipos de una red utilizan estas direcciones para comunicarse, de manera que cada equipo de la red tiene una dirección IP exclusiva.

2.3.4 Consideraciones de Máxima Transferencia de Datos.

Cuando hablamos de máxima transferencia de datos para redes existen muchos parámetros o variables a considerar, pues existen limitaciones a nivel de hardware y protocolos que dificultan el poder obtener una fórmula para obtener este resultado.

2.3.5 MTU - Unidad Máxima de Transferencia.

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

- Ethernet: 1518 bytes
- PPPoE: 1492 bytes
- ATM (AAL5): 8190 bytes

Para el caso de IP, el máximo valor de la MTU es 65.536 bytes. Sin embargo, ése es un valor máximo teórico, pues, en la práctica, la entidad IP determinará el máximo tamaño de los datagramas IP en función de la tecnología de red por la que vaya a ser enviado el datagrama. Por defecto, el tamaño de datagrama IP mínimo es de 576 bytes (512bytes de datos + 64 de cabeceras). Sólo pueden enviarse datagramas más grandes si se tiene conocimiento fehaciente de que la red destinataria del datagrama puede aceptar ese tamaño. En la práctica, dado que la mayoría de máquinas están conectadas a redes Ethernet o derivados, el tamaño de datagrama que se envía es con frecuencia de 1500 bytes.

Los datagramas pueden pasar por varios tipos de redes con diferentes tamaños aceptables antes de llegar a su destino. Por tanto, para que un datagrama llegue sin fragmentación al destino, ha de ser menor o igual que el MTU de todas las redes por las que pase. En el caso de TCP/UDP, el valor máximo está dado por el MSS (Máximo tamaño de segmento), y toma su valor en función de tamaño máximo de datagrama, dado que el MTU = MSS + cabeceras IP + cabeceras TCP/UDP. En concreto, el máximo tamaño de segmento es igual al máximo tamaño de datagrama menos 40 bytes que es número mínimo de bytes que ocuparán las cabeceras IP y TCP/UDP en el datagrama. La mayoría de las redes de área local o que usan ethernet su MTU es de 1500 bytes.

2.3.6 MSS -Tamaño Máximo de Segmento.

El Tamaño Máximo de Segmento es el tamaño más grande de datos, especificado en bytes, que un dispositivo de comunicaciones puede manejar en una única pieza, sin fragmentar. Para una comunicación óptima la suma del número de bytes del segmento de datos y la cabecera debe ser menor que el número de bytes de la unidad máxima de transferencia (MTU) de la red. El MSS tiene gran importancia en las conexiones en bajo IP, particularmente en aplicaciones TCP. Cuando se usa el protocolo TCP para efectuar una conexión, los ordenadores que se conectan deben acordar y establecer el tamaño de la MTU que ambos puedan aceptar. El valor típico de MTU en una red puede ser, por ejemplo, 576 ó 1500 bytes. Tanto la cabecera IP como la cabecera TCP tienen una longitud variable de al menos 20 bytes. En cualquier caso, el MSS es igual a la diferencia MTU - cabecera TCP - cabecera IP.

A medida que los datos son encaminados por la red deben pasar a través de múltiples routers. Idealmente, cada segmento de datos debería pasar por todos los routers sin ser fragmentado. Si el tamaño del segmento de datos es demasiado grande para cualquiera de los routers intermedios, los segmentos son fragmentados. Esto aminora la velocidad de conexión, y en algunos casos esta bajada de velocidad puede ser muy apreciable. La posibilidad de que ocurra esa fragmentación puede ser minimizada manteniendo el MSS tan pequeño como sea razonablemente posible. En la mayoría de los casos, el MSS es establecido automáticamente por el sistema operativo.

2.3.7 Ventana TCP.

Como sabemos, el TCP es un protocolo orientado a conexión, los dos extremos de una conexión dan un seguimiento estricto de todos los datos transmitidos, de modo que todos los segmentos perdidos o mezclados pueden ser retransmitidos o reordenados según sea necesario para mantener un transporte fiable. Para compensar el limitado espacio de búfer (donde los datos recibidos se almacenan temporalmente hasta que la aplicación adecuada puede procesar), los anfitriones TCP se ponen de acuerdo en limitar la cantidad de datos sin acuse de recibo que pueden estar en tránsito en un momento dado. Esto se conoce como el tamaño de la ventana, y se comunica a través de un campo de 16-bit en la cabecera TCP.

Supongamos que tenemos dos hosts, A y B, que forman una conexión TCP. Al comienzo de la conexión, ambas máquinas asignan 32 KB de espacio en el buffer de datos entrantes, de modo que el tamaño de la ventana inicial para cada uno es 32.768.

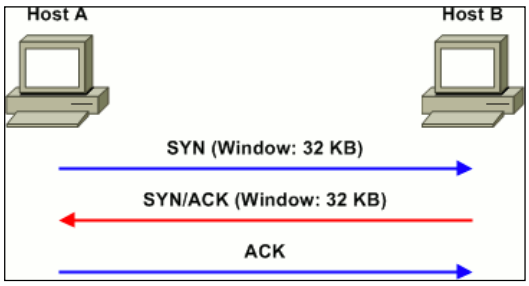

Figura 4. Conexión TCP

Fuente: (Elaborado por el Autor)

Host A necesita enviar datos al host B. Se puede decir que el tamaño de la ventana anunciada seria que B puede transmitir hasta 32.768 bytes de datos (tomando en cuenta el tamaño máximo de segmento en Capa 4 o MMS), antes de que se debe hacer una pausa y esperar un acuse de recibo. Suponiendo un MSS de 1460 bytes, el host A puede transmitir 22 segmentos antes de agotar la ventana TCP del equipo B. Cuando llega el Ack o el acuse de recibo de los datos enviados por el equipo A, el equipo B puede ajustar el tamaño de la ventana. Por ejemplo, si la aplicación de capa superior

tiene solo procesada la mitad del buffer, el host B reduciría su tamaño de la ventana a 16 KB. Si el buffer se encuentra totalmente lleno, el equipo B establece su tamaño de la ventana TCP a cero, lo que indica que no puede aceptar más datos.

En un ambiente LAN con alto ancho de banda y el retardo extremadamente bajo, las ventanas son raramente estresadas a un valor bajo ya que normalmente hay pocos segmentos en tránsito entre dos extremos en un momento dado. En un ambiente de gran ancho de banda y con un alto retardo de la red, ocurre un fenómeno interesante: es posible para maximizar la ventana de recepción del host de destino antes de recibir un acuse de recibo. A modo de ejemplo, supongamos que una conexión TCP se establece entre dos hosts conectados por una ruta de acceso dedicado de 10 Mbps con un retraso de un camino de 80 ms. Ambos anfitriones anuncian el tamaño máximo de ventana de 65.535 bytes (el valor máximo de 16 bits). Podemos calcular la cantidad potencial de los datos en tránsito en una dirección a un punto en el tiempo como el ancho de banda * delay**:** 10.000.000 bps dividido entre 8 bits por byte, multiplicado por 0,08 segundos equivalen a 100,000 bytes.

En otras palabras, si un host. comienza a transmitir al host B de forma continua, se han enviado 100.000 bytes antes de host B recibe el primer byte transmitido Sin embargo, debido a que nuestra máxima ventana de recepción es de sólo 65.535 bytes, el host A tiene que dejar de transmitir una vez que este número se ha alcanzado y espera una confirmación desde el host B. Este retraso pierde el rendimiento potencial, inflando innecesariamente el tiempo que tarda el de transmitir datos a través de la red. Escalado de ventanas TCP se creó para hacer frente a este problema.

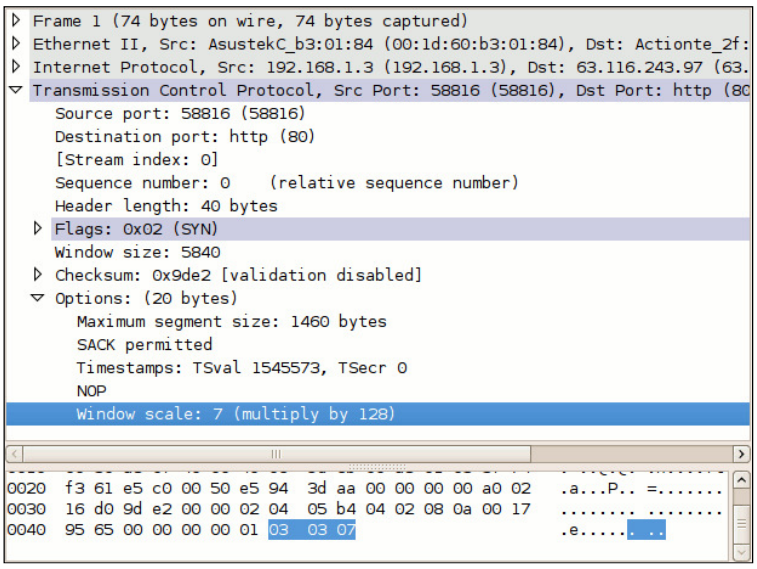

Figura 5. Tamaño de ventana TCP.

Fuente: Programa Wireshark

2.3.8 Ancho de Banda y Throughput.

El ancho de banda y throughput son dos conceptos importantes de la comunicación entre redes que a menudo no son completamente entendidos. El ancho de banda se define técnicamente como la cantidad de información que puede fluir por un elemento de red en un periodo dado de tiempo; por ejemplo, si consideramos un enlace WAN E1 este tiene un ancho de banda simétrico de 2048Kbps; un enlace Fast-Ethernet tiene un ancho de banda de 100Mbps. Como vemos, el ancho de banda se mide en bits por segundo.

Es importante notar que usamos bits (b) por segundo, y la transferencia de archivos se mide en bytes (B). Esto podemos notarlo fácilmente cuando descargamos un archivo y nuestro browser (Firefox, Chrome o Explorer) nos dice que está descargando el archivo a 73.4KB/sec,

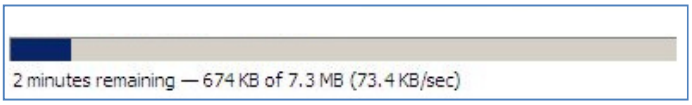

Figura 6. Throughput.

Fuente: (Elaborado por el Autor)

Ahora bien, este ejemplo está basado en un enlace a dedicado a través de un E1 (2048Kbps) este es el ancho de banda del enlace, que se comparte con más usuarios además del archivo, en el caso de las comunicaciones basadas en TCP, hay paquetes de sincronismo (Sync) y acuses de recibo (Ack), relativos al proceso de la ventana TCP y control de flujo, que ocupan ancho de banda pero finalmente no es parte del tráfico interesante, que en este caso es la transferencia del archivo. Se debe considerar que también el otro extremo de la comunicación debe tener un ancho de banda disponible para que la transferencia sea veloz, es decir, si se usara un enlace E3 (34Mbps) y el servidor tiene un ancho de banda de 256Kbps, la descarga será limitada por ese ancho de banda. El ancho de banda es la capacidad teórica disponible de un enlace, 2048Kbps en el ejemplo, pero se puede ver que el archivo baja a una velocidad real de 74.3KB/sec, lo convertimos a Kbps: 74.3x8 = 594Kbps y este es el throughput de la transmisión, si bien el ancho de banda es de 2048Kbps, el throughput es de 594Kbps, es el nivel de utilización real del enlace, o técnicamente es la capacidad de información que un elemento de red puede mover en un periodo de tiempo.

Por ejemplo, un router Cisco 1841 viene equipado con dos puertos Fast Ethernet y sabemos que el ancho de banda de esos puertos es de 100Mbps, pero la capacidad de proceso del router o throughput es de 75Kpps (paquetes por segundo). Teóricamente podemos alcanzar los 100Mbps entre ambas interfaces, pero considerando el paquete mínimo para ethernet con un tamaño de 64bytes el router sólo procesará hasta 38.4Mbps.Adicional a esta consideración se debe tomar en cuenta que el delay (latencia) entre dos puntos afecta el throughput entre ellos. Es decir, si tenemos dos puntos con una latencia alta, la naturaleza de TCP, basado en acuses de recibo (ACK), hará que se inicie el proceso pero con tiempos de espera largos.

La latencia es el tiempo en segundos que le toma a un paquete llegar a un destino. Supongamos que tenemos un enlace Wan de 34Mbps entre dos nodos y queremos pasar un archivo por FTP entre ellos; si la latencia con una tecnología satelital es de 400ms, y la latencia con tecnología de microonda es de 40ms, el mismo enlace presentará throughputs diferentes entre los nodos, donde seguramente rondaremos un throughput en la microonda de aproximadamente diez veces mayor respecto al del enlace satelital, porque al iniciar la sesión de TCP se enviará un paquete que tomará 400ms en ir y venir, y hasta recibir dicha respuesta podremos establecer la sesión; después el control de flujo de TCP exigirá que haya un paquete de acknowledge cada determinado número de paquetes, y debe esperar que llegue, sea procesado y regrese, lo que causa tiempos muertos de utilización del enlace; es decir, tenemos los 34Mbps libres, pero no los estamos usando porque esperamos la respuesta del control de flujo de TCP para continuar.

En conclusión y para efectos de esta tesis, el ancho de banda es la capacidad teórica del elemento de red y el throughput es la utilización que podemos lograr con dicho elemento (router, puerto, enlace WAN, LAN, etc.).

2.4. MPLS – Multi Protocol Label Switching.

MPLS es un método de "forwardear" paquetes a través de una red usando información contenida en etiquetas añadidas en los paquetes IP, se puede considerar un estándar IP de conmutación de paquetes del IETF RFC 3031, que trata de proporcionar algunas de las características de las redes orientadas a conexión a las redes no orientadas a conexión. MPLS soporta múltiple aplicaciones incluyendo: unicast y multicast routing, VPN, ingeniería de tráfico, Qos, etc.

En el encaminamiento IP sin conexión tradicional, la dirección de destino junto a otros parámetros de la cabecera, es examinada cada vez que el paquete atraviesa un router. La ruta del paquete se adapta en función del estado de las tablas de encaminamiento de cada nodo, pero, como la ruta no puede predecirse, es difícil reservar recursos que garanticen la calidad de servicios; además, las búsquedas en tablas de encaminamiento hacen que cada nodo pierda cierto tiempo, que se

incrementa en función de la longitud de la tabla. Sin embargo, MPLS permite a cada nodo, ya sea un switch o un router, asignar una etiqueta a cada uno de los elementos de la tabla y comunicarla a sus nodos vecinos. Esta etiqueta es un valor corto y de tamaño fijo transportado en la cabecera del paquete para identificar un FEC (Forward Equivalence Class), que es un conjunto de paquetes que son reenviados sobre el mismo camino a través de la red, incluso si sus destinos finales son diferentes. MPLS usa un formato de etiqueta de 32-bit la cual es insertada entre la información de capa2 y capa3, y estas etiquetas pueden ser insertadas, cambiadas o removidas.

2.4.1Componentes y características de MPLS.

En MPLS un concepto muy importante es el de LSP (Label Switch Path), que es un camino de tráfico específico a través de la red MPLS, el cual se crea utilizando los LDPs (Label Distribution Protocols), tales como RSVP-TE (ReSerVation Protocol – Traffic Engineering) o CR-LDP (Constraint-based Routing – Label Distribution Protocol).. El LDP posibilita a los nodos MPLS descubrirse y establecer comunicación entre sí con el propósito de informarse del valor y significado de las etiquetas que serán utilizadas en sus enlaces contiguos. Es decir, mediante el LDP se establecerá un camino a través de la red MPLS y se reservarán los recursos físicos necesarios para satisfacer los requerimientos del servicio previamente definidos para el camino de datos. Una red MPLS está compuesta por dos tipos principales de nodos, los LER (Label Edge Routers) y los LSR (Label Switching Routers), tal y como se muestra en el ejemplo de la Figura 7. Los dos nodos son físicamente el mismo tipo de dispositivo, un router o switch que incorporan el software MPLS. Los nodos MPLS al igual que los routers IP normales, intercambian información sobre la topología de la red mediante los protocolos de encaminamiento estándar, tales como ruteo estático, OSPF (Open Shortest Path First), RIP (Routing Information Protocol) y BGP (Border Gateway Protocol), etc, a partir de los cuales construyen tablas de encaminamiento basándose principalmente en la alcanzabilidad a las redes IP destinatarias.

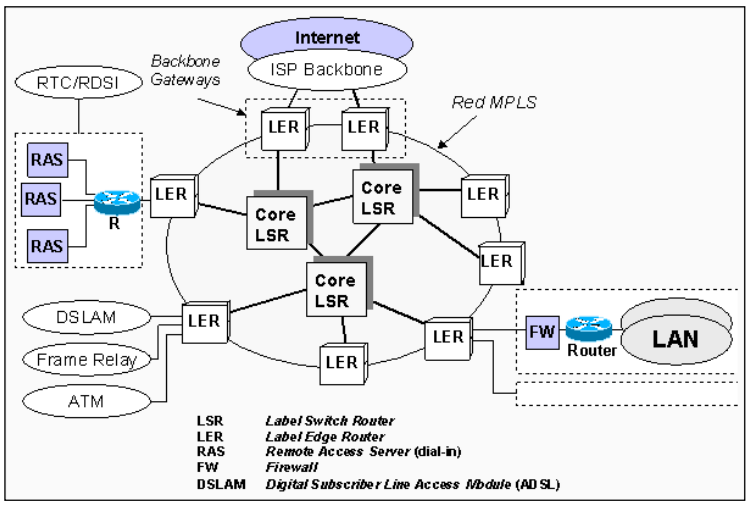

Figura 7. Elementos de MPLS.

Fuente: (http://www.ramonmillan.com/)

Teniendo en cuenta dichas tablas de encaminamiento, que indican la dirección IP del siguiente nodo al que le será enviado el paquete para que pueda alcanzar su destino final, se establecerán las etiquetas MPLS y, por lo tanto, los LSP que seguirán los paquetes.

No obstante, también pueden establecerse LSP que no se correspondan con el camino mínimo calculado por el protocolo de encaminamiento. Los LERs están ubicados en el borde de la red MPLS para desempeñar las funciones tradicionales de encaminamiento y proporcionar conectividad a sus usuarios, generalmente routers IP convencionales.

2.4.2Label Edge Router – LER.

El nodo LER analiza y clasifica el paquete IP entrante considerando hasta el nivel 3, es decir, considerando la dirección IP de destino y la clase de servicio demandada; añadiendo la etiqueta MPLS que identifica en qué LSP está el paquete. Es decir, el LER en vez de decidir el siguiente salto, como haría un router IP normal, decide el camino entero a lo largo de la red que el paquete debe seguir. Una vez asignada la cabecera MPLS, el LER enviará el paquete a un LSR.

2.4.3Label Switching Router – LSR.

Los nodos LSR están ubicados en el núcleo de la red MPLS para efectuar encaminamiento de alto rendimiento basado en la conmutación por etiqueta, considerando únicamente hasta el nivel 2. Cuando le llega un paquete a una interfaz del LSR, éste lee el valor de la etiqueta de entrada de la cabecera MPLS, busca en la tabla de conmutación la etiqueta e interfaz de salida, y reenvía el paquete por el camino predefinido escribiendo la nueva cabecera MPLS. Si un LSR detecta que debe enviar un paquete a un LER, extrae la cabecera MPLS; como el último LER no conmuta el paquete, se reducen así cabeceras innecesarias. Los LSR son conocidos como P Routers (Provider Router) y un LER es conocido también como Edge LSR o PE Router (Provider Edge Router) como se puede ver en la figura 8.

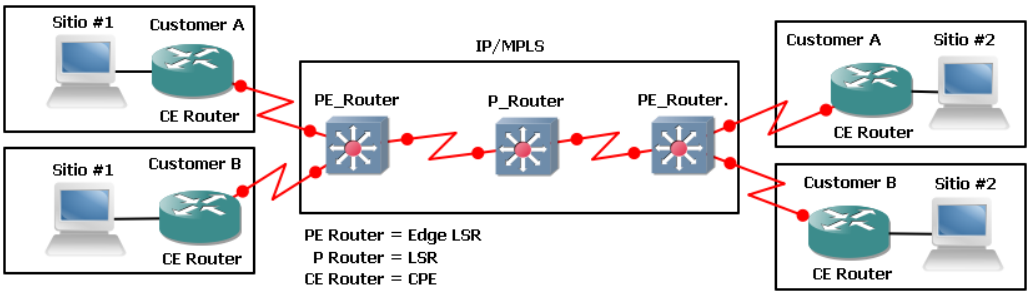

Figura 8. LER y LSR Routers

Fuente: (Elaborado por el Autor)

2.4.4Formato del Paquete MPLS.

El formato de los paquetes MPLS se indica en la figura 9, la cabecera MPLS básica tiene 32 bits, compuesto por los siguientes campos: 20 bits para identificación de la etiqueta o etiqueta MPLS. 3 bits experimentales utilizados para clasificación de servicio. Esto permite identificar el tipo de tráfico. 1 bit para stack o apilamiento jerárquico de etiquetas. Cuando S=0 indica que hay más etiquetas añadidas al paquete. Cuando S=1 indica que es la última etiqueta en el paquete. 8 bits para determinar el tiempo de vida del paquete. Se decrementa en cada salto y si llega a 0 el paquete se descarta

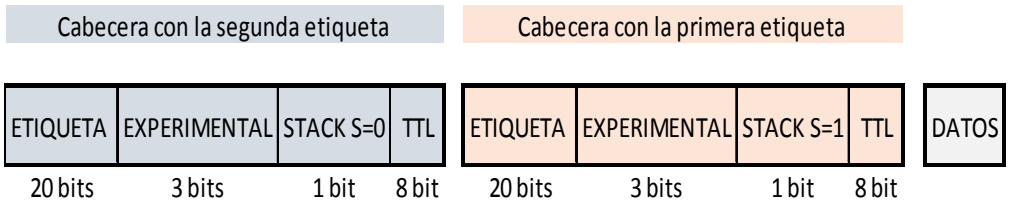

Figura 9. Formato Paquete MPLS.

Fuente: (Elaborado por el Autor)

2.4.5Etiquetas MPLS.

Las etiquetas son campos de la cabecera MPLS de longitud corta y fija (20 bits), que se añaden a los paquetes, con el fin de que estos tengan un determinado tratamiento y encaminamiento en los LSR y en los ruteadores LER que van atravesando hasta llegar a su destino. En cada uno de los equipos de comunicaciones de la red MPLS, se puede realizar los procesos de adición, de extracción o de modificación de las etiquetas de los paquetes, como se muestra en la figura 10.

Esto significa que un determinado paquete puede tener uno o más etiquetas en su cabecera, las cuales serán removidas o modificadas en función del tipo de paquete y en función del destino. Estos procesos permiten realizar el enrutamiento, la agrupación de paquetes, encapsulamiento y la generación de túneles para la transmisión de la información.

Por ejemplo si se desea enviar paquetes de voz, video y datos desde una red de datos IP, los ruteadores LER añaden la etiqueta 0 para cada uno de los paquetes de voz, la etiqueta 1 para los paquetes de video y la etiqueta 2 para los paquetes de datos, posteriormente cada paquete de acuerdo a la etiqueta que lleva es tratado y encolado de acuerdo a la prioridad y ancho de banda asignado para cada FEC en un LSP.

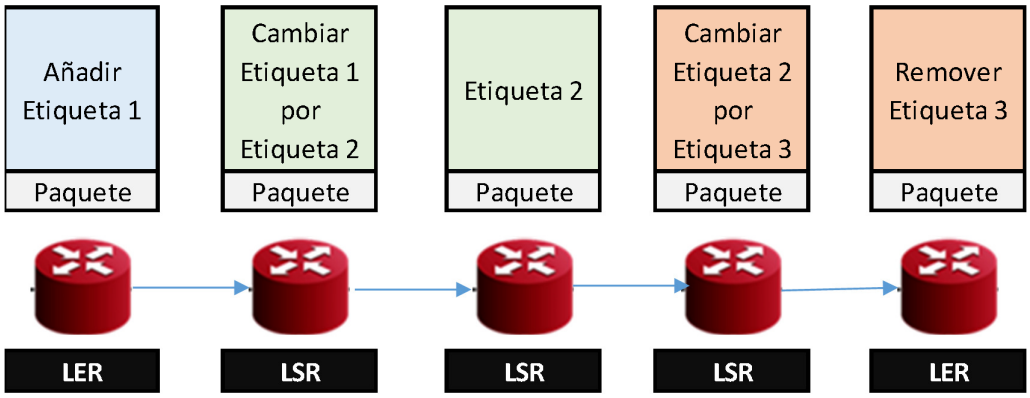

Figura 10. Adición / Modificación / Eliminación de Etiquetas.

Fuente: (Elaborado por el Autor)

2.4.6Clase Equivalente de Reenvío FEC (Forwarding Equivalence Class).

El FEC es un identificador que permite agrupar a los paquetes, para que estos reciban un mismo tratamiento dentro de la red MPLS y puedan ser transmitidos del mismo modo. La agrupación de paquetes se puede realizar por:

Puertos físicos de entrada / salida Origen y destino de los paquetes **-** Prioridad de los paquetes Red origen / red destino **-** Tipo de aplicación Tipo de servicio.

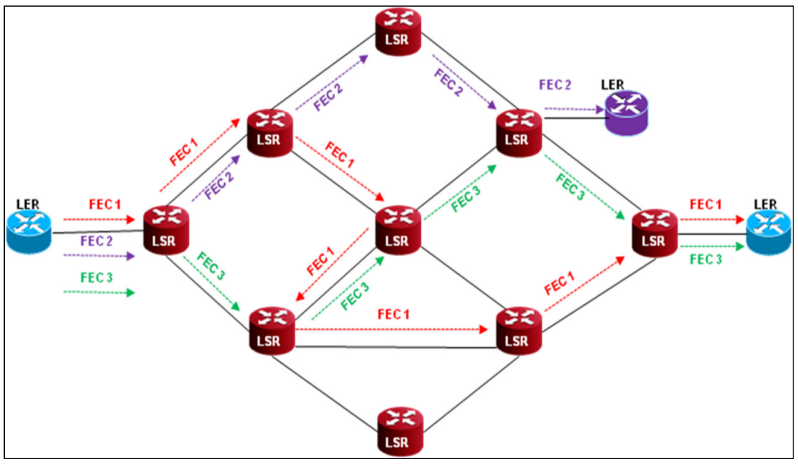

Figura 11. Asignación de FEC's.

Fuente: (Elaborado por el Autor)

Los ruteadores LER clasifican los paquetes de ingreso y los relaciona con un FEC específico. Cada FEC está asociado con una etiqueta apropiada. Cada uno de los FECs son asociados con las etiquetas apropiadas para su re-envío hacia los ruteadores LSR de la red MPLS. Los ruteadores LER son los encargados de poner y remover la primera y la última de las etiquetas de los paquetes, respectivamente. Los ruteadores LSR, reciben los paquetes que transmiten los ruteadores LER y observan únicamente la última etiqueta del paquete y compara con las etiquetas de su tabla de re-envío denominada Base de Información de Etiquetas LIB. Los LSR añadirán, quitarán o cambiarán las etiquetas y reenviarán los paquetes de acuerdo a sus tablas LIB.

Como se observa en la figura 11, todos los paquetes que tienen un mismo FEC, son transmitidos a través de una misma ruta, para lo cual los ruteadores de la red MPLS leen únicamente las etiquetas de los paquetes para determinar los siguientes saltos.

2.4.7Protocolo de Distribución de Etiquetas LDP.

El Protocolo de Distribución de Etiquetas LDP, permite el intercambio de etiquetas entre los equipos de la red MPLS para formar las tablas de rutas Etiquetas / FECs en cada uno de los equipos de comunicaciones. Se utiliza mecanismos de descubrimiento de vecinos cercanos, adyacencia de ruteadores, difusión y notificación de etiquetas y FECs. El protocolo utilizado para el intercambio de etiquetas / FECs entre los ruteadores es el BGP.

2.4.8Redes VPN-MPLS Capa 3

El servicio de VPN en una arquitectura MPLS (RFC2547), permite a un grupo de clientes compartir el medio de transmisión e información de enrutamiento, en donde los ruteadores LSR realizan la separación del tráfico correspondiente a cada uno de los ruteadores LER de los clientes. En un ambiente IPVPN-MPLS los ruteadores LSR se los conoce universalmente como Transit Router o Core Routers. Las IPVPN-MPLS operan en la capa 3 y utilizan el protocolo BGP para generar y trasportar las tablas de enrutamiento. Como ejemplo se tienen dos clientes A, B, que operan en forma independiente los unos de los otros, cuyas redes están identificadas como Red A, Red

B respectivamente, estos clientes internamente en MPLS son identificados a través de VRF's como se indica en la figura 12.

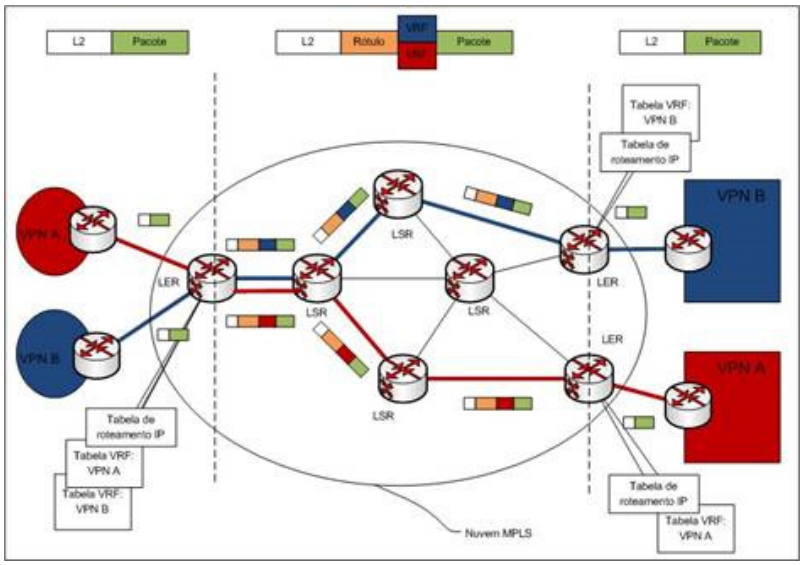

Figura 12. Descripción de IPVPN-MPLS Redes de Clientes Independientes

Fuente: (www.teleco.com.br)

2.4.9VRF - VPN Routing and Forwarding

En redes de datos basadas sobre protocolo IP, la tecnología VRF permite múltiples tablas de rutas separadas las cuales pueden coexistir en el mismo router y al mismo tiempo, crear varios router virtuales sobre un router físico. Al ser todas las tablas de rutas completamente independientes, las mismas direcciones IP que pueden solapar con otras existentes, evitan conflictos y pueden convivir sin problemas. La VPN Routing and Forwarding, es el elemento clave de la tecnología IPVPN-MPLS.

De forma alternativa, un dispositivo de red puede tener la habilidad de configurar diferentes routers virtuales, donde cada uno tiene su propia tabla FIB, la cual no es accesible a los otros posibles routers virtuales en el mismo dispositivo, lo cual garantiza independencia entre clientes en una misma red que comparte infraestructura física como es IPVPN-MPLS las que han sido tradicionalmente desarrolladas por los proveedores de red para dar una estructura de red compartida para múltiples usuarios.

2.4.10Plano de Control de IPVPN-MPLS.

El plano de control de IPVPN-MPLS puede describirse como las tareas a nivel de red que se realiza en la plataforma para el manejo del tráfico dentro de la red, el mismo que está compuesto por :

El uso de las tablas VRF´s dentro de los LER para separar las diferentes rutas de las VPN. El uso de LDP/RSVP para distribuir los LSP para alcanzabilidad de los LER. El uso de MP-BGP para distribuir las rutas VPN y las etiquetas VPN entre y hacia los LER remotos. RD, route-distinguer RT, route-target

2.4.11Protocolos de enrutamiento en IPVPN-MPLS

Para empezar, la función tradicional que realiza el protocolo BGP es la de permitir la interconexión de dos sistemas autónomos mediante el uso de una conexión TCP establecida entre dos enrutadores de borde. En suma, BGP permite interconectar dos sistemas autónomos y cada uno tiene la libertad de escoger el protocolo de enrutamiento interno ya sea RIP, OSPF, IS.IS etc de acuerdo a lo que defina su autoridad administrativa.

La otra mirada de BGP en el contexto de redes VPN basadas en MPLS es que el protocolo BGP permite intercambiar rutas dentro de una misma VPN intercambiadas entre LER a CPE. Cuando BGP está funcionando de esta manera, con frecuencia se le refiere con el nombre MP-BGP (Multiprotocolo BGP). BGP es el protocolo preferido por su flexibilidad. Las rutas transportadas dentro de MP-BGP se conocen como rutas VPNv4 en relación al parámetro de comunidades extendidas manejadas por el protocolo.

BGP se refiere a IPv4, Ipv6, VPNv4, etcétera, como familias de direcciones, esto es lo que permite que BGP pueda distinguir cual tipo de rutas está viendo, enviando o recibiendo. Las rutas VPNv4 enviadas y recibidas, son esencialmente rutas Ipv4 que tienen un valor adicional apuntillado o tacked en el frente de la ruta, el valor anexado se conoce con el nombre de Route Distinguisher (RD).

El formato típico de un RD es ASN:nn, algunas veces el RD tiene la forma IPv4 Address:nn – donde el valor IPv4 address corresponde al valor de un rango de direcciones públicas asignadas. El valor RD se usa para designar y distinguir la instancia VRF a la que pertenece una ruta IPv4 especifica. Una instancia VRF contiene una tabla de enrutamiento que está completamente separada y es independiente tanto de otras tablas de enrutamiento correspondiente a otros VRF como de la tabla de enrutamiento principal del enrutador. Una vez un enrutador LER que esté participando en el intercambio de rutas por MP-BGP reciba una ruta VPNv4, este eliminará el RD de la ruta VPNv4 recibida y colocará la ruta IPv4 original (recibida en la ruta VPNv4) en la tabla de enrutamiento de la instancia VRF correspondiente al RD recibido. Con la sintaxis VPNv4, la ruta hacia la red de 2 clientes diferentes sería por ejemplo:

-192.168.1.0/24 del usuario A se distinguirá con RD#1:192.168.1.0/24
-192.168.1.0/24 del usuario B se distinguirá con RD#2:192.168.1.0/24.

El RT (Route Target). El RT entra en juego cuando necesitamos crear una extranet entre usuarios de diferentes VPN. El RT es un "tag" cuyo valor designa cuáles rutas VPNv4 se importan y exportan en un VRF. El RT es llevado dentro de BGP como un atributo extendido, su sintaxis es muy similar a la del RD y con frecuencia tiene el mismo valor. En la mayoría de casos, cuando no se necesita proporcionar acceso entre usuarios de diferentes VPN, un solo RT es tanto importado como exportado hacia un VRF. Pero si entre dos usuarios necesitan mutuamente tener acceso a las redes del otro usuario, cada usuario requiere importar el RT exportado por el otro.

2.5. IPsec Internet Protocol Security

IPsec es una extensión al protocolo IP que proporciona seguridad a IP y a los protocolos de capas superiores. Fue desarrollado para el nuevo estándar IPv6 y después fue portado a IPv4. La arquitectura IPsec se describe en el RFC2401. Los siguientes párrafos dan una pequeña introducción a IPsec. IPsec emplea dos protocolos diferentes - AH y ESP - para asegurarla autenticación, integridad y confidencialidad de la comunicación. Puede proteger el datagrama IP completo o sólo los protocolos de capas superiores. Estos modos se denominan, respectivamente, modo túnel y modo

transporte. En modo túnel el datagrama IP se encapsula completamente dentro de un nuevo datagrama IP que emplea el protocolo IPsec. En modo transporte IPsec sólo maneja la carga del datagrama IP, insertándose la cabecera IPsec entre la cabecera IP y la cabecera del protocolo de capas superiores

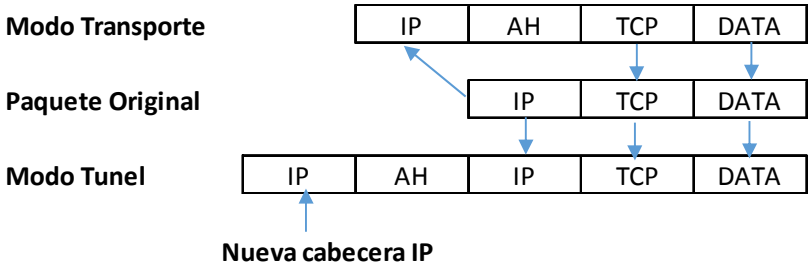

Figura 13. IPsec: modos túnel y transporte

Fuente: (Elaborado por el Autor)

Para proteger la integridad de los datagramas IP, los protocolos IPsec emplean códigos de autenticación de mensaje basados en resúmenes (HMAC - Hash Message Authentication Codes). Para el cálculo de estos HMAC los protocolos HMAC emplean algoritmos de resumen como MD5 y SHA para calcular un resumen basado en una clave secreta y en los contenidos del datagrama IP. El HMAC se incluye en la cabecera del protocolo IPsec y el receptor del paquete puede comprobar el HMAC si tiene acceso a la clave secreta.

Para proteger la confidencialidad de lo datagramas IP, los protocolos IPsec emplean algoritmos estándar de cifrado simétrico. El estándar IPsec exige la implementación de NULL y DES. En la actualidad se suelen emplear algoritmos más fuertes: 3DES, AES y Blowfish. Para protegerse contra ataques por denegación de servicio DDoS, los protocolos IPsec emplean ventanas deslizantes. Cada paquete recibe un número de secuencia y sólo se acepta su recepción si el número de paquete se encuentra dentro de la ventana o es posterior. Los paquetes anteriores son descartados inmediatamente. Esta es una medida de protección eficaz contra ataques por repetición de mensajes en los que el atacante almacena los paquetes originales y los reproduce posteriormente.

Para que los participantes de una comunicación puedan encapsular y desencapsular los paquetes IPsec, se necesitan mecanismos para almacenar las claves secretas, algoritmos y direcciones IP involucradas en la comunicación. Todos estos parámetros se almacenan en asociaciones de seguridad (SA - Security Associations). Las asociaciones de seguridad, a su vez, se almacenan en bases de datos de asociaciones de seguridad (SAD - Security Asocciation Databases). Cada asociación de seguridad define los siguientes parámetros:

-Dirección IP origen y destino de la cabecera IPsec resultante. Estas son las direcciones IP de los participantes de la comunicación IPsec que protegen los paquetes.

-Protocolo IPsec (AH o ESP).

-El algoritmo y clave secreta empleados por el protocolo IPsec.

-Índice de parámetro de seguridad (SPI - Security Parameter Index). Es un número de 32 bits que identifica la asociación de seguridad.

Algunas implementaciones de la base de datos de asociaciones de seguridad permiten almacenar más parámetros:

-Modo IPsec (túnel o transporte)

-Tamaño de la ventana deslizante para protegerse de ataques por repetición.

-Tiempo de vida de una asociación de seguridad.

En una asociación de seguridad se definen las direcciones IP de origen y destino de la comunicación. Por ello, mediante una única SA sólo se puede proteger un sentido del tráfico en una comunicación IPsec full duplex. Para proteger ambos sentidos de la comunicación, IPsec necesita de dos asociaciones de seguridad unidireccionales. Las asociaciones de seguridad sólo especifican cómo se supone que IPsec protegerá el tráfico. Para definir qué tráfico proteger, y cuándo hacerlo, se necesita información adicional. Esta información se almacena en la política de seguridad (SP - Security Policy), que a su vez se almacena en la base de datos de políticas de seguridad (SPD - Security Policy Database).

Una política de seguridad suele especificar los siguientes parámetros:

-Direcciones de origen y destino de los paquetes por proteger. En modo transportes estas serán las mismas direcciones que en la SA. En modo túnel pueden ser distintas.

-Protocolos y puertos a proteger. Algunas implementaciones no permiten la definición de protocolos específicos a proteger. En este caso, se protege todo el tráfico entre las direcciones IP indicadas.

-La asociación de seguridad a emplear para proteger los paquetes.

La configuración manual de la asociación de seguridad es proclive a errores, y no es muy segura. Las claves secretas y algoritmos de cifrado deben compartirse entre todos los participantes de la VPN. Uno de los problemas críticos a los que se enfrenta el administrador de sistemas es el intercambio de claves, para resolver este problema se desarrolló el protocolo de intercambio de claves por Internet (IKE - Internet Key Exchange Protocol). Este protocolo autentica a los participantes en una primera fase. En una segunda fase se negocian las asociaciones de seguridad y se escogen las claves secretas simétricas a través de un intercambio de claves Diffie Hellmann. El protocolo IKE se ocupa incluso de renovar periódicamente las claves para asegurar su confidencialidad.

2.5.1 Componentes y Características de IPsec.

La familia de protocolos IPsec está formada por dos protocolos: el AH (Authentication Header - Cabecera de autenticación) y el ESP (Encapsulated Security Payload - Carga de seguridad encapsulada). Ambos son protocolos IP independientes. AH es el protocolo IP 51 y ESP el protocolo IP 50.

2.5.2 AH - Cabecera de autenticación

El protocolo AH protege la integridad del datagrama IP. Para conseguirlo, el protocolo AH calcula una HMAC basada en la clave secreta, el contenido del paquete y las partes inmutables de la cabecera IP (como son las direcciones IP). Tras esto, añade la cabecera AH al paquete.

La cabecera AH mide 24 bytes. El primer byte es el campo Siguiente cabecera. Este campo especifica el protocolo de la siguiente cabecera. En modo túnel se encapsula un

datagrama IP completo, por lo que el valor de este campo es 4. Al encapsular un datagrama TCP en modo transporte, el valor correspondiente es 6. El siguiente byte especifica la longitud del contenido del paquete. Este campo está seguido de dos bytes reservados.

Los siguientes 4 bytes especifican en Índice de Parámetro de Seguridad (SPI). El SPI especifica la asociación de seguridad (SA) a emplear para el desencapsulado del paquete. El Número de Secuencia de 32 bit protege frente a ataques por repeticón. Finalmente, los últimos 96 bit almacenan el código de resumen para la autenticación de mensaje (HMAC). Este HMAC protege la integridad de los paquetes ya que sólo los miembros de la comunicación que conozcan la clave secreta pueden crear y comprobar HMACs.

Como el protocolo AH protege la cabecera IP incluyendo las aprtes inmutables de la cabecera IP como las direcciones IP, el protocolo AH no permite NAT. NAT (Network address translation - Traducción de direcciones de red, también conocido como Enmascaramiento de direcciones) reemplaza una dirección IP de la cabecera IP (normalmente la IP de origen) por una dirección IP diferente. Tras el intercambio, la HMAC ya no es válida. La extensión a IPsec NAT-transversal implementa métodos que evitan esta restricción.

2.5.3 ESP - Carga de Seguridad Encapsulada

El protocolo ESP puede asegurar la integridad del paquete empleando una HMAC y la confidencialidad empleando cifrado. La cabecera ESP se genera y añade al paquete tras cifrarlo y calcular su HMAC. La cabecera ESP consta de dos partes y se muestra en Figure 14.

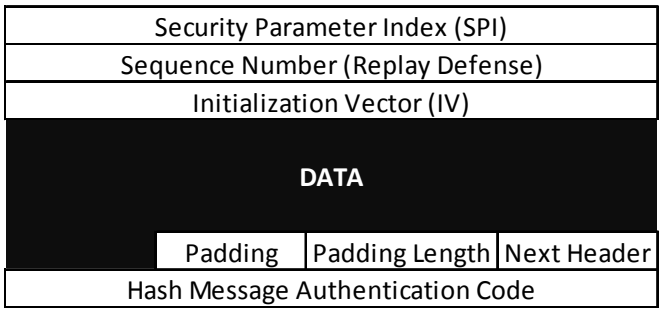

Figura 14. La cabecera ESP.

Fuente: (Elaborado por el Autor)

Los primeros 32 bits de la cabecera ESP especifican el Índice de Parámetros de Seguridad (SPI). Este SPI especifica qué SA emplear para desencapsular el paquete ESP. Los siguientes 32 bits almacenan el Número de Secuencia. Este número de secuencia se emplea para protegerse de ataques por repetición de mensajes. Los siguientes 32 bits especifican el Vector de Inicialización (IV - Initialization Vector) que se emplea para el proceso de cifrado. Los algoritmos de cifrado simétrico pueden ser vulnerables a ataques por análisis de frecuencias si no se emplean IVs. El IV asegura que dos cargas idénticas generan dos cargas cifradas diferentes.

IPsec emplea cifradores de bloque para el proceso de cifrado. Por ello, puede ser necesario rellenar la carga del paquete si la longitud de la carga no es un múltiplo de la longitud del paquete. En ese caso se añade la longitud del relleno (pad length). Tras la longitud del relleno se coloca el campo de 2 bytes Siguiente cabecera que especifica la siguiente cabecera. Por último, se añaden los 96 bit de HMAC para asegurar la integridad del paquete. Esta HMAC sólo tiene en cuenta la carga del paquete: la cabecera IP no se incluye dentro de su proceso de cálculo.

2.5.4 Protocolo de Intercambio de Internet IKE.

El protocolo IKE resuelve el problema más importante del establecimiento de comunicaciones seguras: la autenticación de los participantes y el intercambio de claves simétricas. Crea las asociaciones de seguridad y rellena la SAD (Database). El protocolo IKE emplea el puerto 500 UDP para su comunicación.

El protocolo IKE funciona en dos fases. La primera fase establece un ISAKMP SA (Internet Security Association Key Management Security Association - Asociación de seguridad del protocolo de gestión de claves de asociaciones de seguridad en Internet). En la segunda fase, el ISAKMP SA se emplea para negociar y establecer las SAs de IPsec. La autenticación de los participantes en la primera fase suele basarse en claves compartidas con anterioridad (PSK - Pre-shared keys), claves RSA y certificados X.509.

La primera fase suele soportar dos modos distintos: modo principal y modo agresivo. Ambos modos autentican al participante en la comunicación y establecen un ISAKMP SA, pero el modo agresivo sólo usa la mitad de mensajes para alcanzar su objetivo. Esto, sin embargo, tiene sus desventajas, ya que el modo agresivo no soporta la protección de identidades y, por lo tanto, es susceptible a un ataque man-in-the-middle (por escucha y repetición de mensajes en un nodo intermedio) si se emplea junto a claves compartidas con anterioridad (PSK). El modo agresivo no permite la protección de identidades y transmite la identidad del cliente en claro. Por lo tanto, los participantes de la comunicación se conocen antes de que la autenticación se lleve a cabo, y se pueden emplear distintas claves pre-compartidas con distintos comunicantes.

En la segunda fase, el protocolo IKE intercambia propuestas de asociaciones de seguridad y negocia asociaciones de seguridad basándose en la ISAKMP SA. La ISAKMP SA proporciona autenticación para protegerse de ataques man-in-the-middle. Esta segunda fase emplea el modo rápido. Normalmente, dos participantes de la comunicación sólo negocian una ISAKMP SA, que se emplea para negociar varias (al menos dos) IPsec SAs unidireccionales

2.5.5 Algoritmos de Encriptación.

Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo. En otras palabras, no debería ser de ninguna ayuda para un atacante conocer el algoritmo que se está usando. Sólo si el atacante obtuviera la clave, le serviría conocer el algoritmo. Los algoritmos de cifrado ampliamente utilizados tienen estas

propiedades.Dado que toda la seguridad está en la clave, es importante que sea muy difícil adivinar el tipo de clave. Actualmente, los ordenadores pueden descifrar claves con extrema rapidez, y ésta es la razón por la cual el tamaño de la clave es importante en los criptosistemas modernos.

El algoritmo de cifrado DES (Data Encryption Estándar) usa una clave de 56 bits, lo que significa que hay 2 elevado a 56 claves posibles (72.057.594.037.927.936 claves). Esto representa un número muy alto de claves, pero un ordenador genérico puede comprobar el conjunto posible de claves en cuestión de días.

Una máquina especializada puede hacerlo en horas. Algoritmos de cifrado de diseño más reciente como 3DES, usan claves de 128 bits, lo que significa que existen 2 elevado a 128 claves posibles. Esto equivale a muchísimas más claves, y aun en el caso de que todas las máquinas del planeta estuvieran cooperando, tardarían más tiempo en encontrar la clave que la edad del universo.

AES o también conocido como algoritmo Rijndael fue elegido por el NIST (National Institute of Standards and Technology), para ser el estándar en los próximos 20 años , fue elegido después de pasar un periodo de análisis durante aproximadamente 3 años, Rijndael fue elegido como la mejor opción dentro de 15 candidatos, sus principales características fueron su fácil diseño, su versatilidad en ser implementado en diferentes dispositivos, así como ser inmune a los ataques conocidos hasta la fecha, soportar bloques de datos de 128 bits y claves de 128, 192, y 256 bits. La idea básica general es tener un estándar que mejore el “performance” de 3DES y sea resistente a los ataques conocidos

2.5.6 Topologías de IPSEC

2.5.6.1VPN IPsec Punto a Punto

La forma más básica de VPN IPsec se representa como una arquitectura dedicada de un circuito punto a punto uniendo dos extremos como se puede ver en la figura 15.

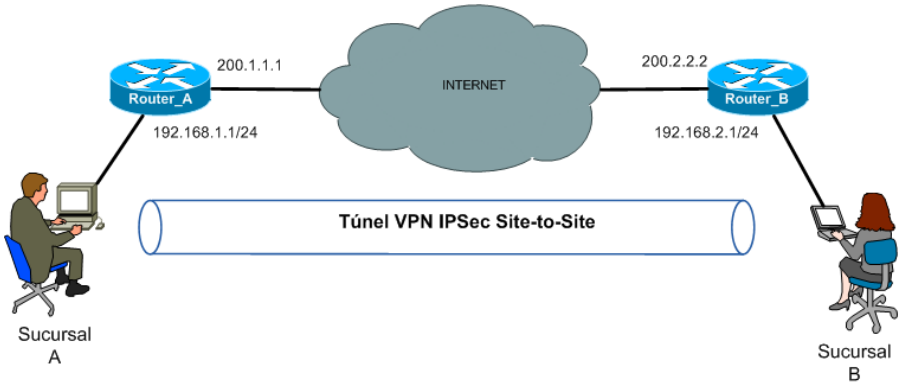

Figura 15. IPsec punto a punto.

Fuente: (www.redescisco.net)

2.5.6.2DMVPN IPsec VPNs Multipunto Dinámicas

DMVPN son las siglas de Dynamic Virtual Private Network. Se trata de una tecnología para el establecimiento de túneles privados sobre redes IP más flexible que la VPN tradicional punto a punto. Permite la convergencia de túneles en tiempo real entre distintos puntos**.** Una de las principales preocupaciones y desafíos que pertenecen a la implementación de VPN sitio a sitio usando la topología Hub & Spoke (concentrador & remotos) con un gran número de sitios es la escalabilidad.

Con el hecho de que la implementación de muchos túneles GRE (Generic Route Encapsulation) sobre IPSec con un protocolo de ruteo dinámico puede escalar bien, sin embargo el número de listas de acceso y de túneles punto a punto será difícil de administrar cuando hay un gran número de sitios remotos usando completa o parcialmente la topología mallada. Además de los problemas de escalabilidad, la implementación de un gran número de VPN sitio a sitio usando la topología Hub & Spoke con un gran número de comunicaciones spoke to spoke, dará lugar a una sobrecarga alta en el CPU y a la memoria del hub router porque todo el tráfico spoke to spoke debe transitar por el hub.

Una de las soluciones más escalables a los problemas mencionados de VPN usando la topología Hub & Spoke con un gran número de comunicaciones spoke to spoke requeridas es VPN multipunto dinámico preparatorio (DMVPN) la cual evaluar su

desempeño es parte de este proyecto. Uno de los requisitos principales de las implementaciones de DMVPN es el uso de la topología Hub & Spoke, pero eso no significa que el tráfico spoke to spoke deba atravesar el hub. El hub solamente es requerido para el registro de dirección de los spokes usando NHRP.

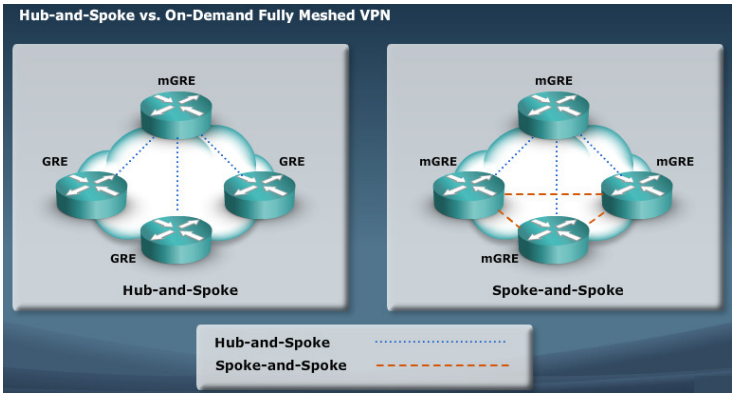

Figura 16. Tipos de DMVPN.

Fuente: (www.cisco.com)

2.5.6.3Arquitectura DMVPN

Podemos describir la arquitectura necesaria para las DMVPN en un diagrama de bloques que consta de:

Tabla 1.

Arquitectura DMVPN

Arquitectura DMVPN	
Mgre	Provee un forma de escalable de tunneling Multiprotocol con opción de ruteo dinámico. Todos los miembros de la DMVPN usan interfaces mGRE para construir túneles entre ellos
NHRP	Provee un método de descubrimiento dinámico de los spokes, los cuales usan NHRP para informar al hub acerca de su túnel interior y dirección IP exterior de la interface física y así mapear el resto de spokes.
IKE + IPsec	Provee la gestión de claves y la transmisión de los datos protegidos, los túneles mGRE usan encapsulación IPsec, los spokes tienen

Continua

	sesiones permanentes de IKE con el hub y sesiones bajo demanda entre ellos.

Fuente: (Elaborado por el Autor)

2.5.6.4Protocolo de Resolución de Salto Siguiente – NHRP.

Definido en el RFC 2332 es usado para el registro de dirección de los spokes en las implementaciones DMVPN. Con DMVPN cualquier flujo de tráfico entre los routers se envía vía un túnel GRE, pero la característica interesante que distingue a DMVPN entre otras implementaciones de VPN es que este túnel GRE es un túnel multipunto.

Es decir el hub y los spokes requerirán un túnel cada uno para alcanzar una conectividad DMVPN completamente mallada. De la información dada es obvio que DMVPN puede proporcionar las siguientes ventajas:

- Simplificar la porción de la configuración del hub router eliminando la necesidad de configurar crypto maps, las interfaces de túnel, y ACL de cada spoke.

- Los spoke routers pueden obtener sus direcciones IP dinámicamente, por ejemplo un router de borde de Internet conectado con un enlace ADSL puede obtener su IP automáticamente del ISP y entonces el túnel se registrará con el hub usando NHRP.

2.6. Análisis de performance y monitoreo de redes.

El análisis y monitoreo generalmente llamado gestión de red se refiere a obtener valores continuos en el tiempo de las variables significativas del sistema, consiste en monitorizar y controlar los recursos de red con el fin de verificar su funcionamiento y evitar degradación en el mismo.

2.6.1Monitoreo de Ancho de Banda.

El monitoreo de ancho de banda sirve para la medición del ancho de banda de conexiones de red y equipos (routers, switches, etc.), encontrar cuellos de botella y

errores de conectividad para evitarlos en el futuro. Generalmente la gestión y monitoreo de equipos en redes IP son realizados utilizando SNMP.

2.6.2Analizadores de Protocolos.

Un analizador de protocolos o sniffer es una herramienta que sirve para desarrollar y depurar protocolos y aplicaciones de red. Permite al ordenador capturar diversas tramas de red para analizarlas, ya sea en tiempo real o después de haberlas capturado.

Por analizar se entiende que el programa puede reconocer que la trama capturada pertenece a un protocolo concreto (TCP, ICMP...) y muestra al usuario la información decodificada. De esta forma, el usuario puede ver todo aquello que en un momento concreto está circulando por la red que se está analizando. Esto último es muy importante para un programador que esté desarrollando un protocolo, o cualquier programa que transmita y reciba datos en una red, ya que le permite comprobar lo que realmente hace el programa.

Además de para los programadores, estos analizadores son muy útiles a todos aquellos que quieren experimentar o comprobar cómo funcionan ciertos protocolos de red, si bien su estudio puede resultar poco ameno, sobre todo si se limita a la estructura y funcionalidad de las unidades de datos que intercambian. También, gracias a estos analizadores, se puede ver la relación que hay entre diferentes protocolos, para así, comprender mejor su funcionamiento.

Los analizadores de protocolos se usan en diversas arquitecturas de red, tales como Redes LAN (10/100/1000 Ethernet; Token Ring; FDDI (Fibra óptica)), Redes Wireless LAN, Redes Gigabit, Redes WAN. Entre los usos principales de los analizadores de protocolos.

-Analizar y soportar demandas de nuevas aplicaciones (como Voip).

-Obtener mayor eficiencia de la red, al analizar todo lo que pasa por ella, detectar problemas concretos.

-Analizar y monitorear varias redes a la vez

2.6.3Wireshark

Wireshark es el analizador de protocolos gratuito que se utilizará para la obtención de las variables de medición necesarias para este proyecto, permite filtra paquetes de acuerdo a parámetros de red como protocolo TCP, UDP, IP fuente, IP destino, número de paquetes etc y obtener estadísticas de las mismas.

Adicionalmente con esta aplicación se verificará las vulnerabilidades de seguridad que tiene la información al no ser encriptada para su transporte en cualquier red IP, por ejemplo Wireshark tiene incorporado un RTP (Real Time Player) que permite reproducir tráfico de voip de los paquetes analizados.

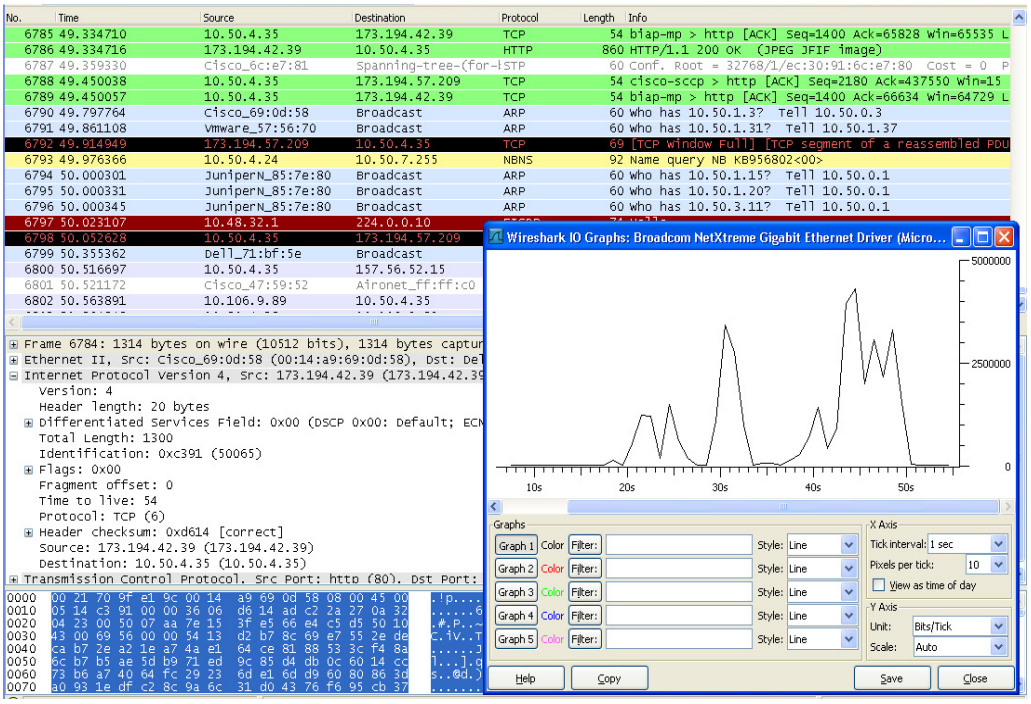

Figura 17. Analizador de Protocolos

Fuente: Programa Wireshark

2.6.4Medidor de Performance JPERF.

La herramienta JPERF es una herramienta o aplicación cliente servidor para medición o pruebas de performance de redes, su interfaz es gráfica y consiste en un generador de flujos TCP y será la aplicación que utilizaremos para las pruebas sobre las maquetas a implementar en este proyecto.

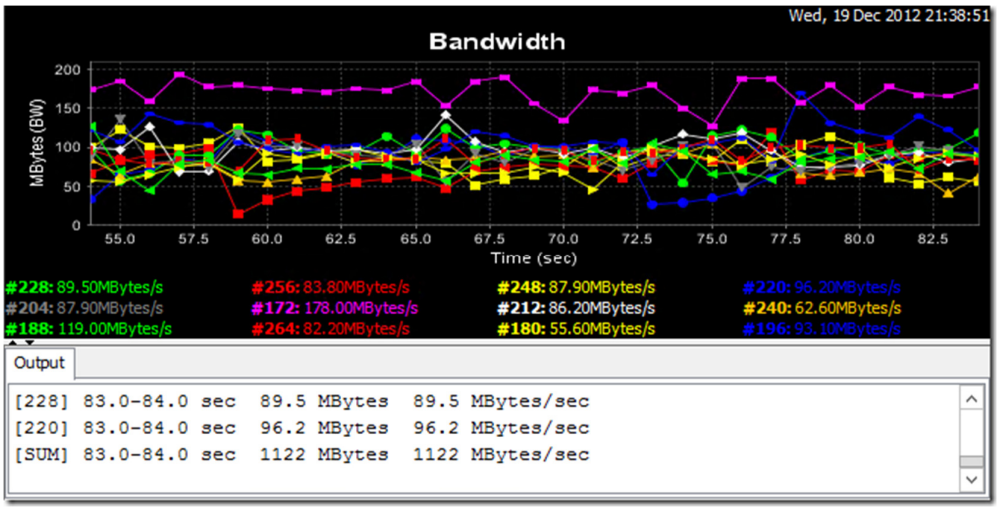

Figura 18. Test de performance -JPERF

Fuente: (Programa JPERF)

CAPITULO III

IMPLEMENTACION DE LAS MAQUETAS DE SIMULACIÓN.

3.1 Implementación de las maquetas de simulación.

Para el desarrollo del proyecto se ha considerado implementar una maqueta de simulación para los tres escenarios a evaluarse, el análisis del comportamiento y desempeño de transmisión de paquetes de diferentes aplicaciones y protocolos nos encamina a considerar que los tres sistemas poseen en cuanto a sus características elementos constantes como son la topología física, ancho de banda del sistema que es función del troughput de los equipos, MTU del protocolo, capacidad de procesamiento de los routers etc, y elementos variables como son la forma de tratamiento de los paquetes que pasan a través de los sistemas, la encriptación, fragmentación, calidad de servicio etc etc.

En otras palabras se implementará una maqueta con una sola topología física en hardware y se configurará los sistemas sobre la misma

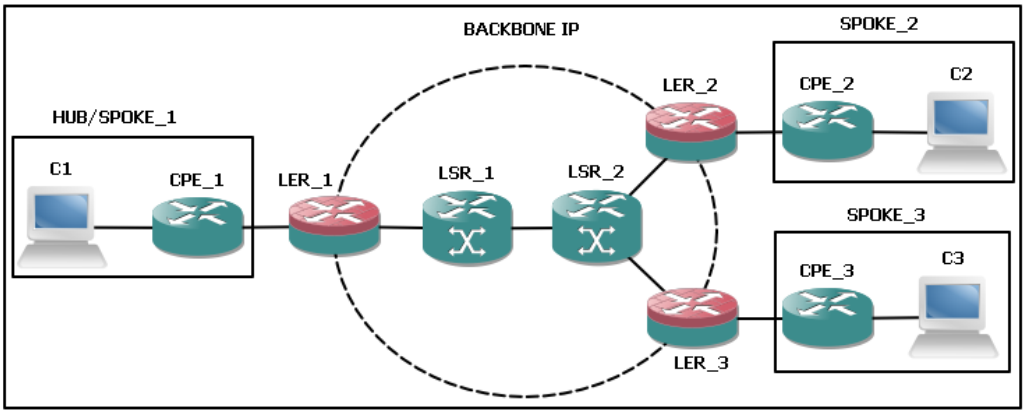

Figura 19. Topología Física de la Maqueta.

Fuente: (Elaborado por el autor)

El escenario a desarrollar en la maqueta es una red corporativa con tres oficinas en donde se tiene una matriz y dos oficinas remotas, para fines del proyecto nos

referiremos a un CPE en modo Hub/Spoke y dos CPE´s en modo Spoke respectivamente. Como se puede observar en la figura 19 la interface entre la red LAN de cada sitio y la red de transporte IP (MPLS o Internet) la hacen los routers CPE. Las puertas de entrada a la red de transporte IP las realizan los routers PE o LER (Label Edge Routers) que son los equipos periféricos del Backbone y los equipos centrales del backbone o core de la red son los routers P o LSR (Label Switching Router).

3.2 Descripción de los Routers.

3.2.1Funciones del CPE – Customer Premises Equipment.

Los routers CPE ubicados tanto en el Hub/Spoke y en los Spoke; son los puntos donde el tráfico generado por las redes Lan de los 3 sitios, generalmente son router de un performance intermedio, para el proyecto se ha considerado utilizar como CPE equipos de la plataforma Cisco 800 cargado el software o IOS adecuado para las funcionalidades de encriptación, enrutamiento y Qos.

El troughput capaz de manejar estos equipos es de 50000 pps (paquetes por segundo) o 13Mbps considerando el paquete mínimo IP de 64bytes; las interfaces a usar son FasthEthernet 100FullDuplex, estos equipos serán los encargados de realizar las siguientes funciones en los tres escenarios a evaluar:

Tabla 2.

Funciones del CPE.

Funciones	IPVPN-MPLS	IPsec- Internet	DMVPN-MPLS
CPE	Enrutamiento	Enrutamiento Encriptación	Enrutamiento Encriptación

Fuente: (Elaborado por el Autor)

3.2.2Funciones del PE o LER Routers.

Los routers PE ubicados al borde de la red IP son equipos de un procesamiento mayor capaz de manejar el tráfico multiusuario, para nuestro proyecto se ha considerado usar equipos de la plataforma Juniper SRX100B y Cisco 2800 con el

software o IOS para soportar funcionalidades de MPLS, LDP, VPN, y enrutamiento dinámico como BGP necesario para Internet y MPLS. El troughput capaz de manejar los equipos Cisco PE es de 90000 pps (paquetes por segundo) o 45Mbps; las interfaces a usar son Fastethernet 100FullDuplex, el troughput capaz de manejar los equipos Juniper SRX100B es de 70000 pps (paquetes por segundo) o 35Mbps considerando paquetes de 64bytes; las interfaces a usar son Fastethernet 100Full Duplex, estos equipos serán los encargados de realizar las siguientes funciones en los 3 escenarios a evaluar:

Tabla 3.

Funciones del PE.

Funciones	IPVPN-MPLS	IPsec-Internet	DMVPN- MPLS
PE/LER	Enrutamiento Colocación de etiquetas	Enrutamiento	Enrutamiento Colocación de etiquetas

Fuente: (Elaborado por el Autor)

3.2.3Funciones del P o LSR Router – Provider Router.

Los routers P están ubicados en el core de la red IP, generalmente son usados como equipos de tránsito pero también pueden cumplir funcionalidad de PE para nuestro proyecto se ha considerado usar equipos de la plataforma Cisco 2800 con el software o IOS para soportar funcionalidades de MPLS, LDP, VPN, RSVP y enrutamiento dinámico como BGP necesario para Internet y MPLS.

El troughput capaz de manejar los equipos Cisco P router es de 90000 pps (paquetes por segundo) o 45Mbps; las interfaces a usar son Fastethernet 100FullDuplex.

Estos equipos serán los encargados de realizar las siguientes funciones en los 3 escenarios a evaluar:

Tabla 4.

Funciones del P.

Funciones	IPVPN-MPLS	IPsec-Internet	DMVPN- MPLS
P/LSR	Enrutamiento Intercambio de etiquetas	Enrutamiento	Enrutamiento Intercambio de etiquetas

Fuente: (Elaborado por el Autor)

3.2.4Diseño de Internetworking de la Maqueta de Evaluación.

El diseño de Internetworking comprende en establecer el plan básico de conectividad del sistema base sobre el cual se montarán los tres escenarios a evaluar, este plan comprende el asignar en los switches, direccionamiento de red y enrutamiento para el sistema.

3.2.5Diseño de Direccionamiento IP de Red.

Para el direccionamiento de red se ha considerado usar la variable X con los valores de 1,2 y 3 para CPE_1, CPE_2 y CPE_3 respectivamente, de acuerdo al siguiente plan de red.

- Para los segmentos Backbone PE_P se designó las subredes 172.16.X.0/24
- Para el segmento Backbone P_1-P_2 se designó la subred 172.16.32.0/30
- Adicionalmente para fines de pruebas y configuraciones del sistema se ha definido una interface de loopback para cada router de la red.

Tabla 5.

Direccionamiento IP.

Equipo	Segmento	Interface Física	Direccionamiento
CPE_1	LAN	Fastethernet0	10.10.1.1/24
CPE_1	CPE_1 - PE_1	Fastethernet4	192.168.1.2/24
CPE_1	Virtual	Loopback0	1.1.1.1/32
CPE_2	LAN	Fastethernet0	10.10.2.1/24
CPE_2	CPE_2 – PE_2	Fastethernet4	192.168.2.2/24
CPE_2	Virtual	Loopback0	2.2.2.2/32
CPE_3	LAN	Fastethernet0	10.10.3.1/24

Continua

CPE_3	CPE_3 – PE_3	Fastethernet4	192.168.3.2/24
CPE_3	Virtual	Loopback0	3.3.3.3/32
PE_1	PE_1 - CPE_1	Fe-0/0/0	192.168.1.1/24
PE_1	PE_1 – P_1	Fe-0/0/1	172.16.1.2/24
PE_1	Virtual	Loopback0	4.4.4.4/32
PE_2	PE_2 – CPE_2	Fastethernet0/0	192.168.2.1/24
PE_2	PE_2 – P_2	Fastethernet0/1	172.16.2.2/24
PE_2	Virtual	Loopback0	5.5.5.5/32
PE_3	PE_3 – CPE_3	Fe-0/0/0	192.168.3.1/24
PE_3	PE_3 – P_2	Fe-0/0/1	172.16.3.2/24
PE_3	Virtual	Loopback0	6.6.6.6/32
P_1	P_1 –PE_1	Fastethernet0/0	172.16.1.1/24
P_1	P_1 – P_2	Fastethernet0/1	172.16.32.1/30
P_1	Virtual	Loopback0	7.7.7.7/32
P_2	P_2 – PE_2	Fastethernet0/0	172.16.2.1/24
P_2	P_2 – PE_3	Fastethernet0/1	172.16.3.1/24
P_2	P_2 – P_1	Fastethernet0/3/2	172.16.32.2/30
P_2	Virtual	Loopback0	8.8.8.8/32

Fuente: (Elaborado por el Autor)

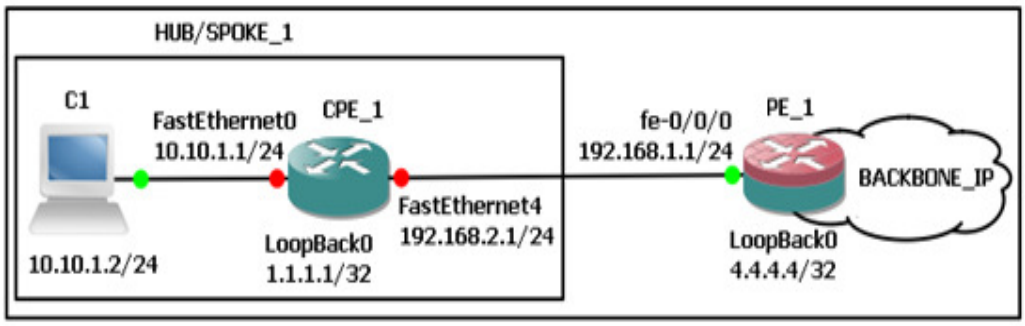

Figura 20. Direccionamiento IP del Hub / Spoke_1.

Fuente: (Elaborado por el Autor).

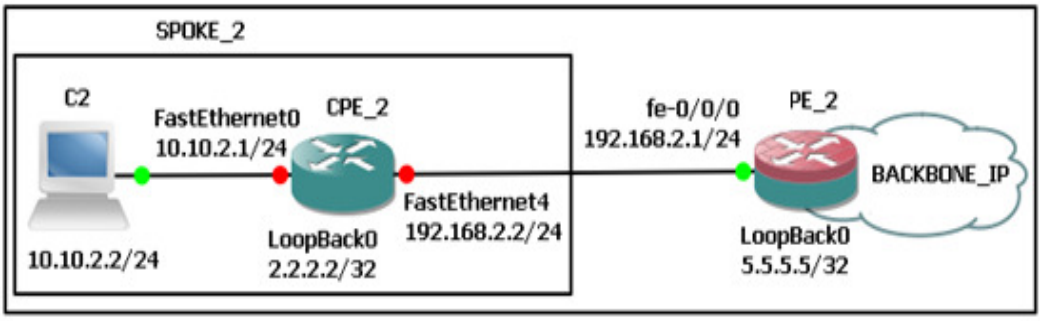

Figura 21. Direccionamiento IP del Spoke_2.

Fuente: (Elaborado por el Autor).

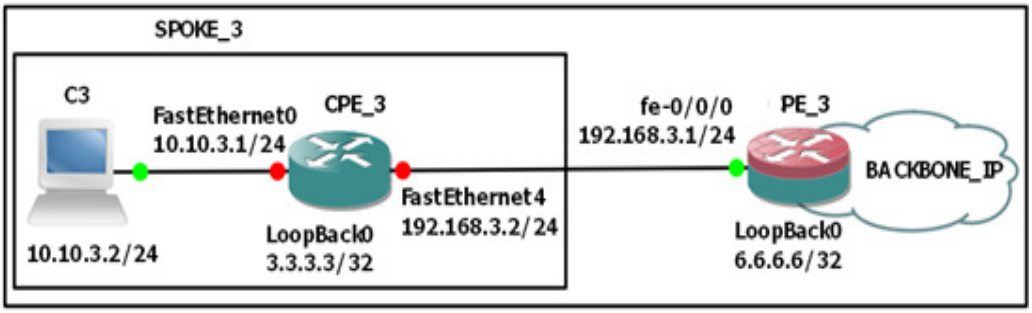

Figura 22. Direccionamiento IP del Spoke_3.

Fuente: (Elaborado por el Autor)

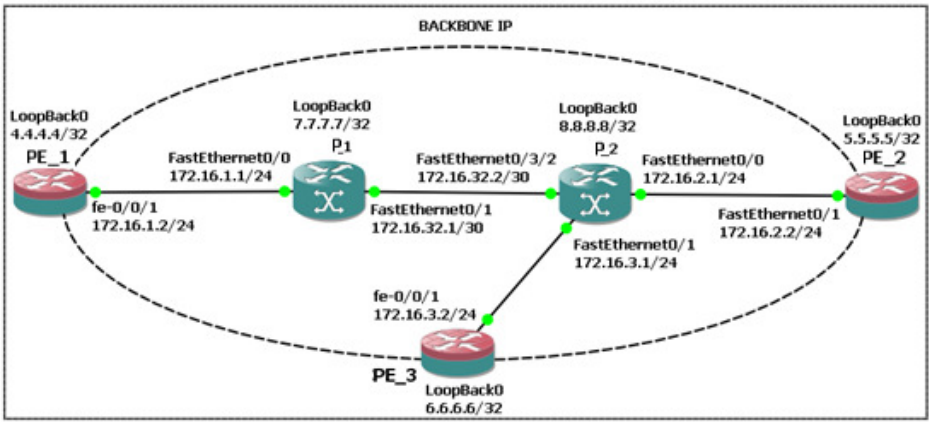

Figura 23. Direccionamiento IP del Backbone IP.

Fuente: (Elaborado por el Autor)

3.2.6Protocolos de Enrutamiento.

El enrutamiento a utilizarse es dependiente del tipo de sistema o esquema de red a implementarse, en lo que respecta al sistema IPVPN-MPLS como se puede observar en la figura 23, es imperativo el uso de un IGP (Interior Gateway Protocol) ente los equipos de backbone y posteriormente levantar MP-BGP para la propagación de los prefijos correspondientes a las distintas VPN de capa 3 o vrf´s, el protocolo de enrutamiento entre el PE y el CPE se ha decidido realizarlo en forma estática ya que no tiene mayor implicación en el proyecto.

Tabla 6.

Protocolos de Enrutamiento para los Sistemas.

Segmento	MPLS	IP/Internet
PC_CPE	Estático	Estático
CPE_PE	Estático	Estático
PE_P	OSPF	BGP
P_P	OSPF	BGP
PE_PE	MP-BGP	BGP

Fuente: (Elaborado por el Autor)

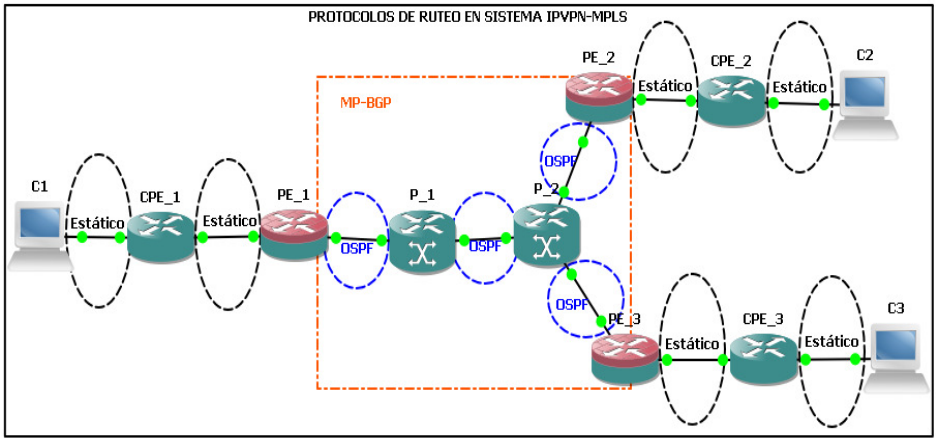

Figura 24. Protocolos de enrutamiento en Sistema IPVPN-MPLS.

Fuente: (Elaborado por el Autor)

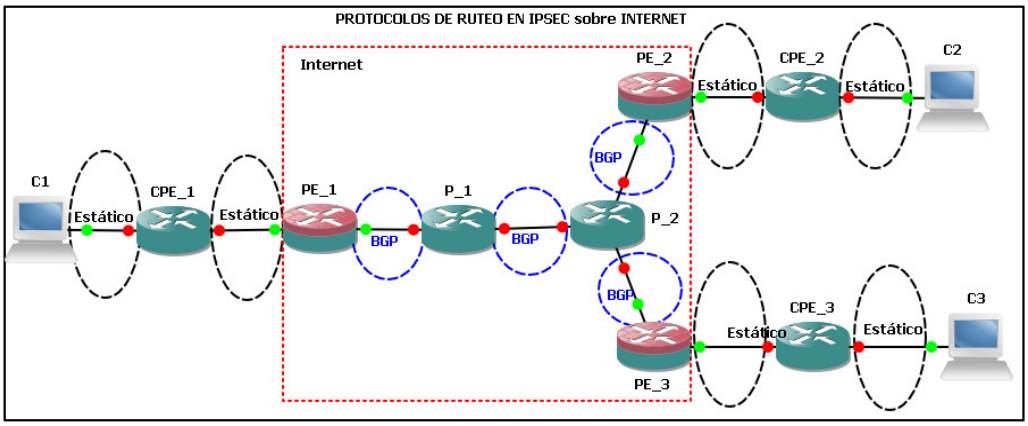

Figura 25. Protocolos de enrutamiento en Sistema Internet.

Fuente: (Elaborado por el Autor)

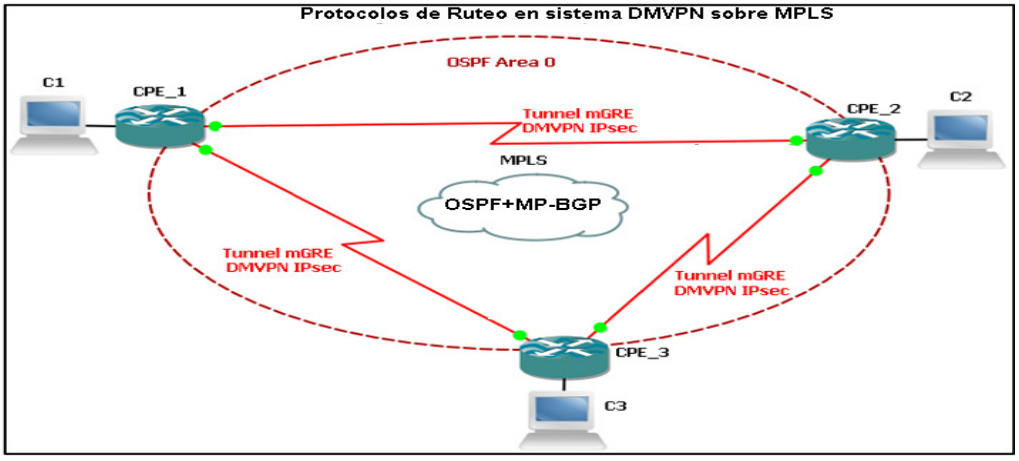

Figura 26. Protocolos de enrutamiento en Sistema DMVPN sobre MPLS.

Fuente: (Elaborado por el Autor)

3.3 Consideraciones técnicas para el sistema IPVPN-MPLS.

3.3.1. Determinación de Software para IPVPN-MPLS.

Las características de software que deben poseer los equipos que van a realizar el switcheo de etiquetas está establecido por el sistema operativo cargado en el hardware, los equipos que utilizaremos para montar un backbone MPLS son de los vendors Cisco y Juniper que poseen las siguientes características.

3.3.2. Router Vendor Juniper.

- **Hardware:** Model: Srx100b.
- **Software:** JUNOS Software Release [10.2R3.10].
- **Features:** OSPF, BGP, MPLS, VRF.
- **Detalle:** el software cargado soporta las características para los fines de nuestro proyecto.
-

3.3.3. Router Vendor Cisco.

- **Hardware:** Cisco 2801.
- **Software:** Cisco IOS, Software (C2801-SPSERVICESK9-M), Version 12.4(15)T10,
- **Features:** OSPF, BGP, MPLS, VRF.
- **Detalle:** el software cargado soporta las características para los fines de nuestro proyecto.
-

3.3.4. Configuraciones y pruebas del sistema IPVPN-MPLS.

Básicamente un backbone o sistema IPVPN-MPLS va a manejar el marcado, identificación y forwardeo de paquetes a través de las etiquetas colocadas por los PE y P entre la cabecera de capa 3 y la cabecera de capa 2, por tal motivo se suele decir que MPLS se encuentra en la capa 2 ½. La configuración se va a realizar en los ruteadores que van a manejar el switcheo de etiquetas, solamente en las interfaces que se ven directamente conectadas y que se encuentran en la misma subred.

La configuración del sistema IPVPN-MPLS comprende 7 pasos:

-Configuración de interfaces y conectividad de PE´s y P´s.

-Configuración de protocolo de ruteo dinámico interno IGP

-Configuración de multiprotocolo BGP – (MP-BGP)

-Configuración de LDP para establecimiento de los LSP (Label Switched Path).

-Configuración de las IPVPN en los PE's.

-Configuración de interfaces y conectividad de los CPE.

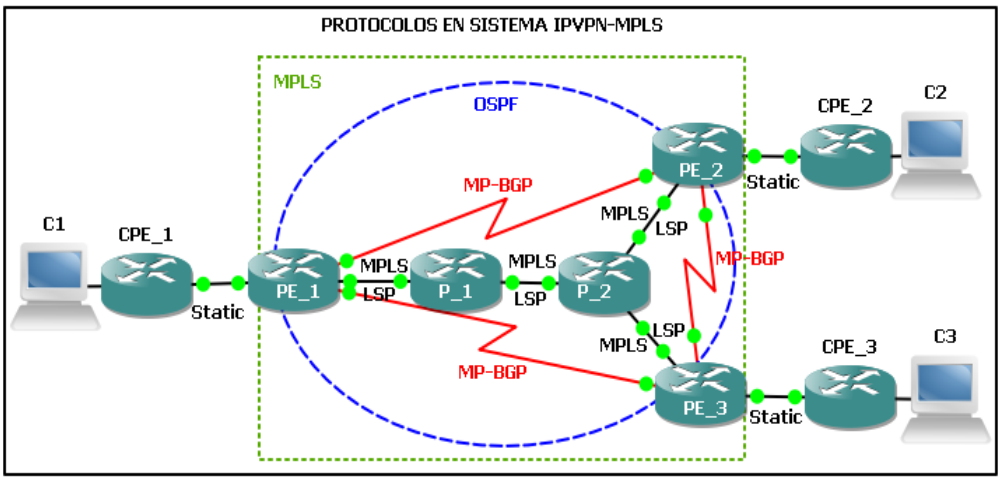

Figura 27. Protocolos en Sistema IPVPN-MPLS.

Fuente: (Elaborado por el Autor)

3.3.5. Configuración de interfaces y conectividad de PE´S y P´s.

3.3.5.1Direccionamiento IP e interfaces de PE_1.

PE_1#

set interfaces fe-0/0/0 unit 0 description PE1_HACIA_CPE_1

set interfaces fe-0/0/0 unit 0 family inet address 192.168.1.1/24

set interfaces fe-0/0/1 unit 0 description PE_1_HACIA_P_1

set interfaces fe-0/0/1 unit 0 family inet address 172.16.1.2/24

set interfaces lo0 unit 0 family inet address 4.4.4.4/32

3.3.5.2Direccionamiento IP e interfaces PE_2.

PE_2#

interface Fastethernet0/1

description PE_2_HACIA_P_2

ip address 172.16.2.2 255.255.255.0

interface Loopback0

description LOOPBACK_5.5.5.5

ip address 5.5.5.5 255.255.255.255

3.3.5.3Direccionamiento IP e interfaces PE_3.

PE_3#

set interfaces fe-0/0/1 unit 0 description PE_3_HACIA_P_2

set interfaces fe-0/0/1 unit 0 family inet address 172.16.3.2/24

set interfaces lo0 unit 0 family inet address 6.6.6.6/32

3.3.5.4Direccionamiento IP e interfaces P_1.

P_1#

interface Fastethernet0/0

 description P1_HACIA_PE_1

ip address 172.16.1.1 255.255.255.0

interface Fastethernet0/1

 description P_1_HACIA_P_2

 ip address 172.16.32.1 255.255.255.252

interface Loopback0

 description LOOPBACK_ 7.7.7.7

 ip address 7.7.7.7 255.255.255.255

3.3.5.5Direccionamiento IP e interfaces P_2.

P_2#

interface Fastethernet0/0

 description P_2_HACIA_PE_2

ip address 172.16.2.1 255.255.255.0

interface Fastethernet0/1

 description P_2_HACIA_PE_3

ip address 172.16.3.1 255.255.255.0

interface Vlan32

 description P_2_HACIA__P_1

 ip address 172.16.32.2 255.255.255.252

interface Loopback0

 description LOOPBACK_8.8.8.8

 ip address 8.8.8.8 255.255.255.255

3.3.6. Configuración del IGP – (Internal Gateway Protocol) en P´s y PE´s.

El IGP o protocolo de ruteo dinámico interno es la base para obtener la conectividad o visibilidad entre los P´s, los protocolos en enrutamiento generalmente usados como IGP son OSPF (Open short first Path) y IS-IS (Intermediate System to Intermediate System) los cuales a nivel de protocolo tienen similar comportamiento respecto al manejo de prefijos y funcionalidades de descrubrimiento de vecindades así como también se usan como protocolo base para tráfico de ingeniería. Para fines de nuestro proyecto se usará OSPF. Las interfaces que participan en el proceso OSPF deben ser las que se encuentran directamente conectadas entre PE´s y P´s así como también las interfaces virtuales de loopback las mismas que servirán de identificadores de cada P´s tanto para OSPF como para MP-BGP y LDP.

3.3.6.1Configuración OSPF en PE_1.

```
PE_1#
set routing-options router-id 4.4.4.4
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface fe-0/0/1
```

3.3.6.2Configuración OSPF en PE_2.

```
PE_2#
router ospf 1
 router-id 5.5.5.5
network 5.5.5.5 0.0.0.0 area 0
 network 172.16.2.0 0.0.0.255 area 0
```

3.3.6.3Configuración OSPF en PE_3.

```
PE_3#
set routing-options router-id 6.6.6.6
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface fe-0/0/1
```

3.3.6.4Configuración OSPF en P_1.

```
P_1#
router ospf 1
 router-id 7.7.7.7
network 7.7.7.7 0.0.0.0 area 0
 network 172.16.1.0 0.0.0.255 area 0
 network 172.16.32.0 0.0.0.3 area 0
```

3.3.6.5Configuración OSPF en P_2.

```
P_2#
router ospf 1
 router-id 8.8.8.8
network 8.8.8.8 0.0.0.0 area 0
 network 172.16.2.0 0.0.0.255 area 0
 network 172.16.3.0 0.0.0.255 area 0
 network 172.16.32.0 0.0.0.3 area 0
```

3.3.6.6Verificación del IGP.

```
P_1#sho ip route ospf
     4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.4 [110/1] via 172.16.1.2, 03:39:27, Fastethernet0/0
     5.0.0.0/32 is subnetted, 1 subnets
O       5.5.5.5 [110/3] via 172.16.32.2, 03:40:32, Fastethernet0/1
     6.0.0.0/32 is subnetted, 1 subnets
O       6.6.6.6 [110/2] via 172.16.32.2, 03:39:27, Fastethernet0/1
     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O       172.16.2.0/24 [110/2] via 172.16.32.2, 03:40:32, Fastethernet0/1
O       172.16.3.0/24 [110/2] via 172.16.32.2, 03:40:32, Fastethernet0/1
     8.0.0.0/32 is subnetted, 1 subnets
O       8.8.8.8 [110/2] via 172.16.32.2, 03:40:32, Fastethernet0/1
```

3.3.7. Configuración de multiprotocolo BGP – (MP-BGP) en PE´s.

MP-BGP es una extensión del protocolo de ruteo BGP para permitir ruteo o llevar información de diferentes capas de red y familia de direcciones a través del backbone, para fines de nuestro proyecto MP-BGP será el encargado de propagar a través de los PE´s los prefijos y rutas. Las vecindades BGP se establecen entre los PE´s y se habilita el tipo de prefijos que se van a intercambiar entre los mismos, para internet se propagan la familia de direcciones unicast y para VPN se propagan la familia de direcciones vpn-unicast o vpnv4.

3.3.7.1Configuración MP-BGP en PE_1.

```
PE_1#
set routing-options autonomous-system 65000
set protocols bgp group igp type internal
set protocols bgp group igp family inet unicast
set protocols bgp group igp family inet-vpn unicast
set protocols bgp group igp neighbor 5.5.5.5 local-address 4.4.4.4
set protocols bgp group igp neighbor 5.5.5.5 description HACIA_PE_2
set protocols bgp group igp neighbor 6.6.6.6 local-address 4.4.4.4
set protocols bgp group igp neighbor 6.6.6.6 description HACIA_PE_3
```

3.3.7.2Configuración MP-BGP en PE_2.

```
PE_2#
router bgp 65000
neighbor 4.4.4.4 remote-as 65000
 neighbor 4.4.4.4 description HACIA_PE_1
 neighbor 4.4.4.4 update-source Loopback0
 neighbor 6.6.6.6 remote-as 65000
 neighbor 6.6.6.6 description HACIA_PE_3
 neighbor 6.6.6.6 update-source Loopback0
address-family ipv4
  neighbor 4.4.4.4 activate
  neighbor 6.6.6.6 activate
```

exit-address-family
address-family vpnv4
neighbor 4.4.4.4 activate
neighbor 4.4.4.4 send-community extended
neighbor 6.6.6.6 activate
neighbor 6.6.6.6 send-community extended
exit-address-family

3.3.7.3Configuración MP-BGP en PE_3.

PE_3#
set routing-options autonomous-system 65000
set protocols bgp group igp type internal
set protocols bgp group igp family inet unicast
set protocols bgp group igp family inet-vpn unicast
set protocols bgp group igp neighbor 4.4.4.4 description HACIA_PE_1
set protocols bgp group igp neighbor 4.4.4.4 local-address 6.6.6.6
set protocols bgp group igp neighbor 5.5.5.5 description HACIA_PE_2
set protocols bgp group igp neighbor 5.5.5.5 local-address 6.6.6.6

3.3.7.4Verificación del MP-BGP.

PE_2#show ip bgp summary
BGP router identifier 5.5.5.5, local AS number 65000
BGP table version is 1, main routing table version 1

Neighbor	VAS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
4.4.4.4	4	65000	498	494	1	0	0 03:43:54	0
6.6.6.6	4	65000	498	494	1	0	0 03:43:54	0

3.3.8. Configuración de LDP en PE's y P's.

3.3.8.1Configuración LDP en PE_1.

PE_1#
set protocols mpls interface fe-0/0/1

set protocols mpls interface lo0.0

set protocols ldp interface fe-0/0/1

set interfaces fe-0/0/1 unit 0 family mpls

3.3.8.2Configuración LDP en PE2.

PE_2#

mpls label protocol ldp

interface Fastethernet0/1

mpls ip

3.3.8.3Configuración LDP en PE3.

PE_3#

set protocols mpls no-propagate-ttl

set protocols mpls interface fe-0/0/1.0

set protocols mpls interface lo0.0

set protocols ldp interface fe-0/0/1.0

set interfaces fe-0/0/1 unit 0 family mpls

3.3.8.4Configuración LDP en P1.

P_1#

mpls label protocol ldp

interface Fastethernet0/0

mpls ip

interface Fastethernet0/1

mpls ip

3.3.8.5Configuración LDP en P2.

P_2#

mpls label protocol ldp

interface Fastethernet0/00

mpls ip

interface Fastethernet0/1

```
 mpls ip
interface Vlan32
 mpls ip
```

3.3.8.6Verificación de LDP en P_2.

```
P_2#show mpls ldp neighbor
    Peer LDP Ident: 5.5.5.5:0; Local LDP Ident 8.8.8.8:0
TCP connection: 5.5.5.5.646 - 8.8.8.8.59209
State: Oper; Msgs sent/rcvd: 277/273; Downstream
Up time: 03:50:05
LDP discovery sources:
  Fastethernet0/00, Src IP addr: 172.16.2.2
        Addresses bound to peer LDP Ident:
          172.16.2.2      5.5.5.5
    Peer LDP Ident: 7.7.7.7:0; Local LDP Ident 8.8.8.8:0
TCP connection: 7.7.7.7.646 - 8.8.8.8.13559
State: Oper; Msgs sent/rcvd: 272/275; Downstream
Up time: 03:49:36
LDP discovery sources:
  Vlan32, Src IP addr: 172.16.32.1
        Addresses bound to peer LDP Ident:
          172.16.1.1      7.7.7.7         172.16.32.1
    Peer LDP Ident: 6.6.6.6:0; Local LDP Ident 8.8.8.8:0
TCP connection: 6.6.6.6.646 - 8.8.8.8.44781
State: Oper; Msgs sent/rcvd: 1580/1379; Downstream
Up time: 03:48:32
LDP discovery sources:
  Fastethernet0/1, Src IP addr: 172.16.3.2
        Addresses bound to peer LDP Ident:
          172.16.3.2
```

3.3.9. Configuración de las IPVPN sobre los equipos PE.

3.3.9.1 Configuración VRF en PE_1.

PE_1#

set interfaces fe-0/0/0 unit 0 description PE_1_HACIA_CPE_1

set interfaces fe-0/0/0 unit 0 family inet address 192.168.1.1/24

set routing-instances cliente instance-type vrf

set routing-instances cliente interface fe-0/0/0.0

set routing-instances cliente route-distinguisher 65000:1

set routing-instances cliente vrf-target target:65000:1

set routing-instances cliente routing-options static route 10.10.1.0/24 next-hop 192.168.1.2

set routing-instances cliente routing-options static route 1.1.1.1/32 next-hop 192.168.1.2

3.3.9.2 Configuración de VRF en PE_2.

PE_2#

ip vrf cliente

rd 65000:1

route-target export 65000:1

route-target import 65000:1

interface FastEthernet0/0

description HACIA_CPE2_F4

ip vrf forwarding cliente

ip address 192.168.2.1 255.255.255.0

ip route vrf cliente 10.10.2.0 255.255.255.0 192.168.2.2

ip route vrf cliente 2.2.2.2 255.255.255.255 192.168.2.2

3.3.9.3 Configuración de VRF en PE_3.

PE_3#

set interfaces fe-0/0/0 unit 0 description PE_3_HACIA_CPE_3

set interfaces fe-0/0/0 unit 0 family inet address 192.168.3.1/24

set routing-instances cliente instance-type vrf

set routing-instances cliente interface fe-0/0/0.0

set routing-instances cliente route-distinguisher 65000:1

set routing-instances cliente vrf-target target:65000:1

set routing-instances cliente routing-options static route 10.10.3.0/24 next-hop 192.168.3.2

set routing-instances cliente routing-options static route 3.3.3.3/32 next-hop 192.168.3.2

3.3.10. Configuración de los CPE's en IPVPN-MPLS.

3.3.10.1Cálculo de MTU y MSS en IPVPN-MPLS.

Como se revisó en el capítulo 2, MPLS opera añadiendo etiquetas al paquete IP para poderlo forwardear a través de los LSP Label Switching Path, un paquete que atraviesa un backbone MPLS generalmente se le añaden 2 etiquetas, esto se conoce como Label Stack de nivel 2, la primera etiqueta identifica el último router del LSP y la segunda etiqueta el siguiente router del LSP, por este motivo y tomando en cuenta que la máximo longitud del paquete en Ethernet o MTU físico de la maqueta es 1514bytes podemos calcular el MTU_IP del sistema MPLS y el MMS correspondiente para TCP.

Cálculo de MTU_IP:

MTU_IP = MTU_Físico – Cabeceras del sistema

MTU_IP = MTU_Físico – Cabeceras_MPLS– Cabecera_Eth - CRC

MTU_IP = 1518bytes – 8bytes – 14bytes – 4 bytes

MTU_IP = 1492bytes

Tabla 7.

Composición paquete MPLS.

Protocolo	Detalle	Longitud
MTU_IP	Máxima unidad de transf IP	1492 bytes
MPLS / L2.5	Cabecera Label Stack nivel 1	4 bytes
MPLS / L2.5	Cabecera Label Stack nivel 2	4 bytes
Ethernet / L2	Cabecera Ethernet	14 bytes
Ethernet / L2	Chequeo de Redundancia Cíclica	4 bytes
	Máxima longitud del paquete	**1518 bytes**

Fuente: (Elaborado por el Autor)

Cálculo del máximo tamaño de segmento MSS para TCP:

MSS_TCP = MTU_IP – Overhead_TCP – Overhead_IP

MSS_TCP = 1492 bytes – 20 bytes – 20 bytes

MSS_TCP = 1452 bytes

3.3.10.2Configuración CPE_1 en IPVPN-MPLS.

```
CPE_1#
interface FastEthernet4
 description CPE_1_HACIA_PE_1
ip address 192.168.1.2 255.255.255.0
interface Vlan1
 description LAN_CPE_1
 ip address 10.10.1.1 255.255.255.0
ip tcp adjust-MSS 1452
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

3.3.10.3Configuración CPE_2 en IPVPN-MPLS.

```
CPE_2#
interface FastEthernet4
 description CPE_2_HACIA_PE_2
ip address 192.168.2.2 255.255.255.0
```

```
interface Vlan1
 description LAN_CPE_2
 ip address 10.10.2.1 255.255.255.0
ip tcp adjust-MSS 1452
ip route 0.0.0.0 0.0.0.0 192.168.2.1
```

3.3.10.4Configuración CPE_3 en IPVPN-MPLS.

```
CPE_3#
interface FastEthernet4
 description CPE_3_HACIA_PE_3
 ip address 192.168.3.2 255.255.255.0
interface Vlan1
 description LAN_CPE_3
 ip address 10.10.3.1 255.255.255.0
ip tcp adjust-MSS 1452
ip route 0.0.0.0 0.0.0.0 192.168.3.1
```

3.3.10.5Verificación de la tabla VRF en PE´s.

```
global@PE_1> show route table cliente
cliente.inet.0: 10 destinations, 10 routes (10 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
1.1.1.1/32         *[Static/5] 00:09:55,
                  > to 192.168.1.2 via fe-0/0/0.0
2.2.2.2/32         *[BGP/170] 00:43:15, MED 0, localpref 100, from 5.5.5.5
                    AS path: ?
                  > to 172.16.1.1 via fe-0/0/1.0, Push 25, Push 17(top)
3.3.3.3/32         *[BGP/170] 00:47:38, MED 0, localpref 100, from 6.6.6.6
                    AS path: ?
                  > to 172.16.1.1 via fe-0/0/1.0, Push 299776, Push 20(top)
10.10.1.0/24       *[Static/5] 00:09:50,
                  > to 192.168.1.2 via fe-0/0/0.0
10.10.2.0/24       *[BGP/170] 00:29:36, MED 0, localpref 100, from 5.5.5.5
```

```
                AS path: ?
              > to 172.16.1.1 via fe-0/0/1.0, Push 23, Push 17(top)
10.10.3.0/24      *[BGP/170] 00:01:22, MED 0, localpref 100, from 6.6.6.6
                AS path: ?
              > to 172.16.1.1 via fe-0/0/1.0, Push 299776, Push 20(top)
192.168.1.0/24    *[Direct/0] 01:29:49
              > via fe-0/0/0.0
192.168.1.1/32    *[Local/0] 01:29:53
                Local via fe-0/0/0.0
192.168.2.0/24    *[BGP/170] 01:28:57, MED 0, localpref 100, from 5.5.5.5
                AS path: ?
              > to 172.16.1.1 via fe-0/0/1.0, Push 24, Push 17(top)
192.168.3.0/24    *[BGP/170] 01:28:50, localpref 100, from 6.6.6.6
                AS path: I
              > to 172.16.1.1 via fe-0/0/1.0, Push 299776, Push 20(top)

PE_2#show ip route vrf cliente
Routing Table: cliente
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set
      1.0.0.0/32 is subnetted, 1 subnets
B        1.1.1.1 [200/0] via 4.4.4.4, 00:40:08
      2.0.0.0/32 is subnetted, 1 subnets
S        2.2.2.2 [1/0] via 192.168.2.2, 00:43:57
      3.0.0.0/32 is subnetted, 1 subnets
```

```
B       3.3.3.3 [200/0] via 6.6.6.6, 00:48:20
     10.0.0.0/24 is subnetted, 3 subnets
B       10.10.1.0 [200/0] via 4.4.4.4, 00:10:32
S       10.10.2.0 [1/0] via 192.168.2.2, 00:30:18
B       10.10.3.0 [200/0] via 6.6.6.6, 00:02:04
B     192.168.1.0/24 [200/0] via 4.4.4.4, 01:29:40
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, Fastethernet0/0
L       192.168.2.1/32 is directly connected, Fastethernet0/0
B     192.168.3.0/24 [200/0] via 6.6.6.6, 01:29:40
PE_2#
global@PE_3> show route table cliente
+ = Active Route, - = Last Active, * = Both

1.1.1.1/32          *[BGP/170] 00:40:53, MED 0, localpref 100, from 4.4.4.4
                     AS path: ?
                    > to 172.16.3.1 via fe-0/0/1.0, Push 299872, Push 20(top)
2.2.2.2/32          *[BGP/170] 00:44:42, MED 0, localpref 100, from 5.5.5.5
                     AS path: ?
                    > to 172.16.3.1 via fe-0/0/1.0, Push 25, Push 16(top)
3.3.3.3/32          *[Static/5] 00:034:50,
                    > to 192.168.3.2 via fe-0/0/0.0
10.10.1.0/24        *[BGP/170] 00:11:17, MED 0, localpref 100, from 4.4.4.4
                     AS path: ?
                    > to 172.16.3.1 via fe-0/0/1.0, Push 299872, Push 20(top)
10.10.2.0/24        *[BGP/170] 00:31:03, MED 0, localpref 100, from 5.5.5.5
                     AS path: ?
                    > to 172.16.3.1 via fe-0/0/1.0, Push 23, Push 16(top)
10.10.3.0/24        *[Static/5]
                     > to 192.168.3.2 via fe-0/0/0.0
192.168.1.0/24      *[BGP/170] 01:30:17, localpref 100, from 4.4.4.4
                     AS path: I
```

> to 172.16.3.1 via fe-0/0/1.0, Push 299872, Push 20(top)

192.168.2.0/24 *[BGP/170] 01:30:24, MED 0, localpref 100, from 5.5.5.5

AS path: ?

> to 172.16.3.1 via fe-0/0/1.0, Push 24, Push 16(top)

192.168.3.0/24 *[Direct/0] 01:31:25

> via fe-0/0/0.0

192.168.3.1/32 *[Local/0] 01:31:28

Local via fe-0/0/0.0

3.3.11. Pruebas de conectividad entre CPE's en IPVPN-MPLS.

3.3.11.1CPE_1 hacia CPE_2 en IPVPN-MPLS.

CPE_1#ping 10.10.2.1 source 10.10.1.1 repeat 100 size 1500

Type escape sequence to abort.

Sending 100, 1500-byte ICMP Echos to 10.10.2.1, timeout is 2 seconds:

Packet sent with a source address of 10.10.1.1

!!!

Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/12 ms

CPE_1#trace 10.10.2.1 source 10.10.1.1

Tracing the route to 10.10.2.1

1 192.168.1.1 4 msec 16 msec 8 msec

2 192.168.2.1 [AS 65000] 0 msec 4 msec 0 msec

3 192.168.2.2 [AS 65000] 0 msec * 0 msec

3.3.11.2CPE_2 hacia CPE_3 en IPVPN-MPLS.

CPE_1#ping 10.10.3.1 source 10.10.2.1 repeat 100 size 1500

Type escape sequence to abort.

Sending 100, 1500-byte ICMP Echos to 10.10.3.1, timeout is 2 seconds:

Packet sent with a source address of 10.10.2.1

!!

Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4 ms

3.3.11.3CPE_1 hacia CPE_3 en IPVPN-MPLS.

CPE_1#trace 10.10.3.1 source 10.10.1.1

Type escape sequence to abort.

Tracing the route to 10.10.3.1

1 192.168.1.1 4 msec 16 msec 8 msec

2 192.168.3.2 [AS 65000] 0 msec * 0 msec

3.4 Consideraciones técnicas para el sistema IPsec sobre Internet.

3.4.1 Determinación de Software para IPsec sobre Internet.

El software que deben poseer los equipos que van a realizar o establecer el sistema de Internet básicamente son de los vendors Cisco y Juniper que poseen las siguientes características.

3.4.2 Router Vendor Juniper.

Hardware: Model: srx100b.

Software: JUNOS Software Release [10.2R3.10].

Features: BGP

Detalle: el software cargado soporta las características para los fines de nuestro proyecto.

3.4.3 Router Vendor Cisco.

Hardware: Cisco 2801.

Software: Software (C2801-SPSERVICESK9-M), Version 12.4(15)T10,

Features: BGP, IPsec.

Detalle: el software cargado soporta las características para los fines de nuestro proyecto.

3.4.4 Configuraciones y pruebas del Sistema IPsec sobre Internet.

Básicamente un backbone o sistema Internet va a manejar el forwardeo de paquetes en base al a información de cabecera de capa 3. El sistema de internet se compone de sistemas autónomos (AS´s) que son generalmente un grupo de router bajo una misma

administración y que usan como protocolo de enrutamiento BGP para recibir o enviar sus redes entre sistemas, para fines del proyecto cada router PE y P es considerado un AS independiente.

La configuración del sistema Internet comprende 4 pasos:

-Configuración de interfaces y conectividad de PE´s y P´s.

-Configuración de protocolo de ruteo dinámico externo EBGP entre AS´s.

-Configuración de interfaces y conectividad de los CPE's a nivel IP.

-Configuración de los tuneles IPsec en los CPE's.

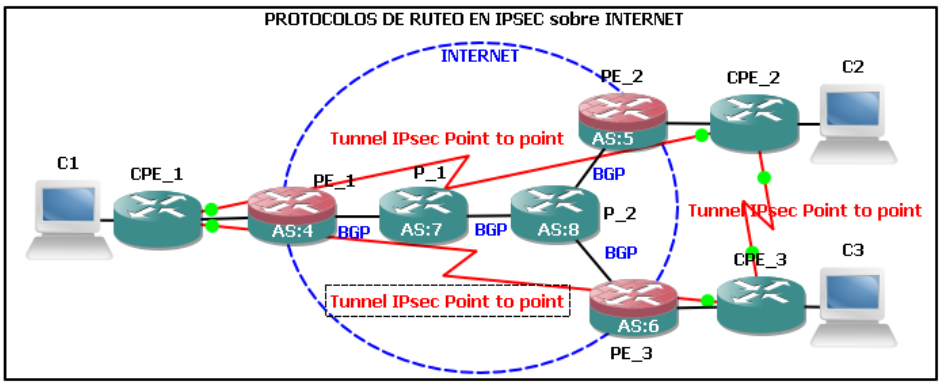

Figura 28. Protocolos en Sistema IPsec sobre Internet.

Fuente: (Elaborado por el Autor)

3.4.5 Configuración de PE´S y P´s en IPsec sobre Internet.

3.4.5.1 Direccionamiento IP e interfaces de PE_1.

PE_1#

set interfaces fe-0/0/0 unit 0 description PE1_HACIA_CPE_1

set interfaces fe-0/0/0 unit 0 family inet address 192.168.1.1/24

set interfaces fe-0/0/1 unit 0 description PE_1_HACIA_P_1

set interfaces fe-0/0/1 unit 0 family inet address 172.16.1.2/24

set interfaces lo0 unit 0 family inet address 4.4.4.4/32

3.4.5.2 Direccionamiento IP e interfaces PE_2.

```
PE_2#
interface Fastethernet0/1
 description PE_2_HACIA_P_2
ip address 172.16.2.2 255.255.255.0
interface Loopback0
 description LOOPBACK_5.5.5.5
 ip address 5.5.5.5 255.255.255.255
```

3.4.5.3 Direccionamiento IP e interfaces PE_3.

```
PE_3#
set interfaces fe-0/0/1 unit 0  description PE_3_HACIA_P_2
set interfaces fe-0/0/1 unit 0  family inet address 172.16.3.2/24
set interfaces lo0 unit 0 family inet address 6.6.6.6/32
```

3.4.5.4 Direccionamiento IP e interfaces P_1.

```
P_1#
interface Fastethernet0/0
 description P1_HACIA_PE_1
ip address 172.16.1.1 255.255.255.0
interface Fastethernet0/1
 description P_1_HACIA_P_2
 ip address 172.16.32.1 255.255.255.252
interface Loopback0
 description LOOPBACK_ 7.7.7.7
 ip address 7.7.7.7 255.255.255.255
```

3.4.5.5 Direccionamiento IP e interfaces P_2.

```
P_2#
interface Fastethernet0/00
 description P_2_HACIA_PE_2
ip address 172.16.2.1 255.255.255.0
```

interface Fastethernet0/1
description P_2_HACIA_PE_3
ip address 172.16.3.1 255.255.255.0
interface Vlan32
description P_2_HACIA__P_1
ip address 172.16.32.2 255.255.255.252
interface Loopback0
description LOOPBACK_8.8.8.8
ip address 8.8.8.8 255.255.255.255

3.4.6 Configuración de ruteo dinámico EBGP entre AS´s .

El EBGP o external BGP es la base para obtener la conectividad o visibilidad entre los AS´s, generalmente los AS usan protocolos IGP como IS-IS internamente entre sus router sin embargo si y solo si el único protocolo a nivel de internet usado para transferir o propagar sus prefijos y tablas de rutas entre AS´s es BGP tipo external Para fines del proyecto se usará como sistema autónomo el número de identificación de las loopback de cada router

3.4.6.1 Configuración EBGP en PE_1.

PE_1#
set routing-options autonomous-system 4
set protocols bgp group EBGP neighbor 172.16.1.1
set protocols bgp group EBGP neighbor 172.16.1.1 export exportar
set protocols bgp group EBGP neighbor 172.16.1.1 peer-as 7
set policy-options policy-statement exportar from protocol direct
set policy-options policy-statement exportar then accept

3.4.6.2 Configuración EBGP en PE_2.

PE_2#
router bgp 5
neighbor 172.16.2.1 remote-as 8
neighbor 172.16.2.1 description PE_2_HACIA_P_2

address-family ipv4

redistribute connected

neighbor 172.16.2.1 activate

3.4.6.3 Configuración EBGP en PE_3.

PE_3#

set routing-options autonomous-system 6

set protocols bgp group EBGP neighbor 172.16.3.1 export exporter

set protocols bgp group EBGP neighbor 172.16.3.1

set protocols bgp group EBGP neighbor 172.16.3.1 peer-as 8

set policy-options policy-statement exportar from protocol direct

set policy-options policy-statement exportar then accept

3.4.6.4 Configuración EBGP en P_1.

P_1#

router bgp 7

neighbor 172.16.1.2 remote-as 4

neighbor 172.16.1.2 description P_1_HACIA_PE_1

neighbor 172.16.32.2 remote-as 8

neighbor 172.16.32.2 description P_1_HACIA_P_2

address-family ipv4

redistribute connected

neighbor 172.16.1.2 activate

neighbor 172.16.32.2 activate

3.4.6.5 Configuración EBGP en P_2.

P_2#

router bgp 8

neighbor 172.16.2.2 remote-as 5

neighbor 172.16.2.2 description P_2_HACIA_PE_2

neighbor 172.16.3.2 remote-as 6

neighbor 172.16.3.2 description P_2_HACIA_PE_3

```
 neighbor 172.16.32.1 remote-as 7
 neighbor 172.16.32.1 description P_2_HACIA_P_1
address-family ipv4
 redistribute connected
 neighbor 172.16.2.2 activate
 neighbor 172.16.3.2 activate
 neighbor 172.16.32.1 activate
```

3.4.7 Configuración de los CPE's en IPsec sobre Internet.

3.4.7.1 Cálculo de MTU y MSS en IPsec sobre Internet.

Como revisamos en el capítulo 2, IPsec es un protocolo estándar que provee privacidad integridad y autenticidad de la información que cruza por una red IP, la encriptación provoca añadir Cabeceras al paquete original dependiendo de la configuración y del modo IPsec que se quiera usar. Considerando que el MTU físico o la máxima longitud del paquete en Ethernet es 1514bytes podemos calcular el MTU_IP y el MSS para el sistema IPsec considerando una encriptación ESP-AES con HA.

Cálculo del MTU_IP:

MTU_IP = MTU_Físico – Cabeceras del sistema

MTU_IP = MTU_Físico – CabIPnew_Cabeceras_IPSEC– Cabecera_Eth – CRC

MTU_IP = 1518bytes – 20bytes - 56bytes – 24 bytes – 14bytes – 4bytes

MTU_IP = 1400bytes.

Tabla 8.

Composición paquete IPsec.

Protocolo	Detalle	Longitud
MTU_IP	Máxima unidad de transferencia IP	1400 bytes
IP/L3	Cabecera IP	20 bytes
ESP /L3	Cabecera ESP	56 bytes
AH / L3	Cabecera AH	24 bytes

Continua

Ethernet / L2	Cabecera Ethernet	14 bytes
Ethernet / L2	Crc – Chequeo de Redundancia Cíclica	4 bytes
	Máxima longitud del paquete	1518 bytes

Fuente: (Elaborado por el Autor)

Cálculo del máximo tamaño de segmento MSS para TCP:

$$MSS\_TCP = MTU\_IP - Overhead\_TCP - Overhead\_IP$$

$$MSS\_TCP = 1400 \text{ bytes} - 20 \text{ bytes} - 20 \text{ bytes}$$

$$MSS\_TCP = 1360 \text{ bytes.}$$

3.4.7.2 Configuración en CPE_1 en IPsec sobre Internet.

```
CPE_1#
crypto isakmp policy 1
 encr aes
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 123456789 address 192.168.2.2
crypto isakmp key 123456789 address 192.168.3.2
crypto ipsec transform-set VPN ah-md5-hmac esp-aes
crypto map VPN_IPSEC 10 ipsec-isakmp
 set peer 192.168.2.2
 set transform-set VPN
 match address VPN_2
crypto map VPN_IPSEC 20 ipsec-isakmp
 set peer 192.168.3.2
 set transform-set VPN
 match address VPN_3
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
interface FastEthernet4
 description CPE_1_HACIA_PE_1
```

```
 ip address 192.168.1.2 255.255.255.0
crypto map VPN_IPSEC
interface Vlan1
 description LAN_CPE_1
 ip address 10.10.1.1 255.255.255.0
ip tcp adjust-MSS 1360
ip route 0.0.0.0 0.0.0.0 192.168.1.1
ip access-list extended VPN_2
 permit ip any 10.10.2.0 0.0.0.255
ip access-list extended VPN_3
 permit ip any 10.10.3.0 0.0.0.255
```

3.4.7.3 Configuración en CPE_2 en IPsec sobre Internet.

```
CPE_2 #
crypto isakmp policy 1
 encr aes
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 123456789 address 192.168.1.2
crypto ipsec transform-set VPN ah-md5-hmac esp-aes
crypto map VPN_IPSEC 10 ipsec-isakmp
 set peer 192.168.1.2
 set transform-set VPN
 match address VPN_1
interface Loopback0
 description LOOPBACK_CPE_2_2.2.2.2
 ip address 2.2.2.2 255.255.255.255
interface FastEthernet4
 description CPE_2_HACIA_PE_2
ip address 192.168.2.2 255.255.255.0
crypto map VPN_IPSEC
```

```
interface Vlan1
 description LAN_CPE2
 ip address 10.10.2.1 255.255.255.0
ip tcp adjust-MSS 1360
ip route 0.0.0.0 0.0.0.0 192.168.2.1
ip access-list extended VPN_1
 permit ip 10.10.2.0 0.0.0.255 any
```

3.4.7.4 Configuración en CPE_3 en IPsec sobre Internet.

```
CPE_3 #
crypto isakmp policy 1
 encr aes
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 123456789 address 192.168.1.2
crypto ipsec transform-set VPN ah-md5-hmac esp-aes
crypto map VPN_IPSEC 10 ipsec-isakmp
 set peer 192.168.1.2
 set transform-set VPN
 match address VPN_1
interface Loopback0
 description LOOPBACK_CPE_3_3.3.3.3
 ip address 3.3.3.3 255.255.255.255
interface FastEthernet4
 description CPE_3_HACIA_PE_3
 ip address 192.168.3.2 255.255.255.0
 crypto map VPN_IPSEC
interface Vlan1
 description LAN_CPE_3
 ip address 10.10.3.1 255.255.255.0
ip tcp adjust-MSS 1360
```

```
ip route 0.0.0.0 0.0.0.0 192.168.3.1
ip access-list extended VPN_1
 permit ip 10.10.3.0 0.0.0.255 any
```

3.4.7.5 Verificación del BGP en PE's.

```
global@PE_1> show route protocol bgp
inet.0: 14 destinations, 15 routes (14 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
5.5.5.5/32         *[BGP/170] 01:12:31, localpref 100
                    AS path: 7 8 5 ?
                   > to 172.16.1.1 via fe-0/0/1.0
6.6.6.6/32         *[BGP/170] 01:12:31, localpref 100
                    AS path: 7 8 6 I
                   > to 172.16.1.1 via fe-0/0/1.0
7.7.7.7/32         *[BGP/170] 01:12:31, MED 0, localpref 100
                    AS path: 7 ?
                   > to 172.16.1.1 via fe-0/0/1.0
8.8.8.8/32         *[BGP/170] 01:12:31, localpref 100
                    AS path: 7 8 ?
                   > to 172.16.1.1 via fe-0/0/1.0
172.16.1.0/24       [BGP/170] 01:12:31, MED 0, localpref 100
                    AS path: 7 ?
                   > to 172.16.1.1 via fe-0/0/1.0
172.16.2.0/24      *[BGP/170] 01:12:31, localpref 100
                    AS path: 7 8 ?
                   > to 172.16.1.1 via fe-0/0/1.0
172.16.3.0/24      *[BGP/170] 01:12:31, localpref 100
                    AS path: 7 8 ?
                   > to 172.16.1.1 via fe-0/0/1.0
172.16.32.0/30     *[BGP/170] 01:12:31, MED 0, localpref 100
                    AS path: 7 ?
                   > to 172.16.1.1 via fe-0/0/1.0
```

192.168.2.0/24 *[BGP/170] 01:12:31, localpref 100
AS path: 7 8 5 ?
> to 172.16.1.1 via fe-0/0/1.0
192.168.3.0/24 *[BGP/170] 01:12:31, localpref 100
AS path: 7 8 6 I
> to 172.16.1.1 via fe-0/0/1.0

3.4.8 Verificación de VPN's en IPsec sobre Internet.

3.4.8.1 Verificación de VPN IPsec en CPE_1.

CPE_1#sho crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
Interface: FastEthernet4
Uptime: 01:57:06
Session status: UP-ACTIVE
Peer: 192.168.2.2 port 500 fvrf: (none) ivrf: (none)
Phase1_id: 192.168.2.2
Desc: (none)
IKE SA: local 192.168.1.2/500 remote 192.168.2.2/500 Active
Capabilities:(none) connid:2007 lifetime:22:02:53
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 10.10.2.0/255.255.255.0
Active SAs: 4, origin: crypto map
Inbound: #pkts dec'ed 6208 drop 0 life (KB/Sec) 4386157/3475
Outbound: #pkts enc'ed 4362 drop 5 life (KB/Sec) 4386157/3475

Interface: FastEthernet4
Uptime: 01:56:49
Session status: UP-ACTIVE
Peer: 192.168.3.2 port 500 fvrf: (none) ivrf: (none)

Phase1_id: 192.168.3.2

Desc: (none)

IKE SA: local 192.168.1.2/500 remote 192.168.3.2/500 Active

Capabilities:(none) connid:2008 lifetime:22:03:10

IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 10.10.3.0/255.255.255.0

Active SAs: 4, origin: crypto map

Inbound: #pkts dec'ed 3569 drop 0 life (KB/Sec) 4536439/3539

Outbound: #pkts enc'ed 3588 drop 2 life (KB/Sec) 4536439/3539

3.4.8.2 Verificación de VPN IPsec en CPE_2.

CPE_2#sho crypto session detail

Crypto session current status

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

K - Keepalives, N - NAT-traversal, T - cTCP encapsulation

X - IKE Extended Authentication, F - IKE Fragmentation

Interface: FastEthernet4

Uptime: 00:10:59

Session status: UP-ACTIVE

Peer: 192.168.1.2 port 500 fvrf: (none) ivrf: (none)

Phase1_id: 192.168.1.2

Desc: (none)

IKE SA: local 192.168.2.2/500 remote 192.168.1.2/500 Active

Capabilities:(none) connid:2010 lifetime:23:49:00

IPSEC FLOW: permit ip 10.10.2.0/255.255.255.0 0.0.0.0/0.0.0.0

Active SAs: 2, origin: crypto map

Inbound: #pkts dec'ed 41 drop 0 life (KB/Sec) 4568226/2940

Outbound: #pkts enc'ed 41 drop 1 life (KB/Sec) 4568226/2940

3.4.8.3 Verificación de VPN IPsec en CPE_3.

CPE_3 #sho crypto session detail

Crypto session current status

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

K - Keepalives, N - NAT-traversal, T - cTCP encapsulation

X - IKE Extended Authentication, F - IKE Fragmentation

Interface: FastEthernet4

Uptime: 00:11:11

Session status: UP-ACTIVE

Peer: 192.168.1.2 port 500 fvrf: (none) ivrf: (none)

Phase1_id: 192.168.1.2 Desc: (none)

IKE SA: local 192.168.3.2/500 remote 192.168.1.2/500 Active

Capabilities:(none) connid:2002 lifetime:23:48:48

IPSEC FLOW: permit ip 10.10.3.0/255.255.255.0 0.0.0.0/0.0.0.0

Active SAs: 2, origin: crypto map

Inbound: #pkts dec'ed 8 drop 0 life (KB/Sec) 4411970/2928

Outbound: #pkts enc'ed 8 drop 1 life (KB/Sec) 4411970/2928

3.4.9 Pruebas de conectividad entre CPE´s en IPsec sobre Internet.

3.4.9.1 CPE_1 hacia CPE_2 en IPsec sobre Internet.

CPE_1#ping 10.10.2.1 source 10.10.1.1 size 1500

Type escape sequence to abort.

Sending 5, 1500-byte ICMP Echos to 10.10.2.1, timeout is 2 seconds:

Packet sent with a source address of 10.10.1.1 !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

3.4.9.2 CPE_1 hacia CPE_3 en IPsec sobre Internet.

CPE_1#ping 10.10.3.1 source 10.10.1.1 size 1500

Type escape sequence to abort.

Sending 5, 1500-byte ICMP Echos to 10.10.3.1, timeout is 2 seconds:

Packet sent with a source address of 10.10.1.1 !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

3.4.9.3 CPE_3 hacia CPE_2 en IPsec sobre Internet.

CPE_3 #ping 10.10.2.1 source 10.10.3.1 size 1500

Type escape sequence to abort.

Sending 5, 1500-byte ICMP Echos to 10.10.2.1, timeout is 2 seconds:

Packet sent with a source address of 10.10.3.1

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms

3.5 Consideraciones técnicas para el sistema DMVPN sobre MPLS.

Para este punto se debe considerar que el backbone MPLS es el mismo que se implementó para el sistema IPVPN-MPLS y que la función DMVPN se realiza solamente en los equipos CPE. El software que deben poseer estos equipos que van a realizar esta tarea son de los vendors Cisco y poseen las siguientes características.

3.5.1 Determinación de Software para DMVPN sobre MPLS.

3.5.2 Router Vendor Cisco.

Hardware: Cisco C881

Software: Cisco IOS, c880data-universalk9-mz.124-24.T.bin

Features: IPsec, NHRP, OSPF

Detalle: el software cargado soporta las características para los fines de nuestro proyecto.

3.5.3 Configuraciones y pruebas del Sistema DMVPN sobre MPLS.

La configuración del escenario DMVPN sobre el sistema IPVPN-MPLS consta de como primera fase, la configuración base en los equipos PE realizada para el escenario IPVPN sobre MPLS, respecto a la configuración de la IPVPN que implica el seteo de los parámetros de red en el Backbone MPLS como son interfaces, nombre de la vrf, route-target, y protocolo de ruteo, para el caso de nuestro proyecto el route-target se usará como identificativo el parámetro 65000:1 y se usará ruteo estático hacia los CPE´s, los prefijos o rutas configuradas se propagarán vía MP-BGP por medio de address family vpnv4 para Cisco y address family inet-vpn para el caso de Juniper.

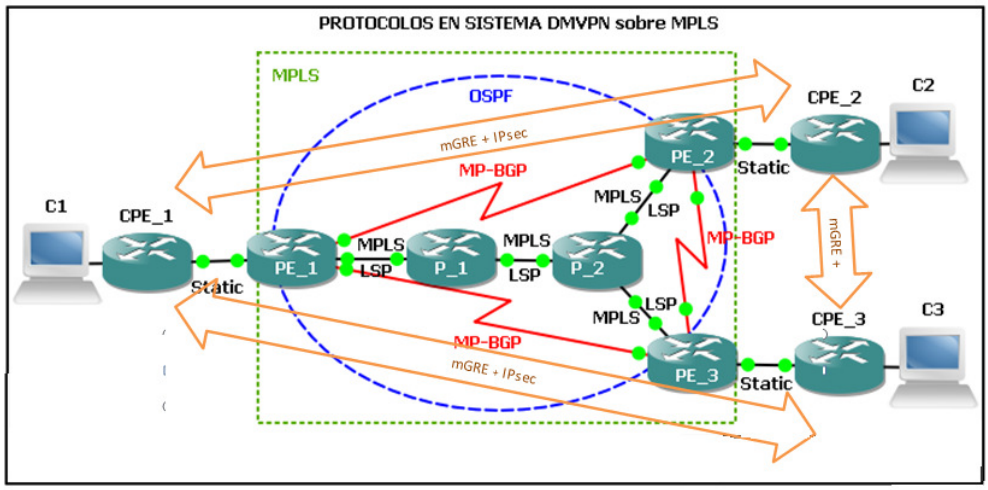

Figura 29. Escenario DMVPN sobre MPLS.

Fuente: (Elaborado por el Autor)

La parte de la DMVPN se configura a nivel de los CPE generando un esquema de conectividad como se puede observar en la figura 30, los pasos para levantar esta configuración son:

- Configuración de interfaces y direccionamiento en CPE´s.
- Configuración del túnel mGRE
- Configuración del IPsec y dominio de encriptación, del NHRP y OSPF

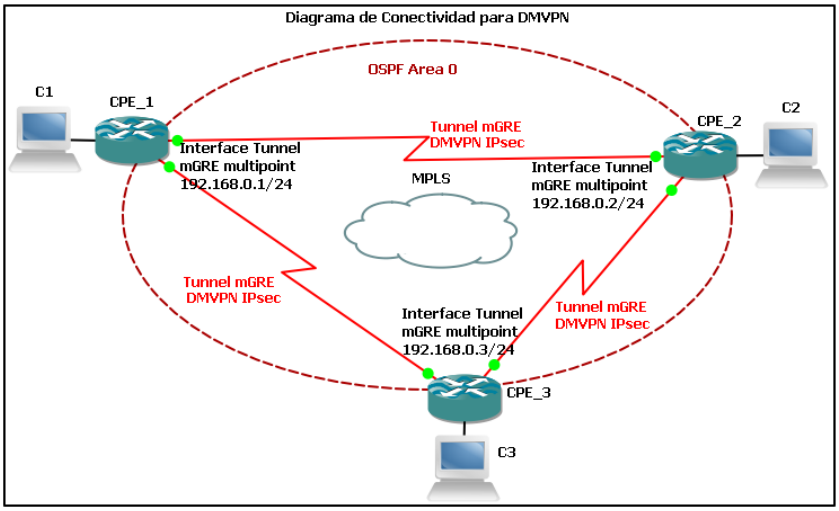

Figura 30. Diagrama de conectividad para DMVPN.

Fuente: (Elaborado por el Autor)

3.5.4 Configuración de los CPE's en DMVPN sobre MPLS.

3.5.4.1 Cálculo de MTU y MSS en DMVPN sobre MPLS.

IPsec es un protocolo estándar que provee privacidad integridad y autenticidad de la información que cruza por una red IP, la encriptación provoca añadir Cabeceras al paquete original dependiendo de la configuración y del modo IPsec que se quiera usar. Adicionalmente a en el backbone MPLS se añaden las Cabeceras de las etiquetas MPLS. Considerando que el MTU físico o la máxima longitud del paquete en Ethernet es 1514bytes podemos calcular el MTU_IP y el MSS para el sistema IPsec considerando una encriptación ESP-AES con HA.

MTU_IP = MTU_Físico – Cabeceras del sistema

MTU_IP = MTU_Físico – Cabecera_MPLS - Cabeceras_IPSEC– Cabecera_Mgre - Cabecera_Ethernet – CRC

MTU_IP = 1518bytes – 8 bytes – 56bytes – 24 bytes – 28 bytes – 14bytes – 4bytes.

MTU_IP = 1384 bytes

Tabla 9.

Composición paquete IPsec sobre MPLS

Protocolo	Detalle	Longitud
MTU_IP	Máxima Uni transferencia IP	1384 byte
ESP /L3	Cabecera ESP	56 bytes
AH / L3	Cabecera AH	24 bytes
MGRE + DMVPN / L3	Cabecera MGRE + DMVPN key	28 bytes
MPLS / L2.5	Cabecera Label Stack nivel 1	4 bytes
MPLS / L2.5	Cabecera Label Stack nivel 2	4 bytes
Ethernet / L2	Cabecera Ethernet	14 bytes
Ethernet / L2	Chequeo de Redundancia Cíclica	4 bytes
	Máxima longitud del paquete	1518 bytes

Fuente: (Elaborado por el Autor)

Cálculo del máximo tamaño de segmento MSS para TCP:

MSS_TCP = MTU_IP – Overhead_TCP – Overhead_IP

MSS_TCP = 1384bytes – 20 bytes – 20 bytes

MSS_TCP = 1344 bytes.

3.5.4.2 Configuración CPE_1 en DMVPN sobre MPLS.

```
CPE_1#
crypto isakmp policy 100
 encr aes
 hash md5
 authentication pre-share
crypto isakmp key key address 0.0.0.0 0.0.0.0 no-xauth
crypto ipsec transform-set set1 esp-aes esp-md5-hmac
crypto ipsec profile profile1
 set transform-set set1

interface Tunnel0
 description DMVPN
 ip address 192.168.0.1 255.255.255.0
 no ip redirects
ip nhrp map multicast dynamic
 ip nhrp network-id 1000
ip ospf network broadcast
 ip ospf 1 area 0
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel protection ipsec profile profile1
interface Loopback0
 description LOOPBACK_CPE_1
 ip address 1.1.1.1 255.255.255.255
interface FastEthernet4
 description CPE1_HACIA_PE1
```

```
 encapsulation dot1Q 10
 ip address 192.168.1.2 255.255.255.0
interface Vlan1
 description LAN_CPE_1
 ip address 10.10.1.1 255.255.255.0
 ip tcp adjust-MSS 1344
ip route 0.0.0.0 0.0.0.0 192.168.1.1 name DEFAULT
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 network 10.10.1.0 0.0.0.255 area 0
```

3.5.4.3 Configuración CPE_2 en DMVPN sobre MPLS.

```
CPE_2#
crypto isakmp policy 100
 encr aes
 hash md5
 authentication pre-share
crypto isakmp key key address 0.0.0.0 0.0.0.0 no-xauth
crypto ipsec transform-set set1 esp-aes esp-md5-hmac
crypto ipsec profile profile1
 set transform-set set1
interface Loopback0
 description LOOPBACK_CPE_2_2.2.2.2
 ip address 2.2.2.2 255.255.255.255
interface Tunnel0
 description DMVPN
 ip address 192.168.0.2 255.255.255.0
 no ip redirects
ip nhrp map 192.168.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1000
```

```
 ip nhrp nhs 192.168.0.1
ip ospf network broadcast
 ip ospf priority 0
 ip ospf 1 area 0
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel protection ipsec profile profile1
interface FastEthernet4
 description CPE_2_CISCO
 encapsulation dot1Q 20
 ip address 192.168.2.2 255.255.255.0
interface Vlan1
 description LAN_CPE2
 ip address 10.10.2.1 255.255.255.0
ip tcp adjust-MSS 1344
ip route 0.0.0.0 0.0.0.0 192.168.2.1 name DEFAULT
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 network 10.10.2.0 0.0.0.255 area 0
```

3.5.4.4 Configuración CPE_3 en DMVPN sobre MPLS.

```
CPE_3#
crypto isakmp policy 100
 encr aes
 hash md5
 authentication pre-share
crypto isakmp key key address 0.0.0.0 0.0.0.0 no-xauth
crypto ipsec transform-set set1 esp-aes esp-md5-hmac
crypto ipsec profile profile1
 set transform-set set1
interface Loopback0
```

```
 description LOOPBACK_CPE_3_3.3.3.3
 ip address 3.3.3.3 255.255.255.255
interface Tunnel0
 description DMVPN
 ip address 192.168.0.3 255.255.255.0
ip nhrp map 192.168.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1000
 ip nhrp nhs 192.168.0.1
ip ospf network broadcast
 ip ospf priority 0
 ip ospf 1 area 0
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel protection ipsec profile profile1
interface FastEthernet4
 description HACIA_PE_3
ip address 192.168.3.2 255.255.255.0
interface Vlan1
 description LAN_CPE_3
 ip address 10.10.3.1 255.255.255.0
ip tcp adjust-MSS 1344
ip route 0.0.0.0 0.0.0.0 192.168.3.1 name DEFAULT
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 network 10.10.3.0 0.0.0.255 area 0
```

3.5.5 Pruebas de conectividad entre CPE's en DMVPN sobre MPLS..

3.5.5.1CPE_1 hacia CPE_2 en DMVPN sobre MPLS.

```
CPE_1#ping 10.10.2.1 source 10.10.1.1 repeat 100 size 1500
```

Type escape sequence to abort.

Sending 100, 1500-byte ICMP Echos to 10.10.2.1, timeout is 2 seconds:

Packet sent with a source address of 10.10.1.1

!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Success rate is 100 percent (100/100), round-trip min/avg/max = 1/4/13 ms

CPE_1#trace 10.10.2.1 source 10.10.1.1

Type escape sequence to abort.

Tracing the route to 10.10.2.1

1 192.168.0.1 4 msec 16 msec 8 msec

2 192.168.0.2 0 msec * 0 msec

3.5.5.2CPE_1 hacia CPE_3 en DMVPN sobre MPLS.

CPE_1#ping 10.10.3.1 source 10.10.1.1 repeat 100 size 1500

Type escape sequence to abort.

Sending 100, 1500-byte ICMP Echos to 10.10.3.1, timeout is 2 seconds:

Packet sent with a source address of 10.10.1.1

!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Success rate is 100 percent (100/100), round-trip min/avg/max = 1/4/12 ms

CPE_1#trace 10.10.3.1 source 10.10.1.1

Type escape sequence to abort.

Tracing the route to 10.10.3.1

1 192.168.0.1 4 msec 16 msec 8 msec

2 192.168.0.3 0 msec * 0 msec

3.5.5.3CPE_2 hacia CPE_3 en DMVPN sobre MPLS.

CPE_2#ping 10.10.3.1 source 10.10.2.1 repeat 100 size 1500

Type escape sequence to abort.

Sending 100, 1500-byte ICMP Echos to 10.10.3.1, timeout is 2 seconds:

Packet sent with a source address of 10.10.2.1

!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4 ms

CPE_2#trace 10.10.3.1 source 10.10.2.1

Type escape sequence to abort.

Tracing the route to 10.10.3.1

1 192.168.0.2 2 msec 5msec 10 msec

2 192.168.0.3 0 msec * 0 msec

CAPITULO IV

DESARROLLO DE LAS PRUEBAS DE DESEMPEÑO

4.1 Desarrollo de las pruebas de desempeño

Las pruebas de desempeño a realizarse sobre los sistemas se realizaron con el uso de dos PC las cuales poseen como sistemas operativo Windows XP Profesional, una PC siempre hará la función de cliente y la otra igualmente de servidor, la aplicación para la generación de los flujos de tráfico a utilizarse es Jperf para Windows en modo Cliente-servidor, para las mediciones se han considerado las parámetros o variables de cada sistema que manejan tanto el transmisor o servidor y el receptor o cliente.

4.2 Herramienta de Evaluación de los Sistemas.

Una vez montada físicamente la maqueta y realizada la configuración de los tres sistemas, el siguiente paso es realizar la evaluación de desempeño de los mismos, este proceso se lo va a realizar con el uso del software JPERF el mismo que es una aplicación en modo Cliente-Servidor, cuyo objetivo es generar una o más transmisiones de tráfico TCP o UDP desde el cliente hacia el servidor, estás transmisiones se las visualiza gráficamente en la herramienta y posteriormente se obtiene o nos da el resultado del total de la carga transmitida y el tiempo de transmisión el cual será la variable a considerar para el cálculo de desempeño de los sistemas.

4.3 Procedimiento de Evaluación de los Sistemas con tráfico TCP

Para la evaluación de los sistemas se ha considerado como variables de entrada a los sistemas, el número de flujos TCP a enviar en una transmisión; la carga o el payload en unidades de bytes que posee cada flujo TCP y el ancho de banda del canal a evaluar.

Los flujos TCP y la carga por flujo son seteados en la herramienta de evaluación JPERF y el ancho de banda del canal es configurado tanto de entrada como en la salida de las interfaces de los CPE’s.

Para cada uno de los sistemas se realizó las siguientes transmisiones:

- Transmisor (TX) CPE_2 hacia Receptor (RX) CPE_1.

Por cada transmisión se generó los siguientes flujos TCP.

- 1 flujo TCP.
- 4 flujos TCP.
- 8 flujos TCP.

Por cada flujo TCP y por cada transmisión se evaluó los siguientes anchos de banda

- 5Mbps.
- 10Mbps.
- 20Mbps.
- 100Mbps (sin limitación en el sistema),

Y por cada transmisión por cada flujo TCP y por cada ancho de banda se generaron la siguiente carga:

- 24419000 Bytes.

4.4 Configuración de JPERF como Servidor para TCP.

En la aplicación JPERF de la PC que realizará la función de servidor se selecciona la función de server y colocamos el número de puerto TCP con la que se realizará la transmisión, se coloca el número máximo de flujos TCP o conexiones permitidas durante cada transmisión y adicionalmente se setea el valor de la ventana TCP a 64Kbytes que es el valor teórico máximo soportado para Windows.

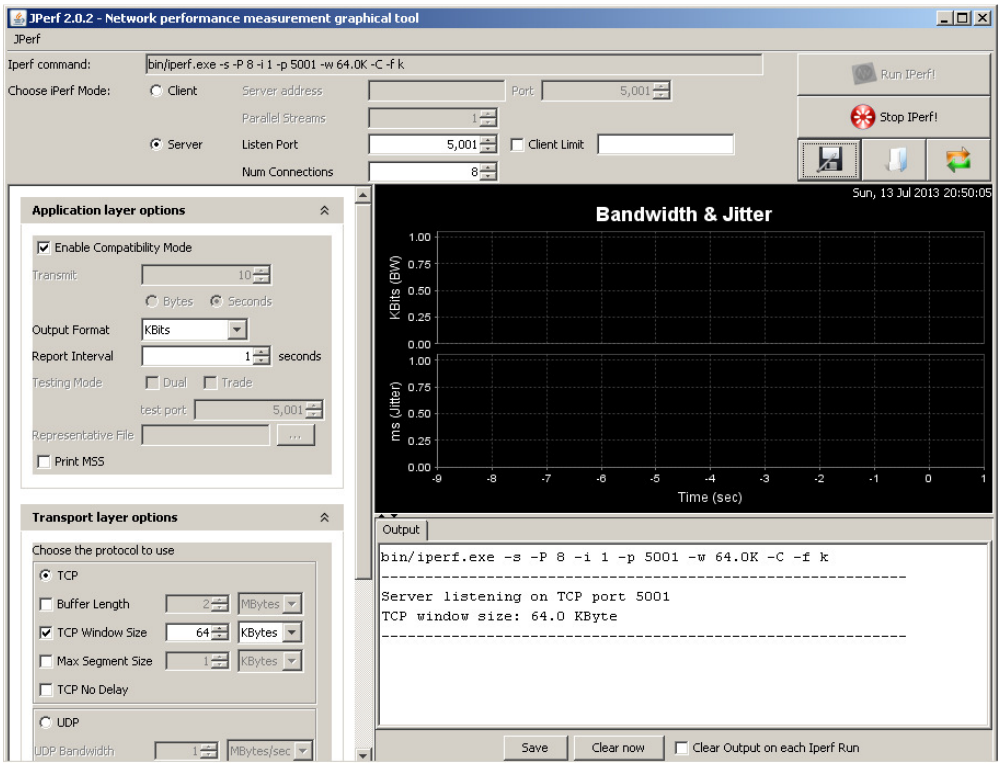

Figura 31: Modo Servidor JPERF

Fuente: (Elaborado por el Autor)

4.5 Configuración de JPERF como Cliente para TCP

Como se muestra en la figura 32 en la PC cliente seleccionamos la función y seteamos la dirección IP del servidor y el puerto TCP del servidor y el número de flujos TCP concurrentes o paralelos que se van enviar al mismo.

En lo que respecta a los parámetros TCP no se modifica y la aplicación toma el valor por defecto de la ventana TCP que maneja Windows XP que es 16Kbytes, este valor no tiene injerencia en las pruebas pues quien maneja el cantidad máxima de bytes que puede transmitir sobre el canal está definida por la ventana TCP del receptor o servidor.

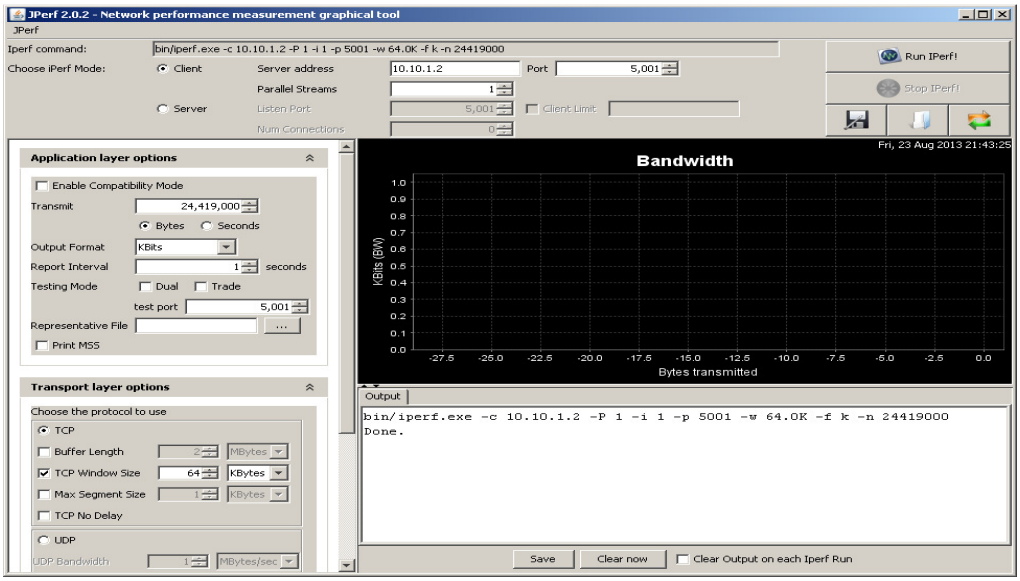

Figura 32: Interface Gráfica JPERF

Fuente: (Elaborado por el Autor)

Una vez terminada la transmisión y como se puede observar en la figura 32 la herramienta JPERF nos da el tiempo en segundos, la carga de datos total y el promedio de la taza de transferencia o troughput de los flujos TCP que se transmitieron, adicionalmente muestra gráficamente el comportamiento de la transmisión por cada flujo, la visualización gráfica no es materia de este proyecto, el valor a recolectar es el tiempo de transferencia.

-

4.6 Configuración de Ancho de Banda del canal para TCP.

La limitación del ancho de banda del canal donde se corren las pruebas se las realizó configurando una política tanto de entrada como de salida en las interfaces wan de todos los CPE's. En la política se define el CIR (Commited Information Rate) en bits por segundo que corresponde al ancho de banda y el BC (burst commited) que equivale al CIR/8, como podemos ver en la siguiente configuración se limita el ancho de banda del canal a 5Mbps del CPE_1

4.7 Parámetros para IPVPN-MPLS con TCP.

En la tabla 10 se detallan los parámetros correspondientes que son manejados durante una comunicación entre cliente-servidor para la evaluación de desempeño.

Tabla 10.

Parámetros para el sistema IPVPN-MPLS con TCP.

Parámetro	Valor	Tipo	Elemento	Aplicación
MTU Int	1518 bytes	Constante	Todos	Nivel físico
IP MTU	1492 bytes	Constante	PC´s	Stack IP/TCP
MSS:	1460 -1452-1000-500	Constante	CPE's	Stack IP/TCP
Carga	24MBytes	Constante	Cliente	Jperf
BW	5-10-20-100 Mbps	Variable	CPE's	IOS
Flujo TCP	1 – 4 – 8	Variable	Cliente	Jperf

Fuente: (Elaborado por el Autor)

4.7.1 Resultados TX en IPVPN-MPLS con TCP.

Tabla 11.

Resultados TX en IPVPN-MPLS

MSS	BW	Flujos	TX1	TX2	TX3	Prom/Tx
(bytes)	(Mbps)	#	(Seg)	(Seg)	(Seg)	(Seg)
1460	5	1	39,1	39,2	39,3	39,2
1460	5	4	159,1	159,3	159,1	159,2
1460	5	8	319,8	319,7	319,7	319,7
1452	5	1	38,9	38,9	39	38,9
1452	5	4	159	159,1	159,3	159,1
1452	5	8	319,4	319,8	319,7	319,6
1000	5	1	39,6	39,7	39,5	39,6
1000	5	4	161,6	161,7	161,5	161,6
1000	5	8	324,2	324,4	324,2	324,3
500	5	1	41,7	41,6	41,5	41,6
500	5	4	169,2	168,9	169,3	169,1
500	5	8	339,1	339,4	339,2	339,2
1460	10	1	19,1	19,4	19,1	19,2
1460	10	4	79	79	78,9	79

Continua

1460	10	8	159	159	159,1	159
1452	10	1	19,4	19,1	19,1	19,2
1452	10	4	79,1	79,5	78,9	79,2
1452	10	8	159,4	159	159	159,1
1000	10	1	19,5	19,5	19,6	19,5
1000	10	4	80,3	80,3	80,2	80,3
1000	10	8	161,4	161,6	161,6	161,5
500	10	1	20,5	20,4	20,3	20,4
500	10	4	84,3	84,2	84,1	84,2
500	10	8	169,1	169,3	168,9	169,1
1460	20	1	9,2	9,2	9,2	9,2
1460	20	4	39	38,9	38,9	38,9
1460	20	8	79	78,9	79,1	79
1452	20	1	9,2	9,1	9,3	9,2
1452	20	4	39,1	38,9	39,1	39
1452	20	8	78,9	78,8	79	78,9
1000	20	1	9,2	9,2	9,2	9,2
1000	20	4	39,7	39,7	39,7	39,7
1000	20	8	80,3	80,3	80,5	80,4
500	20	1	9,6	9,9	9,8	9,8
500	20	4	41,6	41,4	41,5	41,5
500	20	8	83,9	83,9	84	83,9
1460	100	1	2,1	2,1	2,1	2,1
1460	100	4	8,3	8,3	8,3	8,3
1460	100	8	16,6	16,6	16,6	16,6
1452	100	1	2,1	2,1	2,1	2,1
1452	100	4	8,3	8,3	8,3	8,3
1452	100	8	16,6	16,6	16,5	16,6
1000	100	1	2,1	2,1	2,1	2,1
1000	100	4	8,5	8,5	8,5	8,5
1000	100	8	17	17	17,1	17
500	100	1	2,7	2,7	2,7	2,7
500	100	4	11,2	11,2	11,2	11,2
500	100	8	21,7	21,7	21,7	21,7

Fuente: (Elaborado por el Autor)

Los resultados de la tabla 11 se analizan posteriormente en dos tablas independientes tomando en cuenta los valores para un flujo simple y multi-flujo TCP y se evalúa la eficiencia del sistema en base al ancho de banda respecto al tiempo obtenido cuando el MSS máximo como referencia de punto de mejor desempeño.

4.7.2 Promedio General de TX en IPVPN-MPLS con TCP.

Tabla 12.

Promedio General de TX en IPVPN-MPLS con TCP.

MSS	BW	Flujos	Prom/Tx	Prom/Flujo	Prom/MSS	Eficiencia respecto MSS:MAX
(bytes)	**(Mbps)**	**#**	**(Seg)**	**(Seg)**	**(Seg)**	**(%)**
1460	5	1	39,2	39,2	39,7	99,75%
1460	5	4	159,2	39,8		
1460	5	8	319,7	40		
1452	5	1	38,9	38,9	39,6	100,00%
1452	5	4	159,1	39,8		
1452	5	8	319,6	40		
1000	5	1	39,6	39,6	40,2	98,51%
1000	5	4	161,6	40,4		
1000	5	8	324,3	40,5		
500	5	1	41,6	41,6	42,1	94,06%
500	5	4	169,1	42,3		
500	5	8	339,2	42,4		
1460	10	1	19,2	19,2	19,6	100%
1460	10	4	79	19,7		
1460	10	8	159	19,9		
1452	10	1	19,2	19,2	19,6	100%
1452	10	4	79,2	19,8		
1452	10	8	159,1	19,9		
1000	10	1	19,5	19,5	19,9	98%
1000	10	4	80,3	20,1		
1000	10	8	161,5	20,2		
500	10	1	20,4	20,4	20,9	94%

Continua

500	10	4	84,2	21,1		
500	10	8	169,1	21,1		
1460	20	1	9,2	9,2	9,6	100%
1460	20	4	38,9	9,7		
1460	20	8	79	9,9		
1452	20	1	9,2	9,2	9,6	100%
1452	20	4	39	9,8		
1452	20	8	78,9	9,9		
1000	20	1	9,2	9,2	9,7	99%
1000	20	4	39,7	9,9		
1000	20	8	80,4	10		
500	20	1	9,8	9,8	10,2	94%
500	20	4	41,5	10,4		
500	20	8	83,9	10,5		
1460	100	1	2,1	2,1	2,1	100%
1460	100	4	8,3	2,1		
1460	100	8	16,6	2,1		
1452	100	1	2,1	2,1	2,1	100%
1452	100	4	8,3	2,1		
1452	100	8	16,6	2,1		
1000	100	1	2,1	2,1	2,1	100%
1000	100	4	8,5	2,1		
1000	100	8	17	2,1		
500	100	1	2,7	2,7	2,7	78%
500	100	4	11,2	2,8		
500	100	8	21,7	2,7		

Fuente: (Elaborado por el Autor)

En la tabla 12 se puede observar que el promedio general de las tx por cada flujo TCP se mantiene directamente proporcional respecto al tamaño de segmento TCP y al ancho de banda del canal, se observa que existe linealidad en los resultados de eficiencia del desempeño con referencia al valor MSS máximo de cada BW; cuando se trata de paquetes de MSS de 500byte existe degradación de la eficiencia siendo más pronunciada o más baja cuando el BW se encuentra abierto a 100Mbps.

4.7.3 Tiempo Promedio con Tx Simple en IPVPN-MPLS con TCP.

Tabla 13.

Tiempo Promedio con Tx Simple en IPVPN-MPLS con TCP.

MSS	**BW**	**Flujos**	**Prom/MSS**	**Eficiencia resp MSS:MAX**
(bytes)	(Mbps)	#	(Seg)	(%)
1460	5	1	39,2	99,23%
1452	5	1	38,9	100,00%
1000	5	1	39,6	98,23%
500	5	1	41,6	93,51%
1460	10	1	19,2	100,00%
1452	10	1	19,2	100,00%
1000	10	1	19,5	98,46%
500	10	1	20,4	94,12%
1460	20	1	9,2	100,00%
1452	20	1	9,2	100,00%
1000	20	1	9,2	100,00%
500	20	1	9,8	93,88%
1460	100	1	2,1	100,00%
1452	100	1	2,1	100,00%
1000	100	1	2,1	100,00%
500	100	1	2,7	77,78%

Fuente: (Elaborado por el Autor)

En la tabla 13 se puede observar que el promedio general de las tx en flujo simple TCP se mantiene directamente proporcional respecto al tamaño de segmento TCP y al ancho de banda del canal, se observa que existe linealidad en los resultados de eficiencia del desempeño con referencia al valor MSS máximo de cada BW; cuando se trata de paquetes de MSS de 500byte existe degradación de la eficiencia siendo más pronunciada o más baja cuando el BW se encuentra abierto a 100Mbps.

4.7.4 Tiempo promedio multi-flujo en IPVPN-MPLS con TCP.

Tabla 14.

Tiempo promedio multi-flujo en IPVPN-MPLS con TCP.

MSS	BW	Flujos	Prom/Tx	Prom/Flujo	Prom/MSS	Eficiencia resp MSS:MAX
(bytes)	(Mbps)	#	(Seg)	(Seg)	(Seg)	(%)
1460	5	4	159,2	39,8	39,9	100,00%
1460	5	8	319,7	40		
1452	5	4	159,1	39,8	39,9	100,00%
1452	5	8	319,6	40		
1000	5	4	161,6	40,4	40,5	98,52%
1000	5	8	324,3	40,5		
500	5	4	169,1	42,3	42,3	94,33%
500	5	8	339,2	42,4		
1460	10	4	79	19,7	19,8	100,00%
1460	10	8	159	19,9		
1452	10	4	79,2	19,8	19,8	100,00%
1452	10	8	159,1	19,9		
1000	10	4	80,3	20,1	20,1	98,51%
1000	10	8	161,5	20,2		
500	10	4	84,2	21,1	21,1	93,84%
500	10	8	169,1	21,1		
1460	20	4	38,9	9,7	9,8	100,00%
1460	20	8	79	9,9		
1452	20	4	39	9,8	9,8	100,00%
1452	20	8	78,9	9,9		
1000	20	4	39,7	9,9	10	98,00%
1000	20	8	80,4	10		
500	20	4	41,5	10,4	10,4	94,23%
500	20	8	83,9	10,5		
1460	100	4	8,3	2,1	2,1	100,00%
1460	100	8	16,6	2,1		
1452	100	4	8,3	2,1	2,1	100,00%
1452	100	8	16,6	2,1		

Continua

1000	100	4	8,5	2,1	2,1	100,00%
1000	100	8	17	2,1		
500	100	4	11,2	2,8	2,8	75,00%
500	100	8	21,7	2,7		

Fuente: (Elaborado por el Autor)

En la tabla 14 se puede observar que el promedio general de las txen flujo multiple TCP se mantiene directamente proporcional respecto al tamaño de segmento TCP y al ancho de banda del canal, se observa que existe linealidad en los resultados de eficiencia del desempeño con referencia al valor MSS máximo de cada BW; cuando son paquetes de MSS de 500byte existe degradación de la eficiencia siendo más pronunciada o más baja cuando el BW se encuentra abierto a 100Mbps.

4.8 Pruebas de desempeño para TCP en sistema IPsec-Internet.

4.8.1 Parámetros para el sistema IPsec-Internet.

En la tabla 15 se detallan los parámetros y los valores correspondientes que son manejados durante una comunicación entre cliente-servidor para la evaluación de desempeño.

Tabla 15.

Parámetros para el sistema IPsec-Internet

Parámetro	Valor	Tipo	Elemento	Aplicación
MTU INT	1518 bytes	Constante	Todos	Nivel físico
IP MTU	1400bytes	Constante	PC´s	Stack IP/TCP
MSS:	1360 bytes	Constante	CPE's	Stack IP/TCP
Carga	24MBytes	Constante	Cliente	Jperf
BW	5-10-20-100 Mbps	Variable	CPE's	IOS
Flujo TCP	1 – 4 – 8	Variable	Cliente	Jperf

Fuente: (Elaborado por el Autor)

-

-

4.8.2 Resultados TX en IPsec-Internet con TCP.

Tabla 16.

Resultados TX en IPsec-Internet con TCP.

MSS (bytes)	BW (Mbps)	Flujos #	TX1 (Seg)	TX2 (Seg)	TX3 (Seg)	Prom Tx (Seg)
1460 (Default)	5	1	39,5	39,5	39,2	39,4
1460 (Default)	5	4	161	160,7	160,6	160,8
1460 (Default)	5	8	322,5	322,9	322,7	322,7
1360 (Máx)	5	1	38,5	38,7	38,8	38,7
1360 (Máx)	5	4	158	157,7	158	157,9
1360 (Máx)	5	8	316,6	316,4	316,6	316,5
1000	5	1	39,1	39,1	39,2	39,1
1000	5	4	159,1	158,9	159,1	159
1000	5	8	319	319	319	319
500	5	1	40,3	40,5	40,3	40,4
500	5	4	163,7	163,8	163,7	163,7
500	5	8	328,6	328,3	328,5	328,5
1460 (Default)	10	1	19,6	19,3	19	19,3
1460 (Default)	10	4	79,4	79,5	79,2	79,4
1460 (Default)	10	8	159	158,6	158,7	158,8
1360 (Máx)	10	1	18,8	18,8	19	18,9
1360 (Máx)	10	4	78,2	78,1	78,3	78,2
1360 (Máx)	10	8	157,1	157,3	157,3	157,2
1000	10	1	19,3	19,7	19,5	19,5
1000	10	4	79,1	78,7	78,8	78,9
1000	10	8	158,9	158,8	158,7	158,8
500	10	1	22,7	25,4	22,7	23,6
500	10	4	81,5	81,8	81,9	81,7
500	10	8	164,9	164,2	164,2	164,4
1460 (Default)	20	1	14,6	13,2	13,5	13,8
1460 (Default)	20	4	39,3	39,3	39,4	39,3
1460 (Default)	20	8	78,9	78,9	79	78,9
1360 (Máx)	20	1	13	13,6	12,1	12,9
1360 (Máx)	20	4	39	39,3	38,9	39,1
1360 (Máx)	20	8	78,8	78,3	78,3	78,5

Continua

1000	20	1	13,5	13,1	13,4	13,3
1000	20	4	40,2	39,6	39,5	39,8
1000	20	8	79	79,1	79,1	79,1
500	20	1	25,4	23,9	26,5	25,3
500	20	4	45,5	46,6	46,5	46,2
500	20	8	97,1	95	95,5	95,9
1460 (Default)	100	1	9,5	8,2	9,5	9,1
1460 (Default)	100	4	20,6	20,1	21,1	20,6
1460 (Default)	100	8	44,5	45,3	44,1	44,6
1360 (Máx)	100	1	9,1	10	9,2	9,4
1360 (Máx)	100	4	17,8	17,4	17,4	17,5
1360 (Máx)	100	8	35,5	36,4	38,2	36,7
1000	100	1	11	10,6	11,8	11,1
1000	100	4	21,2	22,7	22	22
1000	100	8	48	48,4	46	47,5
500	100	1	18,4	18,7	18,4	18,5
500	100	4	37,7	38,7	40,6	39
500	100	8	82	83,4	82,9	82,8

Fuente: (Elaborado por el Autor)

-

Los resultados de la tabla 16 se analizan posteriormente en dos tablas independientes tomando en cuenta los valores para un flujo simple y multi-flujo TCP y se evalúa la eficiencia del sistema en base al ancho de banda respecto al tiempo obtenido cuando el MSS máximo como referencia de punto de mejor desempeño

-

4.8.3 Promedio General de TX en IPsec-Internet con TCP.

Tabla 17.

Promedio General de TX en IPsec-Internet con TCP.

MSS	**BW**	**Flujos**	**Prom Tx**	**Prom/Flujo**	**Prom/MSS**	**Eficiencia MSS:MAX respecto**
(bytes)	(Mbps)	#	(Seg)	(Seg)	(Seg)	(%)
1460	5	1	39,4	39,4	39,98	98,2%
1460	5	4	160,8	40,19		

Continua

1460	5	8	322,7	40,34		
1360	5	1	38,7	38,67	39,24	100,0%
1360	5	4	157,9	39,48		
1360	5	8	316,5	39,57		
1000	5	1	39,1	39,13	39,59	99,1%
1000	5	4	159	39,76		
1000	5	8	319	39,88		
500	5	1	40,4	40,37	40,79	96,2%
500	5	4	163,7	40,93		
500	5	8	328,5	41,06		
1460	10	1	19,3	19,3	19,66	98,4%
1460	10	4	79,4	19,84		
1460	10	8	158,8	19,85		
1360	10	1	18,9	18,87	19,36	100,0%
1360	10	4	78,2	19,55		
1360	10	8	157,2	19,65		
1000	10	1	19,5	19,5	19,69	98,3%
1000	10	4	78,9	19,72		
1000	10	8	158,8	19,85		
500	10	1	23,6	23,6	21,53	89,9%
500	10	4	81,7	20,43		
500	10	8	164,4	20,55		
1460	20	1	13,8	13,77	11,16	97,0%
1460	20	4	39,3	9,83		
1460	20	8	78,9	9,87		
1360	20	1	12,9	12,9	10,83	100,0%
1360	20	4	39,1	9,77		
1360	20	8	78,5	9,81		
1000	20	1	13,3	13,33	11,05	98,0%
1000	20	4	39,8	9,94		
1000	20	8	79,1	9,88		
500	20	1	25,3	25,27	16,27	66,6%
500	20	4	46,2	11,55		
500	20	8	95,9	11,98		
1460	100	1	9,1	9,07	6,60	92,9%
1460	100	4	20,6	5,15		
1460	100	8	44,6	5,58		

Continua

1360	100	1	9,4	9,43	6,13	100,0%
1360	100	4	17,5	4,38		
1360	100	8	36,7	4,59		
1000	100	1	11,1	11,13	7,52	81,6%
1000	100	4	22	5,49		
1000	100	8	47,5	5,93		
500	100	1	18,5	18,5	12,87	47,7%
500	100	4	39	9,75		
500	100	8	82,8	10,35		

Fuente: (Elaborado por el Autor)

En la tabla 17 se puede observar que el promedio general de las tx se mantiene directamente proporcional respecto al tamaño de segmento TCP y al ancho de banda del canal hasta 20Mbps, se observa que existe linealidad en los resultados de eficiencia con respecto al valor de MSS máximo de cada BW cuando el tamaño de segmento TCP es mayor o igual a 1000 bytes; cuando el sistema fragmenta los paquetes en MSS default o 1460bytes existe un 2% de degradación del performance; sin embargo se pierde la linealidad y estabilidad con MSS de 500 bytes en todos los anchos de banda evaluados con una gran caída o degradación de la eficiencia cuando el BW se encuentra abierto a 100Mbps lo cual coincide con la recomendación de que el C881 soporta hasta 20Mbps con IPsec.

4.8.4 Tiempo Promedio con Tx Simple en IPsec-Internet con TCP.

Tabla 18.

Tiempo Promedio con Tx Simple en IPsec-Internet con TCP.

MSS	**BW**	**Flujos**	**Prom/MSS**	**Eficiencia Respecto MSS:MAX**
(bytes)	**(Mbps)**	**#**	**(Seg)**	**(%)**
1460	5	1	39,4	98,22%
1360	5	1	38,7	100,00%
1000	5	1	39,1	98,98%
500	5	1	40,4	95,79%

Continua

1460	10	1	19,3	97,93%
1360	10	1	18,9	100,00%
1000	10	1	19,5	96,92%
500	10	1	23,6	80,08%
1460	20	1	13,8	93,48%
1360	20	1	12,9	100,00%
1000	20	1	13,3	96,99%
500	20	1	25,3	50,99%
1460	100	1	9,1	103,30%
1356	100	1	9,4	100,00%
1000	100	1	11,1	84,68%
500	100	1	18,5	50,81%

Fuente: (Elaborado por el Autor)

En la tabla 18 se puede observar que el promedio general de las tx en el sistema IPsec-internet para flujo simple se mantiene directamente proporcional respecto al tamaño de segmento TCP y al BW del canal hasta 20Mbps, se observa que existe linealidad en los resultados de eficiencia con respecto al valor de MSS máximo de cada BW cuando el tamaño de segmento TCP es mayor o igual a 1000 bytes; cuando el sistema fragmenta los paquetes en MSS default o 1460bytes existe hasta un 7% de degradación del performance, sin embargo se pierde la linealidad y estabilidad con MSS de 500 bytes en todos los anchos de banda evaluados con una gran caída o degradación de la eficiencia cuando el BW se encuentra abierto a 100Mbps lo cual coincide con la recomendación de que el C881 soporta hasta 20Mbps con IPsec.

4.8.5 Tiempo promedio multi-flujo en IPsec-Internet con TCP.

Tabla 19.

Tiempo promedio multi-flujo en IPsec-Internet con TCP

MSS	BW	Flujos	Prom/Flujo	Prom/MSS	Eficiencia respecto MSS:MAX
(bytes)	**(Mbps)**	**#**	**(Seg)**	**(Seg)**	**(%)**
1460	5	4	40,19	40,27	98,16%

Continua

1460	5	8	40,34		
1360	5	4	39,48	39,53	100,00%
1360	5	8	39,57		
1000	5	4	39,76	39,82	99,26%
1000	5	8	39,88		
500	5	4	40,93	41,00	96,41%
500	5	8	41,06		
1460	10	4	19,84	19,85	98,77%
1460	10	8	19,85		
1360	10	4	19,55	19,60	100,00%
1360	10	8	19,65		
1000	10	4	19,72	19,79	99,06%
1000	10	8	19,85		
500	10	4	20,43	20,49	95,66%
500	10	8	20,55		
1460	20	4	9,83	9,85	99,39%
1460	20	8	9,87		
1360	20	4	9,77	9,79	100,00%
1360	20	8	9,81		
1000	20	4	9,94	9,91	98,79%
1000	20	8	9,88		
500	20	4	11,55	11,77	83,21%
500	20	8	11,98		
1460	100	4	5,15	5,37	83,60%
1460	100	8	5,58		
1360	100	4	4,38	4,49	100,00%
1360	100	8	4,59		
1000	100	4	5,49	5,71	78,55%
1000	100	8	5,93		
500	100	4	9,75	10,05	44,63%
500	100	8	10,35		

Fuente: (Elaborado por el Autor)

En la tabla 19 se puede observar que el promedio general de las tx en el sistema IPsec-internet para flujo múltiple se mantiene directamente proporcional respecto al tamaño de segmento TCP y al bw del canal hasta 20Mbps, se observa que existe

linealidad en los resultados de eficiencia con respecto al valor de MSS máximo de cada BW cuando el tamaño de segmento TCP es mayor o igual a 1000 bytes; cuando el sistema fragmenta los paquetes en MSS default o 1460bytes existe hasta un 2% de degradación del performance, sin embargo se pierde la linealidad y estabilidad con MSS de 500 bytes en todos los bw evaluados con una gran caída o degradación de la eficiencia cuando el BW se encuentra abierto a 100Mbps lo cual coincide con la recomendación de que el C881 soporta hasta 20Mbps con IPsec.

4.9 Pruebas de desempeño para TCP en sistema DMVPN-MPLS.

4.9.1 Parámetros para el sistema DMVPN-MPLS

En la tabla 20 se detallan los parámetros y los valores que son manejados durante una comunicación entre cliente-servidor para la evaluación de desempeño.

Tabla 20.

Parámetros para el sistema DMVPN-MPLS

Parámetro	Valor	Tipo	Elemento	Aplicación
IP MTU INT	1518 bytes	Constante	Todos	Nivel físico
IP MTU	1384 bytes	Constante	PC´s	Stack IP/TCP
MSS:	1344 bytes	Constante	CPE's	Stack IP/TCP
Carga	24MBytes	Constante	Cliente	Jperf
BW	5-10-20-100Mbps	Variable	CPE's	IOS
Flujo TCP	1 – 4 – 8	Variable	Cliente	Jperf

Fuente: (Elaborado por el Autor)

4.9.2 Resultados TX en DMVPN-MPLS con TCP.

Tabla 21.

Resultados TX en DMVPN-MPLS con TCP.

MSS (bytes)	BW (Mbps)	Flujo #	TX1 (Seg)	TX2 (Seg)	TX3 (Seg)	Prom Tx (Seg)
1460 (Default)	5	1	43,4	43,2	43,4	43,3
1460 (Default)	5	4	177,3	177,4	177,1	177,3

Continua

1460 (Default)	5	8	356,4	356,3	356,2	356,3
1344 (Máx)	5	1	41,9	42,1	42	42
1344 (Máx)	5	4	170,9	170,7	170,9	170,8
1344 (Máx)	5	8	343,2	343,2	343	343,1
1000	5	1	43,6	43,4	43,8	43,6
1000	5	4	177,2	177,2	177,3	177,2
1000	5	8	355,5	355,7	355,6	355,6
500	5	1	48,8	49	48,8	48,9
500	5	4	198	197,9	198	198
500	5	8	408	401,8	396,9	402,2
1460 (Default)	10	1	21,1	21	21,1	21,1
1460 (Default)	10	4	86,6	86,6	86,7	86,6
1460 (Default)	10	8	175	174,9	175	175
1344 (Máx)	10	1	20,7	20,5	20,6	20,6
1344 (Máx)	10	4	85,2	85,1	84,7	85
1344 (Máx)	10	8	170,6	170,8	170,8	170,7
1000	10	1	21,6	21,5	21,4	21,5
1000	10	4	87,8	88,1	87,8	87,9
1000	10	8	176,6	177	176,8	176,8
500	10	1	24,3	24,2	24,5	24,3
500	10	4	98,4	98,5	98,9	98,6
500	10	8	198,2	197,6	198,1	198
1460 (Default)	20	1	18,5	18,6	18,4	18,5
1460 (Default)	20	4	68,3	68,2	68,8	68,4
1460 (Default)	20	8	136,9	137,1	137,3	137,1
1344 (Máx)	20	1	10	10	10,5	10,2
1344 (Máx)	20	4	42,3	42,1	42,3	42,2
1344 (Máx)	20	8	84,7	85,1	85,1	85
1000	20	1	10,9	11,8	11,5	11,4
1000	20	4	43,7	43,7	44,2	43,9
1000	20	8	87,9	88,4	88,1	88,1
500	20	1	21,6	23,7	21,9	22,4
500	20	4	49,7	49,3	49,6	49,5
500	20	8	99,1	99,8	99,2	99,4
1460 (Default)	100	1	18,5	16,4	17,8	17,6
1460 (Default)	100	4	56,2	56,3	56	56,2
1460 (Default)	100	8	111,2	111,7	111,2	111,4

Continua 

1344 (Máx)	100	1	8,2	7,5	9,5	8,4
1344 (Máx)	100	4	17,6	17,6	17,9	17,7
1344 (Máx)	100	8	35,5	36,6	37,8	36,6
1000	100	1	9,9	11,2	11,4	10,8
1000	100	4	22,7	22,2	22,2	22,4
1000	100	8	47	46,4	47,2	46,9
500	100	1	19,6	18	18,4	18,7
500	100	4	39,8	39,3	38,5	39,2
500	100	8	82,8	81,5	82,8	82,4

Fuente: (Elaborado por el Autor)

Los resultados de la tabla 21 se analizan posteriormente en dos tablas independientes tomando en cuenta los valores para un flujo simple y multi-flujo TCP y se evalúa la eficiencia del sistema en base al ancho de banda respecto al tiempo obtenido cuando el MSS máximo como referencia de punto de mejor desempeño

4.9.3 Promedio General de TX en DMVPN-MPLS con TCP.

Tabla 22.

Promedio General de TX en DMVPN-MPLS con TCP

MSS	**BW**	**Flujos**	**Prom Tx**	**Prom/Flujo**	**Prom/MSS**	**Efi Resp MSS:MAX**
(bytes)	(Mbps)	#	(Seg)	(Seg)	(Seg)	(%)
1460	5	1	43,3	43,33	44,06	96,53%
1460	5	4	177,3	44,32		
1460	5	8	356,3	44,54		
1344	5	1	42	42	42,53	100,00%
1344	5	4	170,8	42,71		
1344	5	8	343,1	42,89		
1000	5	1	43,6	43,6	44,12	96,40%
1000	5	4	177,2	44,31		
1000	5	8	355,6	44,45		
500	5	1	48,9	48,87	49,55	85,83%
500	5	4	198	49,49		
500	5	8	402,2	50,28		

Continua

1460	10	1	21,1	21,07	21,53	97,82%
1460	10	4	86,6	21,66		
1460	10	8	175	21,87		
1344	10	1	20,6	20,6	21,06	100,00%
1344	10	4	85	21,25		
1344	10	8	170,7	21,34		
1000	10	1	21,5	21,5	21,86	96,34%
1000	10	4	87,9	21,98		
1000	10	8	176,8	22,1		
500	10	1	24,3	24,33	24,58	85,68%
500	10	4	98,6	24,65		
500	10	8	198	24,75		
1460	20	1	18,5	18,5	17,58	59%
1460	20	4	68,4	17,11		
1460	20	8	137,1	17,14		
1344	20	1	10,2	10,17	10,45	100%
1344	20	4	42,2	10,56		
1344	20	8	85	10,62		
1000	20	1	11,4	11,4	11,13	94%
1000	20	4	43,9	10,97		
1000	20	8	88,1	11,02		
500	20	1	22,4	22,4	15,73	66%
500	20	4	49,5	12,38		
500	20	8	99,4	12,42		
1460	100	1	17,6	17,57	15,18	38%
1460	100	4	56,2	14,04		
1460	100	8	111,4	13,92		
1344	100	1	8,4	8,4	5,8	100%
1344	100	4	17,7	4,43		
1344	100	8	36,6	4,58		
1000	100	1	10,8	10,83	7,43	78%
1000	100	4	22,4	5,59		
1000	100	8	46,9	5,86		
500	100	1	18,7	18,67	12,92	45%
500	100	4	39,2	9,8		
500	100	8	82,4	10,3		

Fuente: (Elaborado por el Autor)

En la tabla 22 se puede observar que el promedio general de las transmisiones se mantiene directamente proporcional respecto al tamaño de segmento TCP y al ancho de banda del canal hasta 10Mbps, se observa que existe linealidad en los resultados de eficiencia con respecto al valor de MSS máximo de cada BW cuando el tamaño de segmento TCP es mayor o igual a 1000 bytes; cuando el sistema fragmenta los paquetes en MSS default o 1460bytes existe un 4% de degradación del performance; sin embargo se pierde la linealidad a partir de los 10Mbps y estabilidad con MSS de 500 bytes en todos los BW evaluados con una gran caída o degradación de la eficiencia cuando el BW se encuentra abierto a 100Mbps.

4.9.4 Tiempo Promedio con Tx Simple en DMVPN-MPLS con TCP.

Tabla 23.

Tiempo Promedio con Tx Simple en DMVPN-MPLS con TCP.

MSS	BW	Flujos	Prom/MSS	Efi resp MSS:MAX
(bytes)	**(Mbps)**	**#**	**(Seg)**	**(%)**
1460	5	1	43,3	97,00%
1344	5	1	42	100,00%
1000	5	1	43,6	96,33%
500	5	1	48,9	85,89%
1460	10	1	21,1	97,63%
1344	10	1	20,6	100,00%
1000	10	1	21,5	95,81%
500	10	1	24,3	84,77%
1460	20	1	18,5	55,14%
1344	20	1	10,2	100,00%
1000	20	1	11,4	89,47%
500	20	1	22,4	45,54%
1460	100	1	17,6	47,73%
1344	100	1	8,4	100,00%
1000	100	1	10,8	77,78%
500	100	1	18,7	44,92%

Fuente: (Elaborado por el Autor)

En la tabla se puede observar que el promedio general de las tx con flujo simple se mantiene directamente proporcional respecto al tamaño de segmento TCP y al ancho de banda del canal hasta 10Mbps.

4.9.5 Tiempo promedio con TX multiple en DMVPN-MPLS con TCP.

Tabla 24.

Tiempo promedio con TX multiple en DMVPN-MPLS con TCP.

MSS	BW	Flujos	Prom/Flujo	Prom/MSS	Efic resp MSS:MAX
(bytes)	**(Mbps)**	**#**	**(Seg)**	**(Seg)**	**(%)**
1460	5	4	44,3	44,4	96,40%
1460	5	8	44,5		
1344	5	4	42,7	42,8	100,00%
1344	5	8	42,9		
1000	5	4	44,3	44,4	96,40%
1000	5	8	44,5		
500	5	4	49,5	49,9	85,77%
500	5	8	50,3		
1460	10	4	21,7	21,8	97,71%
1460	10	8	21,9		
1344	10	4	21,3	21,3	100,00%
1344	10	8	21,3		
1000	10	4	22	22	96,82%
1000	10	8	22,1		
500	10	4	24,7	24,7	86,23%
500	10	8	24,7		
1460	20	4	17,1	17,1	61,99%
1460	20	8	17,1		
1344	20	4	10,6	10,6	100,00%
1344	20	8	10,6		
1000	20	4	11	11	96,36%
1000	20	8	11		
500	20	4	12,4	12,4	85,48%
500	20	8	12,4		
1460	100	4	14	14	32,14%

Continua

1460	100	8	13,9		
1344	100	4	4,4	4,5	100,00%
1344	100	8	4,6		
1000	100	4	5,6	5,7	78,95%
1000	100	8	5,9		
500	100	4	9,8	10	45,00%
500	100	8	10,3		

Fuente: (Elaborado por el Autor)

En la tabla 24 se puede observar que el promedio general de las transmisiones con flujo multiple se mantiene directamente proporcional respecto al tamaño de segmento TCP y al ancho de banda del canal hasta 10Mbps.

4.10Promedio por Flujo Simple en los Sistemas.

Tabla 25.

Promedio por Flujo Simple en los Sistemas.

MSS (bytes)	BW (Mbps)	IPVPN-MPLS (Seg)	DMVPN-MPLS (Seg)	IPsec-Internet (Seg)
1460	5	39,2	43,3	39,4
1344	5	38,93	42	38,67
1000	5	39,6	43,6	39,13
500	5	41,6	48,9	40,37
1460	10	19,2	21,1	19,3
1344	10	19,2	20,6	18,87
1000	10	19,53	21,5	19,5
500	10	20,4	24,3	23,6
1460	20	9,2	18,5	13,77
1344	20	9,2	10,2	12,9
1000	20	9,2	11,4	13,33
500	20	9,77	22,4	25,27
1460	100	2,1	17,6	9,07
1344	100	2,1	8,4	9,43
1000	100	2,1	10,8	11,13
500	100	2,7	18,7	18,5

Fuente: (Elaborado por el Autor)

En la tabla 25 se puede observar que los sistemas IPVPN-MPLS e IPsec-Internet dentro de la zona lineal hasta 10Mbps con MSS >=1000 bytes mantienen un performance similar, a diferencia del sistema DMVPN-VPN que tiene un menor performance. IPVPN-MPLS mantiene su linealidad en todos los anchos de banda a diferencia de los sistemas encriptados en donde a partir de los 20Mbps se vuelven inestables. Los sistemas encriptados tienden a degradar su desempeño cuando manejan paquetes pequeños en tamaño en todos los anchos de banda.

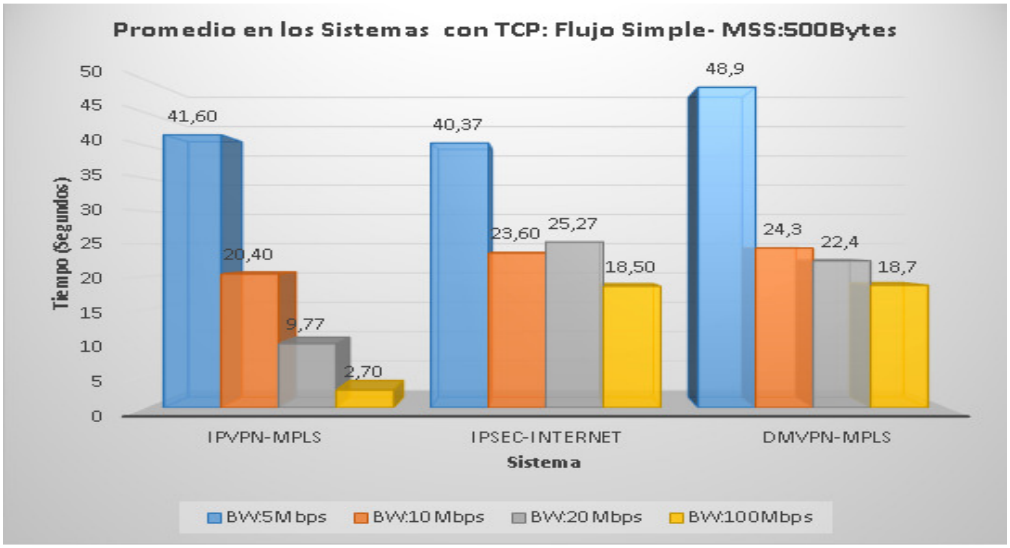

Figura 33: Promedio en los Sistemas con TCP: Flujo Simple - MSS:500bytes.
Fuente: (Elaborado por el Autor)

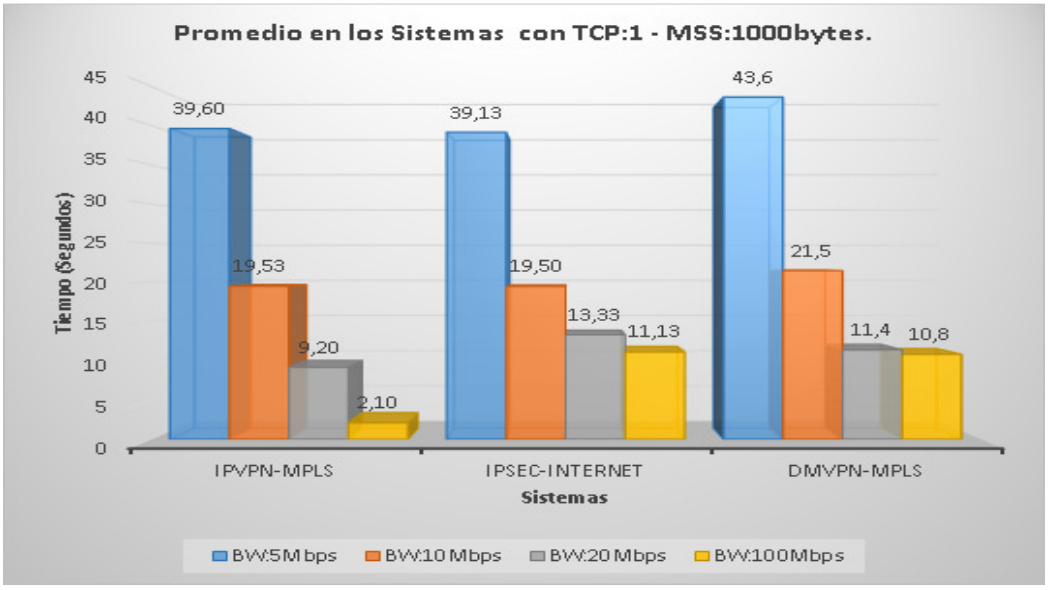

Figura 34: Promedio en los Sistemas con TCP: Flujo Simple - MSS:1000bytes

Fuente: (Elaborado por el Autor)

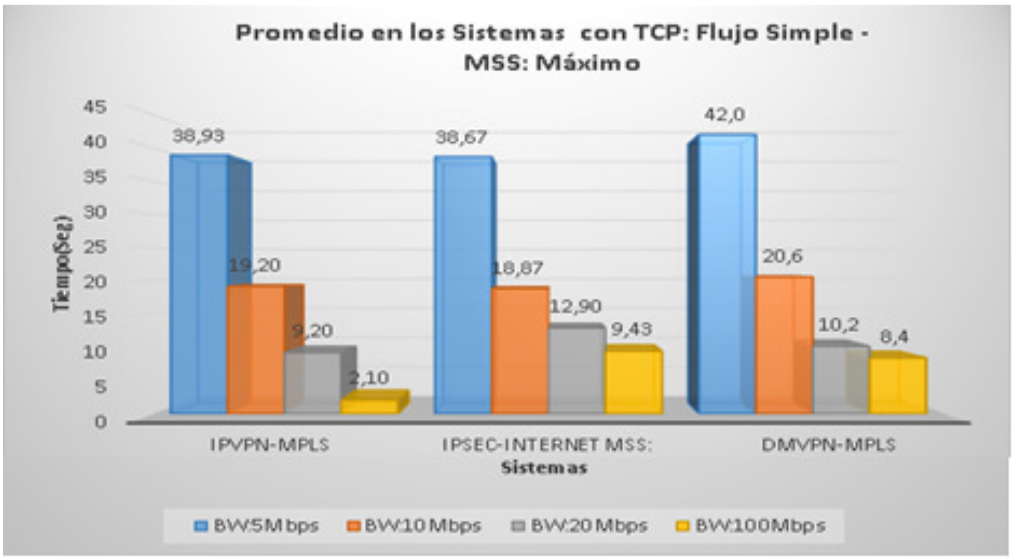

Figura 35: Promedio en los Sistemas con TCP: Flujo Simple - MSS:Máximo

Fuente: (Elaborado por el Autor)

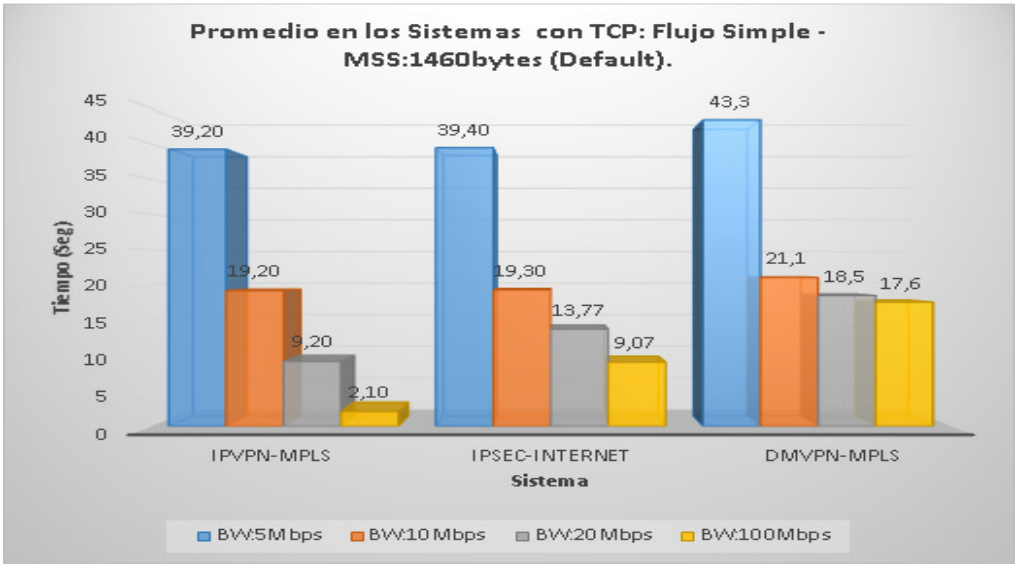

Figura 36: Promedio en los Sistemas con TCP: Flujo simple MSS:(default).

Fuente: (Elaborado por el Autor)

4.11Promedio por Flujo Múltiple TCP en los Sistemas.

Tabla 26.

Promedio por Flujo Múltiple TCP en los Sistemas.

MSS (bytes)	BW (Mbps)	IPVPN-MPLS (Seg)	DMVPN-MPLS (Seg)	IPSec-Internet (Seg)
1460	5	39,9	44,4	40,26
Max	5	39,9	42,8	39,52
1000	5	40,5	44,4	39,82
500	5	42,3	49,9	41
1460	10	19,8	21,8	19,84
Max	10	19,8	21,3	19,6
1000	10	20,1	22	19,78
500	10	21,1	24,7	20,49
1460	20	9,8	17,1	9,85
Max	20	9,8	10,6	9,79
1000	20	10	11	9,91
500	20	10,4	12,4	11,77
1460	100	2,1	14	5,36
Max	100	2,1	4,5	4,49

Continua

1000	100	2,1	5,7	5,71
500	100	2,8	10	10,05

Fuente: (Elaborado por el Autor)

En la tabla 26 se puede observar que los sistemas IPVPN-MPLS e IPsec-Internet dentro de la zona lineal hasta los 20Mbps con MSS >=1000 bytes mantienen un performance similar, a diferencia del sistema DMVPN-VPN que tiene un menor performance. IPVPN-MPLS mantiene su linealidad en todos los anchos de banda a diferencia de DMVPN-MPLS que partir de los 10Mbps se vuelve inestables e IPsec-Internet a partir de 20Mbps.

Los sistemas encriptados tienden a degradar su desempeño cuando manejan paquetes pequeños en tamaño en todos los anchos de banda.

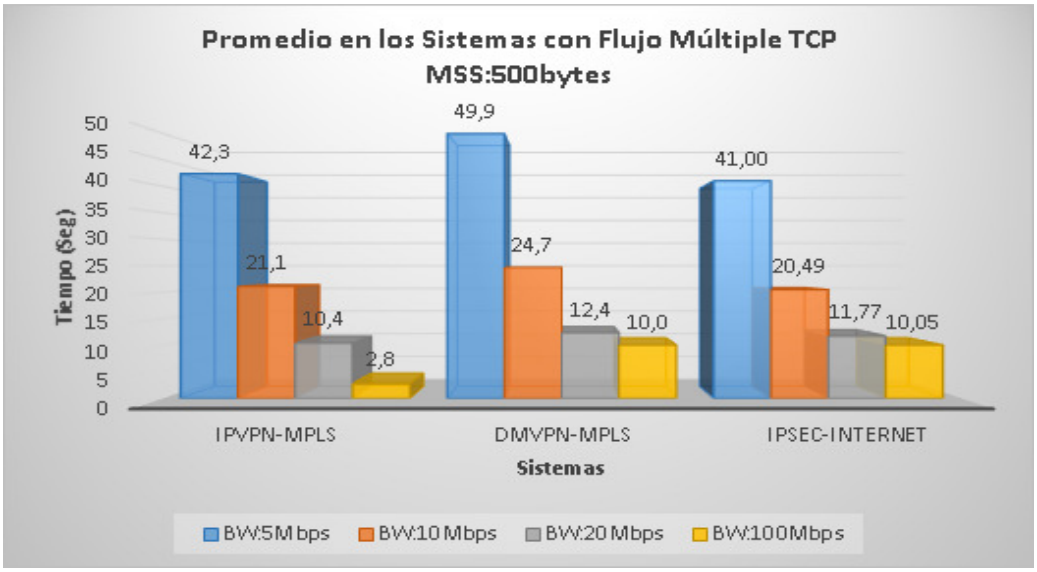

Figura 37: Promedio en los Sistemas con Flujo Múltiple TCP – MSS:500byte.
Fuente: (Elaborado por el Autor)

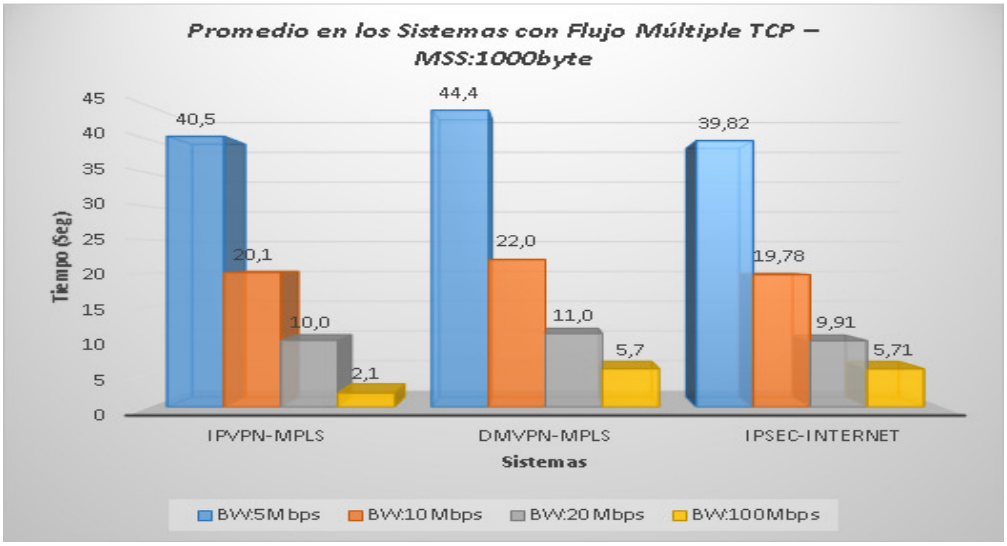

Figura 38: Promedio en los Sistemas con Flujo Múltiple TCP – MSS:1000byte.

Fuente: (Elaborado por el Autor)

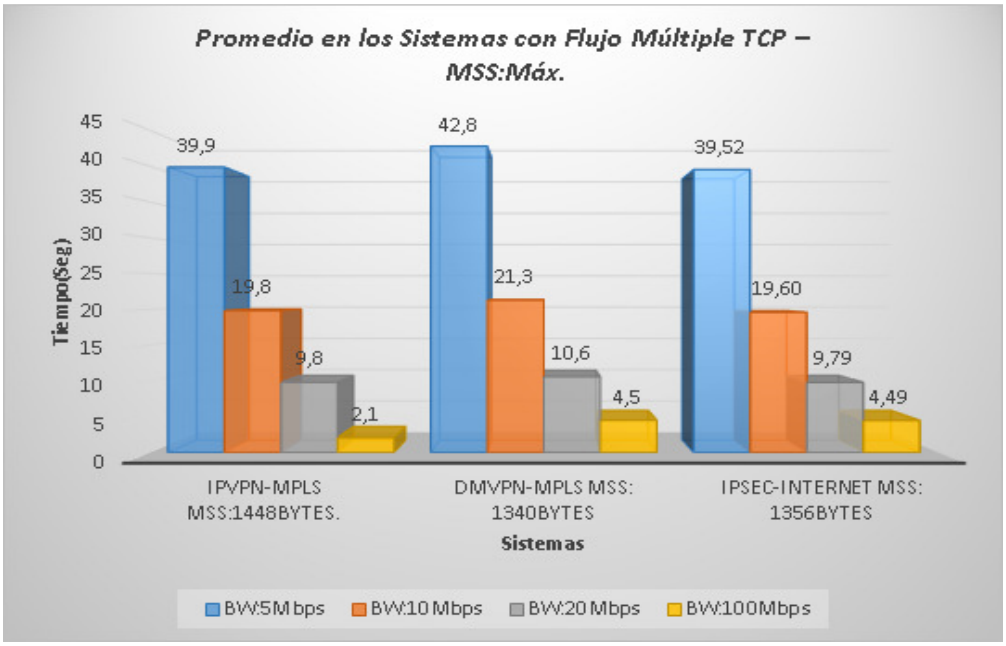

Figura 39: Promedio en los Sistemas con Flujo Múltiple TCP – MSS:Máx.

Fuente: (Elaborado por el Autor)

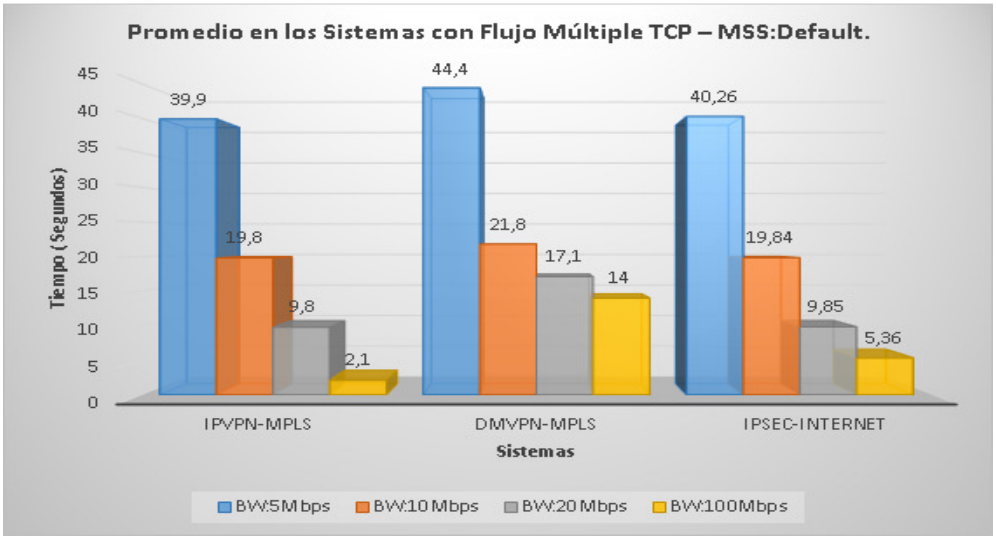

Figura 40: Promedio en los Sistemas con Flujo Múltiple TCP – MSS:Default.

Fuente: (Elaborado por el Autor)

4.12Eficiencia con flujo TCP Simple en los Sistemas

Tabla 27.

Eficiencia con flujo TCP simple en los Sistemas.

MSS (Bytes)	BW (Mbps)	IPVPN-MPLS (%)	DMVPN-MPLS (%)	IPSec-Internet (%)
DEFAULT	5	100%	85%	103%
MAX	5	100%	91%	101%
1000	5	100%	93%	101%
500	5	100%	90%	99%
DEFAULT	10	100%	84%	86%
MAX	10	100%	91%	100%
1000	10	100%	93%	102%
500	10	100%	91%	99%
DEFAULT	20	100%	44%	39%
MAX	20	100%	81%	69%
1000	20	100%	90%	71%
500	20	100%	50%	67%
DEFAULT	100	100%	14%	15%
MAX	100	100%	19%	19%

Continua

1000	100	100%	25%	22%
500	100	100%	12%	23%

Fuente: (Elaborado por el Autor)

Para flujo TCP simple como se puede observar en la tabla 27 la eficiencia de los sistemas IPVPN-MPLS e IPsec-Internet hasta los 10Mbps y con segmentos MSS>=1000 bytes son casi iguales, incluso IPsec-Internet presenta un valor infimo mayor y esto se debe a que el delay ingresado por la encriptación en los CPE's es compensando con la rapidez del switcheo de los paquetes en los PE y P pues sus tablas de ruteo son mínimas en un ambiente de laboratorio, dentro de la linealidad IPsec-Internet tuvo mejor desempeño frente a DMVPN-MPLS y a partir de los 20Mbps los sistemas se vuelven inestables debido al troughput de encriptación que manejan los equipos CPE.

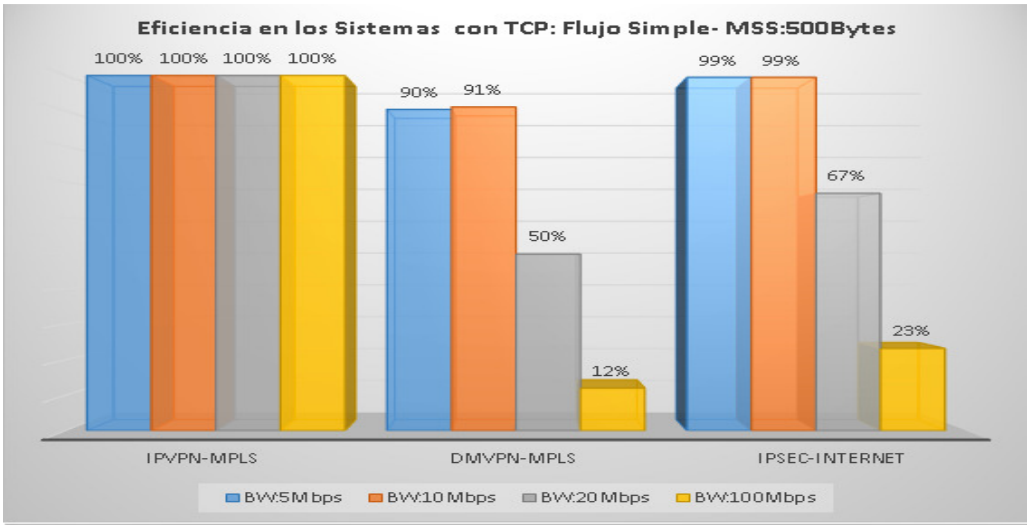

Figura 41: Eficiencia en los Sistemas con TCP: Flujo Simple- MSS:500Bytes.
Fuente: (Elaborado por el Autor)

Para flujo simple el manejo de paquetes de segmento MSS=500bytes en sistemas encriptados es más eficiente en el sistema IPsec-Internet frente al sistema DMVPN-MPLS. El sistema IPVPN-MPLS tiene el mejor performance para todos los anchos de banda respecto a los otros dos sistemas encriptados.

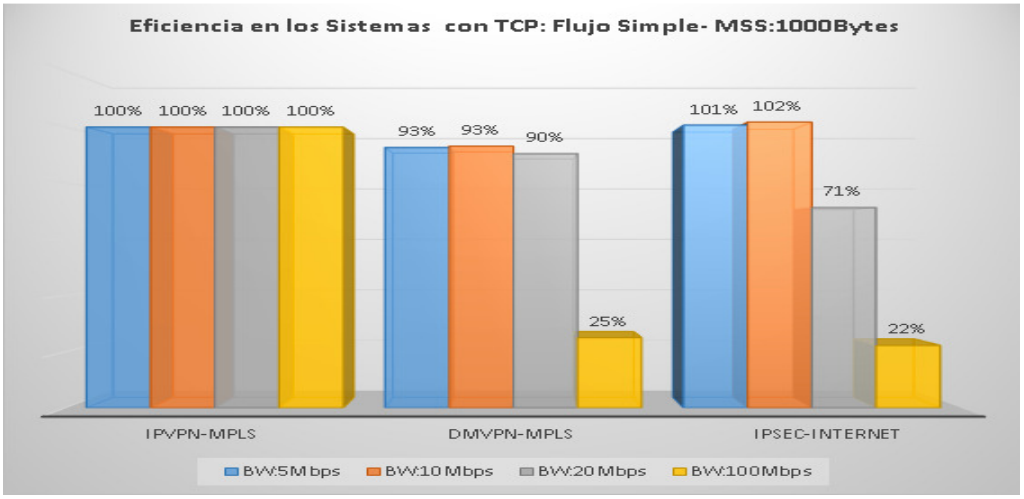

Figura 42: Eficiencia en los Sistemas con TCP: Flujo Simple- MSS:1000Bytes.

Fuente: (Elaborado por el Autor)

Para flujo simple el manejo de paquetes de segmento MSS=1000bytes en sistemas encriptados es más eficiente en el sistema IPsec-Internet frente al sistema DMVPN-MPLS. El sistema IPVPN-MPLS tiene el mejor performance para todos los anchos de banda respecto a los otros dos sistemas encriptados.

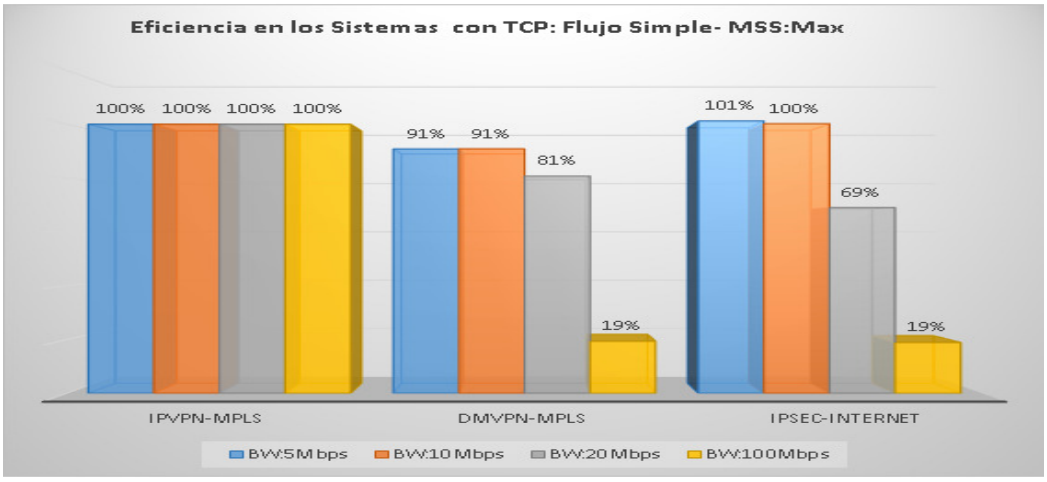

Figura 43: Eficiencia en los Sistemas con TCP: Flujo Simple- MSS: Máx.

Fuente: (Elaborado por el Autor)

Para flujo simple el manejo de paquetes de segmento con tamaño de segmento máximo para que no exista la fragmentación del mismo en sistemas encriptados es más eficiente en el sistema IPsec-Internet frente al sistema DMVPN-MPLS. El sistema IPVPN-MPLS tiene el mejor performance para todos los anchos de banda respecto a los otros dos sistemas encriptados.

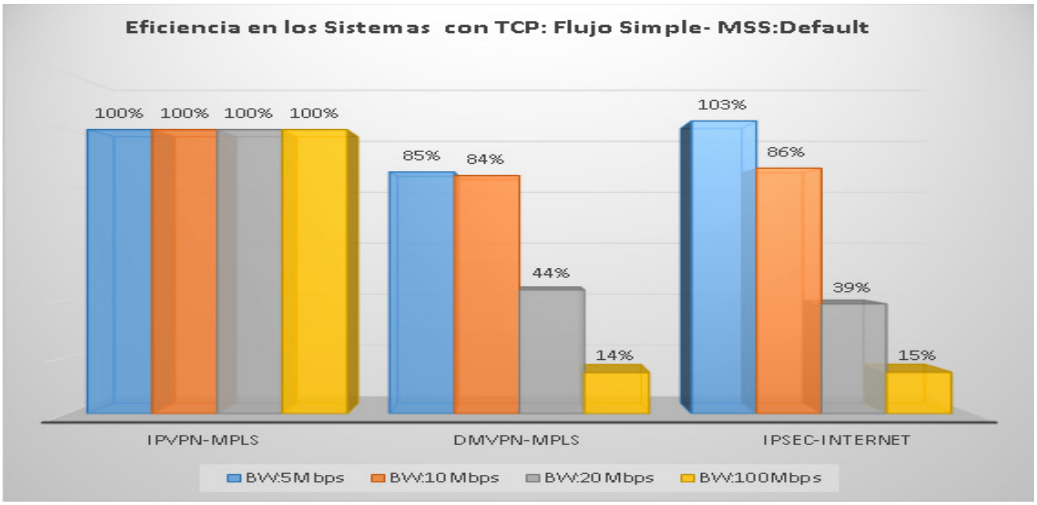

Figura 44: Eficiencia en los Sistemas con TCP: Flujo Simple- MSS:Default.
Fuente: (Elaborado por el Autor)

Para flujo simple el manejo de paquetes de segmento por default en los sistemas encriptados frente al no encriptado tiene igual performance solamente cuando se manejó un BW de 5Mbps entre IPVPN-MPLS e IPsec-Internet, la fragmentación de los paquetes ocasiona que el desempeño de los sistemas encriptados frente a los no encriptados dentro de la zona de linealidad tenga un 15% menor frente a IPVPN-MPLS; a partir de los 20Mbps los sistemas encriptados se vuelven inestables para este escenario de laboratorio.

4.13Eficiencia en los Sistemas con Flujo Múltiple TCP.

Tabla 28.

Eficiencia en los Sistemas con Flujo Múltiple TCP.

MSS (Bytes)	BW (Mbps)	IPVPN-MPLS (%)	DMVPN-MPLS (%)	IPSec-Internet (%)
DEFAULT	5	100%	68%	83%
MAX	5	100%	73%	81%
1000	5	100%	74%	81%
500	5	100%	90%	99%
DEFAULT	10	100%	85%	103%
MAX	10	100%	91%	102%
1000	10	100%	93%	101%
500	10	100%	91%	100%
DEFAULT	20	100%	67%	70%
MAX	20	100%	73%	81%
1000	20	100%	74%	80%
500	20	100%	46%	80%
DEFAULT	100	100%	27%	27%
MAX	100	100%	37%	37%
1000	100	100%	46%	46%
500	100	100%	15%	39%

Fuente: (Elaborado por el Autor)

Para flujo TCP múltiple como se puede observar en la tabla 28 la eficiencia de los sistemas IPVPN-MPLS e IPsec-Internet en los 10Mbps y con todos los tamaños de segemento son casi iguales, incluso IPsec-Internet presenta un valor infimo mayor y esto se debe a que el delay ingresado por la encriptación en los CPE's es compensando con la rapidez del switcheo de los paquetes en los PE y P pues sus tablas de ruteo son mínimas en un ambiente de laboratorio, dentro de la linealidad IPsec-Internet tuvo mejor desempeño frente a DMVPN-MPLS y a partir de los 20Mbps los sistemas se vuelven inestables debido al troughput de encriptación que manejan los equipos CPE.

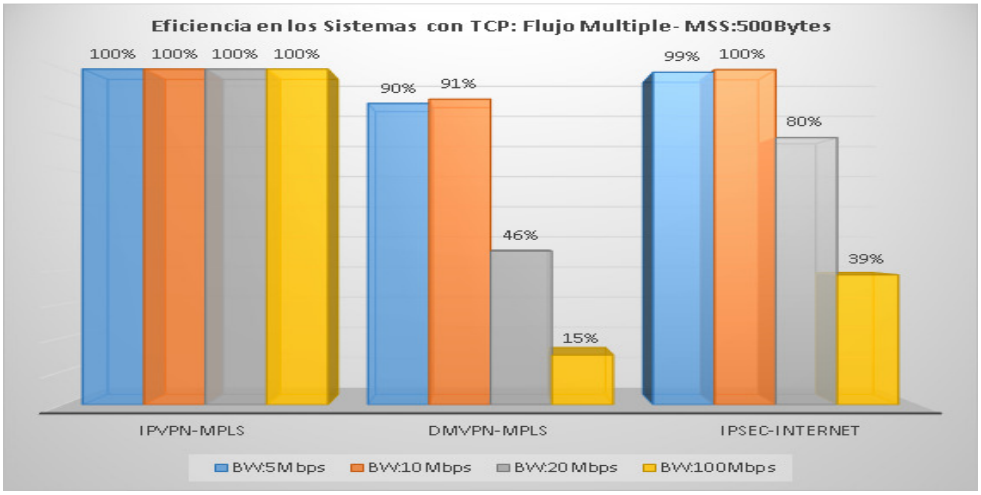

Figura 45: Eficiencia en los Sistemas con Flujo Múltiple TCP – MSS:500bytes.
Fuente: (Elaborado por el Autor)

Para flujo múltiple el manejo de paquetes de segmento MSS=500bytes en sistemas encriptados es más eficiente en el sistema IPsec-Internet frente al sistema DMVPN-MPLS. El sistema IPVPN-MPLS tiene el mejor performance para todos los anchos de banda respecto a los otros dos sistemas encriptados. DMVPN-MPLS tiene un desempeño de aproximadamente 10% menor que IPVPN-MPLS e IPsec-Internet dentro de la zona de linealidad.

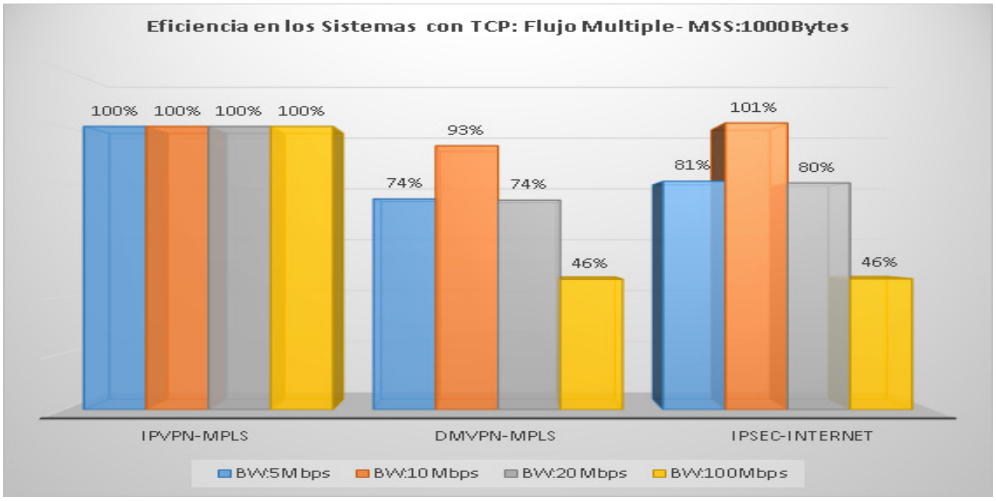

Figura 46: Eficiencia en los Sistemas con Flujo Múltiple TCP – MSS:1000bytes.
Fuente: (Elaborado por el Autor)

Para flujo múltiple el manejo de paquetes de segmento MSS=1000bytes en sistemas encriptados es más eficiente en el sistema IPsec-Internet frente al sistema DMVPN-MPLS. El sistema IPVPN-MPLS tiene el mejor performance para todos los anchos de banda respecto a los otros dos sistemas encriptados. Se observa que Ipsec-Internet tuvo un mejor desempeño de uso del canal a los 10Mbps igualando su desempeño con IPVPN-MPLS.

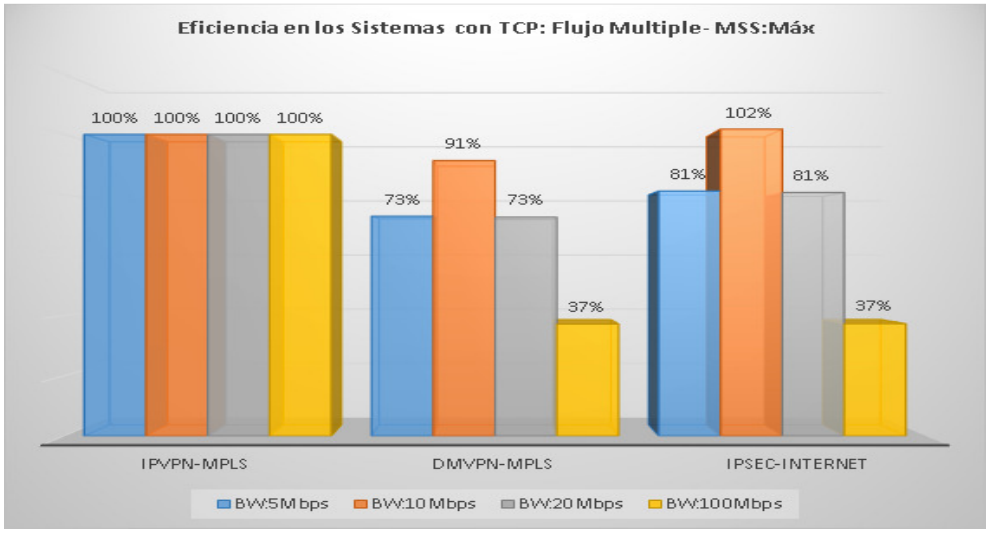

Figura 47: Eficiencia en los Sistemas con Flujo Múltiple TCP – MSS:Máximo.
Fuente: (Elaborado por el Autor)

Para flujo múltiple el manejo de paquetes de segmento máximo para que no exista fragmentación en sistemas encriptados es más eficiente en el sistema IPsec-Internet frente al sistema DMVPN-MPLS. El sistema IPVPN-MPLS tiene el mejor performance para todos los anchos de banda respecto a los otros dos sistemas encriptados. Los sistemas encriptados se vuelven inestables a partir de los 20Mbps y con paquetes pequeños. Se observa que Ipsec-Internet tuvo un mejor desempeño de uso del canal a los 10Mbps igualando su desempeño con IPVPN-MPLS.

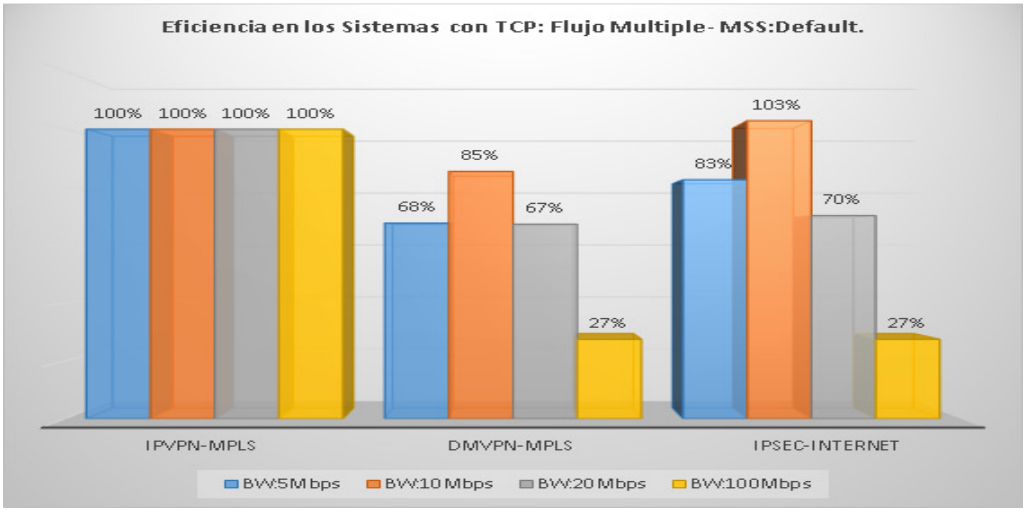

Figura 48: Promedio en los Sistemas con Flujo Múltiple TCP – MSS:Default.

Fuente: (Elaborado por el Autor)

Para flujo múltiple el manejo de paquetes de segmento por default donde existe fragmentación en los sistemas es más eficiente en el sistema IPsec-Internet frente al sistema DMVPN-MPLS. El sistema IPVPN-MPLS tiene el mejor performance para todos los anchos de banda respecto a los otros dos sistemas encriptados. Los sistemas encriptados se vuelven inestables a partir de los 20Mbps y con paquetes pequeños. Se observa que Ipsec-Internet tuvo un mejor desempeño de uso del canal a los 10Mbps igualando su desempeño con IPVPN-MPLS.

4.14Procedimiento de Evaluación de los Sistemas con tráfico UDP y/o Video.

Para la evaluación de los sistemas se ha considerado como variables de entrada a los sistemas, un flujo UDP a enviar en una transmisión; la carga, el ancho de banda de la transmisión y el MSS o tamaño de paquete UDP, los mismos que son seteados en la herramienta de evaluación JPERF, no se setea limitación de ancho de banda en el sistemas ya que UDP no es orientado a conexión y la evaluación se la realiza en base al número de paquetes o datagramas transmitidos.

-

Para cada uno de los sistemas se realizó una transmisión desde el CPE_2 hacia CPE_1, no se realiza transmisiones desde el CPE_1 a CPE_3 o viceversa pues la evaluación en este protocolo se orienta a la sobrecarga en el ancho de banda de la

transmisión. Por cada transmisión se generó un flujo UDP con una carga de 24419000Bytes. El flujo UDP se transmite con los siguientes anchos de banda: 5Mbps - 10Mbps - 20Mbps.- 100Mbps.

**Nota: el tráfico de video a diferencia del tráfico de Voip, aplicaciones TCP y UDP en las cuales está determinado el tamaño de paquete y el comportamiento del flujo de la transmisión como Windowing para TCP y el ancho de banda para UDP ; el video está comprendido por más de las tres cuartas partes de paquetes IP mayores a 1280 bytes y el resto de paquetes más pequeños, el comportamiento del video no es determinístico y los flujos no son constantes debido a los algoritmos de optimización y ecualización por lo que para fines de este proyecto se ha considerado las transmisiones UDP como transmisiones de Video.

4.14.1 Configuración de JPERF como Servidor para UDP.

En la aplicación JPERF de la PC que realizará la función de servidor se selecciona la función de server y colocamos el número de puerto UDP con la que se realizará la transmisión, se coloca el número máximo de flujos UDP que en nuestro caso es uno y se setea el tamaño de paquete UDP que se espera recibir .

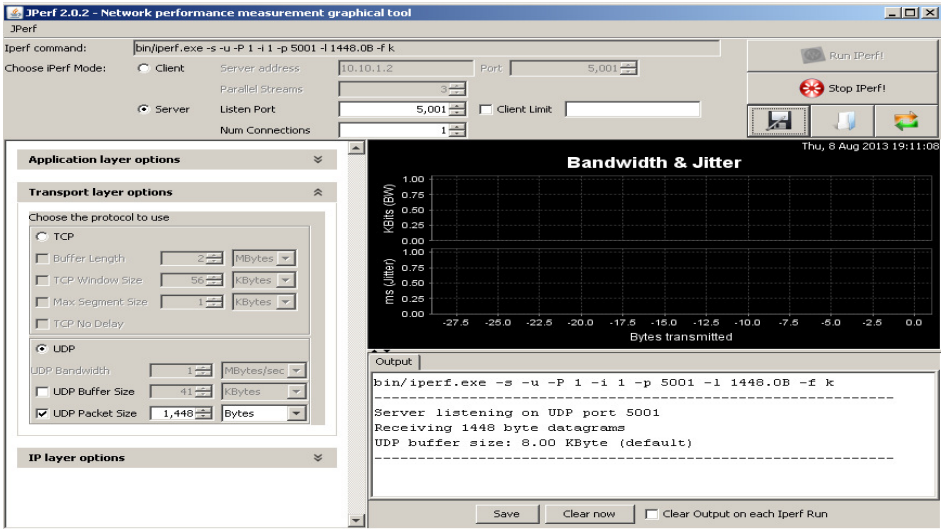

Figura 49: Modo Servidor JPERF para UDP.

Fuente: Programa Jperf

4.14.2 Configuración de JPERF como Cliente para UDP.

Como se muestra en la figura 50 en la PC cliente seleccionamos la función y seteamos la dirección IP del servidor y el puerto UDP del servidor y el número de flujos, la carga en bytes y el tamaño del paquete UDP a transmitir.

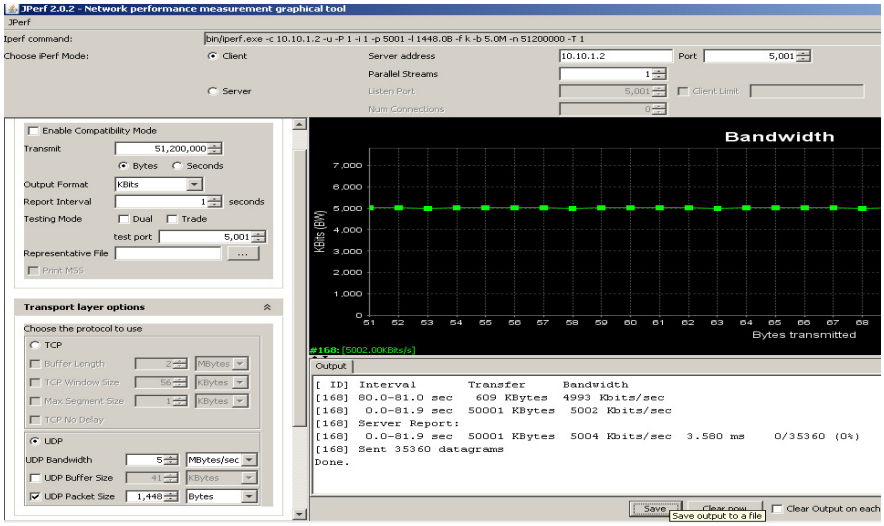

Figura 50: Interface Gráfica JPERF

Fuente: Programa Jperf

Una vez terminada la transmisión y como se puede observar en la figura 50 la herramienta JPERF nos brinda un reporte desde con los resultados desde el servidor con el tiempo de transmisión en segundos, la carga transmitida, la taza de transferencia y el número de datagramas enviados.

-

4.15Pruebas de desempeño para UDP en sistema IPVPN-MPLS.

4.15.1 Parámetros para IPVPN-MPLS con UDP.

En la tabla 29 se detallan los parámetros y los valores correspondientes que son manejados durante una comunicación entre cliente-servidor para la evaluación de desempeño.

Tabla 29.

Parámetros para el sistema IPVPN-MPLS con UDP.

Parámetro	Valor	Tipo	Elemento	Aplicación
UDP Size	500-1000-1476-1484 bytes	Variable	Cliente	Jperf
Carga	24419000Bytes	Constante	Cliente	Jperf
BW	5-10-20-100 Mbps	Variable	Cliente	Jperf
Flujo UDP	1	Variable	Cliente	Jperf

Fuente: (Elaborado por el Autor)

4.15.2 Resultados TX en IPVPN-MPLS con UDP.

Tabla 30.

Resultados TX en IPVPN-MPLS con UDP.

Packet Size (Bytes)	BW Mbps	Tiempo TX (Seg)	Paq Gen	Carga total TX (Bytes)	Sobrecarga resp Payload (%)
Default (1484)	5	39,06	16597	25127858	102,90%
Max(1476)	5	41,447	16743	25147986	102,99%
1000	5	39,07	24430	25456060	104,25%
500	5	39,07	48863	26482396	108,45%
Default (1484)	10	19,53	16597	25127858	102,90%
Max(1476)	10	21,92	16743	25147986	102,99%
1000	10	19,53	24430	25456060	104,25%
500	10	19,53	48860	26482120	108,45%
Default (1484)	20	9,75	16597	25127858	102,90%
Max(1476)	20	12,16	16743	25147986	102,99%
1000	20	12,1	24439	25465438	104,29%
500	20	9,77	48860	26482120	108,45%
Default (1484)	100	10,07	16597	25127858	102,90%
Max(1476)	100	9,96	16743	25147986	102,99%
1000	100	3,88	24430	25456060	104,25%
500	100	6,27	48868	26486456	108,47%

Fuente: (Elaborado por el Autor)

Como se puede ver en la tabla 30 para la tx de un flujo UDP, la eficiencia respecto a la carga original se mantiene estable y proporcional de acuerdo al tamaño de paquete,

teniendo la mayor sobrecarga de 8% cuando se trata de paquetes de 500bytes, los resultados no son función del ancho de banda sino del tamaño de paquete

4.16Pruebas de desempeño para UDP en sistema IPsec-Internet.

4.16.1Parámetros para IPsec-Internet con UDP.

En la tabla 31 se detallan los parámetros y los valores que son manejados durante una comunicación entre cliente-servidor para la evaluación de desempeño.

Tabla 31.

Parámetros para el sistema Ipsec-Internet con UDP.

Parámetro	Valor	Tipo	Elemento	Aplicación
UDP Size	500-1000-Max1384-Default 1484 b	Constante	Cliente	Jperf
Carga	24419000Bytes	Constante	Cliente	Jperf
BW	5-10-20-100 Mbps	Variable	Cliente	Jperf
Flujo UDP	1	Variable	Cliente	Jperf

Fuente: (Elaborado por el Autor)

4.16.2Resultados TX en IPsec-Internet con UDP.

Tabla 32.

Resultados TX en IPsec-Internet con UDP.

Packet Size	BW	Tiempo TX	Paquetes	Carga total TX	Sobrecargares Payload
(Bytes)	**(Mbps)**	**(Seg)**	**Generados**	**(Bytes)**	**(%)**
Max(1384)	5	39,11	17860	26611400	108,98%
Default (1484)	5	39,09	33196	28216600	115,55%
1000	5	39,08	24431	27411582	112,26%
500	5	39,08	48860	30586360	125,26%
Max(1384)	10	19,54	17860	26611400	108,98%
Default (1484)	10	19,53	33196	28216600	115,55%
1000	10	26,03	24432	27412704	112,26%
500	10	20,3	40347	5257222	103,43%

Continua

Max(1384)	20	9,77	17860	26611400	108,98%
Default (1484)	20	9,78	33196	28216600	115,55%
1000	20	9,79	24431	27411582	112,26%
500	20	10,8	29967	18759342	76,82%
Max(1384)	100	7,67	17860	26611400	108,98%
Default (1484)	100	7,62	33196	28216600	115,55%
1000	100	4,7	8904	9990288	40,91%
500	100	6,32	8936	5593936	22,91%

Fuente: (Elaborado por el Autor)

Como se puede observar en la tabla 32 la sobrecarga respecto al payload en el sistema IPsec- Internet tiene su mayor valor cuando se maneja paquetes pequeños de 500 bytes, posteriormente se observa que el sistema se vuelve inestable al no poder manejar un flujo de más ancho de banda con paquetes pequeños, se puede concluir que los valores cuando el BW es 5M corresponde a la eficiencia del sistema.

4.17Pruebas de desempeño para UDP en sistema DMVPN-MPLS.

4.17.1Parámetros para DMVPN-MPLS con UDP.

En la tabla 33 se detallan los parámetros y los valores correspondientes que son manejados durante una comunicación entre cliente-servidor para la evaluación de desempeño.

Tabla 33.

Parámetros para el Sistema DMVPN-MPLS

Parámetro	Valor	Tipo	Elemento	Aplicación
UDP Size	500-1000-Max1368-Default1484 bytes	Variable	Cliente	Jperf
Carga	24419000Bytes	Constante	Cliente	Jperf
BW	5-10-20-100Mbps	Variable	Cliente	Jperf
Flujo UDP	1	Variable	Cliente	Jperf

Fuente: (Elaborado por el Autor)

4.17.2Resultados TX en DMVPN-MPLS con UDP.

Tabla 34:

Resultados TX en DMVPN-MPLS con UDP.

acket Size	BW	Tiempo TX	Paquetes	Carga total TX	Eficiencia respecto Payload
(Bytes)	**(Mbps)**	**(Seg)**	**Generados**	**(Bytes)**	**(%)**
Max(1368)	5	41,472	18079	26937710	110,31%
Default (1484)	5	39,08	49802	29579188	121,13%
1000	5	41,72	24443	27804538	113,86%
500	5	41,52	48880	31375316	128,49%
Max(1368)	10	21,9	18079	26937710	110,31%
Default (1484)	10	19,5	49798	29578412	121,13%
1000	10	19,5	24431	27802478	113,86%
500	10	21,27	40417	25945026	106,25%
Max(1368)	20	12,14	18079	26937710	110,31%
Default (1484)	20	12,14	49799	29574654	121,11%
1000	20	9,76	24431	27802478	113,86%
500	20	11,11	30204	19390968	79,41%
Max(1368)	100	7,7	18071	26925790	110,27%
Default (1484)	100	9,9	34618	17278660	70,76%
1000	100	4,959	8106	9224628	37,78%
500	100	6,28	9314	5978692	24,48%

Fuente: (Elaborado por el Autor)

Como se puede observar en la tabla 34 la sobrecarga respecto al payload en el sistema DMVPN-MPLS tiene su mayor valor cuando se maneja paquetes pequeños de 500 bytes, posteriormente se observa que el sistema se vuelve inestable al no poder manejar un flujo de más BW con paquetes pequeños.

4.17.3Comparación de los Sistemas con UDP respecto a la Sobrecarga.

Tabla 35:

Sobrecarga en TX de Sistemas con UDP

		IPVPN-MPLS	IPsec-Internet	DMVPN-MPLS
Packet Size	**BW**	**Sobrecarga respecto Payload**		
(Bytes)	**(Mbps)**		**(%)**	
Default	5	102,90%	108,98%	110,31%
Máx	5	102,99%	115,55%	121,13%
1000	5	104,25%	112,26%	113,86%
500	5	108,45%	125,26%	128,49%
Default	10	102,90%	108,98%	110,31%
Máx	10	102,99%	115,55%	121,13%
1000	10	104,25%	112,26%	113,86%
500	10	108,45%	103,43%	106,25%
Default	20	102,90%	108,98%	110,31%
Máx	20	102,99%	115,55%	121,11%
1000	20	104,29%	112,26%	113,86%
500	20	108,45%	76,82%	79,41%
Default	100	102,90%	108,98%	110,27%
Máx	100	102,99%	115,55%	70,76%
1000	100	104,25%	40,91%	37,78%
500	100	108,47%	22,91%	24,48%

Fuente: (Elaborado por el Autor)

4.18Comparación de los Sistemas con UDP respecto a los Paquetes TX y RX.

Tabla 36:

Eficiencia de paquetes TX vs RX en el sistema IPVPN-MPLS.

		IPVPN-MPLS		
Bandwidth	**Packet Size**	**Paquetes**	**Paquetes**	**Porcentaje**
(Mbps)	**(Bytes)**	**TX**	**RX**	**(%)**
5	Default	16589	16597	100%
10	Default	16589	16610	100,13%
20	Default	16589	16609	100,12%

Continua

100	Default	16589	16606	100,10%
5	Max	16725	16743	100,11%
10	Max	16725	16743	100,11%
20	Max	16725	16743	100,11%
100	Max	16725	16743	100,11%
5	1000	24419	24430	100,05%
10	1000	24419	24430	100,05%
20	1000	24419	24439	100,08%
100	1000	24419	24430	100,05%
5	500	48838	48863	100,05%
10	500	48838	48860	100,05%
20	500	48838	48860	100,05%
100	500	48838	48868	100,06%

Fuente: (Elaborado por el Autor)

Como se puede ver observar en la tabla 36 en un sistema IPVPN-MPLS el número de paquetes generados en la transmisión son iguales al número de paquetes recibido en la recepción.

Tabla 37:

Eficiencia de paquetes TX vs RX en el sistema DMVPN-MPLS.

		DMVPN-MPLS		
Bandwidth	**Packet Size**	**Paquetes**	**Paquetes**	**Porcentaje**
(Mbps)	**(Bytes)**	**TX**	**RX**	**(%)**
5	Default	16589	49802	300,21%
10	Default	16589	49798	300,19%
20	Default	16589	49799	300,19%
100	Default	16589	34618	208,68%
5	Max	18061	18079	100,10%
10	Max	18061	18079	100,10%
20	Max	18061	18079	100,10%
100	Max	18061	18071	100,05%
5	1000	24419	24443	100,10%
10	1000	24419	24431	100,05%
20	1000	24419	24431	100,05%

Continua

100	1000	24419	8106	33,20%
5	500	48838	48880	100,09%
10	500	48838	40417	82,76%
20	500	48838	30204	61,85%
100	500	48838	9314	19,07%

Fuente: (Elaborado por el Autor)

Como se puede observar en la tabla 37 los paquetes generados por DMVPN-MPLS cuando se maneja paquetes con tamaño por default donde existe fragmentación genera el triple de paquetes que el sistema debe procesar, cuando no existe fragmentación en el sistema el número de paquetes rx es igual a los transmitidos, manejando un BW de 100Mbps y de 500bytes el sistema se vuelve inestable.

Tabla 38:

Porcentaje de paquetes RX vs TX en el sistema IPsec-Internet.

		IPsec-Internet		
Bandwidth	**Packet Size**	**Paquetes**	**Paquetes**	**Porcentaje**
(Mbps)	**(Bytes)**	**TX**	**RX**	**(%)**
5	Default	16589	33196	200,11%
10	Default	16589	33196	200,11%
20	Default	16589	33196	200,11%
100	Default	16589	33196	200,11%
5	Max	17850	17860	100,06%
10	Max	17850	17860	100,06%
20	Max	17850	17860	100,06%
100	Max	17850	17860	100,06%
5	1000	24419	24431	100,05%
10	1000	24419	24432	100,05%
20	1000	24419	24431	100,05%
100	1000	24419	8904	36,46%
5	500	48838	48860	100,05%
10	500	48838	40347	82,61%
20	500	48838	29967	61,36%
100	500	48838	8936	18,30%

Fuente: (Elaborado por el Autor)

Como se puede observar en la tabla 38 los paquetes generados por el sistema IPsec-Internet cuando se maneja paquetes con tamaño por default donde existe fragmentación se recibe el doble de paquetes de los transmitidos, cuando no existe fragmentación en el sistema el número de paquetes recibidos es igual a los transmitidos, manejando un BW de 100Mbps y paquetes de 500bytes el sistema se vuelve inestable

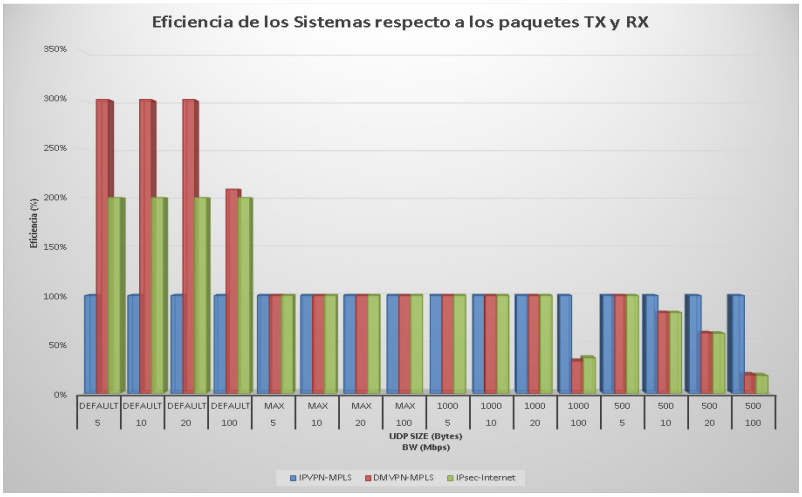

Figura 52: Porcentaje de paquetes RX vs TX en los sistemas.

Fuente: (Elaborado por el Autor)

4.19Procedimiento de Evaluación de los Sistemas con tráfico de VOIP.

El tráfico de voip se caracteriza por usar como protocolo de transporte UDP y tamaños pequeños de paquetes de acuerdo al códec de compresión. Para la evaluación de los sistemas se ha considerado como variables de entrada: 1 flujo UDP a enviar en una transmisión, el ancho de banda de la tx que corresponde al códec de compresión de la voip y el MSS o tamaño de paquete UDP que corresponde al tamaño de paquete que maneja el códec de compresión, los mismos que son seteados en la herramienta de evaluación JPERF, no se setea limitación de ancho de banda en el sistemas ya que UDP no es orientado a conexión y la evaluación se la realiza en base al ancho de banda adicional generado por cada sistema a la salida del CPE. Para cada uno de los sistemas se realizó una tx de 60 segundos desde el CPE_2 hacia CPE_1, no se realiza transmisiones desde el CPE_1 a CPE_3 o viceversa pues la evaluación en este

protocolo se orienta a la sobrecarga en el ancho de banda de la transmisión. Como códec de compresión de voip vamos a evaluar: G.711 – G.728 – G729 y G723.1, en la tabla 39 se muestra los parámetros correspondientes a los códec.

Tabla 39.

Parámetros de códec de VoIP a evaluar

Codec & Bit Rate (Kbps)	Voice Payload Size (Bytes)	Voice Payload Size (ms)	Packets Per Sec (PPS)
G.711 (64 Kbps)	160 Bytes	20 ms	50
G.728 (16 Kbps)	60 Bytes	30 ms	33.3
G.729 (8 Kbps)	20 Bytes	20 ms	50
G.723.1 (5.3 Kbps)	20 Bytes	30 ms	33.3

Fuente: (Elaborado por el Autor)

4.19.1Configuración de JPERF como Servidor para VoIP.

En la aplicación JPERF de la PC que realizará la función de servidor se selecciona la función de server y colocamos el número de puerto UDP con la que se realizará la transmisión, se coloca el número máximo de flujos UDP o llamadas concurrentes voip que en nuestro caso es máximo 40 y se setea el tamaño de paquete UDP que se espera recibir que equivale al tamaño de paquete de voip que maneja cada códec de compresión.

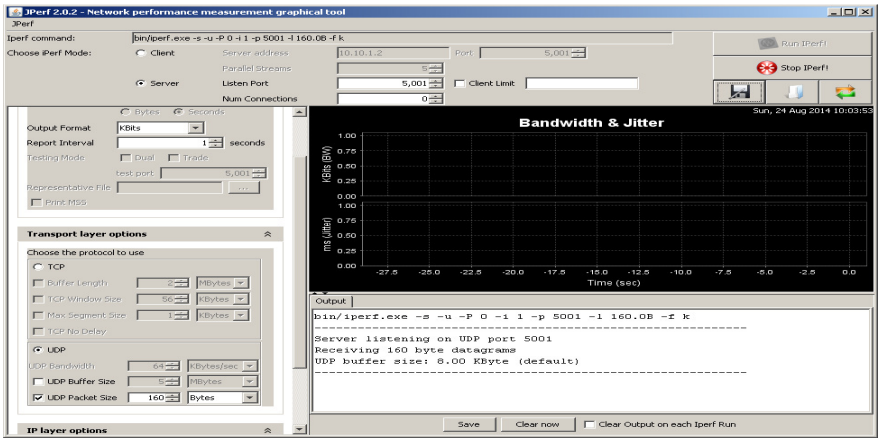

Figura 53: Modo Servidor JPERF para VOIP.

Fuente: Programa Jperf

4.19.2Configuración de JPERF como Cliente para UDP.

Como se muestra en la figura 54 en la PC cliente seleccionamos la función y seteamos la dirección IP del servidor y el puerto UDP del servidor y el número de flujos, la carga en bytes, el tiempo de Tx (60seg) y el tamaño del paquete UDP a transmitir que corresponde al tamaño que maneja el códec de compresión y el UDP bandwidth (kbps) que corresponde a la taza de compresión del códec de compresión de Voip.

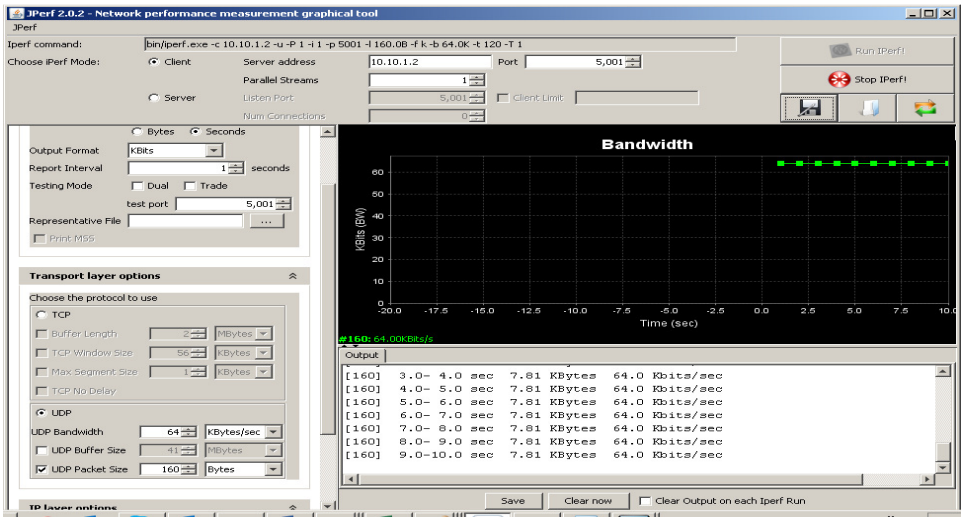

Figura 54: Interface Gráfica JPERF

Fuente: Programa Jperf

4.19.3Obtención de ancho de banda para VoIP en los Sistemas.

Se utilizó el analizador de protocolos Wireshark para capturar los paquetes generados a la salida del CPE_2 por cada transmisión de 60 segundos realizada con el fin de evaluar el ancho de banda promedio que se genera, como se observa en la figura 55 filtramos solamente los paquetes de la TX que corresponde y obtenemos el ancho de banda (Avg. Mbit/sec) promedio en el menú “Statistics/Summary”

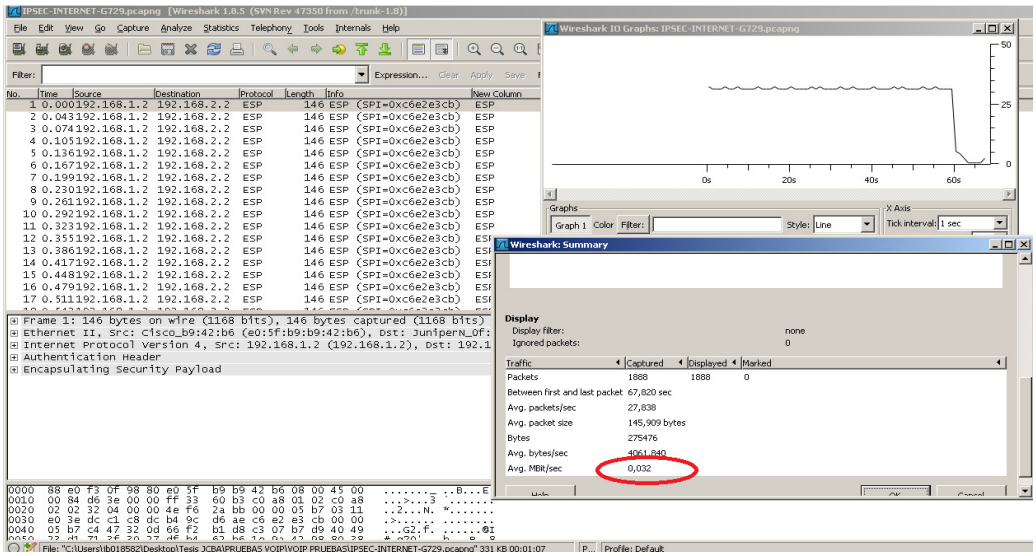

Figura 55: Obtención de BW para VoIP.

Fuente: (Programa Jperf)

4.19.4Resultados Transmisiones de VoIP en los Sistemas.

Tabla 40.

Resultados Transmisiones de VoIP en los Sistemas

CodecBitate (Kbps)	Flujos VoIP	IPVPN-MPLS (kbps)	DMVPN-MPLS (kbps)	IPsec-Internet (kbps)
G.711 (64 Kbps)	1	80	120	104
G.728 (16 Kbps)	1	25	45	42
G.729 (8 Kbps)	1	19	43	35
G.723.1(5.3 Kbps)	1	12	29	23

Fuente: (Elaborado por el Autor)

Como se puede observar en la tabla 40 el ancho de banda generado al pasar un canal de voip por los sistemas con los diferentes tipos de codec de comprensión, el sistema IPVPN-MPLS es más eficiente seguido por el sistema IPsec-internet y el menos eficiente es el sistema DMVPN-MPLS.

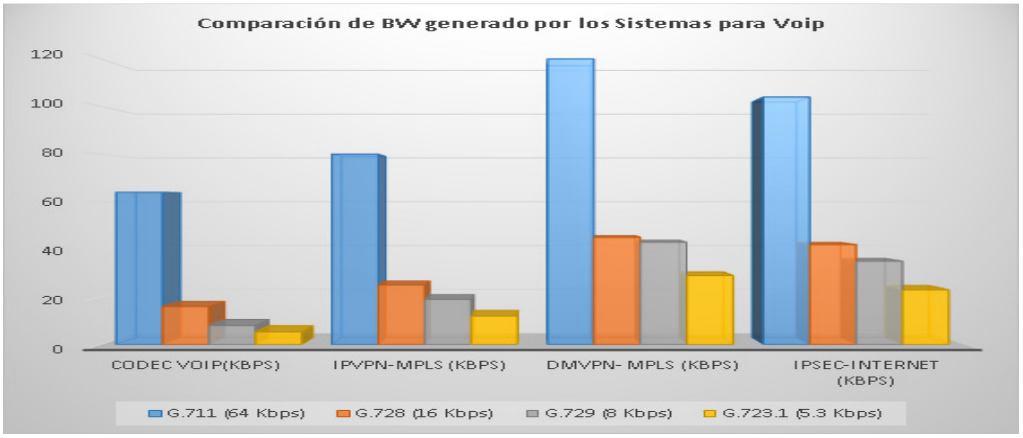

Figura 56: Comparación de BW generado para Voip en los Sistemas.

Fuente: (Elaborado por el Autor)

4.19.5Porcentaje de Overhead para VoIP respecto al Codec en los Sistemas.

Tabla 41.

Porcentaje de Overhead para Voip vs Codec.

Codec Bit Rate (Kbps)	Codec Voip(Kbps)	IPVPN-MPLS (%)	DMVPN- MPLS (%)	IPsec-Internet (%)
G.711 (64 Kbps)	100%	125%	188%	163%
G.728 (16 Kbps)	100%	156%	281%	263%
G.729 (8 Kbps)	100%	238%	538%	438%
G.723.1(5.3 Kbps)	100%	226%	547%	434%

Fuente: (Elaborado por el Autor)

Como se puede observar en la tabla 41 el sistema IPVPN-MPLS es más eficiente respecto a la sobrecarga generada para la transmisión de VoIP, seguido por el sistema IPsec-internet y el menos eficiente es el sistema DMVPN-MPLS se puede concluir que mientras más eficiente es el codec menos eficiente es el sistema que los transmite.

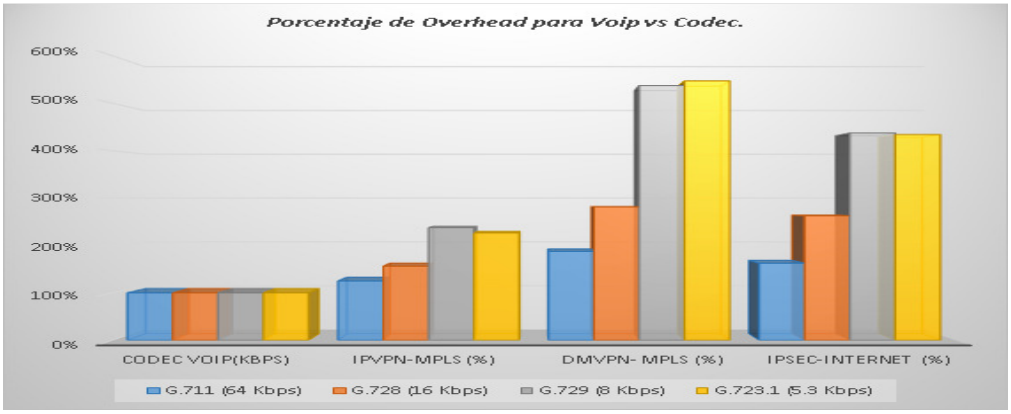

Figura 57: Porcentaje de Overhead para Voip vs Codec.

Fuente: (Elaborado por el Autor)

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- La eficiencia de los sistemas IPsec-Internet y DMVPN-MPLS es dependiente directamente de la capacidad de procesamiento de los CPE's.
- La eficiencia de los sistemas para aplicaciones TCP es dependiente del delay generado extremo a extremo.
- Los equipos de encriptación poseen un ancho de banda limitado para encriptar, fuera de los sistemas se vuelven inestables en cuento a desempeño.
- Tanto para el sistema IPsec-Internet como para el sistema DMVPN-MPLS en la transmisión tanto de un flujo simple como con multiflujo TCP los tiempos de Tx se mantienen directamente proporcional respecto al tamaño del MSS mayores a 1000 bytes y al BW hasta 20Mbps donde los resultados son lineales, fuera de estos parámetros el sistema se vuelve inestable y degradado no por temas inherentes al protocolo IPsec sino por troughput y procesamiento de los equipos CPEs, lo cual coincide con la recomendación de que el C881 soporta hasta 20Mbps con IPsec.
- Tomando como referencia un ancho de banda de 10Mbps en donde existe linealidad en todos los sistemas, se puede concluir en base a la siguiente tabla:

Tabla 42.

Eficiencia para TCP Multiflujo en los sistemas

Eficiencia para TCP Multiflujo en los sistemas				
MSS	**BW**	**IPVPN-MPLS**	**DMVPN-MPLS**	**IPSec-Internet**
(Bytes)	(Mbps)	(%)	(%)	(%)
MAX	10	100%	91%	100%
DEFAULT	10	100%	84%	86%
1000	10	100%	93%	102%
500	10	100%	91%	99%

Fuente: (Elaborado por el Autor)

- Para cuando no existe fragmentación de paquetes usando un MSS máximo, el sistema IPsec-Internet posee el mismo performance que el sistema IPVPN-MPLS, esto se debe a que el delay ingresado en el sistema IPVPN-MPLS al añadir y quitar etiquetas en los P y PE´s es comparable con el delay ingresado en los CPE en el sistema IPsec-internet al encriptar. En el ambiente de laboratorio no existe delay al leer las tablas de rutas en el sistema IPsec-internet a diferencia de un ambiente real en donde las tablas de rutas se componen de miles de prefijos lo que generan un alto delay y degradación del performance en una transmisión TCP.
- Para cuando no existe fragmentación de paquetes usando un MSS máximo el sistema DMVPN-MPLS es menos eficiente que los otros dos sistemas, esto se debe al delay producido al encriptar y posteriormente al delay introducido en los P y PE's al añadir y quitar etiquetas.
- Para cuando existe fragmentación con un MSS por default, el sistema IPsec-Internet y DMVPN-MPLS son menos eficientes en un 15% respecto a un sistema sin encriptar como lo es IPVPN-MPLS.
- Para cuando existe fragmentación manejando un MSS por default en el sistema DMVPN-MPLS y como se puede ver en la figura, el primer fragmento es encriptado y el otro es transmitido sin encriptar como un paquete IPv4, constituyéndose una falla de seguridad del sistema mas no del protocolo IPsec
- Para tráfico TCP los sistemas DMVPN-MPLS e IPsec-Internet poseen bajo desempeño manejando paquetes de segmento menores a 500bytes.
- Para tráfico UDP el sistema IPVPN-MPLS posee total estabilidad respecto a los sistemas encriptados en referencia al tamaño de segmento y/o ancho de banda del flujo.
- Para tráfico UDP el sistema DMVPN-MPLS genera mayor sobrecarga de cabeceras respecto al sistema IPVPN-MPLS e IPsec-Internet, la sobrecarga es inversamente proporcional al tamaño de paquete UDP, a mayor tamaño menor sobrecarga y a menor tamaño mayor sobrecarga.
- Para tráfico de Voip que usan UDP el sistema IPVPN-MPLS es más eficiente en comparación a los sistemas encriptados DMVPN-MPLS e IPsec-Internet.
- Para tráfico de Voip que usan UDP el sistema IPsec-Internet es más eficiente en comparación al sistema DMVPN-MPLS.

- Mientras menor sea la taza de compresión de un códec de Voip menor es la eficiencia de los sistemas encriptados versus los no encriptados.

5.2 Recomendaciones.

- Para TCP se recomienda ajustar los valores de MSS y MTU a los calculados para evitar fragmentación de los paquetes y por consiguiente bajar el performance de las aplicaciones.
- Para la encriptación de aplicaciones de tiempo real como VoIP y video se recomienda el uso de DMVPN-MPLS por la capacidad de manejo de calidad de servicio, IPsec-Internet no lo maneja.
- El dimensionamiento para redes IPsec-Internet y DMVPN-MPLS se lo debe realizar evaluando directamente el troughput de encriptación que manejan los equipos CPE y llevando a segundo plano la capacidad de forwardeo o switcheo de paquetes (pps).
- El dimensionamiento para redes IPVPN-MPLS se lo debe realizar evaluando directamente la capacidad de forwardeo o switcheo de paquetes (pps).
- El dimensionamiento de una red encriptada para tráfico de Voip debe considerar que la sobrecarga por llamada puede llegar hasta el 500% del ancho de banda de compresión del codec de voip.

5.3 BIBLIOGRAFIA

Cisco Systems Inc. (2004). *Implementing Cisco MPLS v2.1* (2.1 ed., Vol. 1). San José California.

Cisco Systems Inc. (2009). *Configuring Dynamic Multipoint VPN (DMVPN) using GRE over IPSec between Multiple Routers.* San José California. Obtenido de http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/29240-dcmvpn.html

Cisco Systems, Inc. (2006). *Cisco IOS IP Configuration Guide* (12.2 ed.). San José California: Cisco.

Juniper Networks Inc. (2012). *Advanced Junos Service Provider Routing* (11.a ed.). Sunnyvale California.

Juniper Networks Inc. (2012). *Junos MPLS and VPNs* (10.a ed.). Sunnyvale California.

Juniper Networks Inc. (2012). *Junos OS MPLS Configuration Guide for Security Devices* (12.1 ed.). Sunnyvale California.

The Internet Engineering Task Force. (1994). *Generic Routing Encapsulation (GRE) RFC1701.* Obtenido de https://www.ietf.org/rfc/rfc1701.txt

The Internet Engineering Task Force. (2005). *Security Architecture for the Internet Protocol – RFC4301.* Obtenido de https://tools.ietf.org/html/rfc4301

The Internet Society. (March de 1999). *BGP/MPLS VPNs RFC2547.* San José California. Obtenido de https://tools.ietf.org/html/rfc2547: https://tools.ietf.org/html/rfc2547