UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:
INGENIERÍA ELECTRÓNICA

Trabajo de titulación previo a la obtención de título de:
INGENIERO E INGENIERA ELECTRÓNICOS

TEMA:
ANÁLISIS Y SIMULACIÓN DE TRÁFICO DE LA RED DE DATOS DE LAS FUERZAS ARMADAS CON TECNOLOGÍAS MPLS

AUTORES:
CRISTHIAN DAVID APOLO ARTURO
YULIANA XIMENA CORAL ROJAS

TUTOR:
LUIS GERMÁN OÑATE CADENA

Quito, Junio del 2017

CESIÓN DE DERECHOS DE AUTOR

Nosotros Cristhian David Apolo Arturo con documento de identificación N° 172109039-5 y Yuliana Ximena Coral Rojas con documento de identificación N° 070644374-4, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de grado/titulación intitulado: "ANÁLISIS Y SIMULACIÓN DE TRÁFICO DE LA RED DE DATOS DE LAS FUERZAS ARMADAS CON TECNOLOGÍAS MPLS", mismo que ha sido desarrollado para optar por el título de: Ingenieros Electrónicos, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

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

.....

Cristhian David Apolo Arturo
C.I.: 172109039-5
Junio del 2017

.....

Yuliana Ximena Coral Rojas
C.I.: 070644374-4
Junio del 2017

DECLARATORIA DE COAUTORÍA DEL DOCENTE TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el trabajo de titulación, ANÁLISIS Y SIMULACIÓN DE TRÁFICO DE LA RED DE DATOS DE LAS FUERZAS ARMADAS CON TECNOLOGÍAS MPLS, realizado por Cristhian David Apolo Arturo y Yuliana Ximena Coral Rojas, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana para ser considerado como trabajo final de titulación.

Quito, Junio del 2017

…….

Ing. Luis Germán Oñate Cadena M.Sc.

C.I: 1712157401

ÍNDICE DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

La creciente demanda de tráfico de voz, datos y video de la red MPLS (Multiprotocolo de Conmutación de Etiquetas) de las Fuerzas Armadas así como también la necesidad de transportar servicios en tiempo real con bajas pérdidas, retardos y jitter a través de una red de transporte de baja capacidad hacen necesario la implementación de técnicas que ayuden a reducir los cuellos de botella y mejorar la subutilización de recursos. Una de estas técnicas constituye la ingeniería de tráfico sobre MPLS para enviar por enlaces alternativos un determinado tipo de tráfico. Este mecanismo fue simulado y analizado en el software OPNET (Herramienta de Ingeniería para Redes Optimizadas), aplicándolo a la red de las Fuerzas Armadas enviando el tráfico de la VPN (Red Privada Virtual) Armada a través de un túnel LSP (Camino de Conmutación de Etiquetas) creado mediante una ruta explícita con la ayuda del algoritmo RSVP-TE (Protocolo de Reserva de Recursos - Ingeniería de Tráfico). Se observó que después del diseño de la red se logró disminuir la carga de tráfico que manejaban los routers de Quito y Guayaquil en un 40% logrando además la posibilidad de aumentar el número de unidades militares que se podrían añadir a la infraestructura de red MPLS para una comunicación de manera más segura y confiable usando los recursos de red propios. Además, se disminuyó la tasa de pérdida de paquetes en un 60% en el tráfico de datos, 50% en el tráfico de video y manteniendo el tráfico de voz sin pérdidas.

ABSTRACT

The growing demand for voice, data and video traffic from the MPLS (Multiprotocol Label Switching) network of the Fuerzas Armadas as well as the need to transport services in real time with low losses, delays and jitter through a low capacity transport network make it necessary to implementation of techniques that help to reduce bottlenecks and improve the underutilization of resources, one of these techniques is the traffic engineering on MPLS to send by alternate links a certain type of traffic in order to avoid saturation of the channel, this mechanism was simulated and analyzed in the OPNET (Optimized Network Engineering Tool) software, applying it to the Fuerzas Armadas network sending the VPN Armada (Virtual Private Network) traffic through an LSP (Label Switched Path) tunnel created through an explicit route with the help of the algorithm RSVP-TE (Resource Reservation Protocol - Traffic Engineering). It was observed that after the design of the network it was possible to reduce the traffic load that the routers of Quito and Guayaquil handled by 40% and increase the number of military units that adhere to the MPLS network infrastructure for a communication more safely and reliably using their own network resources. In addition, it was possible to reduce the packet loss rate by showing a 60% improvement in data traffic, 50% in video traffic and maintaining voice traffic without losses.

INTRODUCCIÓN

La demanda actual de las telecomunicaciones necesita de redes convergentes que ofrezcan servicios como: voz, video conferencia y datos, que deben cumplir con parámetros eficientes de pérdidas de datos, retardos, jitter y rendimiento, y considerando que existen mecanismos de reenvió como TCP y configuraciones de calidad de servicio, existen servicios en tiempo real en los que no es eficiente el reenvió o pérdida de paquetes y retardos fuera del rango permitido.

Debido al tipo de tecnología y al tiempo de funcionamiento, la red de datos de las FF.AA (Fuerzas Armadas) ya no cumple con las exigencias de una red de transporte, ya que su nivel jerárquico en la capa de núcleo está formada por enlaces SDH (Jerarquía Digital Sincrónica) y a nivel de distribución con enlaces PDH (Jerarquía Digital Plesiócrona). Por otra parte existe uso desequilibrado de los recursos de la red debido a la existencia de algunos enlaces y equipos intermedios muy utilizados y otros en cambio con poco uso. Considerando la demanda y escalabilidad actual de la red de datos de las FF.AA.es necesario aplicar técnicas que mejoren el uso de los recursos de la red y eviten los cuellos de botellas para una transmisión con menores pérdidas.

Partiendo de la situación inicial de la red de las Fuerzas Armadas el diseño propuesto plantea realizar un incremento de routers en la capa de distribución para reducir la carga de tráfico que procesan los routers ubicados en Quito y Guayaquil, adicionalmente con la ayuda de la simulación en el software OPNET, se analizó la técnica de ingeniería de tráfico mediante la creación de túneles LSP, para desviar el tráfico de la VPN de menor ancho de banda por una ruta alterna y reducir la carga de las rutas más congestionadas usando de mejor manera todos los recursos de la red, además se garantiza un ancho de banda para el flujo de tráfico enviado a través de la ruta explicita por medio del algoritmo RSVP-TE.

El presente documento consta de 4 capítulos: En el capítulo I se detallan los antecedentes del proyecto de diseño de la red de las FF.AA y se incluye además el planteamiento del problema, los objetivos, la justificación y la metodología utilizada

en el proyecto. El capítulo II hace referencia al marco teórico en el cual se detalla la metodología PPDIOO, los elementos que componen la arquitectura MPLS que será la tecnología aplicada a la red de las Fuerzas Armadas, el funcionamiento del algoritmo RSVP-TE que se establecerá en base a rutas explicitas y será aplicado en la ingeniería de tráfico orientada a recursos, la QoS (Calidad de Servicio) donde se detalla la clasificación de los servicios diferenciados y por último el software OPNET que se utiliza para el análisis y la simulación de la red.

En el capítulo III se realiza el análisis actual de la red que permite determinar la disponibilidad y escalabilidad para él envío de paquetes, y de esta forma identificar las rutas más congestionadas para realizar ingeniería de tráfico mediante la creación del túnel con rutas explícitas y garantizar un ancho de banda para el flujo en el túnel, finalmente se analiza los resultados del tráfico en la red comparando la red actual con la red diseñada con el fin de mejorar el rendimiento de la red. En el capítulo IV se realiza la factibilidad económica del proyecto a partir del cálculo de dos variables económicas el TIR (Tasa Interna de Retorno) y VAN (Valor Actual Neto) tomando a consideración el ahorro mensual de la empresa por el pago de proveedor servicios de internet para determinar si el proyecto es favorable para las Fuerzas Armadas y dentro de que tiempo genera ahorros.

Finalmente se presenta las conclusiones en base a los resultados de los tráficos obtenidos de la simulación en el software OPNET, y las recomendaciones para futuros diseños y mejoras en la red. Como última parte se presentan los anexos de las gráficas de la ruta Guayaquil – Cotacachi donde también se aplicó ingeniería de tráfico ya que esta ruta tiene menos congestión en comparación a la ruta Guayaquil – Quito.

CAPÍTULO 1
ANTECEDENTES

1.1.Planteamiento del problema

La demanda de velocidad y escalabilidad de la red datos de las FF.AA ha incrementado la necesidad de aplicar técnicas para el uso eficiente de los recursos de la red. Una de estas técnicas es la ingeniería de tráfico, la cual se emplea para evitar los cuellos de botella e identificar prioridades de los servicios para ser enrutados por enlaces principales o alternos basándose en los recursos que el servicio requiere, mejorando de esta forma la calidad de servicio en la red. Para el desarrollo de la ingeniería de tráfico y calidad de servicio se requiere un análisis del tráfico de la red, del retardo y de la capacidad que tiene cada canal para el envío de paquetes con el fin de descongestionar ciertos enlaces y usar rutas secundarias.

1.2.Tema

Análisis y simulación de tráfico de la red de datos de las Fuerzas Armadas con tecnologías MPLS.

1.3.Justificación

La red de datos de las Fuerzas Armadas con tecnología MPLS cuenta con una red de transporte SDH y PDH, en la que se da mayor prioridad a los servicios en tiempo real como la voz, videoconferencia, sin omitir los protocolos de enrutamiento, de reservación de recursos y de distribución de etiquetas. Los servicios en tiempo real necesitan de QoS para otorga mayor prioridad, razón por la cual este tipo de tráfico no debe ser encolado, obteniendo una comunicación por voz y video eficiente y sin retardos, debiendo para ello enrutar estos servicios por el canal principal y los servicios menos importantes por rutas alternas.

Por tales razones es primordial analizar y simular el tráfico en la red MPLS ya que permitirá obtener otras alternativas de solución aplicadas en la red de datos de las FF.AA. para su óptimo funcionamiento.

1.4.Objetivos

1.4.1. Objetivo General

Analizar y simular el tráfico de la red de datos de las Fuerzas Armadas mediante el software OPNET para realizar una ingeniería de tráfico que permita mejorar el rendimiento de la Red.

1.4.2. Objetivos Específicos

- Determinar el estado actual de la red de datos basados en los parámetros principales como escalabilidad, tipo de enlaces entre dispositivos intermedios, calidad de servicio y protocolos de enrutamiento para determinar las falencias y mediante este análisis mejorar el rendimiento de la Red.
- Elaborar una simulación de la red de las Fuerzas Armadas mediante el software OPNET para aplicar ingeniería de tráfico de acuerdo a la diferenciación de los servicios y comparar la red actual y la red diseñada.
- Realizar el diseño que permita una reserva de recursos de la red y verificar las rutas óptimas para descongestionar los enlaces, enrutando el tráfico por rutas alternativas de acuerdo a la prioridad de los datos para mejorar el desempeño de la Red.
- Analizar la viabilidad económica de la solución propuesta para la red de datos de las Fuerzas Armadas mediante TIR y VAN para determinar si se puede implementar el diseño.

1.5.Metodología

- Estudio de los temas por medio de la lectura y el análisis de artículos científicos publicados en bases de datos científicos internacionales como Science Direct, IEEE Explorer, entre otras; además de artículos publicados por prestigiosas universidades alrededor del mundo. Es decir, se utilizará el método deductivo para este apartado.
- La información recopilada permitirá obtener conocimientos para realizar una ingeniería de tráfico en la red y de esta forma determinar la ruta más óptima para la transmisión de datos.

- Elaborar una simulación de la red mediante el Software OPNET que facilitara la obtención de los parámetros principales dentro de la red y aplicar la ingeniería de tráfico de acuerdo con las prioridades de los servicios en los paquetes.
- Determinar el estado actual de la red de datos mediante un análisis del tráfico en los canales comparando el desempeño de cada ruta en la transmisión aplicando una calidad de servicio en los paquetes.
- Los resultados obtenidos en el análisis y la simulación nos permitirán desviar el tráfico por las rutas en desuso basados en las prioridades en los paquetes dentro de la red.

CAPÍTULO 2
MARCO CONCEPTUAL

En el presente capítulo se detallará los conceptos teóricos más relevantes y necesarios para el análisis y simulación de tráfico sobre la red de datos de las Fuerzas Armadas del Ecuador, que se irán desarrollando en los siguientes capítulos.

2.1.Metodología PPDIOO

La metodología PPDIOO es un modelo para el diseño y gestión de una red implementada por CISCO, por sus siglas significa: preparar, planear, diseñar, implementar, operar y optimizar. A continuación se define cada una de estas fases:

- **Preparación**

Mediante esta fase se definen los objetivos empresariales a conseguir mediante una estrategia de red, proponiendo un diseño y la identificación de tecnologías para impactar positivamente al negocio. (Saavedra, 2015)

- **Planeación**

En esta fase se identifican los requerimientos de red mediante un análisis de las características técnicas y niveles de servicio requeridos por las diferentes clases de tráfico de la red para finalizar con éxito el proyecto. (Saavedra, 2015)

- **Diseño**

Con la información de las fases anteriores se diseña y prueba métodos de optimización para la red de acuerdo a los requerimientos técnicos y de negocios antes de su implementación, en esta sección se incluye topologías, seguridades, escalabilidad y calidad de servicio. (Saavedra, 2015)

- **Implementación**

Se ejecuta el diseño de red aprobado de acuerdo a las especificaciones de la fase anterior en periodos de baja actividad de la empresa para no comprometer su disponibilidad y funcionamiento. (Saavedra, 2015)

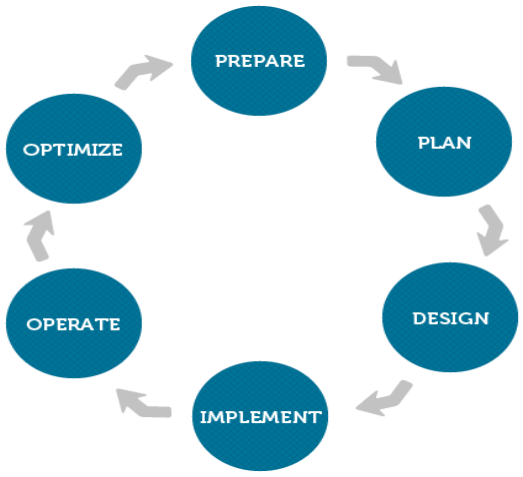
- **Operación**

En esta fase se observa el estado de la red diariamente, esto incluye la administración, gestión de la red, el monitoreo de la red, el mantenimiento, la identificación y corrección de errores de red. Esta fase es la prueba final de diseño. (Saavedra, 2015)

- **Optimización**

En esta fase se monitorean los niveles de servicio implementados y se previenen futuros problemas que afecten al correcto funcionamiento de la red. En esta fase se puede realizar una modificación del diseño inicial si los problemas son graves, mejorando la eficiencia y desempeño de la red. (Saavedra, 2015)

Figura 2.1. Diseño de red con Top-Down.



Metodología PPDIOO (Saavedra, 2015)

2.2.MPLS

Las siglas MPLS significa Multiprotocolo de Conmutación de Etiquetas, es una técnica que se desarrolló para solucionar múltiples problemas de envió de paquete y para unificar el servicio de transporte de datos, opera entre la capa de enlace de datos y la capa de red del modelo OSI, se la puede considerar como un protocolo de la unión entre la capa de enlace y la capa de red. De tal forma que combina de manera óptima el direccionamiento lógico o enrutamiento con la rapidez de la conmutación de nivel dos. (Boris Salas, 2012)

Puede ser utilizado para el transporte de diversos tipos de tráfico como por ejemplo: tráfico de voz, paquetes IP, multimedia. MPLS se lo identifica como un sustituto de una de las arquitecturas IP sobre ATM o como un protocolo para hacer tunelización, siendo una de las técnicas más eficientes para el encaminamiento de paquetes. (Garcia, 2008)

“La tecnología MPLS se despliega en el núcleo de la red del proveedor de servicios, proporcionando un control sobre la calidad del servicio”. (ACENS, 2005)

MPLS dispone de varias especificaciones que permite enrutar los paquetes por la red usando datos que se obtienen en las etiquetas de los paquetes IP, ayudando a los routers a determinar el camino para enviar los datos considerando QoS y el desempeño de la red. Al aplicar MPLS se logra diversas funcionalidades en la ingeniera de tráfico, que permite “gestionar y controlar una red en telecomunicaciones, además soporte de VPN’s y aumentar la QoS con diversas clases de CoS. (Henao, 2010)

Las clases de servicios a las que se aplica prioridades son: video, voz, datos de alta prioridad, datos prioritarios, datos de baja prioridad, en los que se considera el consumo del ancho de banda para su funcionamiento óptimo. (Henao, 2010)

“MPLS ocupa un lugar preponderante dentro de las redes de transporte”, (Jiménez M., 2013) considerado como un avance en la evolución de tecnologías de enrutamiento, lo que mejora la forma de gestionar y diseñar redes. (Boris Salas, 2012)

2.2.1.Arquitectura de una red MPLS

La red MPLS consta de los siguientes elementos:

2.2.1.1.LSR (Label Switching Router)

Se encuentran en el interior de una red MPLS, generan procedimientos de distribución de etiquetas y también se encargan del reenvió de paquetes en el dominio MPLS, mediante el “análisis de etiquetas adosadas a cada paquete hasta la capa 2”. (Jiménez M., 2013)También se les denomina Router P (provider) y son los routers que forman el núcleo de la red MPLS. (Boris Salas, 2012)

2.2.1.2.LER (Label Edge Router)

Se encuentran en el extremo del dominio MPLS, su función es “insertar etiquetas a los paquetes IP para enviarlos dentro del dominio MPLS o removerlos para enviarlos fuera del dominio, considerando hasta la capa 3”. (Jiménez M., 2013) Los routers LER se encuentran ubicados al borde de una red MPLS y se les denomina PE, utilizan BGP para realizar una comunicación entre los nodos teniendo un sistema autónomo. (Boris Salas, 2012)

2.2.1.3. FEC (Forwarding Equivalence Class)

Equivale al conjunto de paquetes con características parecidas o idénticas que se transmiten de forma similar sobre un mismo canal LSP que tienen distintos destinos

finales. En el ingreso de la red MPLS, “los paquetes son clasificados y asignados a un FEC especifico usando una etiqueta”. La FEC tienen una ruta definida por los LSR’s de la red, lo que facilita a MPLS convertir las redes IP sin conexión en redes orientadas a conexión. (Jiménez M., 2013)

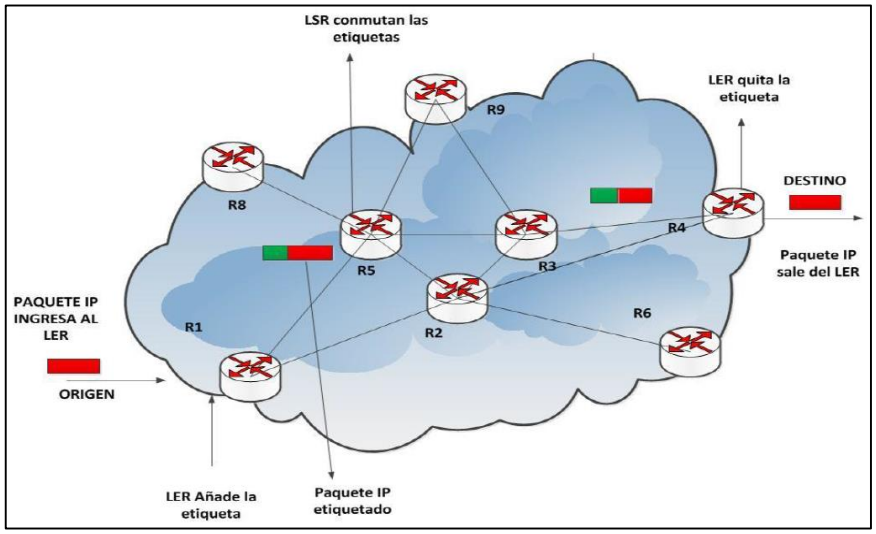
2.2.1.4. LSP (Label Switched Path)

Es un camino unidireccional que dirige todos los paquetes etiquetados de acuerdo a un FEC, mediante un conjunto de LSR’s para alcanzar el destino. En la creación de un LSP se requiere de un protocolo de enrutamiento para difundir las tablas de enrutamiento en todos los LSRs para determinar el camino más corto hacia el destino. (Jiménez M., 2013)

Básicamente el funcionamiento de MPLS depende de la creación de los LSP usando el intercambio de etiquetas y la conmutación del tráfico de datos en las rutas establecidas. (Jiménez M., 2013) .Se le denomina como “el camino específico del tráfico a través de la red”. (Boris Salas, 2012)

En la figura 2.2 se observa la estructura principal de una red MPLS y de los elementos que la conforman la red.

Figura 2.2. Arquitectura de una Red MPLS



Estructura principal de una red MPLS y diferentes elementos. (Boris Salas, 2012)

2.2.2.Etiquetas MPLS

“La etiqueta MPLS es un identificador corto y de longitud fija entre el encabezado de capa 2 y capa 3” que facilita la clasificación de un paquete respecto a la FEC que

pertenece. Es empleado por los LSR del núcleo de una red para él envió de paquetes, al determinar la ruta que atraviesa el paquete.

En las etiquetas MPLS los LSR en una red toman una decisión independiente para representar el valor de la etiqueta asociado a un FEC. “El encabezado MPLS se encuentra formado por 32 bits distribuidos en cuatro campos”.

- **Etiqueta**

Está formado por 20 bits, en donde se encuentra “el valor de la etiqueta asignada que se cambia en cada LSR”.

- **Exp o experimental**

Está formado por 3 bits, se utiliza para determinar la clase de servicio (CoS, Class of Service) que necesita el paquete.

- **S (Stack)**

Está formado por 1 bit, el bit determina si la etiqueta es la última del paquete MPLS.” Si S=1 es la última, si S=0 existen etiquetas añadidas al paquete.”.

- **TTL (Time To Live)**

Está formado por 8 bits, y ayuda a que los paquetes no ingresen en un bucle. (Jiménez M., 2013)

2.3. Ingeniería de tráfico

La ingeniería de tráfico permite optimizar el uso de los recursos disponibles dentro de una red para evitar los cuellos de botella, esto se produce por él envió de tráfico a través de la ruta más corta, que es escogida por el protocolo de enrutamiento y no se toma a consideración rutas alternas, lo cual puede congestionar algunos enlaces dentro de la red. Mediante la ingeniería de tráfico se desea proveer calidad de servicio y obtener un control de uso de los recursos de la red. (Garcia, 2008)

Una ingeniería de tráfico permite diferentes mecanismos para realizar la optimización del rendimiento y tráfico en una red, de esta forma mejorar el servicio ofrecido al usuario. La característica más relevante de la ingeniería de tráfico consiste en enrutar determinados paquetes por rutas alternas más descongestionadas, aunque no sean el camino más corto, con respecto a la ruta principal. (Delfino, Rivero, & San Martín, 2005)

La ingeniería de tráfico puede proveer las siguientes funciones dentro de una red MPLS:

- Definir rutas secundarias en entornos de congestión de la red.
- Asegurar un uso más eficiente del ancho de banda y recursos de la red, sin dejar enlaces o segmentos de red inutilizados y tomándolos en cuenta como caminos alternos en escenarios de congestión de recursos sobre utilizados.
- Minimizar la congestión y pérdida de paquetes transportados a través de la red y maximizar la eficiencia de la red.
- Facilitar un adecuado control sobre el sistema de re-enrutamiento de paquetes cuando el camino secundario encuentra puntos de falla.

La ingeniería de tráfico se divide en dos partes de acuerdo a sus objetivos: orientada a tráfico y orientada a recursos.

2.3.1.Orientada a tráfico

La ingeniería de tráfico en esta modalidad tiene como objetivo hacer más eficiente el transporte de datos y reducir el retardo, la perdida de paquetes, maximizar el throughput y brindar calidad de servicio para los datos transportados a través de la red.

2.3.2.Orientada a recursos

La ingeniería de tráfico orientada a recursos tiene como objetivo la optimización de los recursos de una red para evitar congestiones en ciertas partes de la red mientras otras permanecen descongestionadas o muy poco transitadas, en este método se usa la optimización del ancho de banda.

Por cualquiera de los dos métodos descritos se llega a un objetivo común, el cual es el de optimizar los recursos de una red haciendo más eficiente su uso para minimizar la congestión de la red.

Los servicios tales como voz, datos o video compiten entre sí para ser transportados a través de los recursos disponibles de red como pueden ser los equipos intermedios o Routers, se dice que un recurso de red esta congestionado cuando la velocidad de entrada de paquetes es mayor que la velocidad de salida en el recurso en un tiempo dado. (Delfino, Rivero, & San Martín, 2005)

2.3.3.Congestión de red

La congestión de red se da cuando los recursos de una red cursan más tráfico del que son capaces de soportar y deriva en la degradación de la calidad de servicio, la congestión puede causar efectos indeseables como: el retardo de paquetes, el descarte de paquetes y el uso ineficiente de los recursos de red. Uno de los motivos de la congestión es tener un reducido ancho de banda, el cual se puede solucionar aumentado su capacidad, también puede darse por el uso ineficiente de recursos el cual se puede solucionar mediante una ingeniería de tráfico que consiste en ajustar la circulación del tráfico a los recursos disponibles de red. (Calderon, 2003)

2.3.4. Componentes de la Ingeniería de Tráfico

La ingeniería de tráfico está conformada por 4 componentes que son:

- Componente del reenvío de paquetes.
- Componente de distribución de información.
- Componente de selección de camino.
- Componente de señalización.

- **Componente del reenvío de paquetes**

La componente de reenvió de paquetes es la encargado de enrutar un flujo de paquetes IP a lo largo de un camino predeterminado a través de la red. (Hernández, 2015)

- **Componente de distribución de información**

La componente de distribución de información se basa en obtener un conocimiento detallado de la topología de la red, así como también información dinámica de la carga en la red. La componente de distribución de información se realiza dando extensiones a los IGPs (Interior Gateway Protocol), como son OSPF-TE e IS-IS TE, tal que los atributos de los enlaces son incluidos como parte de cada aviso del estado de enlace en cada router. Cada router contiene características de los enlaces de la red e información de la topología de la red en la base de datos de la ingeniería de tráfico (TED). La TED se usa para el cálculo de rutas explícitas, para la ubicación de LSPs a lo largo de la topología física, de manera que el cálculo subsiguiente de la ingeniería de tráfico sea independiente del IGP. (Delfino, Rivero, & San Martín, 2005)

- **Componente de selección de camino**

En la componente de selección de camino los routers utilizan la base de datos de la ingeniería de tráfico para calcular los caminos en la red MPLS de su propio conjunto de LSPs a lo largo del dominio de ruteo. El camino para cada LSP puede ser representado por una ruta explícita. El router de ingreso determina el camino físico para cada LSP aplicando un algoritmo de camino más corto basado en restricciones (CSPF) a la información en la base de datos de la ingeniería de tráfico.

- **Componente de señalización**

La componente de señalización es la encargada de que los routers LSP sean establecidos para su correcto funcionamiento en el intercambio de etiquetas dentro de la red MPLS. Esta señalización se realiza utilizando RSVP-TE. (Hernández, 2015)

2.4.Algoritmo RSVP -TE

RSVP-TE dispone de extensiones especiales para establecer rutas ópticas y hacer una red ágil, además es conocido también como un algoritmo basado en restricciones, común mente usada como protocolo de señalización y requiere de datagramas IP para comunicarse entre LSR's (Hernández, 2015). RSVP-TE se encuentra basado en la distribución de etiquetas sobre una red MPLS, denominado como extensión del protocolo RSVP. Este protocolo facilita el re-enrutamiento de los túneles LSP para evitar cuellos de botella, congestión en la red, pérdida de paquetes y el retardo en un flujo de información, además permite la creación de rutas explicitas con o sin reserva de recursos a través de la ruta establecida (Hernández, 2015). La ruta explícita es una secuencia de nodos lógicos LSR entre un enrutador (LER) de ingreso y de egreso a una red, además proporciona listas de direcciones IP y a su vez especifica los primeros saltos y salto a salto, se considera una función relevante para habilitar la ingeniería de tráfico en MPLS (Danilo Alfonso López Sarmiento, 2009).

Los túneles LSP son utilizados en re-encaminamientos cuando se distribuye el tráfico por múltiples rutas el cual es imperceptible para los routers a lo largo de la ruta LSP independientes del algoritmo IGP , dentro de la ingeniería de tráfico se lo define como túnel TE (TELECOM PROTOCOL FINDER, 2002).

2.5.Calidad de Servicio

La calidad de Servicio (QoS) es la capacidad que tiene una red para brindar diferenciación de servicios (DiffServ) y otorga prioridades a los distintos tipos de

tráfico de acuerdo a su importancia dentro de una organización, para el usuario final la calidad de servicio es la percepción que se tiene acerca del correcto funcionamiento de los servicios y aplicaciones de una red los cuales son la voz, el video y los datos. (Romero, 2009)

Para marcar la diferenciación de servicios en un paquete IP se cuenta con el campo ToS dentro de los paquetes en donde los 3 primeros bits son conocidos como precedencia y define prioridades desde 0 (mínimo) a 7 (máximo) y los cuales están divididos como se muestra en la Tabla No. 2.1:

Tabla 2.1 Valores del campo precedencia.

VALOR BINARIO	VALOR DECIMAL	NOMBRE
111	7	Reservado para red
110	6	Enrutamiento
101	5	Voz
100	4	Video
011	3	Señalización/control de llamada
010	2	Datos de alta prioridad
001	1	Datos de menor prioridad
000	0	Mejor esfuerzo

Determinación de los valores de precedencia dentro del campo ToS. (Lorge, 2015)

Los 6 primeros bits Del campo ToS son asignados para el valor DSCP (DiffServ code point), mediante la diferenciación de servicios se otorga un tratamiento de reenvío a los paquetes marcados con un valor DSCP (Lorge, 2015), a este tratamiento diferenciado se le denomina PHB (Per Hop Behavior) y está clasificado de la siguiente manera:

- **Expedited Forwarding (EF)**

Tiene un valor DSCP 46 y garantiza en un servicio bajas pérdidas de paquetes, bajo retardo, bajo jitter y asegura un ancho de banda para el servicio. (Lorge, 2015)

- **Assured Forwarding (AF)**

Establece 4 clases de prioridad de servicio, cuyos valores de acuerdo a su prioridad de mayor a menor son AF4x, AF3x, AF2x, AF1x, y x representa la preferencia de

descarte que se le da al paquete al cual se le asigna los siguientes valores: 1 = bajo descarte, 2 = medio descarte, 3 = alto descarte. (Lorge, 2015)

- **Default**

Tiene un valor DSCP 0 y también es conocida como "Mejor esfuerzo", no otorga ningún tipo de prioridad al paquete. (Lorge, 2015)

- **Class Selector**

Está determinado por los tres primeros bits dentro del campo ToS, y otorga 7 niveles de servicio desde el CS1 al CS7, donde cada valor tiene una mayor prioridad de envió que su antecesor. (Lorge, 2015)

- **RSVP**

RSVP es un protocolo de la capa de trasporte para señalización, proporciona garantías de calidad de servicio de extremo a extremo mediante el suministro del ancho de banda requerido para la transferencia de datos, permitiendo alcanzar un retardo mínimo. RSVP fue diseñado para interoperar con protocolos de enrutamiento para optimizar el uso de recursos y lograr un mejor rendimiento de la red. (Hernández, 2015)

2.6.Opnet

Es un software de simulación, siendo de gran ayuda para simular el tráfico en redes considerando los diferentes niveles que existen dentro de una red y del modelo que se utilice. Además se lo conoce como un lenguaje de simulación guiado en las comunicaciones y es utilizado en empresas de telecomunicaciones porque facilita el diseño de redes, la administración de dispositivos, protocolos y aplicaciones proporcionando gran utilidad en el desarrollo de proyectos. El software OPNET facilita el modelado de topologías y determinar el comportamiento de la red, ya que cuenta con cuatrocientos modelos para funciones específicas, este software puede ser usado como una herramienta de docencia, es necesario destacar que también cuenta con la orografía del lugar donde se realizará el diseño de la red y dispone de diferentes modelos de propagación, trabajando en conjunto con el software Radio Mobile. (Departamento de Ingenieria Telamatica, Septiembre 2004)

CAPÍTULO 3
ANÁLISIS DE LA RED ACTUAL

En este capítulo se describirá el estado actual de la red y los parámetros básicos a considerarse para el funcionamiento de una red de datos como: la topología lógica y física, el direccionamiento IP, la seguridad de la red, la escalabilidad, el protocolo de enrutamiento principal y las prioridades que otorgan la calidad de servicio en las aplicaciones. Los cuales se obtendrán al buscar esta información con los ingenieros y técnicos de la red de las Fuerzas Armadas que son los responsables de su óptimo funcionamiento.

3.1.Análisis de la red actual

La Red de Datos de las Fuerzas Armadas fue creada con ciertos requerimientos y fundamentos para los servicios ofrecidos dentro de la red. Con la implementación de la tecnología MPLS se solucionó problemas de comunicaciones dentro de la red. La red actual provee diferentes aplicativos a las Fuerzas Armadas dependiendo de los requerimientos de las unidades Militares.

Se debe considerar que la Red de Core cuenta con 6 routers de la familia ASR 9000 Cisco y emplea el protocolo de enrutamiento ISIS para su direccionamiento, además cabe recalcar que dentro de esta infraestructura se implementa la tecnología MPLS para el etiquetado de los paquetes.

Los problemas que enfrenta la red en la actualidad son: la escalabilidad y optimización de los canales, causando la subutilización de canales para los servicios establecidos. El incremento de usuarios y la calidad del servicio, genera saturación en los canales de la red de datos de las Fuerzas Armadas, el limitado desempeño de los equipos impide la aplicación de parámetros necesarios para el óptimo funcionamiento de la red como es el uso QoS, balanceo de carga e ingeniería de tráfico dentro de la red lo que genera retardos en los servicios de tiempo real.

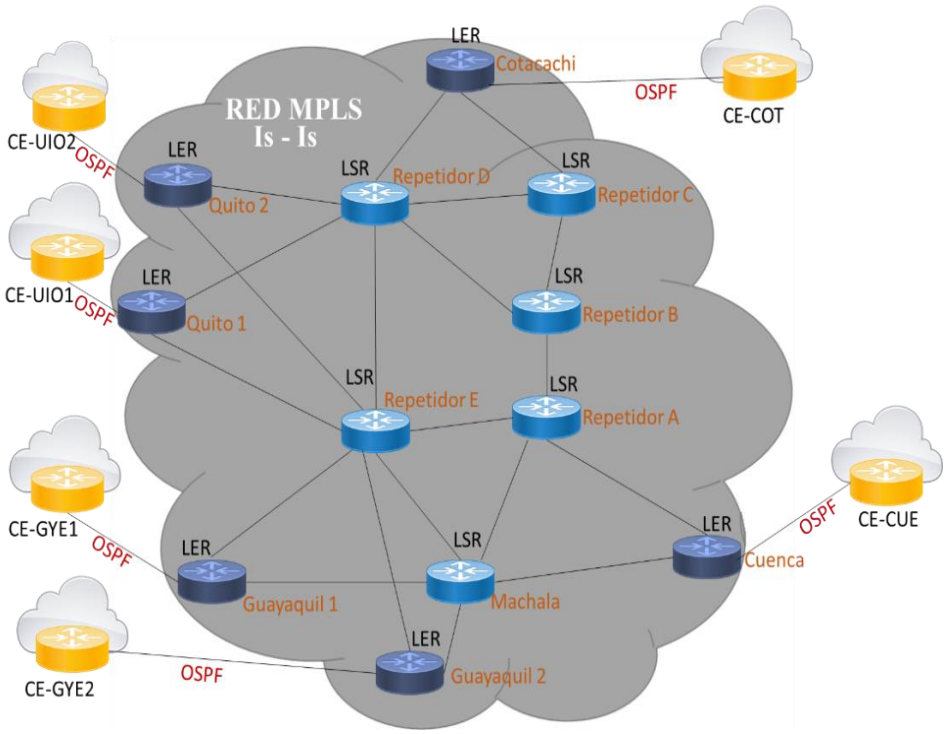
Dentro de los aspectos relevantes de la red, se deben considerar los requerimientos del usuario para brindar un buen servicio basados en la optimización de recursos como: voz, video y datos. Estableciendo la habilitación rápida de servicios convergentes en la plataforma única dentro de la red.

Es necesario realizar la simplificación de la red, para de esta forma lograr mejorar el servicio al usuario, tomando en cuenta los requerimientos citados anteriormente.

3.1.1.Topología de la red actual

En la figura 3.1 se muestra la forma en la que está la topología de la red de las Fuerzas Armadas a nivel del Ecuador, la red cuenta con routers cisco de la serie 9000 distribuidos de forma jerárquica en las capas de núcleo, distribución y acceso. De acuerdo a su ubicación se dividen en P o LSR para dirigir el tráfico dentro de la red MPLS o en PE o LER si están encargados de la distribución de etiquetas de la red MPLS para llevar los servicios como voz, datos y video a través de todas las unidades militares del Ecuador.

Figura 3.1. Topología de la Red Actual



Representación de la topología física de la red de datos de las Fuerzas Armadas.(Cristhian Apolo & Yuliana Coral, 2016)

3.1.2.Direccionamiento IP

Para el direccionamiento IP usan direcciones privadas de clase A entre los routers dentro de la red, es decir entre el LSR-LSR y el LSR-LER. La red usada para cada

enlace es la 10.64.0.0 con una máscara /30, misma que se describe a continuación en la tabla 3.1:

Tabla 3.1. Direccionamiento actual de la red MPLS de las Fuerzas Armadas.

Número	Nombre del Origen	Dirección IP de Origen	Nombre del Destino	Dirección IP de Destino
1	LSR-REPETIDOR A	10.64.0.33 /30	LSR-REPETIDOR B	10.64.0.34 /30
2	LSR- REPETIDOR B	10.64.0.18 /30	LSR-REPETIDOR C	10.64.0.17 /30
3	LSR- REPETIDOR C	10.64.0.81 /30	LSR-REPETIDOR D	10.64.0.82 /30
4	LSR- REPETIDOR D	10.64.0.37 /30	LSR-REPETIDOR E	10.64.0.38 /30
5	LSR- REPETIDOR E	10.64.0.53 /30	LSR-REPETIDOR A	10.64.0.54 /30
6	LSR- REPETIDOR D	10.64.0.22 /30	LSR-REPETIDOR B	10.64.0.21 /30
7	LSR- REPETIDOR E	10.64.0.45 /30	LSR-MACHALA	10.64.0.46 /30
8	LSR- MACHALA	10.64.0.69 /30	LSR-REPETIDOR A	10.64.0.70 /30
9	LSR- REPETIDOR C	10.64.0.89 /30	LER-COTACACHI	10.64.0.90 /30
10	LSR- REPETIDOR D	10.64.0.2 /30	LER-COTACACHI	10.64.0.1 /30
11	LSR- REPETIDOR D	10.64.0.9 /30	LER-QUITO 2	10.64.0.10 /30
12	LSR- REPETIDOR E	10.64.0.5 /30	LER-QUITO 2	10.64.0.6 /30
13	LSR- REPETIDOR E	10.64.0.73 /30	LER-QUITO 1	10.64.0.74 /30
14	LSR- REPETIDOR D	10.64.0.13 /30	LER-QUITO 1	10.64.0.14 /30
15	LSR- REPETIDOR E	10.64.0.29 /30	LER-GUAYAQUIL1	10.64.0.30 /30
16	LSR- REPETIDOR E	10.64.0.61 /30	LER-GUAYAQUIL2	10.64.0.62 /30
17	LSR- MACHALA	10.64.0.94 /30	LER-GUAYAQUIL1	10.64.0.93 /30
18	LSR- MACHALA	10.64.0.105 /30	LER-GUAYAQUIL2	10.64.0.106/30
19	LSR- REPETIDOR A	10.64.0.117 /30	LER-CUENCA	10.64.0.118/30
20	LSR- MACHALA	10.64.0.78 /30	LER-CUENCA	10.64.0.77 /30

Direcciones IP de la capa núcleo y distribución. Cristhian Apolo & Yuliana Coral.

De igual forma se establece el direccionamiento entre los routers LER en el borde de la red MPLS y los routers CE que están fuera del dominio MPLS, la red usada para cada enlace es la 10.63.0.0 con mascara 30 y se describe a continuación en la tabla 3.2:

Tabla 3.2. Direccionamiento entre routers LER y CE de la red de datos de las Fuerzas Armadas.

Número	Nombre del Origen	Dirección IP de Origen	Nombre del Destino	Dirección IP de Destino
1	LER-QUITO2	10.63.0.9 /30	CE-UIO2	10.63.0.10 /30
2	LER-COTACACHI	10.63.0.21 /30	CE-COT	10.63.0.22 /30
3	LER-QUITO1	10.63.0.17 /30	CE-UIO1	10.63.0.18 /30
4	LER-GUAYAQUIL1	10.63.0.13 /30	CE-GYE1	10.63.0.14 /30
5	LER-GUAYAQUIL2	10.63.0.25 /30	CE-GYE2	10.63.0.26 /30
6	LER-CUENCA	10.63.0.29 /30	CE-CUE	10.63.0.30 /30

Direcciones IP entre LER Y CE. Cristhian Apolo & Yuliana Coral.

Además se usará direcciones loopback para cada router, la red usada para cada dirección loopback es la 10.64.254.0 con una máscara /30, que se describe a continuación en la tabla 3.3:

Tabla 3.3. Direccionamiento LOOPBACK de la red de datos de las Fuerzas Armadas.

Número	Nombre	Dirección IP	Número	Nombre	Dirección IP
1	LSR-REPETIDOR A	10.64.254.1	10	LER-GUAYAQUIL1	10.64.254.55
2	LSR-REPETIDOR B	10.64.254.2	11	LER-GUAYAQUIL2	10.64.254.56
3	LSR-REPETIDOR C	10.64.254.3	12	LER- CUENCA	10.64.254.57
4	LSR-REPETIDOR D	10.64.254.4	13	CE-UIO2	10.64.254.151
5	LSR-REPETIDOR E	10.64.254.5	14	CE-UIO1	10.64.254.152
6	LSR-MACHALA	10.64.254.6	15	CE-COT	10.64.254.153
7	LER-COTACACHI	10.64.254.52	16	CE-GYE1	10.64.254.154
8	LER-QUITO 1	10.64.254.53	17	CE-GYE2	10.64.254.155
9	LER-QUITO 2	10.64.254.54	18	CE-CUE	10.64.254.156

Direcciones IP Loopback. Cristhian Apolo & Yuliana Coral.

3.1.3.Usuarios de la red de datos de las Fuerzas Armadas

Los usuarios de la red de datos de las Fuerzas Armadas están divididos por sectores a lo largo de las diferentes unidades militares en el Ecuador y se describe en la siguiente tabla 3.4:

Tabla 3.4. Número de Usuarios de la red de datos de las Fuerzas Armadas.

Sector	Número de Usuarios
Sector Occidental	45
Sector Central	133
Sector Sur	70
Sector Norte	87
Sector Oriental	35
TOTAL	370

Número de usuarios total y por sectores. Cristhian Apolo & Yuliana Coral.

3.1.4.Equipos de la red actual en las capas de Core, distribución y acceso

A continuación se detallan los modelos y las características de los equipos usados en cada una de las capas de la red jerárquica de las Fuerzas Armadas:

3.1.4.1.Equipo en la capa de Core

Actualmente el equipo usado en la capa de Core es el Cisco ASR de la serie 9000 el cual cuenta con las siguientes características:

- Dispone de interfaces Gigabit Ethernet, 10 Gigabit Ethernet y 100 Gigabit Ethernet.
- Soporta protocolos de enrutamiento como: OSPF, IS-IS, BGP, entre otros.
- Soporta protocolos de capa 2 como VLAN’s.
- Soporta funcionalidades de MPLS, VPN y VRF.
- Soporta calidad de servicio sobre MPLS y señalización RSVP y LDP.
- Soporta IPv6.
- Opciones de alimentación de AC y CC. (Cisco, Cisco ASR 9000 Series Route Switch Processor Data Sheet, 2016)

3.1.4.2.Equipo en la capa de Distribución

Actualmente el equipo usado en la capa de Distribución es el Cisco ASR de la serie 900 el cual cuenta con las siguientes características:

- Dispone de interfaces Ethernet, Fast Ethernet y Gigabit Ethernet
- Soporta protocolos de enrutamiento como: OSPF, IS-IS, BGP.
- Soporta protocolos de capa 2 como VLAN's.
- Soporta funcionalidades de MPLS, VPN y VRF.
- Soporta calidad de servicio sobre MPLS y señalización RSVP y LDP.
- Opciones de alimentación de 110 AC. (Cisco, Cisco ASR 900 Route Switch Processor Data Sheet, 2016)

3.1.4.3.Equipos en la capa de Acceso

Actualmente el equipo usado en la capa de Acceso es el Cisco de la serie 3600 el cual cuenta con las siguientes características: (Resource, 2013)

- Ofrece la capacidad de integrar acceso telefónico y la voz con enrutamiento LAN integrando aplicaciones de multiservicio como voz, video y datos en una sola plataforma. (Resource, 2013)
- Admite variedad de módulos de red y dispone de gran capacidad de configuración.
- Dispone de un soporte avanzado para estándares de voz a través de IP y a través de Frame Relay. (Resource, 2013)
- Dispone del Software Cisco IOS y ofrece características de seguridad, costos reducidos de servicios WAN, soporte de QoS. (Resource, 2013)
- Permite la gestión y monitorización remota mediante SNMP (Simple Network Ma

0nagement Protocol). (Resource, 2013)

- Soporta funcionalidades de LAN virtuales: IGMP, RSVP, PIM, WFQ, SMRP, ISL. (Resource, 2013)

- Permite seguridad en el equipo mediante la autenticación del usuario y el conjunto de características IOS Firewall que solo permiten el tráfico aprobado por la red. (Resource, 2013)

3.1.5.Seguridad de la red

La red de datos de las Fuerzas Armadas consta de dos tipos de seguridades para su red, una se emplea en la capa de distribución, es decir en los equipos LER de la topología MPLS; y la otra es usada específicamente en el aplicativo de Video-Conferencia.

- **Seguridad en la capa de distribución**

La seguridad en la capa de distribución se basa en equipos IPS en cada router LER, su función es la de monitorear el tráfico que cursa por la red, detectar y descartar cualquier tipo de código malicioso como virus, gusanos, spyware entre otros. La segunda función es la de evitar la denegación de servicio mediante el monitoreo del tráfico en sus puertos y detectar patrones anormales de dicho tráfico, en este escenario el puerto es bloqueado.

- **Seguridad en la Video-Conferencia**

La Video-Conferencia utiliza encriptación como mecanismo de protección en cada uno de los terminales de video y tiene las siguientes características:

- El código de encriptación es un algoritmo matemático desarrollado por las Fuerzas Armadas.
- Tiene un número de combinaciones de $1.16x10^{77}$, está formado de 256 bits.
- Cuenta con 24 rondas para el cambio de posición en una matriz de 16 x16.
- Utiliza la misma clave y proceso de codificación y decodificación en el origen y en el destino por lo que es un algoritmo simétrico.
- La clave de des-encriptación está formada por 128 bits.

3.1.6.Enlaces Redundantes

En la red de las Fuerzas Armadas se cuenta con enlaces redundantes los que ayudan a desviar el tráfico de los enlaces principales en caso de colapsar uno de los enlaces o por fallas en los puertos del equipo, de esta forma remplazaría la avería de la red dando solución a problemas de confiabilidad y protegiendo datos vulnerables de la red,

además se puede administrar la carga de tráfico en la red aumentando la capacidad del enlace.

Los enlaces redundantes de la red de las FF.AA cuentan con diferentes características detalladas a continuación:

- Los equipos que conforman la red poseen más de dos enlaces redundantes, que ayudan a evitar colapsos en la red o pérdidas de información.
- Después de la capa de distribución se dispone de enlaces puntuales en la red.
- Los enlaces redundantes de la capa distribución se dirigen a dos equipos diferentes para agilitar la rápida convergencia de la red.
- En los puertos se usa dos tarjetas diferentes, que son previstos por el procesador de puertos de la tarjeta.

3.1.7.Escalabilidad

La escalabilidad de la red de datos de las Fuerzas Armadas se considera en base a las capas que conforman la red, teniendo como prioridad el presupuesto asignado para aumentar la capacidad de los equipos mediante a la escalabilidad de sus usuarios.

- La arquitectura de la Capa Core se encuentra completa, basada en 6 equipos LSR de la marca Cisco ASR 9000.
- La arquitectura de la Capa Distribución dispone de 6 equipos LER de la marca Cisco ASR 900, y tiene una proyección de ampliación de 15 equipos LER, para mejorar el rendimiento de los servicios ofrecidos lo que proporciona mayor escalabilidad a la red.
- La arquitectura de la Capa Acceso se define mediante el aumento del número de usuarios, y consta de 30 equipos Cisco 3600.

3.1.8.Disponibilidad

La disponibilidad de la red de las Fuerzas Armadas está basada en los medios redundantes que dispone la red, donde los anillos de la red constan de más de un nodo o enlaces redundantes para mejorar la confiabilidad de los recursos utilizados por el usuario en el periodo de funcionamiento de la red.

$$\text{Disponibilidad} = \left(\frac{A-B}{A}\right) X100\% \qquad (3.1)$$

Dónde:

A = Horas comprometidas de disponibilidad: 24 x 365 = 8,760 Horas/año.

B = Número de horas fuera de línea (Horas de "caída del sistema" durante el tiempo de disponibilidad comprometido). (Microsoft, 2005)

De esta forma se obtiene una disponibilidad de:

$$\text{Disponibilidad} = \left(\frac{8760 - 0.05}{8760}\right) \text{X}100\% = 99.9994$$

La red tiene una disponibilidad de 99.999% con un tiempo de inactividad o caída del sistema en la red de 5 minutos en un año, donde la prioridad es garantizar los recursos al usuario final de la red, disminuyendo problemas de inaccesibilidad a la red o pérdida de información a usuarios que requieren datos en tiempo real.

3.1.9. VPN's

Los servicios de las Fuerzas Armadas está basado en el uso de las VPN's de capa 3, cuya creación facilita el acceso a la red de las agregadurías militares como son: COMACO, EJÉRCITO, ARMADA a las cuales se provee servicios de voz, video, datos y aplicativos de cada fuerza, que constituyen abonados remotos dentro de la red. Cada VPN se encuentra asociada con una VRF (Ruteo/Renvió Virtual), la VRF proporciona las rutas disponibles de la VPN para acceder desde los sitios de los clientes o CE.

Los routers LER con los CE intercambian información sobre las VPNs a los otros routers LER al usar el protocolo MP-BGP (Multiprotocolo BGP), donde el router LER agrega como prefijo a la dirección IPV4 una cantidad de bits conocido como Router Distinguisher (RD), el valor del RD está asignado por un sub-campo administrador de 2 bytes que contiene el número del sistema autónomo y sub-campo de número determinado por el proveedor de servicio de 4 bytes, los valores de los RD para cada VRF se detallan en la siguiente tabla 3.5:

Tabla 3.5. Valor del Router Distinguisher para las agregadurías militares.

VPN	Router Distinguisher
EJÉRCITO	65100:1001
ARMADA	65100:4001
COMACO	65100:4002

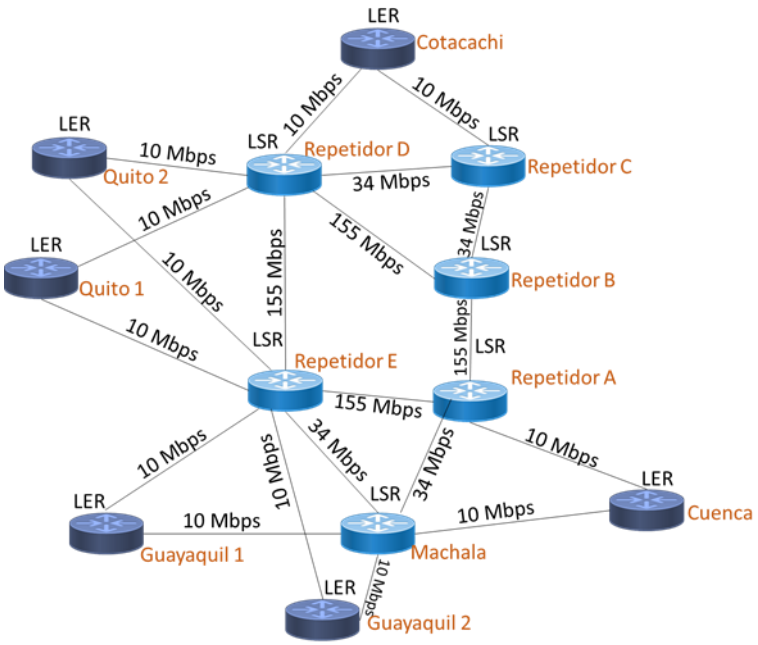
Valor del Router Distinguisher para las agregadurías militares. Cristhian Apolo & Yuliana Coral.

Las VPN's de capa 3 Complejas permite compartir los servicios de un usuario arbitrario con un usuario especifico, sin que el servicio se comparta por otros usuarios dentro de la red. Este tipo de VPN facilita que los usuarios se comuniquen entre si y entre otra VPN dentro de la red. Para la aplicación de este servicio se necesita configurar dos Route Target dentro del RD: import y export con los valores descritos en la tabla anterior para cada VPN.

3.1.10.Capacidad de los enlaces de la red MPLS de las Fuerzas Armadas

Las capacidades de cada enlace en la red MPLS están definidos de acuerdo a la capacidad de las tecnologías de transporte SDH, PDH e IP por anillos usados en las Fuerzas Armadas, y quedan determinados de acuerdo a la figura No. 3.2:

Figura 3.2. Capacidad de los enlaces de la red MPLS de las FF.AA



Representación de la capacidad de los enlaces de la red MPLS de las Fuerzas Armadas. (Cristhian Apolo & Yuliana Coral, 2017).

3.1.11.Calidad de servicio

3.1.11.1.Clasificación y marcaje

La calidad de servicio de la red de datos de las Fuerzas Armadas está determinada dentro del paquete IP con el campo ToS (Tipo de servicio) que permite clasificar y marcar a los diferentes servicios prestados como: voz, datos y video y otorgarle una prioridad de acuerdo a su importancia dentro de la organización, se realiza mediante la diferenciación de servicios DiffServ y de esta manera permitir que los distintos aplicativos de la red puedan ser enviados en un orden de importancia.

Dentro del campo ToS los 3 primeros bits son usados para la precedencia y mediante este valor poder mapear la calidad de servicio dentro de la cabecera MPLS en el campo EXP, el cual al igual que la "precedencia" usa 3 bits. Los 6 primeros bits del campo ToS son denominados DSCP (Diferenciación de servicios por punto de código) el cual indica el tratamiento que debe recibir el paquete dentro de los routers que no forman parte de la red MPLS.

La configuración de los valores para los diferentes tipos de servicio queda determinada por la siguiente tabla 3.6:

Tabla 3.6. Calidad de Servicio.

SERVICIO	PRECEDENCE (PHP)	DIFFSERV CODE POINT (DSCP)	PER HOPE BEHAVIOR (PHB)
Voz	5 (101)	46 (101110)	EF
Video	4 (100)	34 (100010)	AF41
Datos	3 (011)	30 (011110)	AF33

Valores DSCP para la calidad de servicio de las FF.AA. Cristhian Apolo & Yuliana Coral.

3.1.11.2. Administración de la congestión.

Para el control de la congestión se utiliza la técnica CBWFQ y su extensión LLQ para la administración de congestión de servicios en tiempo real de baja latencia, mediante estos métodos se aplican políticas a las interfaces de salida de los routers con el objetivo de garantizar un determinado ancho de banda para cada servicio asignándoles

un porcentaje del ancho de banda del canal los cuales quedan definidos de la siguiente forma como se muestra en la tabla 3.7:

Tabla 3.7. Anchos de banda CBWFQ.

SERVICIO	ANCHO DE BANDA
Voz	20 %
Video	30 %
Datos	10 %

Valores de ancho de banda para la calidad de servicio de las FF.AA. Cristhian Apolo & Yuliana Coral.

3.1.11.3.Prevención de congestión

Para evitar la congestión se aplicaran políticas de tráfico, el cual descartará paquetes que excedan un ancho de banda fijado, esta política será aplicada a los servicios de voz y video, debido a que no tiene sentido encolar paquetes de servicios en tiempo real y se lo hará de acuerdo a los siguientes criterios:

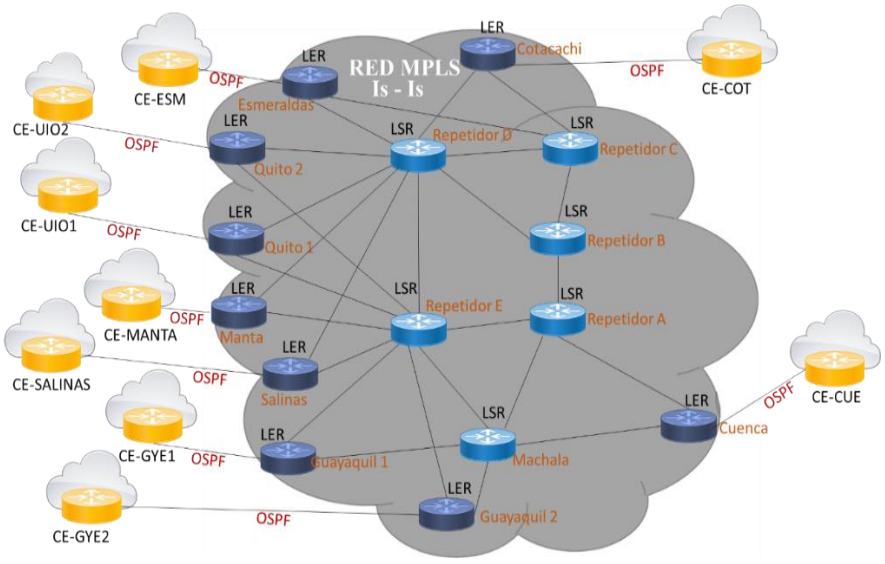
- Para el servicio de voz se aplicará una política a la entrada de la interfaz de los routers que descarte paquetes que excedan el 20% de la capacidad del canal.
- Para el servicio de video se aplicará una política a la entrada de la interfaz de los routers que descarte paquetes que excedan el 30% de la capacidad del canal.

3.2.Diseño

3.2.1.Topología MPLS diseñada

En la figura No. 3.3 se observa la topología de red actual con los equipos LER-Esmeraldas, LER-Manta y LER-Salinas adicionados, debido a que la ruta Quito - Guayaquil es la más congestionada porque son las ciudades con mayor número de comandos operacionales (284). Algunos de ellos son: Brigadas del Ejército, Brigadas de combate de la Fuerza Aérea, Bases Navales, Batallones del Ejército, Capitanías de la Armada y Campamentos militares. Adicionalmente por falta de infraestructura de red, los nodos LER-Guayaquil 1 y 2 reciben tráfico proveniente desde Salinas y Manta al igual que los nodos LER-Quito 1 y 2 los cuales reciben tráfico de Esmeraldas y parte de Manabí. Por estas razones se ha considerado necesario añadir un router en cada provincia mencionada y así disminuir la carga que manejan los nodos Quito y Guayaquil.

Figura 3.3. Topología de red diseñada



Diseño de la topología de red MPLS (Cristhian Apolo & Yuliana Coral, 2017)

3.2.2.Ingeniería de tráfico con rutas explícitas

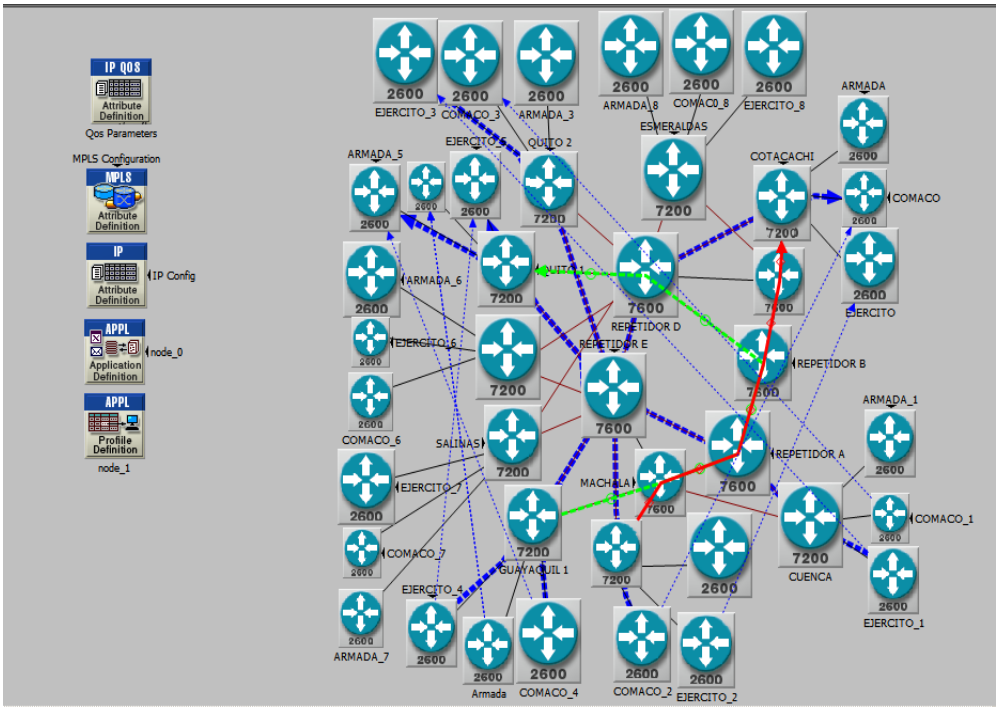
Para la aplicación de ingeniería de tráfico en la red de las Fuerzas Armadas se usó el protocolo RSVP-TE para la creación de túneles LSP usando rutas explícitas, tomando a consideración los siguientes criterios:

- Análisis de la red basada en la simulación en el Software OPNET, en el cual se verificó el tráfico existente en las rutas más utilizadas según la capacidad de los enlaces y las rutas con saturación.
- Basados en la información de las tablas de enrutamiento que el Software OPNET otorga, se pretende mejorar el rendimiento de las rutas al crear los túneles LSP con reserva de recursos para flujo de tráfico y los requisitos establecidos de calidad de servicio en cada VPN.

En la figura No. 3.4 se observa la red diseñada que esta simulada en el Software OPNET, donde se incrementó los routers de Manta, Salinas y Esmeraldas a las cuales se les añadió el tráfico correspondiente de los comandos operacionales. También se observa las rutas más utilizadas en la red (de color azul), con tendencia a saturación del canal, de esta forma facilito la decisión de crear los túneles LSP por rutas no usadas actualmente y por enlaces sin congestión evitando cuellos de botella. Además se detalla la creación de las nuevas rutas en base a los túneles LSP usando el mecanismo de rutas explícitas, dentro del diseño de la red se establecieron 2 túneles que se

diferencia de las rutas anteriores por los colores (rojo, y verde) en los que se enviara el tráfico de la VPN Armada debido a que esta tiene el menor ancho de banda, los túneles siguen caminos adyacentes a los antes establecidos por el protocolo de enrutamiento a los cuales se les proporciona una reservación de recursos.

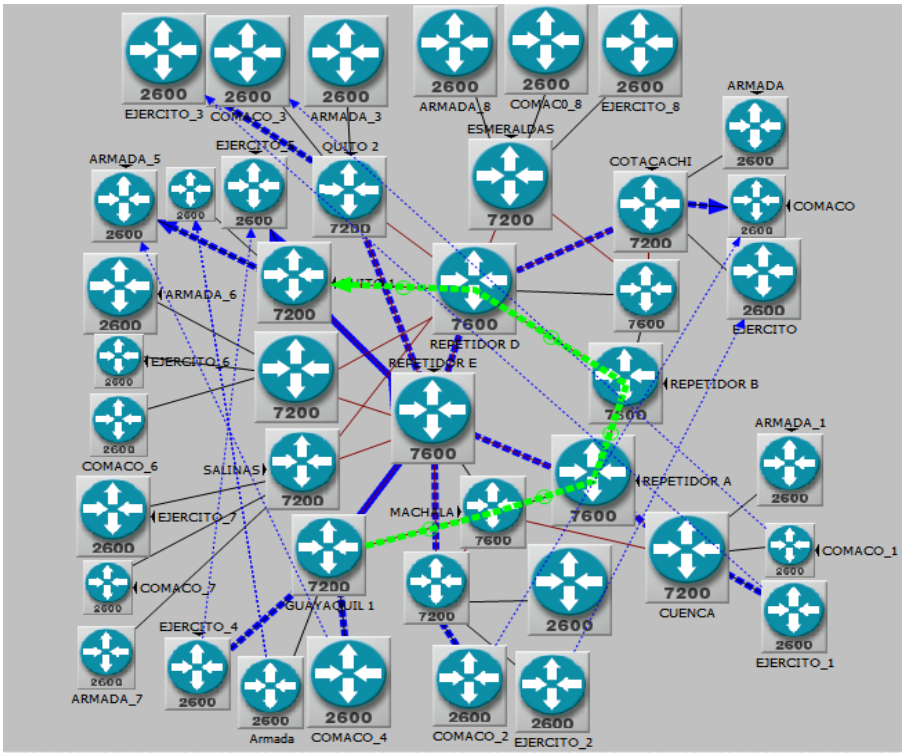
Figura 3.4. Simulación de la topología de la red diseñada



Simulación de la topología de la red diseñada. (Cristhian Apolo & Yuliana Coral, 2017).

Para el análisis de tráfico del diseño propuesto, se procedió a seleccionar la ruta más congestionada que fue Guayaquil1- Quito 1 como se observa en la figura 3.5. Esta ruta tiene mayor congestión en comparación a la ruta de Cotacachi-Guayaquil 2 por ende se aplicó ingeniería de tráfico con rutas explícitas donde se creó el túnel LSP (color verde) que inicia desde el router LER GUAYAQUIL 1 como entrada del túnel y pasa por los routers LSR's de Machala, Repetidor A, Repetidor B, Repetidor D hasta el router LER de salida Quito 1, además se toma a consideración el poco tráfico enviado a través de las rutas subutilizadas y la capacidad de cada enlace, este túnel tiene una reserva de recursos de 3Mbps.

Figura 3.5. Simulación de la red diseñada para la ruta más congestionada



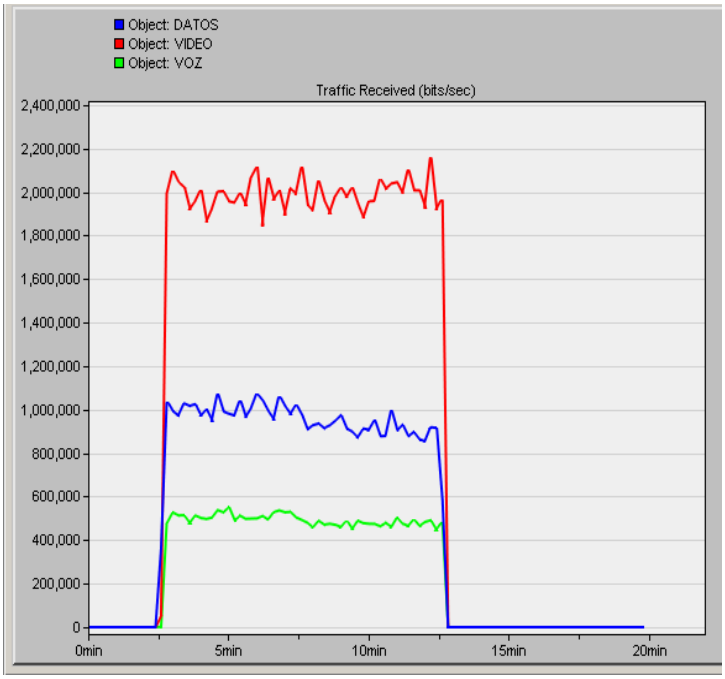
Simulación de la red diseñada para la ruta más congestionada. (Cristhian Apolo & Yuliana Coral, 2017).

3.3.Análisis y resultados del tráfico de la red de datos de las Fuerzas Armadas

Para el análisis y resultados del tráfico en la red actual de las Fuerzas Armadas se necesitó de la configuración de QoS en cada router LER para cada uno de los servicios enviados a los cuales se asignó la prioridad y el ancho de banda de acuerdo a los requerimientos establecidos por el administrador de la red como se observa en la tabla 8. Con el fin de obtener las gráficas se varía el valor del tráfico de acuerdo a la información proporcionada por el administrador de la red. Y en el análisis y resultados del tráfico después del diseño realizado, se compara los tráficos de los servicios antes establecidos en relación a los tráficos de la red sin ingeniería de tráfico.

En la figura No. 3.6 se envía el tráfico de solo una VPN de la red de las Fuerzas Armadas entre el router LER_Guayaquil1-Quito1, donde no existe saturación en el enlace y el tráfico está enviando el ancho de banda establecido.

Figura 3.6. Tráfico de los servicios de la ruta Guayaquil1-Quito1 sin saturación.

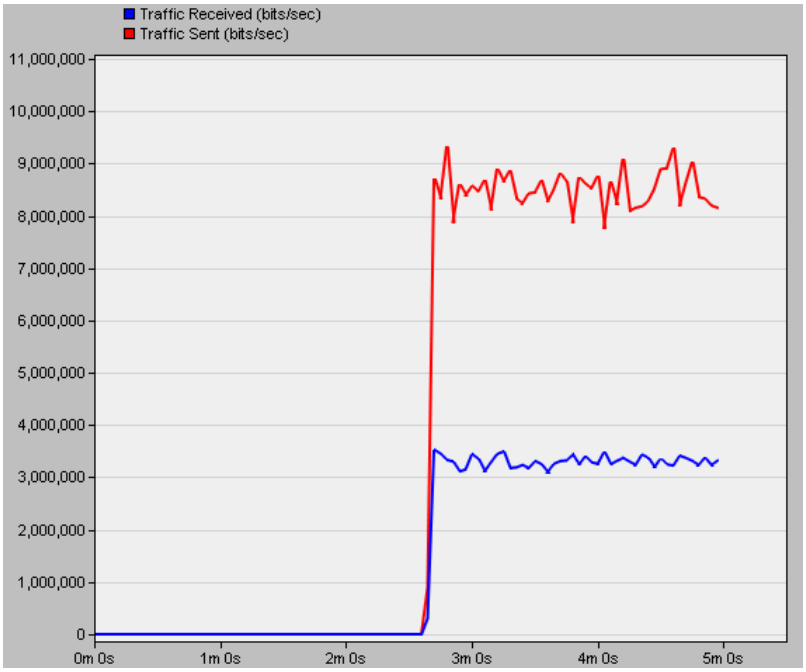


Tráfico de los servicios de la ruta Guayaquil1-Quito1 sin saturación. (Cristhian Apolo & Yuliana Coral, 2016)

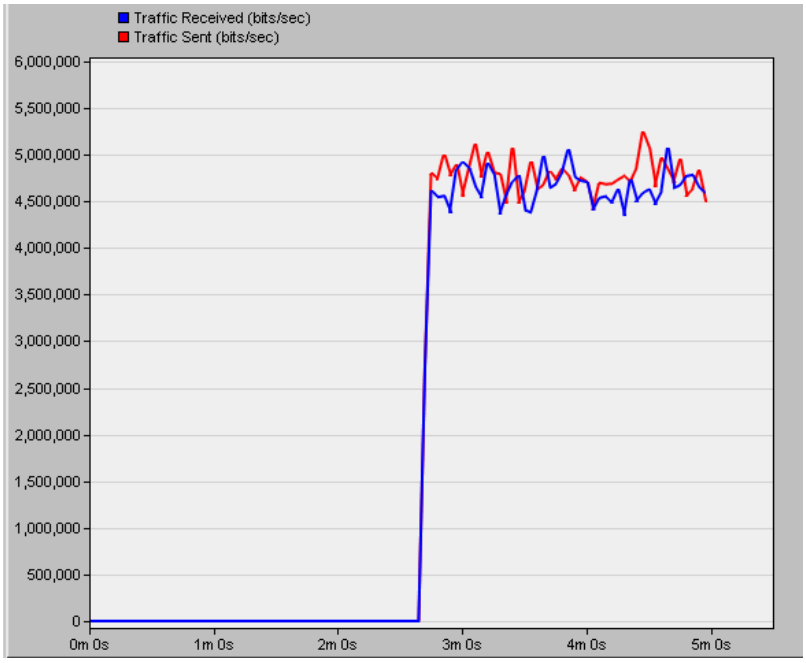
En la figura No. 3.7 se observa el tráfico del servicio de datos (bits/segundos) de la ruta LER_Guayaquil1- Quito1. En el tráfico de la red actual se envían 8.8 Mbps correspondiente a las 3 VPNs y se recibe aproximadamente 3.4 Mbps por ende existe una cierta cantidad de descarte de información. En la figura del tráfico de la red diseñada, en las 2 VPNs más importantes que son: Ejército y COMACO se envían 5Mbps y se recibe la misma cantidad enviada por tanto se demuestra que no existe pérdidas de paquetes. La ingeniería de tráfico configurada en la red mediante la creación de túneles LSP con rutas explícitas ayuda a evitar la pérdida de paquetes de los servicios de voz, video y datos, debido a que se envía por el túnel el tráfico de la VPN Armada que se considera de menor importancia, esto permite reducir la saturación en los enlaces y enviar el tráfico más prioritario por la ruta Guayaquil – Quito. Por lo tanto, la transmisión de datos resulta ser eficiente en comparación a la figura del literal a, donde se tiene una pérdida del 62.5%, por la saturación del enlace de la red actual.

Figura 3.7. Tráfico del servicio datos en (bits/segundos) de la ruta Guayaquil1-Quito1.

a) Red Actual



b) Red Diseñada



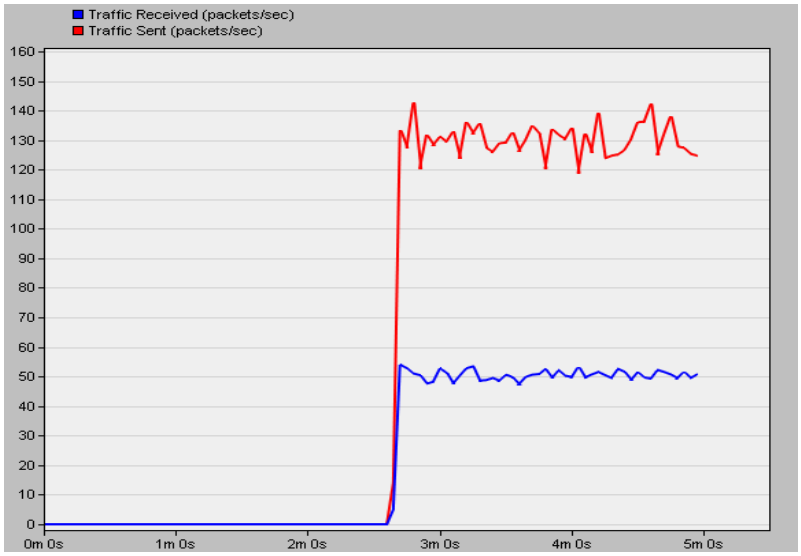
Tráfico del servicio DATOS de la ruta Guayaquil1-Quito1. (Cristhian Apolo & Yuliana Coral, 2017)

En la figura No. 3.8 se observa el tráfico de datos (paquetes/segundos) de la ruta mencionada anteriormente. En la figura del tráfico de la red actual se envían 140

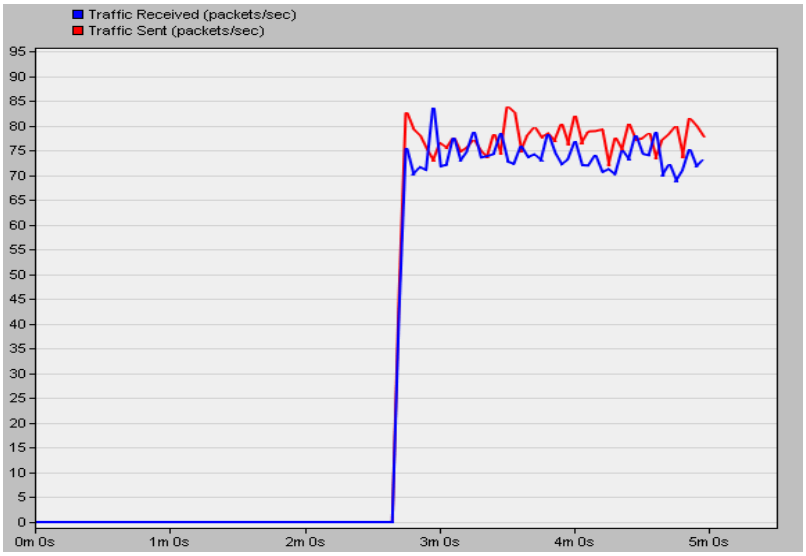
paquetes como tráfico inicial y se reciben 50 paquetes, teniendo un valor de descarte de 60% de paquetes debido al marcaje asignado al servicio por la QoS y a la saturación del canal, en comparación a la figura del literal b en la cual se envían 75 paquetes y se reciben la misma cantidad enviada mediante la ingeniería de tráfico realizada con la creación de túneles LSP para la desviación de tráfico menos prioritario.

Figura 3.8. Tráfico de datos (paquetes/segundos) de la ruta Guayaquil 1-Quito 1.

a) Red Actual



b) Red Diseñada

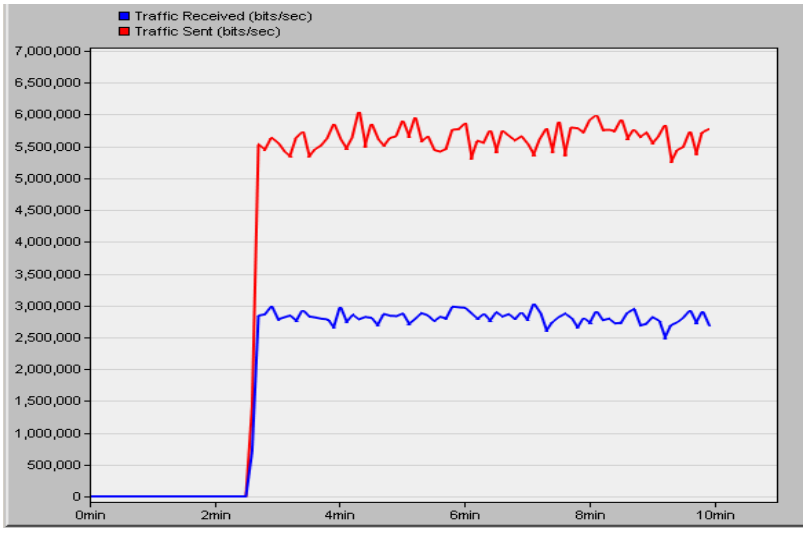


Tráfico del servicio datos en (paquetes/segundos) de la ruta Guayaquil1-Quito1. (Cristhian Apolo & Yuliana Coral, 2017)

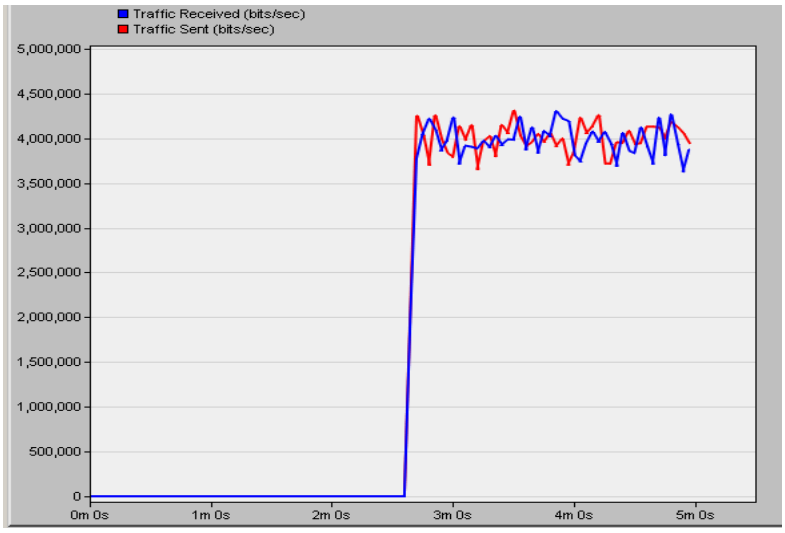
En la figura No. 3.9 se observa el tráfico de video (bits/segundos) enviado en la red actual, mismo que fue de 5.6 Mbps, pero se recibieron aproximadamente la mitad siendo este valor de 2.8 Mbps. En la figura del literal b se observa el tráfico de la red diseñada donde se tiene mayor prioridad en la QoS respecto al servicio de datos y mediante ingeniería de tráfico se demostró que no existen pérdidas, lo cual determinó una entrega óptima de información en el router de destino en comparación al tráfico de la red actual en la cual existe una pérdida del 50% de paquetes, debido a la saturación del canal.

Figura 3.9. Tráfico del servicio de video en (bits/segundos) de la ruta Guayaquil1-Quito1.

a) Red Actual



b) Red Diseñada

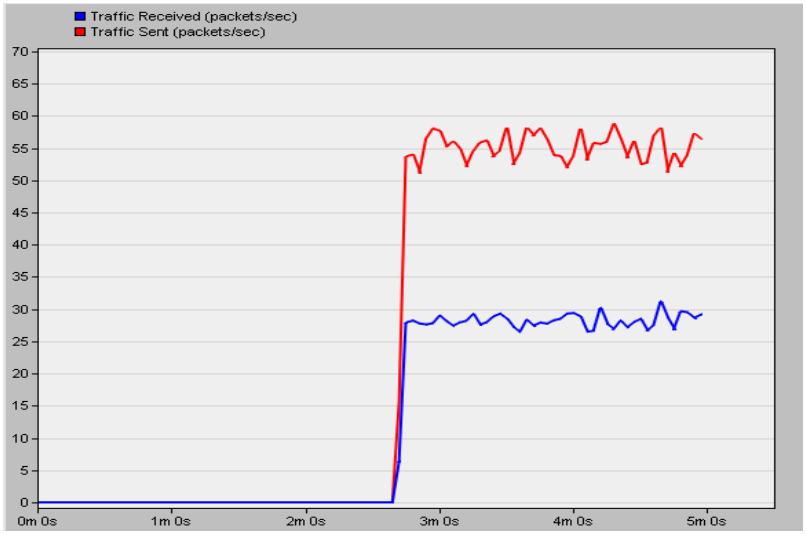


Tráfico del servicio de video en (bits/segundos) de la ruta Guayaquil1-Quito1. (Cristhian Apolo & Yuliana Coral, 2017)

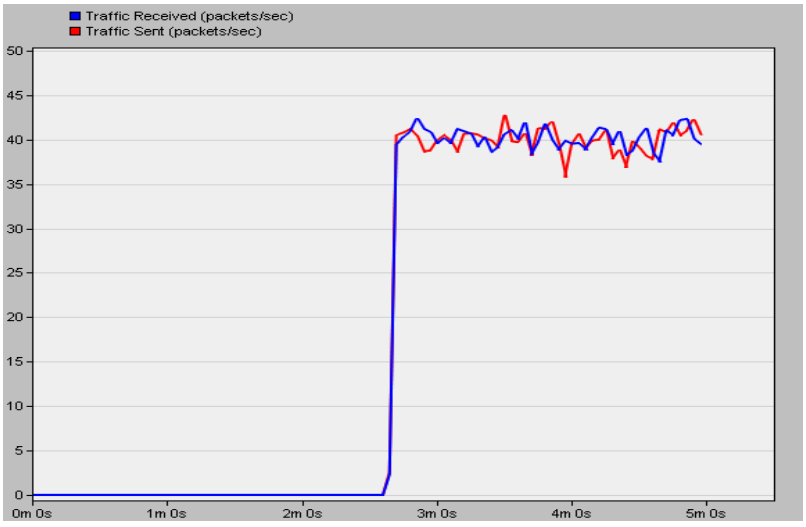
En la figura No. 3.10 se observa el análisis del tráfico de video (paquetes/segundos) enviado de la red inicial y que fue de 55 paquetes y se recibieron aproximadamente 27 paquetes lo que equivale al 50% de pérdidas. En la figura del tráfico de video de la red diseñada, al aplicar ingeniería de tráfico se determina que no existen pérdidas de paquetes por lo tanto recibe y entrega 40 paquetes en toda su transmisión de esta forma se demuestra que existe un bajo nivel de saturación en el enlace en comparación al tráfico de la red actual que descarta la mitad de los paquetes.

Figura 3.10. Tráfico del servicio de video en (paquetes/segundos) de la ruta Guayaquil1-Quito 1.

a) Red Actual



b) Red Diseñada

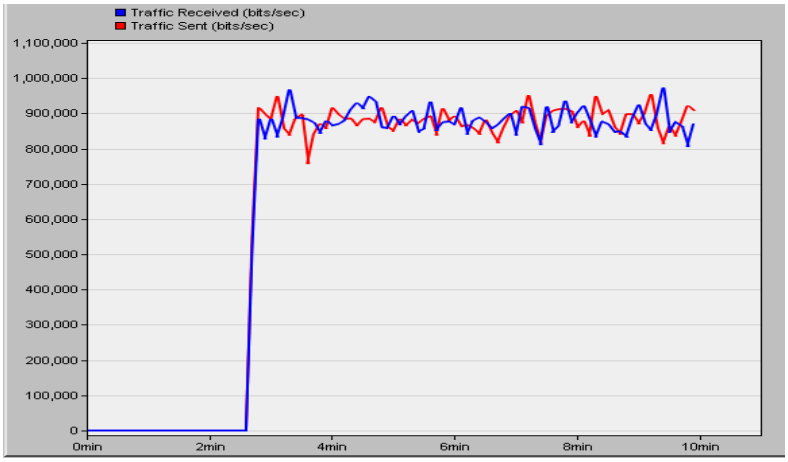


Tráfico del servicio de video en (paquetes/segundos) de la ruta Guayaquil1-Quito1. (Cristhian Apolo & Yuliana Coral, 2017)

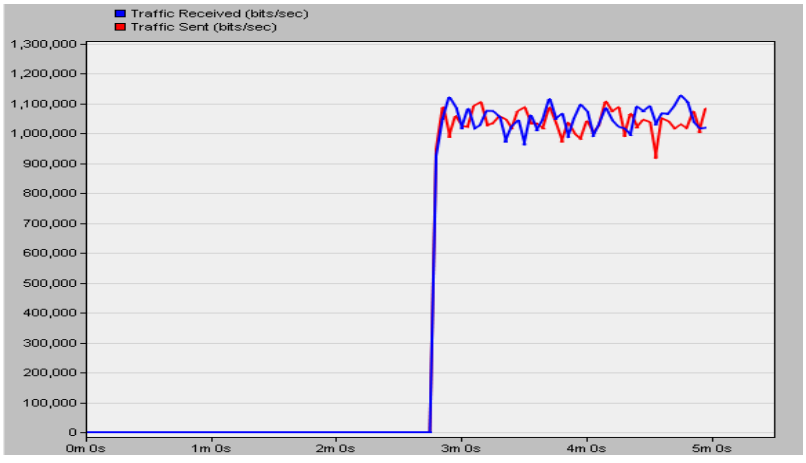
En la figura No. 3.11, la gráfica correspondiente al literal a de la red actual muestra el tráfico de voz en la ruta que va desde el LER-Guayaquil 1 al LER-Quito1, en la cual se puede observar que no existen mayores pérdidas en la transmisión debido a que por ser un servicio importante en las FF. AA. se lo clasifican con una prioridad EF (Expedited Forwarding). El tráfico de voz es bajo, aproximadamente de 900 Kbps por las 3 VPN's usadas en la red de datos de las Fuerzas Armadas. En la gráfica del literal b de la red diseñada se observa el tráfico de voz después de aplicar ingeniería de tráfico. El tráfico observado es de 2 VPN's las cuales son Ejército y COMACO que son de mayor importancia, de igual manera se observa que no existen pérdidas en el servicio aun cuando se mantiene la configuración de calidad de servicio del estado actual de la red.

Figura 3.11. Tráfico de voz (bits/segundos) en la ruta Guayaquil 1-Quito 1.

a) Red Actual



b) Red Diseñada

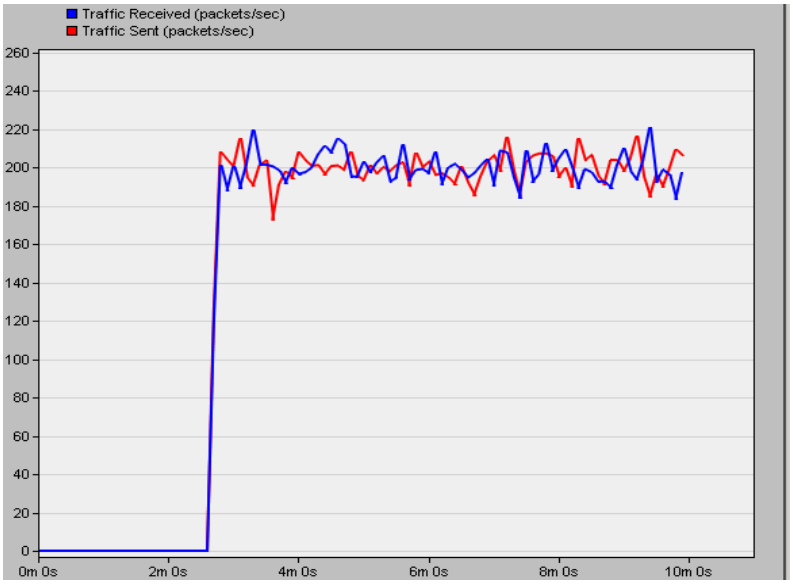


Tráfico de voz en la ruta Guayaquil1-Quito1. (Cristhian Apolo & Yuliana Coral, 2017)

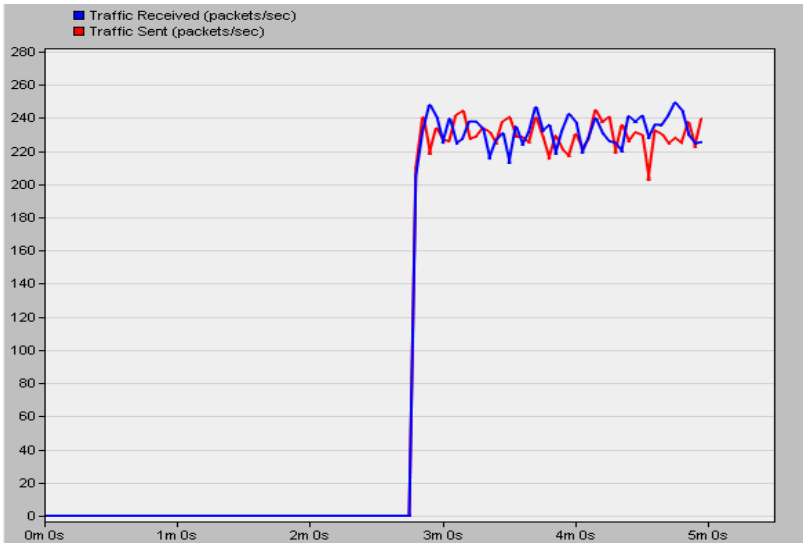
En la figura No. 3.12, la gráfica de la red actual muestra el tráfico de voz (paquetes/segundo), en este servicio se envía 200 paquetes de prueba como tráfico inicial y se recibe el mismo número, lo que significa que no existen pérdidas por tratarse de un servicio crítico y de mayor prioridad. En la gráfica de la red diseñada se observa el tráfico de voz después del diseño, se envían 240 paquetes como tráfico inicial y se recibe la misma cantidad, lo que implica que no existe pérdida en el servicio.

Figura 3.12. Tráfico de voz (paquetes/segundos) en la ruta Guayaquil1-Quito1.

a) Red Actual



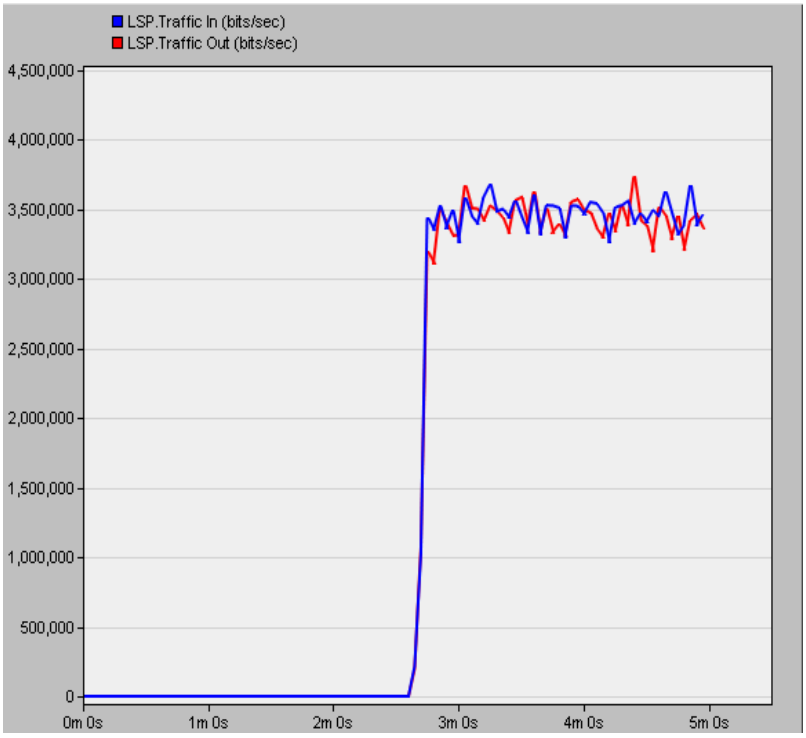
b) Red diseñada



Tráfico de voz (paquetes/segundos) en la ruta Guayaquil1-Quito1. (Cristhian Apolo & Yuliana Coral, 2017)

En la figura No. 3.13 se observa el tráfico enviado a través del túnel de la ruta explicita creada para descongestionar el enlace principal, se ha elegido el tráfico de la VPN Armada para ser dirigido por el túnel debido a que utiliza menor ancho de banda por no tener mayor número de unidades militares que transporten información a través de la red, al garantizarle un ancho de banda al flujo de tráfico de la VPN Armada y por ser un tráfico bajo se observa que no existen pérdidas de información en bits por segundo.

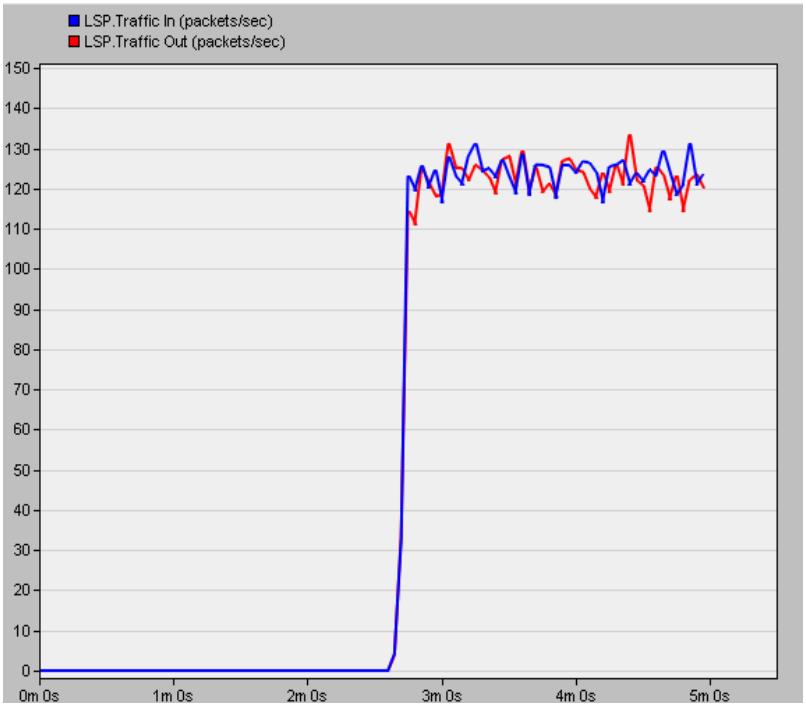
Figura 3.13. Tráfico del LSP (bits/segundos) cursando por el túnel de la ruta explícita.



Tráfico del LSP (bits/segundos) cursando por el túnel de la ruta explícita. (Cristhian Apolo & Yuliana Coral, 2017)

De igual manera en la figura No. 3.14 se aprecia el tráfico enviando por el túnel de ingeniería de tráfico en paquetes por segundo donde se envían aproximadamente 130 paquetes como tráfico inicial y se reciben un valor similar lo que evidencia que no existen pérdidas.

Figura 3.14. Tráfico del LSP (paquetes/segundos) cursando por el túnel de la ruta explicita.



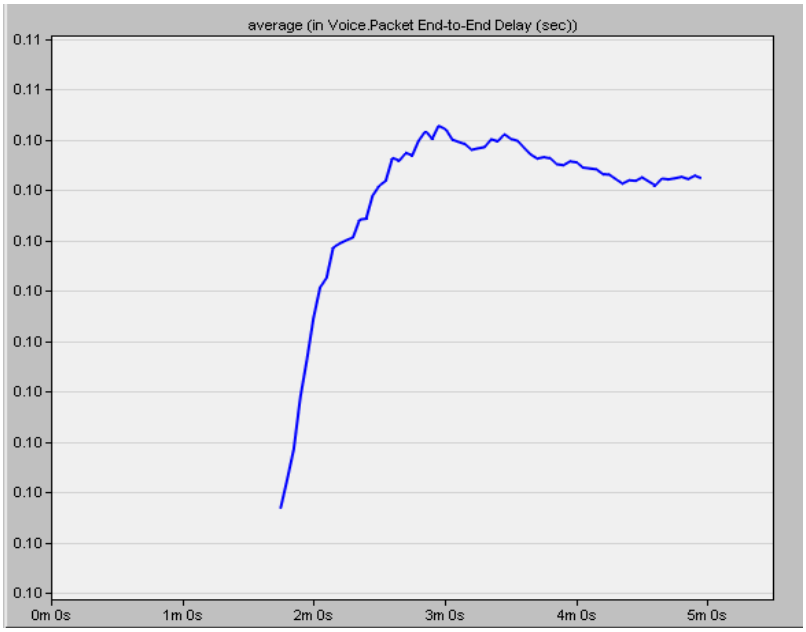
Tráfico del LSP (paquetes/seg) cursando por el túnel de la ruta explicita. (Cristhian Apolo & Yuliana Coral, 2017)

3.3.1.Retardo en los paquetes

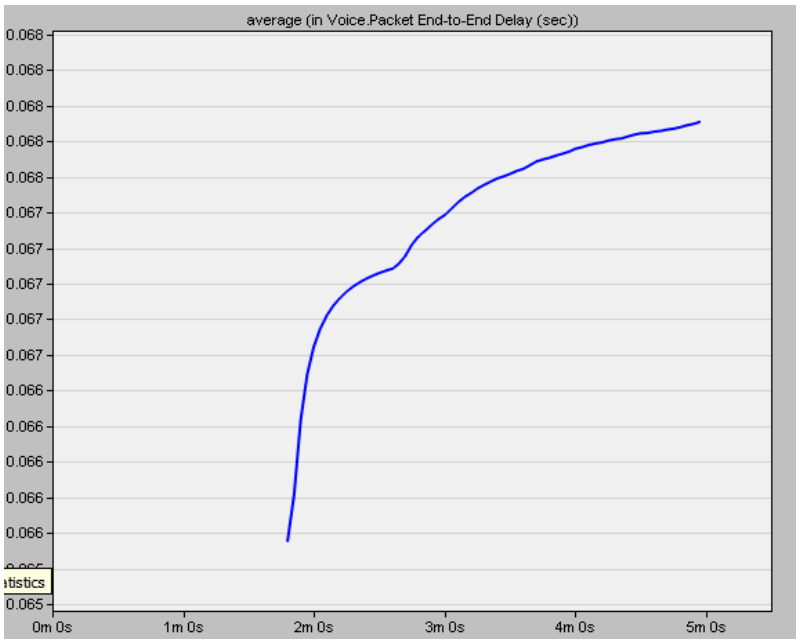
Al tener congestión en la ruta Guayaquil1 - Quito1 de la red de datos de las Fuerzas Armadas. En la figura No. 3.15, la gráfica de la red actual muestra un retardo end-to-end promedio con un valor de 100 milisegundos. El rango tolerable de retardo en la voz es de 0 a 100 milisegundos casi sin percepción entre los interlocutores (Joskowicz, 2013) pasando de los 100 milisegundos el retardo de los paquetes de voz son percibidos cada vez con mayor notoriedad conforme el valor de retardo va aumentando. Al tener un retardo de extremo a extremo de 100 milisegundos era necesario disminuirlo, a través de reducir la congestión en el enlace Guayaquil1- Quito1 mediante la creación de una ruta explicita para el tráfico de la VPN Armada. Se logró la reducción en los retardos de los paquetes de voz y se observa un retardo promedio de 67 milisegundos, que en relación con el retardo del estado actual de la red presenta una mejora de 33 ms y con ello se pudo obtener una transmisión de voz más eficiente.

Figura 3.15. Retardo end-to-end en el servicio de voz.

a) Red actual



b) Red diseñada

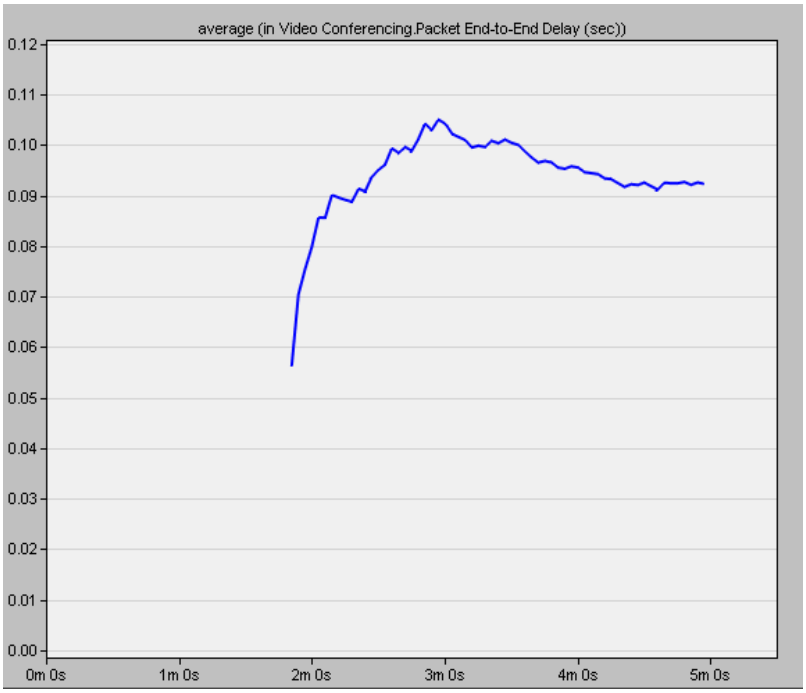


Retardo en el servicio de voz. (Cristhian Apolo & Yuliana Coral, 2017)

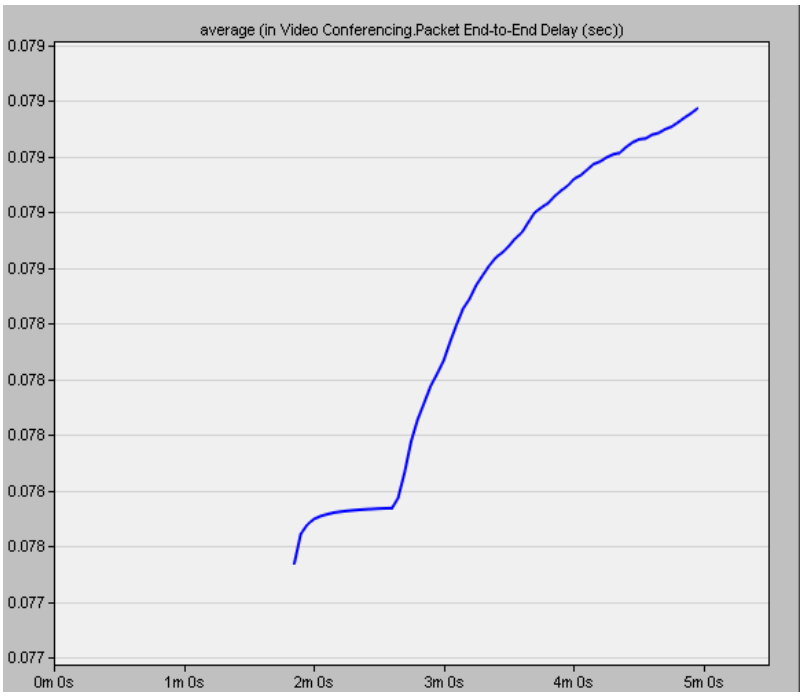
Según el estado inicial de la red, en la figura No. 3.16 se observa el retardo extremo a extremo promedio en el servicio de video cuyo valor pico es de 100 ms y su valor mínimo es de 60ms. En la gráfica de la red diseñada se observa un valor que va de 78 a 79 ms. obteniendo así una mejora de 30 ms con respecto a su valor pico.

Figura 3.16. Retardo end-to-end en el servicio de video.

Red actual



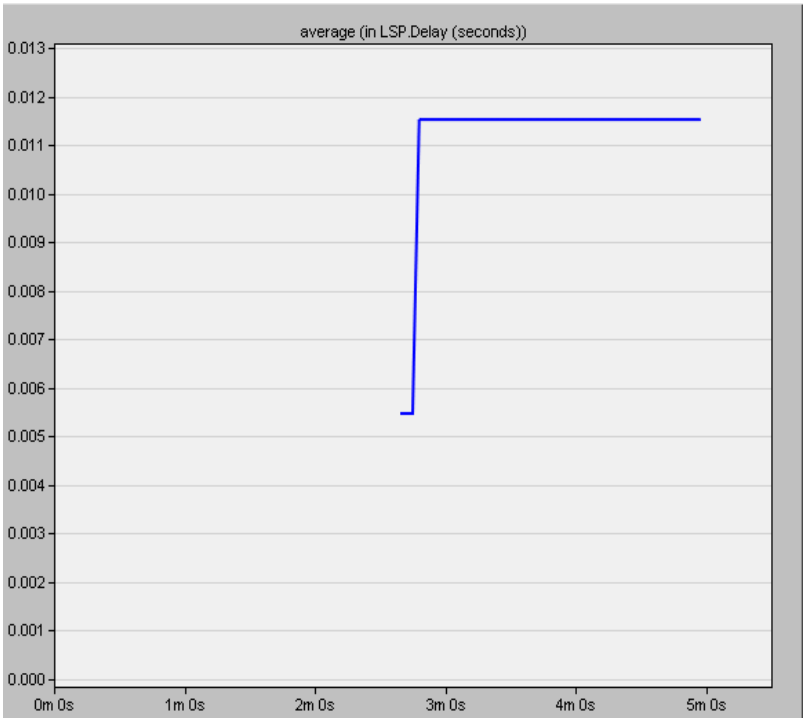
Red diseñada



Retardo en el servicio de video. (Cristhian Apolo & Yuliana Coral, 2016)

En la figura No. 3.17 se aprecia el retardo de los paquetes enviados por el túnel de la ruta explicita, con un valor pico de 11.5 milisegundos el cual no representa un problema para los servicios en tiempo real como la voz o el video.

Figura 3.17. Retardo en el túnel de la ruta explícita.



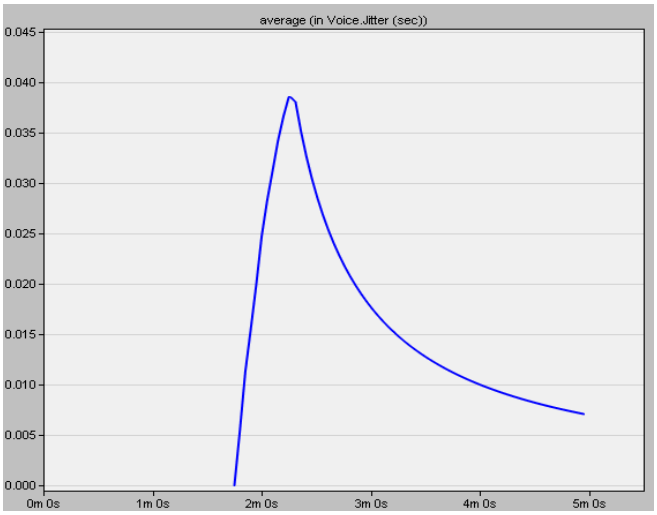
Retardo en la ruta explícita. (Cristhian Apolo & Yuliana Coral, 2017)

3.3.2.Jitter

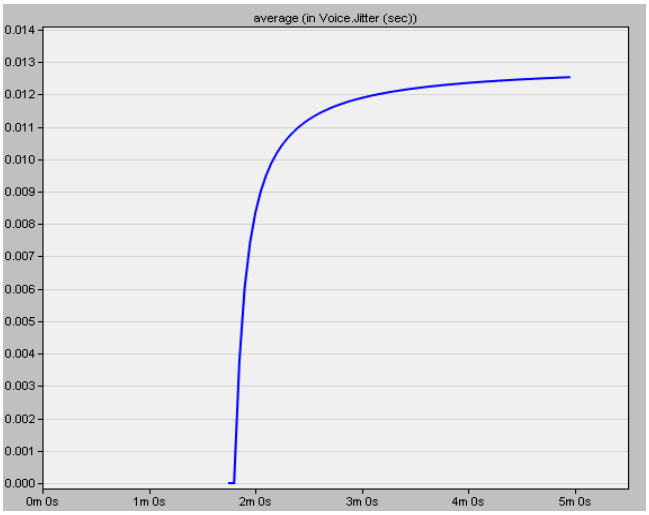
Según el estado inicial de la red, en la figura No. 3.18 se observa la variación de las demoras (Jitter) del servicio de voz con que los paquetes llegan a su destino y se encuentra en un valor máximo de 38 ms. En la gráfica de la red diseñada el jitter se encuentra en un valor máximo constante de 13 milisegundos, presentando una pequeña mejora en el jitter del estado actual de la red con una disminución aproximada de 27 ms.

Figura 3.18. Jitter del servicio de voz.

a) Red actual



b) Red diseñada

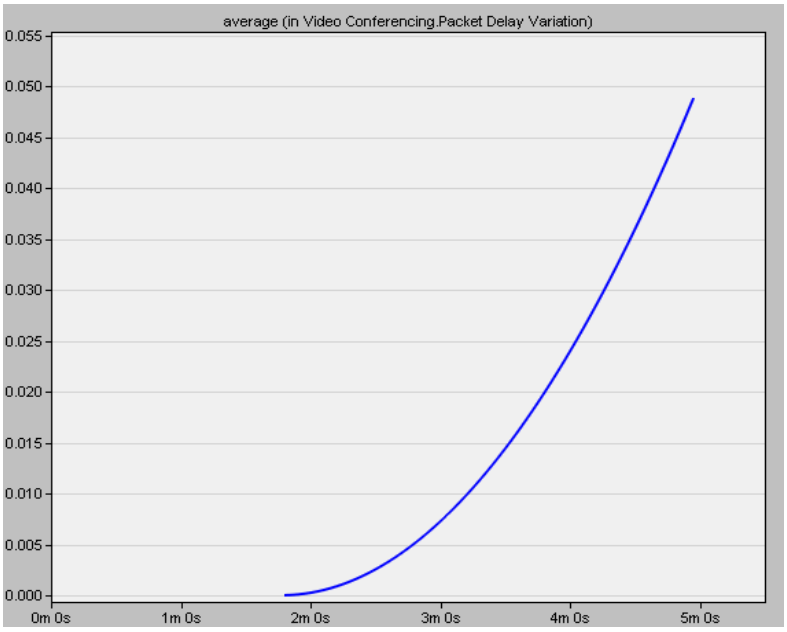


Jitter del servicio de voz. (Cristhian Apolo & Yuliana Coral, 2017)

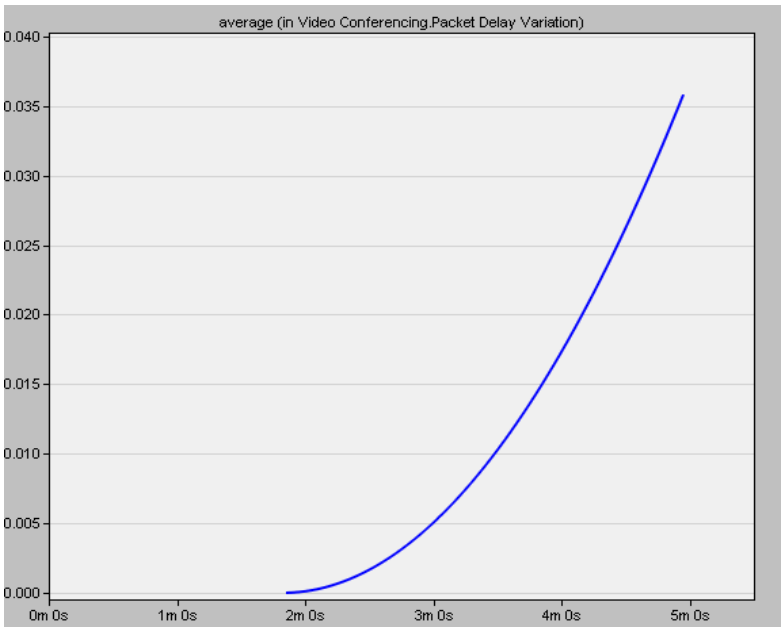
En la figura No. 3.19, se puede observar la gráfica de la red inicial en cuanto el jitter del tráfico de video, que indica un valor mínimo de 5 ms y alcanza a 50 ms en su valor máximo. El jitter de este servicio es aceptable pero debe ser mejorado para compensar el tiempo de llegada de paquetes causada por la congestión de los enlaces de la red. En la gráfica de la red diseñada se observa un valor máximo de 35 milisegundos que significa una reducción aproximada de 15 milisegundos con respecto a la variación del retardo de la red actual.

Figura 3.19. Jitter del servicio de video.

a) Red actual



b) Red diseñada



Jitter del servicio de video. (Cristhian Apolo & Yuliana Coral, 2016)

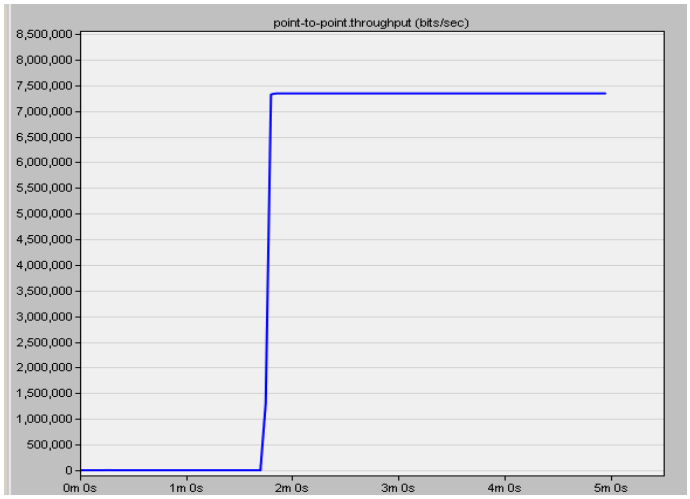
3.3.3.Throughput

En la figura No. 3.20 se observa el flujo de datos máximos o Throughput en el router de Guayaquil 1, donde en la red actual se identifica que el rendimiento decrece notablemente siendo de 7.4Mbps la cantidad de información transferida, en relación a la tasa de información enviada que es de 14.84 Mbps lo que representa un 49.86% del

flujo de transferencia de información real de la red en comparación a la figura del túnel LSP de la VPN Armada, en el cual la cantidad de información transferida en relación a la tasa de información enviada es del 100%, lo que determina que es un enlace eficiente para la transferencia de información real de la red debido a la reserva de recursos establecido para el túnel. En la figura de las 2 VPN's Ejército y COMACO, se identifica que el flujo de datos máximos enviados decrece, siendo de 9.8 Mbps la cantidad de información transferida, en relación a la tasa de información enviada de 9.84 Mbps lo que representa el 100% del flujo de transferencia de información real de la red siendo notable que existe mayor eficiencia en la figura del literal b y c en comparación a la figura del literal a producido por la saturación del enlace.

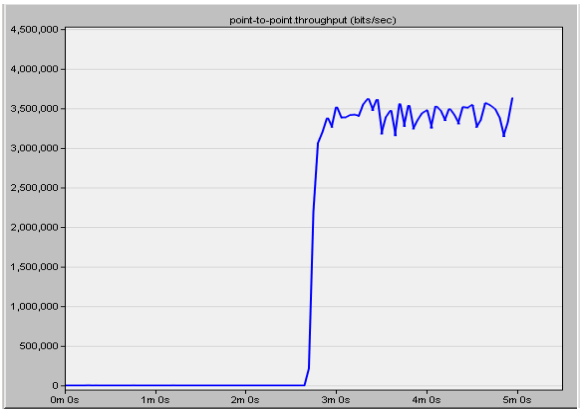
Figura 3. 20. Throughput de la ruta Guayaquil 1- Quito 1.

a) Red Actual

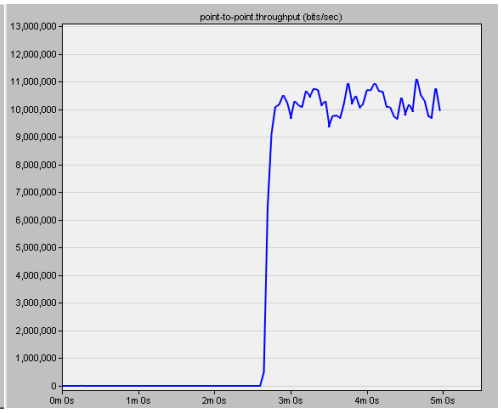


b) Red diseñada

Túnel LSP



2 VPN's Ejército y COMACO



Throughput de la ruta Guayaquil 1- Quito 1. (Cristhian Apolo & Yuliana Coral, 2016)

CAPÍTULO 4
ANÁLISIS DE LA FACTIBILIDAD ECONÓMICA DEL PROYECTO

En este capítulo, se detalla el estudio económico del proyecto técnico para evaluar si el diseño propuesto de la Red de las Fuerzas Armadas genera pérdidas o ganancias dentro de 1 año que es el tiempo considerado en la proyección de la red, así como en la vida útil de los equipos implementados y la actualización de sus modelos. Es necesario establecer la inversión inicial del proyecto y en base a dos herramientas de cálculo que son: el Valor Actual Neto (VAN) y la Tasa Interna de Retorno (TIR) se determina la factibilidad económica del diseño mencionado anteriormente.

4.1.Costos de implementación

Dentro de los costos de implementación del diseño de la red de las Fuerzas Armadas se consideraron los costos de los equipos que fueron utilizados para el diseño de la red y los costos de operación.

4.1.1.Costo de equipamiento

En los costos de equipamiento se detallan los precios de materiales y enlaces a utilizarse dentro de la implementación del diseño en la red de las Fuerzas Armadas como se observa en la tabla 9 de acuerdo con lo descrito en el capítulo tres, el valor de los enlaces se obtuvo en base a información proporcionada por un ingeniero de la empresa Grutel que toma en cuenta todo el equipo para la trasmisión del enlace como las antenas, IDU y ODU respectivamente.

Tabla 4.1. Costos de Equipos y enlaces de interconexión.

Cantidad	**Descripción**	**Modelo**	**Valor Unitario ($)**	**Valor Total ($)**
3	Router Distribución	Cisco ASR-900	48000,00	144000,00
6	Enlaces entre LER y LSR	IP de 10 Mbps	15000,00 (anual)	90000,00
			TOTAL($)	**243000,00**

Costos de Equipos y enlaces de interconexión. (Cristhian Apolo & Yuliana Coral, 2017)

4.1.2.Costos de operación

En la tabla 10, se detallan los costos de instalación y configuración de los equipos usados en el diseño de la red de las Fuerzas Armadas donde se establece un valor unitario para cada sitio de instalación y el costo por mantenimiento de los equipos se basa en el servicio de soporte técnico SMARTNET (Cisco) que facilita la resolución rápida de problemas, capacitación del personal de TI y mitigación de riesgos, los valores de los costos de operación se obtienen por exclusividad del ingeniero de la empresa Grutel que es el encargado de supervisar el estado de la red tomando a consideración el precio emitido por la empresa CISCO para el soporte técnico.

Tabla 4.2. Costos de Operación.

Operación	**Valor Unitario ($)**	**Valor Total ($)**
Instalación y configuración de equipos	5000,00	15000,00
Mantenimiento	7800,00	7800,00
		22800,00

Costos de Operación. (Cristhian Apolo & Yuliana Coral, 2017)

4.1.3.Costo total

En la tabla 11 se detalla el costo total de implementación de la red de las Fuerzas Armadas la cual equivale a la suma de los costos de las tablas 9 y 10 como se detalló anteriormente.

Tabla 4.3. Costo Total de Implementación.

Costos	**Valor Total ($)**
Costos de Equipamiento	234000,00
Costos de Operación	22800,00
	256800,00

Costos de Total de Implementación. (Cristhian Apolo & Yuliana Coral, 2017)

4.2.Beneficios Cuantificables

Para determinar los beneficios cuantificables al aumentar 3 routers LER en la red MPLS se tomará en cuenta el número de unidades militares que se usará en la

infraestructura de red de las Fueras Armadas y que anteriormente se conectaban con otras unidades militares contratando un proveedor de servicios, además tomando en cuenta que se reducirá la carga de tráfico en los routers de Quito y Guayaquil también se podrán añadir más unidades militares que utilicen la infraestructura de red. Se deberá tener en cuenta que se podrá aumentar el tráfico en la red de acuerdo a la capacidad de los enlaces y la infraestructura de red existente que con la ingeniería de tráfico diseñada pueda soportar.

Al añadir más unidades militares a la red MPLS cada una de ellas tendrá un ahorro de 1000 dólares por concepto de la tarifa mensual cancelada a un proveedor de servicio, ello implica que son 25 unidades militares que dejarían de pagar este valor según datos proporcionados por el ingeniero responsable de la administración de la red de las Fuerzas Armadas. En la tabla No. 12 Se detalla el ahorro que tendrán las Unidades militares al dejar de cancelar una tarifa a un proveedor de servicios.

Tabla 4.4. Costo total de ahorro anual.

Concepto de ahorro	**Ahorro mensual por unidad militar (USD)**	**Ahorro anual por unidad militar (USD)**	**Ahorro total anual (USD)**
Pago a un proveedor de internet	1000,00	12000,00	300000,00

Costos totales de ahorro anual por pago a proveedor de servicios. (Cristhian Apolo & Yuliana Coral, 2017)

Además del ahorro por concepto de pago de una tarifa mensual a un proveedor de servicios, al ser una entidad sin fines de lucro, el principal beneficio es la privacidad y seguridad en los datos que se envíen entre diferentes unidades militares al utilizar una infraestructura de red propia y no una propietaria de un proveedor de servicios.

4.3.Cálculo del VAN (Valor Actual Neto)

4.3.1.VAN

El VAN es un indicador financiero usado para la evaluación de proyectos de inversión que calcula los flujos de ingresos y futuros egresos que se obtendrán con el proyecto, lo que facilita evaluar si se obtiene ganancias luego del descuento de la inversión inicial. (Muñoz, 2011) En forma general se lo interpreta de la siguiente manera:

VAN > 0 => Que la empresa genera beneficios, por encima de la rentabilidad exigida. (El proyecto se acepta)

VAN = 0 => No hay beneficio ni pérdidas. (La decisión se basa en el mejor posicionamiento en el mercado

VAN < 0 => hay pérdidas en la empresa. (El proyecto se rechaza)

La fórmula que nos permite el cálculo del Valor Actual Neto es:

$$VAN = -I_0 + \sum_{t=1}^{n} \frac{F_t}{(1+k)^t} \qquad (4.1)$$

En donde:

F_t : Flujos de dinero en cada periodo t (ahorro obtenido en por el pago del servicio proveedor)

I_0 : Inversión realizada en el momento t=0 (costo total para la implementación del diseño de la red)

n : Número de periodos de tiempo (vida útil de los equipos, en nuestro caso es de 1 año)

k : Tipo de interés exigido a la inversión (se considera un interés del 9% que es la tasa de interés fijada por el Banco Central para proyectos del Estado.)

Al remplazar los valores en la ecuación 4.1 se tiene:

$$VAN = -118800{,}00 + \sum_{t=1}^{1} \frac{30000}{(1+0.09)^1}$$

$$VAN = \frac{300000}{(1+0.09)^1} - 256800$$

$$VAN = (275229.4) - 256800$$

$$VAN = \$\,18429\ \ USD$$

Al considerar el resultado del VAN que es mayor a cero, se determina que el proyecto es beneficioso.

4.4.Cálculo del TIR (Tasa Interna de Retorno)

La Tasa Interna de Retorno se le denomina como la tasa de interés en la que se iguala a cero el valor actual neto de una inversión. Este indicador se lo considera aconsejable

cuando es igual o superior a la tasa de descuento del inversor y será de mejor rendimiento obtener un TIR mayor. Cuando el TIR es menor a la tasa de descuento el proyecto no es aconsejable por ende se rechaza. (Muñoz, 2011)

El TIR se lo utiliza para saber si un proyecto es conveniente o no, se lo conoce también como indicador de rentabilidad relativa del proyecto, para representar la tasa de descuento que genera el VAN al igualar a cero siendo lo que el inversionista paga sin pérdidas. (Muñoz, 2011)

El cálculo del TIR se lo puede calcular con la siguiente fórmula:

$$VAN = -I_0 + \sum_{t=1}^{n} \frac{F_t}{(1+TIR)^t} = 0 \quad (4.2)$$

En donde:

VAN: Valor actual neto para el cálculo del TIR.

F_t : Flujos de dinero en cada período t (ahorro obtenido en por el pago del servicio proveedor)

I_0 : Inversión realizada en el momento t=0 (costo total para la implementación del diseño de la red)

n : Número de períodos de tiempo (vida útil de los equipos, en nuestro caso es de 1 año)

Al remplazar los valores en la ecuación 4.2 se tiene:

$$\frac{300000}{(1+TIR)^1} = 256800$$

$$\frac{300000}{256800} = (1+TIR)$$

$$1 + TIR = 1.168$$

$$TIR = 1.168 - 1$$

$$TIR_1 = 0.168$$

$$TIR = 17\ \%$$

Este valor indica que el proyecto generara beneficios.

CONCLUSIONES

Al realizar las simulaciones de los enlaces actuales, se pudo verificar que existe mayor saturación en el enlace Quito – Guayaquil lo que causa una importante pérdida de paquetes y problemas de desempeño en la red como bajo rendimiento y retardos elevados, lo cual afecta principalmente a los servicios en tiempo real.

Al aplicar ingeniería de tráfico, se logró reducir la congestión mediante la creación de túneles con rutas alternas obteniendo una mejora del 60% en el tráfico de datos, del 50% en el tráfico de video y el tráfico de voz se mantuvo sin variación referente al tráfico recibido en la ruta Quito –Guayaquil de la red actual.

Al analizar los retardos de la red actual con respecto a la red diseñada se aprecia una mejora importante del 33% en el tráfico de voz, el tráfico de video mejora en 21%, esto debido a la reducción de la congestión en el enlace lo que acorta el tiempo de llegada de paquetes a su destino.

Para los valores de jitter también se observa una disminución con respecto a la red actual debido a la relación directa que tienen con los retardos extremo a extremo, donde la variación del retardo del tráfico de voz mejora en un 70% y para el tráfico de video mejora en 30%, lo que determina una comunicación de voz y video eficiente.

En la factibilidad económica del proyecto se determinó que la empresa obtiene un ahorro de $300000 USD anuales. Al realizar los cálculos de las variables económicas se obtuvo un VAN= $18429 USD y un TIR=17% lo que equivale a que el proyecto generara ahorros después del primer año que es lo adecuado en un proyecto de telecomunicaciones y es favorable para las FF.AA.

RECOMENDACIONES

Para futuros proyectos se recomienda migrar la tecnología de transporte PDH y SDH a una red de Fibra Óptica lo cual permitirá el manejo de mayores cantidades de tráfico confome a los requerimientos de escalabilidad y proyección de tráfico en la red de las Fuerzas Armadas.

Para ampliar la cantidad de dispositivos que se utilizan en una red MPLS y facilitar la interacción con nuevas tecnologías de transporte, se recomienda usar el protocolo GMPLS que facilitará la obtención de mayores velocidades en la transimisión de información.

Sería importante realizar una capacitación técnica al personal técnico de la dirección de telecomunicaciones de las Fuerzas Armadas para dar a conocer los beneficios de implementar ingeniería de tráfico en la red MPLS y usar el presente trabajo como referencia.

LISTA DE REFERENCIAS

ACENS. (08 de Febrero de 2005). *ACENS THE CLOUD SERVICES COMPANY*. Obtenido de http://www.acens.com/articulos/la-tecnologia-mpls-al-servicio-de-las-redes-privadas/

Boris Salas, J. C. (2012). *ANÁLISIS, DISEÑO DE UNA RED MPLS CON IPV6 EN LAS UTICS DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO.* Sangolquí.

Calderon, M. (27 de Mayo de 2003). *Control de congestión*. Obtenido de http://www.it.uc3m.es/~maria/asignaturas/rysc1/alumnos/05-Congestion.pdf

Cisco. (24 de marzo de 2016). *Cisco ASR 900 Route Switch Processor Data Sheet*. Obtenido de http://www.cisco.com/c/en/us/products/collateral/routers/asr-903-series-aggregation-services-routers/data_sheet_c78-715296.html

Cisco. (06 de Mayo de 2016). *Cisco ASR 9000 Series Route Switch Processor Data Sheet*. Obtenido de http://www.cisco.com/c/en/us/products/collateral/routers/asr-9000-series-aggregation-services-routers/data_sheet_c78-500699.html

Danilo Alfonso López Sarmiento, N. Y. (2009). Ingeniería de tráfico en redes de conmutacion de etiquetas. *Revista Visión Electrónica*, 86.

Delfino, A., Rivero, S., & San Martín, M. (Agosto de 2005). *Ingenieria de tráfico en redes MPLS.* Obtenido de http://iie.fing.edu.uy/investigacion/grupos/artes/fce/net-te/Ingenieria_de_Tráfico_en_Redes_MPLS.pdf

Departamento de Ingenieria Telamatica. (Septiembre 2004). *OPNET : Manual de Usuario.*

Garcia, M. O. (2008). *MPLS, El presente de las redes Ip.* UNIVERSIDAD TECNOLOGICA DE PEREIRA, FACULTAD DE INGENIERIAS ELECTRICA, ELECTRONICA, FISICA Y SISTEMAS, Pereira.

Henao, J. S. (2010). *MPLS, GMPLS, ASON.* Obtenido de http://www.tecnologia.technology/wp-content/uploads/2010/06/Caracteristicas_definicion_MPLS_GMPLS_ASON.pdf

Hernández, T. (2015). *Estudio de la ingenieria de tráfico en redes MPLS mediante casos de uso practico con la herramenta VNX*. Obtenido de http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Tatiana_Hernandez_Camacho_2015.pdf

Jiménez M., R. A. (2013). Diseño del Backbone de la red óptica metropolitana con tecnología MPLS para un Proveedor de Servicios de Internet dentro del Distrito Metropolitano de Quito. *Revista Politécnica*, 23-25.

Joskowicz, J. (Aggosto de 2013). *VOZ, VIDEO Y TELEFONIA.* Obtenido de http://iie.fing.edu.uy/ense/asign/ccu/material/docs/Voz%20Video%20y%20Telefonia%20sobre%20IP.pdf

Lorge, F. (2015). *Calidad de servicio 2 IP QoS-MPLS.* Obtenido de http://www.labredes.unlu.edu.ar/sites/www.labredes.unlu.edu.ar/files/site/data/aygr/AyG_Redes_2015_06_QoS2.pdf

Microsoft. (20 de 05 de 2005). *Descripción de la disponibilidad, la confiabilidad y la escalabilidad*. Obtenido de https://technet.microsoft.com/es-es/library/aa996704(v=exchg.65).aspx

Muñoz, M. P. (2011). *VAN y TIR.* Obtenido de Mpuga: www.mpuga.com

Peña, A. G. (2010). *Nivel de desempeño en redes IPV4 con respecto a redes IPV6 con MPLS y RSVP.* Bogotá.

Resource, C. N. (28 de 11 de 2013). *NSRC.* Obtenido de https://nsrc.org/workshops/2015/walc/routing/raw-attachment/wiki/Agenda/04-ISIS-vs-OSPF.pdf

Romero, M. d. (2009). Programa de doctorado informatica industrial. Sevilla, España.

Saavedra, J. (2015). *Diseño de redes Top-Down*. Obtenido de http://www.juancarlossaavedra.me/2015/01/diseno-de-red-con-top-down.html

Saunders, J. (s.f.). *Unidad empresarial de servicios.* Obtenido de ftp://espectrocrom.com/pub/manuales/cisco/pdfs/cisco2620-3620.pdf

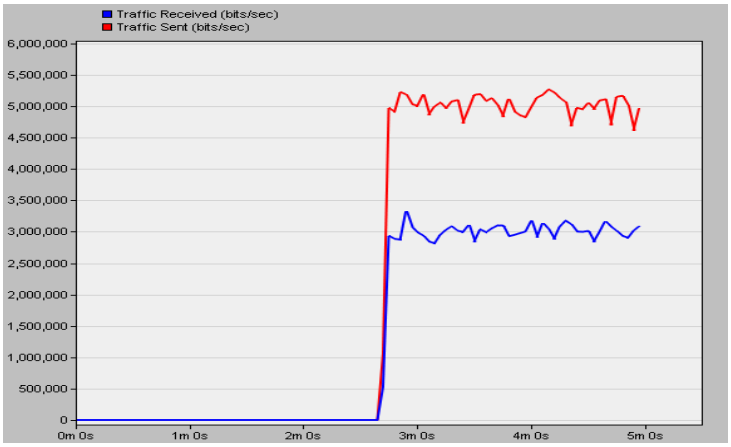
TELECOM PROTOCOL FINDER. (2002). *Guía completa de protocolos de telecomunicaciones.* Madrid: McGRAW-HILL/INTERAMERICANA DE ESPAÑA, S.A.U.

ANEXOS

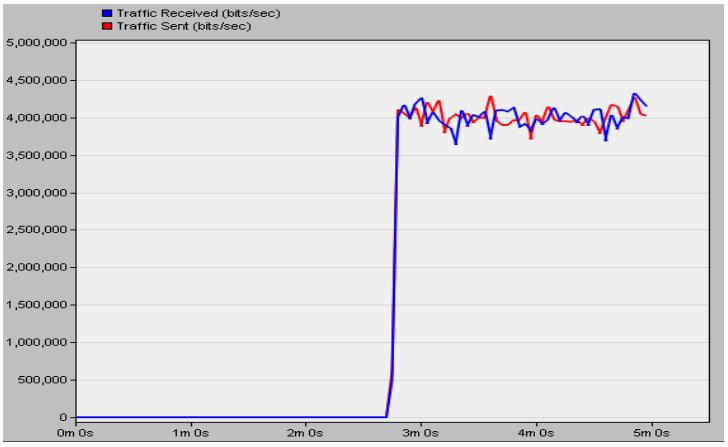
ANEXO 1

Tráfico de datos (bits/segundos) en la ruta Guayaquil 2- Cotacachi.

a) Red Actual



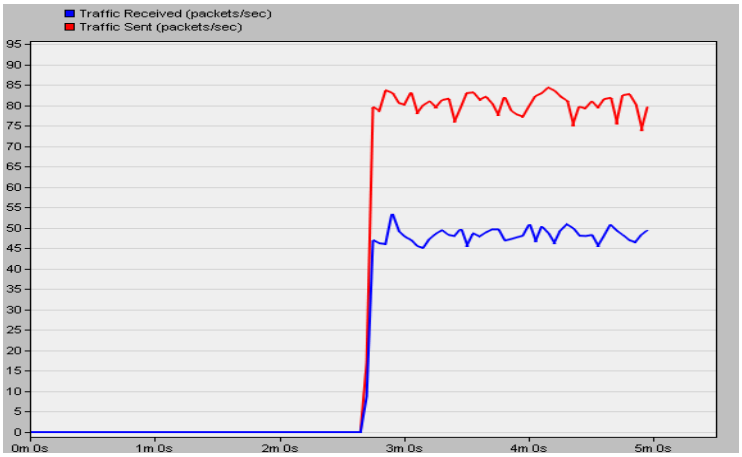
b) Red diseñada



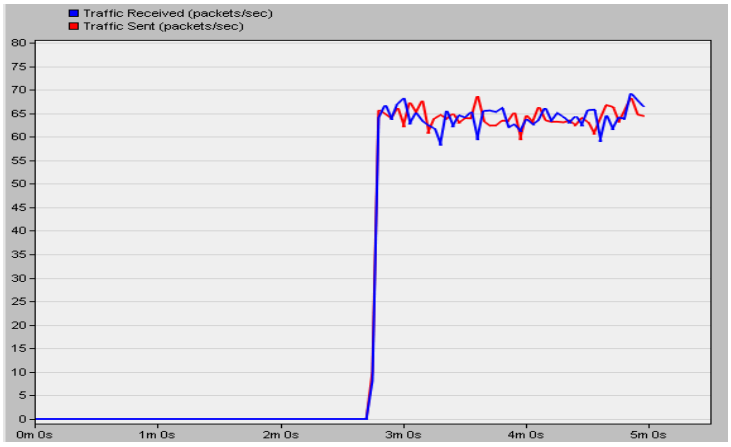
ANEXO 2

Tráfico de datos (paquetes/segundos) en la ruta Guayaquil 2- Cotacachi.

a) Red Actual



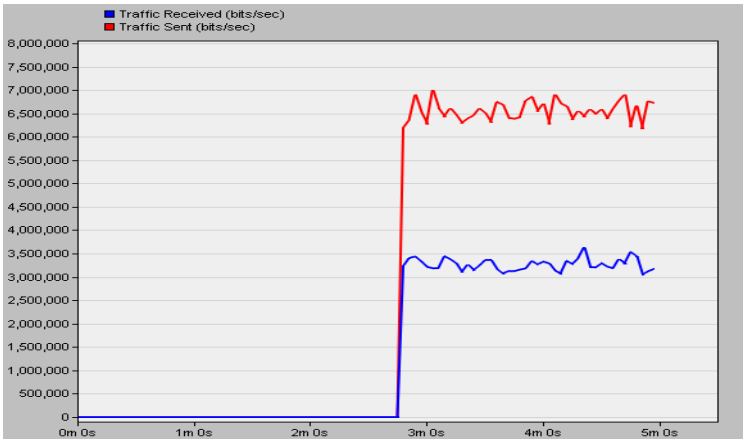
b) Red diseñada



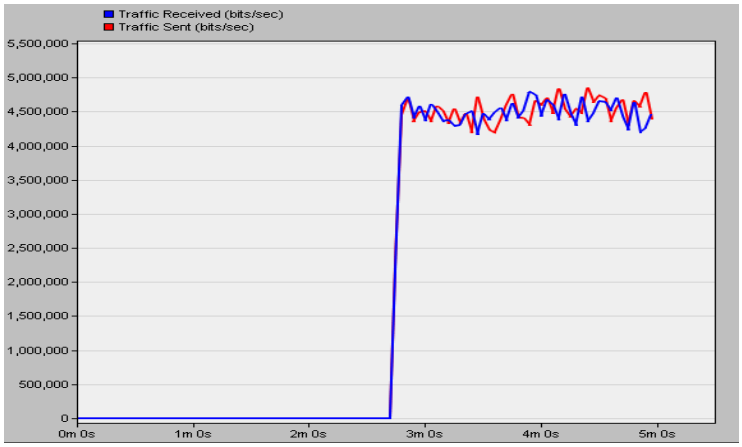
ANEXO 3

Tráfico de video (bits/segundos) en la ruta Guayaquil 2- Cotacachi.

a) Red Actual



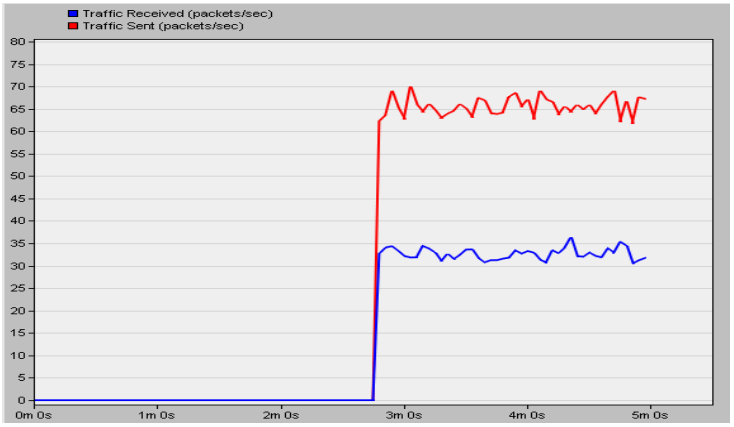
b) Red diseñada



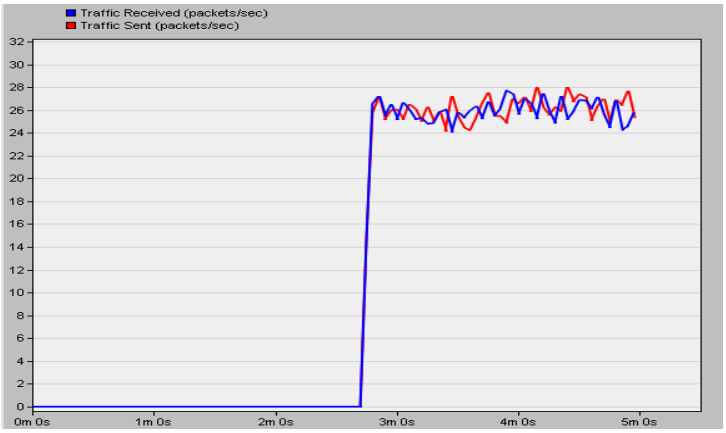
ANEXO 4

Tráfico de video (paquetes/segundos) en la ruta Guayaquil 2- Cotacachi.

a) Red Actual



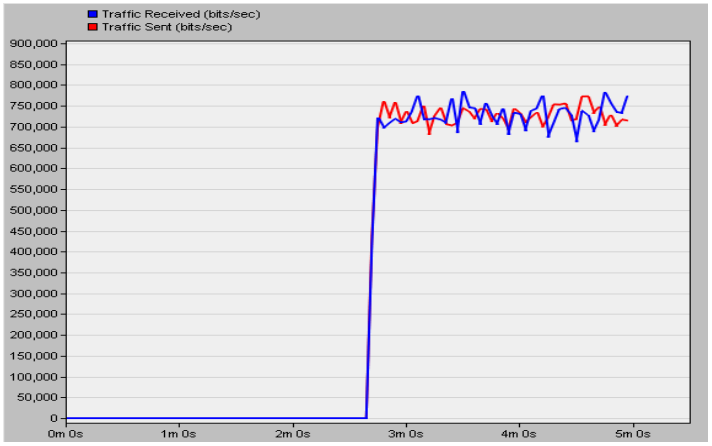
b) Red diseñada



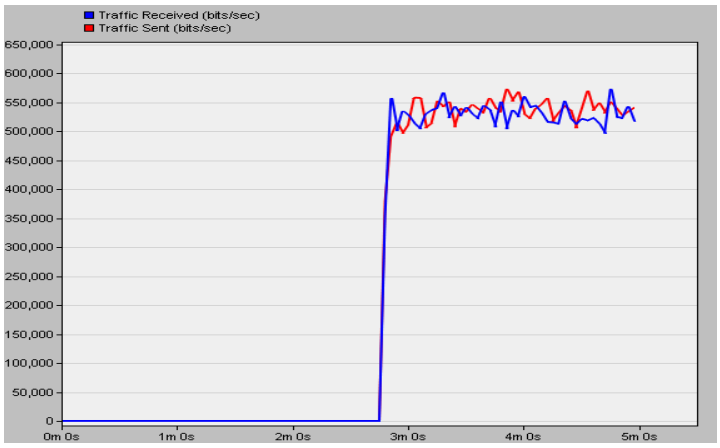
ANEXO 5

Tráfico de voz (bits/segundos) en la ruta Guayaquil 2- Cotacachi.

a) Red Actual



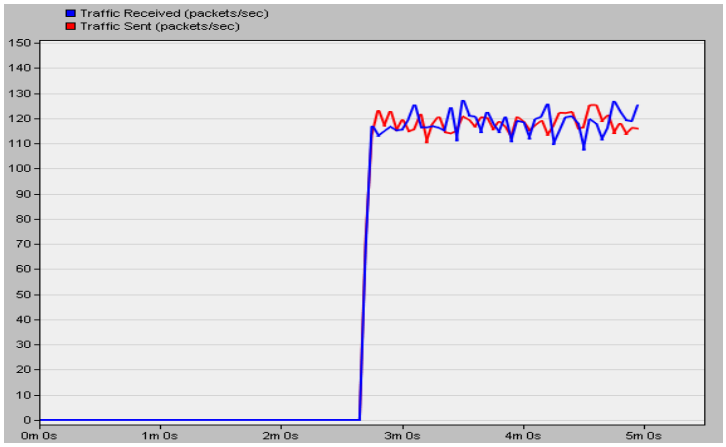
b) Red diseñada



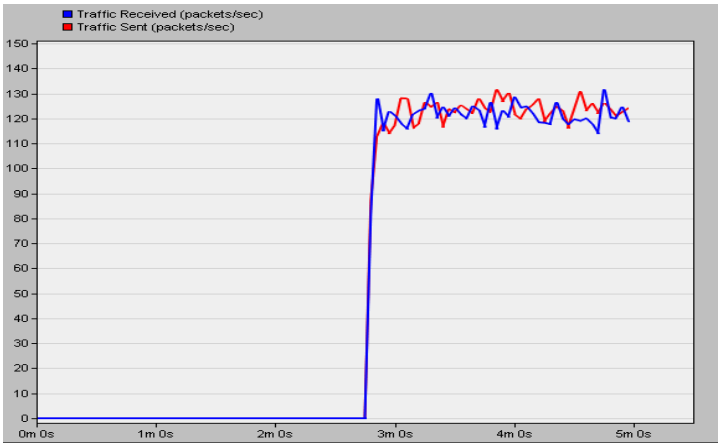
ANEXO 6

Tráfico de voz (paquetes/segundos) en la ruta Guayaquil 2- Cotacachi.

a) Red Actual



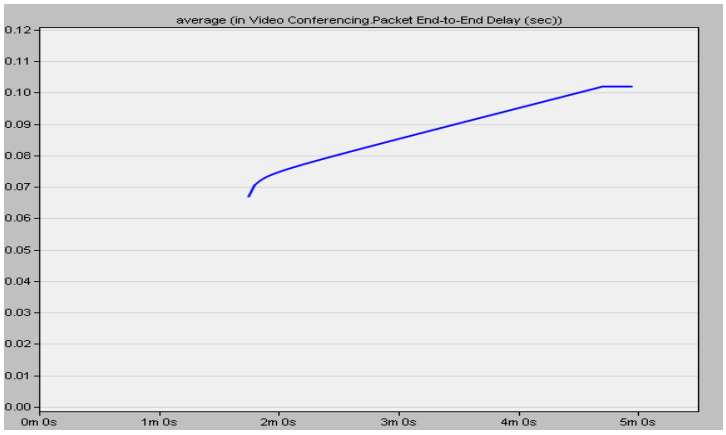
b) Red diseñada



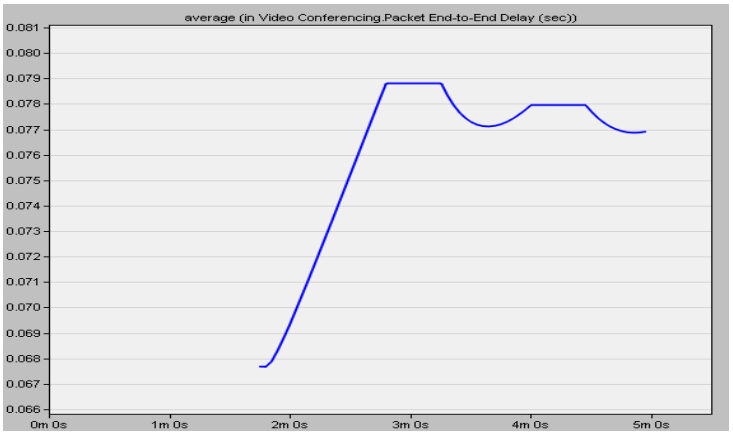
ANEXO 7

Retardo video en la ruta Guayaquil 2- Cotacachi.

a) Red Actual



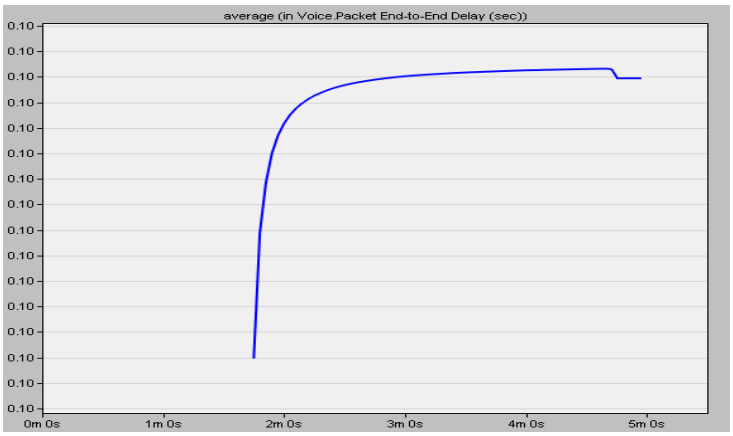
b) Red diseñada



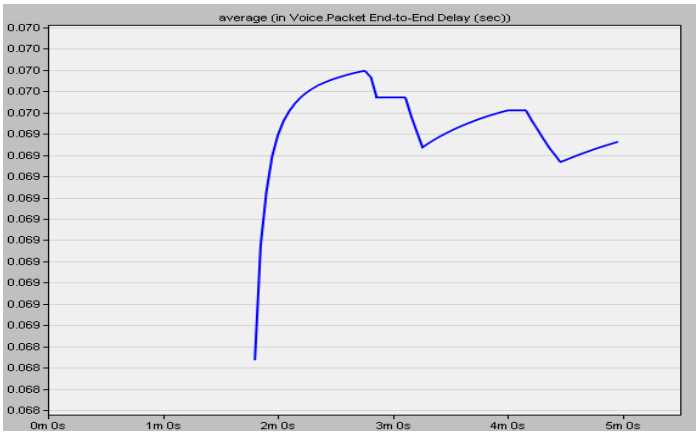
ANEXO 8

Retardo voz en la ruta Guayaquil 2- Cotacachi.

a) Red Actual



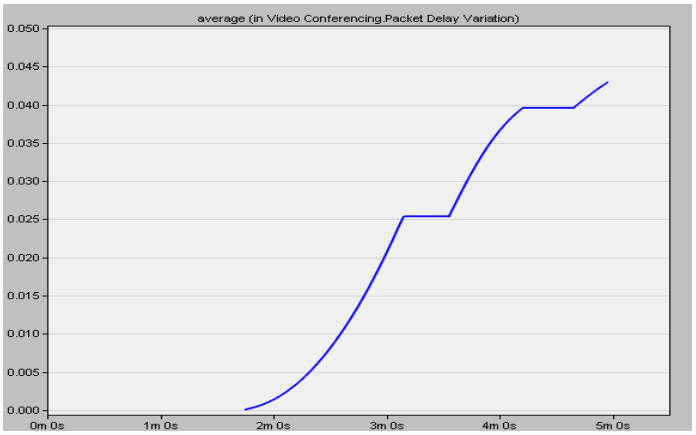
b) Red diseñada



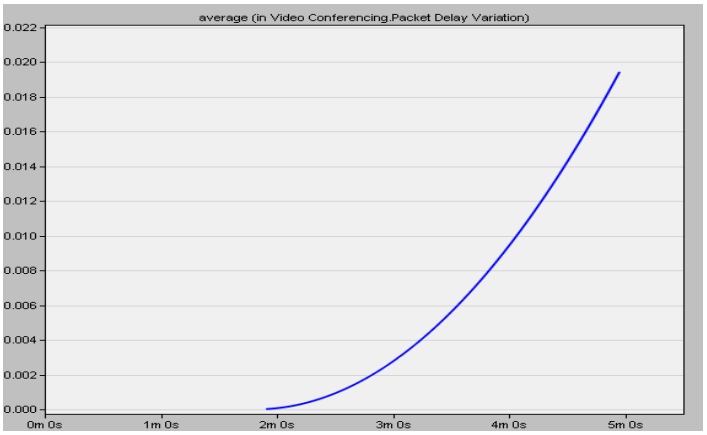
ANEXO 9

Jitter video en la ruta Guayaquil 2- Cotacachi.

a) Red Actual



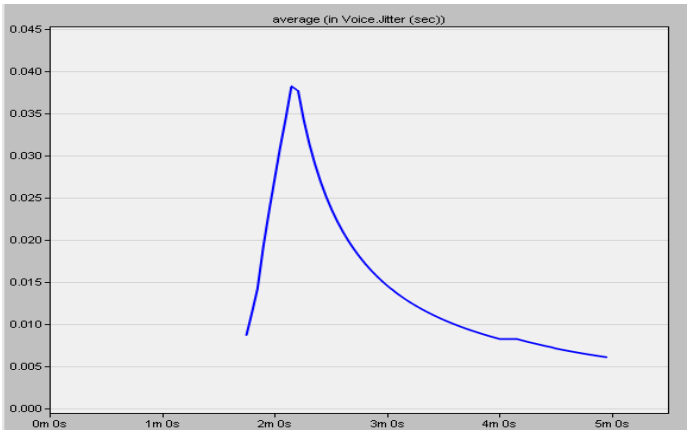
b) Red diseñada



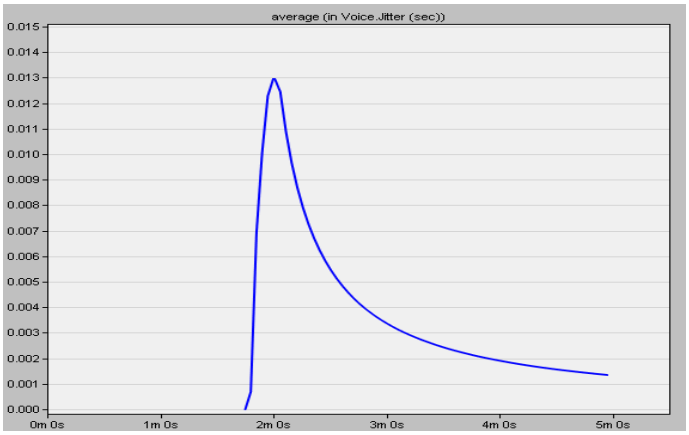
ANEXO 10

Jitter voz en la ruta Guayaquil 2- Cotacachi.

a) Red Actual



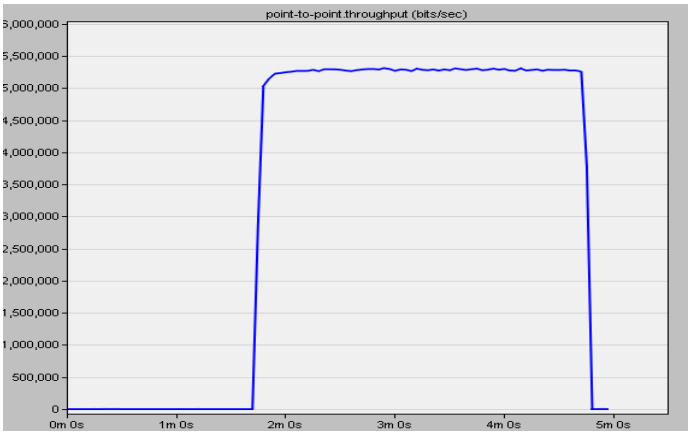
b) Red diseñada



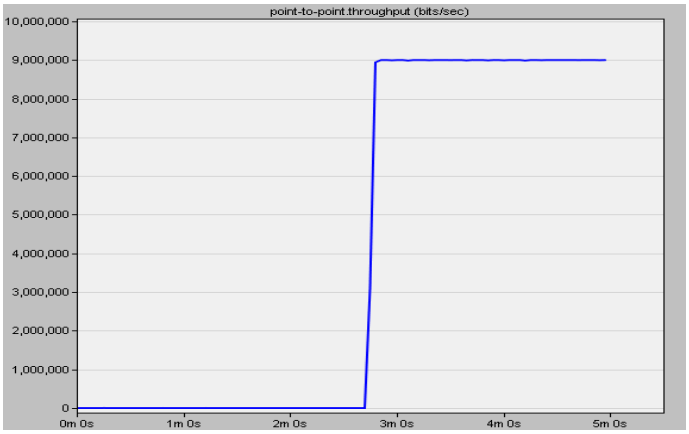
ANEXO 11

Throughput de la ruta Guayaquil 2- Cotacachi.

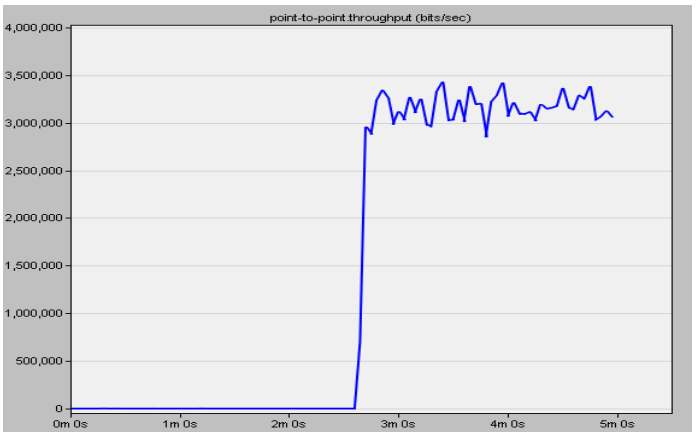
a) Red Actual



b) 2 VPN's

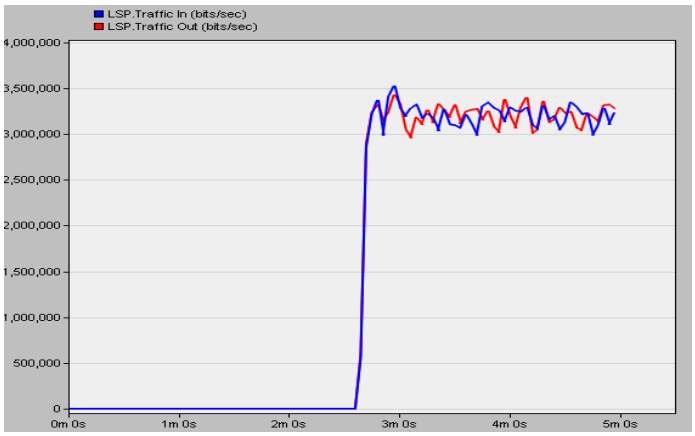


c) Túnel LSP



ANEXO 12

Tráfico del túnel LSP red diseñada



ANEXO 13

Retardo túnel LSP red diseñada