UNIVERSIDAD NACIONAL DE HUANCAVELICA

(Creada por Ley N° 25265)

ESCUELA DE POSGRADO

FACULTAD DE CIENCIAS DE INGENIERÍA

UNIDAD DE POSGRADO

TESIS

MODELO DE RED CON TECNOLOGÍA MPLS PARA LA MEJORA DE LA CALIDAD DE SERVICIO EN LA RED WAN DE LA UNIVERSIDAD NACIONAL DE HUANCAVELICA

LÍNEA DE INVESTIGACIÓN: Desarrollo de aplicaciones en redes avanzadas y protocolos de seguridad

PRESENTADO POR:

Bach. WILLIAM DANTY RAMOS PAUCAR

PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN CIENCIAS DE INGENIERÍA

MENCIÓN:

PLANEACIÓN ESTRATÉGICA Y GESTIÓN EN INGENIERÍA DE PROYECTOS

HUANCAVELICA - PERÚ

2019

UNIVERSIDAD NACIONAL DE HUANCAVELICA

(Creado por Ley N° 25265)

ESCUELA DE POSGRADO

FACULTAD DE CIENCIAS DE INGENIERIA

UNIDAD DE POSGRADO

(APROBADO CON RESOLUCIÓN N° 736-2005-ANR)

"Año de la Lucha Contra la Corrupción e Impunidad"

ACTA DE SUSTENTACIÓN DE TESIS

Ante el Jurado conformado por los docentes: Dr. Javier Francisco MARQUEZ CAMARENA, MSc. Jorge Luis HUERE PEÑA, Mg. Luis Ángel GUERRA MENENDEZ

Asesor (a): Mg. Carlos Alcides ALMIDÓN ORTIZ

De conformidad al Reglamento único de grados y títulos de la Universidad Nacional de Huancavelica, aprobado mediante Resolución Nº 330-2019-CU-UNH y ratificado con Resolución N° 378-2019-CU-UNH.

El candidato al GRADO DE MAESTRO EN CIENCIAS DE INGENIERÍA MENCIÓN EN PLANEACIÓN ESTRATÉGICA Y GESTIÓN EN INGENIERÍA DE PROYECTOS

Don, WILLIAM DANTY RAMOS PAUCAR, procedió a sustentar su trabajo de Investigación titulado "MODELO DE RED CON TECNOLOGÍA MPLS PARA LA MEJORA DE LA CALIDAD DE SERVICIO EN LA RED WAN DE LA UNIVERSIDAD NACIONAL DE HUANCAVELICA".

Luego de haber absuelto las preguntas que le fueron formulados por los Miembros del Jurado, se dio por concluido al ACTO de sustentación, realizándose la deliberación y calificación, resultando:

Con el calificado: APROBADO POR UNANIMIDAD

Y para constancia se extiende la presente ACTA, en la ciudad de Huancavelica, a los veinti seis días del mes de setiembre del año 2019.

Dr. Javier Francisco MARQUEZ CAMARENA
Presidente del Jurado.

MSc. Jorge Luis HUERE PEÑA
Secretario del Jurado

Mg. Luis Ángel GUERRA MENENDEZ
Vocal del Jurado

ASESOR:

Mg. Carlos Alcides ALMIDÓN ORTIZ

DEDICATORIA

El presente trabajo de investigación va dedicado a mi querida madre con amor y cariño por la razón de mi existencia, quien me ilumina indirectamente día a día a fortalecer mis conocimientos.

AGRADECIMIENTO

Expreso mi agradecimiento a los trabajadores de la Dirección de Tecnología de Información y Comunicación de la Universidad Nacional de Huancavelica, por su colaboración con la información requerida para el desarrollo del trabajo de investigación.

A mi asesor de tesis por la orientación y ayuda que me brindó durante la ejecución del trabajo de investigación, y por otro parte a todas las personas que me ayudaron de alguna y otra forma en enriquecer en el tema de investigación.

RESUMEN

El presente trabajo de investigación tuvo como problema el interrogante siguiente: ¿Cómo influye un modelo de red con tecnología *MPLS* en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018?, como objetivo: Determinar la influencia del modelo de red con tecnología *MPLS* en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018, y la hipótesis: Un modelo de red con tecnología *MPLS* influirá significativamente en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018. Se realizó un estudio experimental de Pretest y Postest, de tipo explicativo llevado a cabo en un laboratorio de simulación mediante el software *GNS3* y *D-ITG*, tomando la topología de la red *WAN* de la Universidad. La población está constituida por todas las redes *WAN* de la Universidad, la muestra se consideró las diez redes *WAN* y el muestreo fue de manera no probabilística, en cada red se realizaron las pruebas de calidad de servicio, con los tres tipos de tráfico: datos, voz y video, y para la toma de datos se utilizó la ficha técnica de observación. Se llegó a la siguiente conclusión: Un modelo de red con tecnología *MPLS* influye significativamente en la calidad de servicio en comparación con la tecnología *IP*, porque el valor de P es mayor a 0.05 del nivel significancia, en cado uno de los indicadores.

Palabras Clave: Parámetros de calidad de servicio**,** redes *MPLS*/*VPN*, *VRF*, *BGP*, *OSPF*, *WAN*.

ABSTRACT

The present research work had the following question as a problem: How to influence a network model with MPLS technology in improving the quality of service in the WAN network of the National University of Huancavelica, 2018?, As an objective: To determine the The influence of the network model with MPLS technology is the improvement of the quality of service in the WAN network of the National University of Huancavelica, 2018, and the hypothesis: A network model with MPLS technology influences the improvement of the quality of service in the WAN network of the National University of Huancavelica, 2018. The GNS3 and D-ITG program, at the top of the university's WAN network The population is made up of all the University's WAN networks, the sample shows the networks of networks The local social network of the social network, voice and transmission, and for data collection it is found in the observation data sheet. The following conclusion was reached: A network model with MPLS technology influences the improvement of the quality of service compared to IP technology, because the value of P is greater than 0.05 of the level of significance, in each case indicators.

Keywords: *Quality of service parameters, MPLS / VPN networks, VRF, BGP, OSPF, WAN.*

ÍNDICE

ÍDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE CUADROS

INTRODUCCIÓN

El presente trabajo de investigación tiene como título: Modelo de red con tecnología *MPLS* para la mejora de la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica.

La tesis de grado elaborado tuvo como problema general el interrogante siguiente: ¿Cómo influye un modelo de red con tecnología *MPLS* en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018? y los problemas específicos de la investigación fueron: ¿Cómo influye un modelo de red con tecnología *MPLS* en el *delay* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018?, ¿Cómo influye un modelo de red con tecnología *MPLS* en el *jitter* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018? y ¿Cómo influye un modelo de red con tecnología *MPLS* en la *packet loss* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018?

El objetivo del trabajo de investigación ha sido: Determinar la influencia del modelo de red con tecnología *MPLS* en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018 y los objetivos específicos fueron: Determinar la influencia del modelo de red con tecnología *MPLS* en el *delay* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018, Determinar la influencia del modelo de red con tecnología *MPLS* en el *jitter* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018 y Determinar la influencia del modelo de red con tecnología *MPLS* en la *packet loss* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

La hipótesis general del trabajo de investigación ha sido: Un modelo de red con tecnología *MPLS* influirá en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018 y los hipótesis específicos fueron: Un modelo de red con tecnología *MPLS* influirá significativamente en el *delay* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018, Un modelo red con tecnología *MPLS* influirá significativamente en el *jitter* en la red *WAN* de la Universidad Nacional de

Huancavelica, 2018 y Un modelo red con tecnología *MPLS* influirá significativamente en la *packet loss* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

La estructura del trabajo de investigación está conformada por cuatro capítulos que a continuación se detalla:

Capítulo I: Se desarrolla el planteamiento del problema, la formulación del problema, los objetivos tanto general como específico, así como la justificación e importancia de estudio.

Capítulo II: En este capítulo **s**e desarrolla el marco teórico, los antecedentes de la investigación, las bases teóricas, la formulación de la hipótesis, las definiciones de los términos, la identificación de las variables, así como la operacionalización de las variables.

Capítulo III: Se tomó en consideración la metodología de la investigación, el tipo, nivel, método y diseño de investigación, se determinó la población, muestra y muestreo, las técnicas e instrumentos de recolección de datos, las técnicas de procesamiento y análisis de datos, así como la descripción de la prueba de hipótesis.

Capítulo IV: Está referido a la presentación de los resultados obtenidos, los cuales fueron sometidos a un análisis riguroso con el apoyo del Excel y SPSS, donde se dio el tratamiento, tanto a la estadística descriptiva como inferencial, para luego arribar a la presentación e interpretación de datos, discusión de los resultados, así como el proceso de prueba de hipótesis.

Por último, se señala las conclusiones, recomendaciones, referencias bibliográficas y los anexos respectivos de la presente investigación.

Finalmente: Se le agradece a la Universidad Nacional de Huancavelica por la contribución en mi formación profesional y por otro lado a todas las personas que colaboraron de uno u otra forma en la realización de este trabajo de investigación y especialmente al docente del curso de seminario de tesis.

El investigador

CAPÍTULO I

EL PROBLEMA

1.1. Planteamiento del problema

En el esquema actual la combinación de voz y datos, trabajan en una sola misma plataforma que es insuficiente para los requerimientos de cada tipo o clase de servicio, en donde en una red de internet la transferencia de datos entre los sitios remotos o sucursales de una empresa u organización, se realiza por vía email, web u otras aplicaciones, lo cual origina en una convergencia de voz y datos, con aplicaciones en tiempo real tanto de voz y también de video, un servicio de baja calidad y que necesitan de una eficiente plataforma de trasporte.

"Más de la mitad del tráfico en Internet se corresponden con servicios de streaming de vídeo, ya que la transmisión de contenidos multimedia a través de la red es una de las aplicaciones más demandadas actualmente, que garantizan la calidad en la percepción de los contenidos frente a la gran demanda del servicio es el gran desafío al que se enfrentan los servicios de vídeo *streaming*" (Pozueco, 2014, pág. 3).

En la actualidad el servicio de internet no es confiable en lo que respecta a la entrega de paquetes o en la conectividad. Esto se debe a que el internet actual

está basado en un esquema *Best-Effort* bajo el protocolo IPV4 que se caracteriza por un bajo nivel de rendimiento, que genera la lentitud en la transmisión, tráfico, desconexión y las pérdidas de información, que todo aquello no permite garantizar la calidad de servicio para las nuevas aplicaciones y para el funcionamiento eficiente de la red.

La presencia de cortes del servicio de internet en determinados horarios o intervalos de tiempo, es ocasionado por la cantidad de usuarios que acceden al servicio, que satura el ancho de banda contratado del proveedor de ISP, lo cual origina la aparición del tráfico en exceso por encima del ancho de banda disponible que ocasiona el colapso de la red.

El limitado ancho de banda y la presencia de tráfico en la red, lo cual origina el *packet loss* e incremento de *delay* en el enrutamiento, como consecuencia origina la baja velocidad de transferencia de información, que crea el malestar en los usuarios directos de la red.

En la red tradicional, se puede transportar la convergencia de los servicios como son: voz, video y datos, lo cual requiere mayores recursos de la red para las aplicaciones nuevas que cada vez va apareciendo, por lo que incrementa el flujo del tráfico IP en la red y necesita equipos con mayor capacidad de procesamiento, todo esto ocasiona la pérdida de calidad de servicio y a la vez implica el incremento en el costo, que afecta la economía de la organización o empresa.

La Universidad Nacional de Huancavelica cuenta con seis campus universitarios, ubicados en distintos lugares y provincias de la región Huancavelica, la comunicación entre los campus es a través de correo, web y *VPN*, que todo esto no es suficiente para garantizar la calidad de servicio porque presenta la pérdida de comunicación de las sedes con la sede central. Los servidores de los diferentes servicios internos que cuenta la Universidad se encuentra en la sede central, por lo cual es necesario contar con una red que garantice la calidad de conexión y transporte para realizar los trámites administrativos y académicos entre las sedes correspondientes.

Los problemas que se observa dentro de la Universidad Nacional de Huancavelica es en el acceso a los diferentes servicios que cuenta son: la baja velocidad de navegación de internet con promedio de 1.11Mbps, pérdida de paquetes en un promedio de 15% aproximadamente, alta *delay* de respuesta con un TTL de 185mseg en promedio, alto tráfico (el consumo del ancho de banda asignada a cada sede está en el rango de 80 a 95% en promedio); los cuales generan muchas veces inaccesibilidad a los distintos servicios desde las sedes correspondientes, así mismo, crea incomodidad del personal administrativo y docentes que labora.

En el diagnóstico realizado en la infraestructura de la red de datos, en la ciudad universitaria de Paturpampa, Casa rosada, Sede Lircay, Sede Acobamba y sede Pampas, es necesario realizar un nuevo rediseño o reingeniería en la red de datos, de acuerdo a las nuevas tecnologías existentes para garantizar una red eficiente y de calidad, que responda los nuevos servicios y aplicaciones que va implementando, estos servicios requieren mayores recursos como el ancho de banda y entre otros, todo esto generaría en el futuro un colapso o la caída total de la red, que dejaría incomunicado con todas las sedes.

1.2. Formulación del problema

1.1.1. Problema general

¿Cómo influye un modelo de red con tecnología *MPLS* en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018?

1.1.2. Problemas específicos

a) ¿Cómo influye un modelo de red con tecnología *MPLS* en el ***delay*** en la red *WAN* de la Universidad Nacional de Huancavelica, 2018?

b) ¿Cómo influye un modelo de red con tecnología *MPLS* en el ***jitter*** en la red *WAN* de la Universidad Nacional de Huancavelica, 2018?

c) ¿Cómo influye un modelo de red con tecnología *MPLS* en la ***packet loss*** en la red *WAN* de la Universidad Nacional de Huancavelica, 2018?

1.3. Objetivos

1.3.1. Objetivo general

Determinar la influencia del modelo de red con tecnología *MPLS* en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

1.3.2. Objetivos específicos

a) Determinar la influencia del modelo de red con tecnología *MPLS* en el ***delay*** en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

b) Determinar la influencia del modelo de red con tecnología *MPLS* en el ***jitter*** en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

c) Determinar la influencia del modelo de red con tecnología *MPLS* en la ***packet loss*** en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

1.4. Justificación e importancia

El proyecto de investigación desarrollado encontró su justificación e importancia en los siguientes niveles proposicionales:

1.1.3. Justificación teórica

El proyecto de investigación a emprender expresó su justificación "teórica" en las siguientes proposiciones; "La tecnología *MPLS* es dominante a las Redes privadas virtuales (*VPN*) escalable y a la calidad de servicio *end-to-end* (*QoS*), habilitando la utilización eficiente de las redes existentes para resolver el crecimiento futuro y la corrección rápida del incidente del enlace y de la falla de nodo"(Cisco), "La saturación de los

enlaces de la red de internet, se debe a las aplicaciones masivas disponibles en Internet que tiendan a usar todo el ancho de banda disponible, pues en la definición de IPv4 no se contempló la calidad de servicio, con la implementación masiva a nivel mundial de IPv4" (Velurtas, 2009, pág. 3), es más "La **s**aturación en el ancho de banda de la red**,** es ocasionado por el uso inadecuado de los recursos de una red, lo cual provoca la generación de cuello de botella, que ocasionan que el envío de datos se torne imposible, causando problema en los enlaces de VoIP en la transmisión de la voz y también afectando el trabajo diario de los usuarios en la red" (Abad, 2014, pág. 2), finalmente a todo ello se aúna; "que no se tiene un control de la utilización del recurso ni equidad en la distribución del canal por el cual se tiene acceso a Internet y esto pasa principalmente en los sitios donde varios usuarios usan el recurso al mismo tiempo, ocasionado por la falta de control en la distribución del ancho de banda, en donde los usuarios absorben todo el canal en actividades no permitidas por la organización y a los usuarios que realmente lo necesiten, les quedará muy reducido" (Grajales Bartolo, 2011, pág. 17). Motivo por el cual, el propósito del presente proyecto ha sido; Determinar la influencia del modelo de red con tecnología *MPLS* en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

1.1.4. Justificación práctica

El proyecto de investigación a emprender expresó su justificación "práctica" en el enunciado siguiente; el bajo rendimiento de la red *WAN* entre las sedes de la Universidad Nacional de Huancavelica, tuvo como causa "La baja velocidad de transferencia de información, ocasionado por la presencia del tráfico en la red; la cual originará la inaccesibilidad a los servicios internos que tiene la universidad, que crea el malestar en los usuarios", es más; "la presencia de entrecortes en las aplicaciones de multimedia en internet, por la saturación del ancho de banda, causa distorsión y perdida de la señal en la transmisión de video por la red", finalmente a todo ello se aúna; " la demora en el acceso al servicio de

internet, así mismo a los servicios internos que tiene la universidad por el limitado ancho de banda y la presencia de tráfico en la red, lo cual ocasiona la pérdida de comunicación con los sitios remotos". Motivo por el cual, el objetivo del presente proyecto ha sido; Determinar la influencia del modelo de red con tecnología *MPLS* en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

1.1.5. Justificación metodológica

El proyecto de investigación a emprender expresó su justificación "metodológica" en el modo de simular una metodología eficiente para asegurar la mejora del rendimiento de la red *WAN* con una nueva tecnología para la comunicación entre las sedes de la Universidad Nacional de Huancavelica. Motivo por el cual, el propósito del presente proyecto ha sido; Determinar la influencia del modelo de red con tecnología *MPLS* en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

1.1.6. Limitaciones

La investigación comprende en determinar la influencia de la tecnología *MPLS* en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica.

Para la evaluación de la calidad de servicio de la red de transporte fue limitada los indicadores en base a los parámetros de calidad de servicio establecida por la Unión Internacional de Telecomunicaciones.

CAPÍTULO II
MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Internacional

Yadav y Jeyakumar (2016) en el artículo científico titulado *"DESIGN OF TRAFFIC ENGINEERED MPLS VPN FOR PROTECTED TRAFFIC USING GNS SIMULATOR"*, investigación realizado en el *Department of Electrical Engineering, Veermata Jijabai Technological Institute, Mumbai* 400039, India en el año 2016. La investigación se basó en los siguientes problemas: los clientes tenían la necesidad de establecer un vínculo privado entre sus distintas oficinas, al solicitar al proveedor de servicios un enlace separado que demandaría una inversión costosa. Además, los clientes no podían utilizar las mismas direcciones IP privadas al conectarse a la red de proveedores de servicios, ya que el proveedor de servicios no podía distinguir entre los distintos clientes. El objetivo fue realizar un estudio del diseño de MPLS *VPN* (*Red Privada Virtual*) junto con túneles de tráfico dedicados para cada *VPN* con la ayuda de *OSPF* (*Open Shortest Path First*) y MP-*BGP* (Protocolo de puerta de enlace Multiprotocolo). Para lo cual se realizó un diseño de escenario a nivel de

propuesta, para satisfacer determinadas restricciones dadas por lo clientes, y que se demostró a través del emulador *GNS3* (*Graphical Network Simulator*) que es aplicable para escenario en tiempo real, llegando a la siguiente conclusión: la tecnología *MPLS* ha demostrado ser una solución prometedora que ofrece diferentes características en la misma red del proveedor de servicios, reemplazando así muchas tecnologías de transporte. Una de las características más excepcionales de *MPLS* es la Ingeniería de Tráfico que permite optimizar el flujo de tráfico de un proveedor de servicios, así mismo se da una cantidad sustancial de control en las manos del proveedor de servicios con respecto a la utilización óptima de los recursos disponibles y seguridad.

Zapata (2016) en la tesis titulada "EVALUACIÓN DE PARÁMETROS DE CALIDAD DE SERVICIO (*QoS*) PARA EL DISEÑO DE UNA RED *VPN* CON *MPLS*" trabajo realizado en la Pontificia Universidad Católica del Ecuador en el año 2016, Quito – Ecuador. La investigación se realizó debido a la generalidad del diseño de redes orientadas al soporte de voz, video y datos no se contemplan requerimientos de parámetros de calidad de servicio en el diseño de una red. El objetivo de la tesis consistió en diseñar una red *VPN*/*MPLS* en el ambiente del laboratorio (Simulación) mediante la evaluación de parámetros de *QoS* para garantizar la disponibilidad y escalabilidad de la red. La tecnología *VPN MPLS* permite a una empresa u organización integrar voz, video y datos en una plataforma común con garantía de calidad de servicio que es necesario en la actualidad ya que el tráfico de red es muy diverso y cada tipo de tráfico tiene diferentes requerimientos como ancho de banda, *jitter*, *delay* y disponibilidad. Llegando a la siguiente conclusión: el mecanismo *DiffServ* permite dividir el tráfico en clases, controlando la cantidad de tráfico que cada cliente envía a la red y priorizándolo el envío a través de políticas de clasificación mejorando la eficiencia de una red significativamente.

Peña, Sanatana, Contreras (2014) en la tesis titulado "DISEÑO E IMPLEMENTACIÓN DE UNA RED *MPLS* PARA EL SISTEMA DE COMUNICACIÓN DE EDITORIAL OCÉANO DOMINICANA, EN SANTO

DOMINGO Y ZONA METROPOLITANA DE SANTIAGO, AGOSTO-DICIEMBRE 2014" trabajo realizado en la Universidad del Caribe Escuela de Negocios Carrera Informática en el año 2014, Santo Domingo - República Dominicana. El problema identificado en la empresa Editorial Océano Dominicana corresponde a la necesidad de adecuar sus plataformas tecnológicas para realizar un transporte eficiente de la información, permitiendo comunicar la oficina principal con sus sucursales. El objetivo de la tesis consistió en realizar el diseño e implementación de una solución de comunicación basada en el protocolo *MPLS* en la empresa Editorial Océano Dominicana y sus sucursales. El diseño de una red que permita implementar el protocolo de comunicación *MPLS* será la propuesta que le mostrará a la Empresa Editorial Océano Dominicana sus actuales limitantes al prescindir de esta tecnología para sus sucursales y aquellas que pretendan dar apertura. Llegando a la siguiente conclusión: la implementación del protocolo de comunicación *MPLS* mejora el rendimiento de la red de Editorial Océano Dominicana, ya que los paquetes son conmutados en base a etiquetas obviando la lectura de las cabeceras IP, además facilita la adopción de mecanismos de balanceo de carga para evitar la congestión con la Ingeniería de Tráfico y posibilidad de ofrecer servicios de *VPN*'s a través de túneles virtuales eliminando las dificultades de las *VPN*'s tradicionales.

2.1.2. Nacional

Victoria y Igor (2009) en la tesis titulada "MEDICIÓN Y ANÁLISIS DE TRÁFICO EN REDES *MPLS*" trabajo realizado en la Pontificia Universidad Católica del Perú en el año 2009, Lima – Perú, tuvo como problema: El esquema *Best Effort* se caracteriza por presentar un bajo nivel de rendimiento, el cual se refleja en la lentitud de las trasmisiones, pérdidas de información, pérdidas de conexión y graves casos de congestión. A pesar de que se proporciona a las aplicaciones y servicios clásicos (Telnet, FTP, Correo Electrónico, entre otros) un esquema en el que pueden funcionar de manera adecuada, es perjudicial para las nuevas aplicaciones ya que no permite proporcionar calidad de servicio

necesario para su funcionamiento. El objetivo de la tesis consistió en Simular una topología que soporte *MPLS VPN* en diferentes escenarios *MPLS* utilizando el simulador OMNET++, el cual medirá el rendimiento de la red, así como el comportamiento con diferentes tipos de tráfico relacionado con UDP y TCP. La tecnología *MPLS* surge como la mejor opción que se puede encontrar actualmente para el manejo del *backbone* de Internet por sus diferentes características: ingeniería de tráfico, bajo costo de implementación, así como adaptación con tecnologías de capa de enlace y de red, como resultado llegó a la siguiente conclusión: gracias a la capacidad de *MPLS* de crear túneles de manera dinámica, puede recuperarse de eventuales fallas en los nodos de la red, esto quiere decir que, si se creasen nuevos protocolos de enrutamiento para la capa de red, *MPLS* podría usarlos para el establecimiento de sus túneles LSP en su tabla LIB. Estas rutas de contingencia también pueden ser definidas de manera estática según los criterios que el administrador de la red *Backbone* del ISP lo vea más conveniente.

Calcina (2011) tesis *titulada* "DISEÑO DE RED *LAN* UTILIZANDO EL PROTOCOLO *MPLS* PARA LA TRANSMISIÓN DE VOZ, DATO Y VIDEO EN LA EPIS – UNA – PUNO 2011" trabajo realizado en la Universidad Nacional del Altiplano en el año 2013, Puno – Perú, investigación realizada tuvo como problema: La red tradicional, cuyo nivel de transporte se basa en IP, se puede transportar los servicios como voz, video y datos, etc; sin embargo, este protocolo ya no cumple con las exigencias de calidad de servicio para los usuarios debido al aumento en la complejidad de las aplicaciones ya existentes y que irán apareciendo en el futuro. El objetivo de la tesis consistió en elaborar un diseño de red *LAN* utilizando el protocolo *MPLS* para la transmisión de voz, video y datos de la EPIS – UNA – PUNO. Es importante para los operadores y proveedores de redes la implementación de nuevas tecnologías para por un lado satisfacer la demanda de los usuarios y por otro permanecer competitivos en este mercado. Una de las tecnologías que se deben implementar y quizá la más importante es MLPS que ofrece los mecanismos para integrar otras tecnologías y servicios con *QoS* facilitando la migración a las redes NGN, como resultado

llegó a las siguientes conclusiones: Con el nuevo diseño de red *LAN* se logró transmitir eficientemente voz, datos en *MPLS* optimizando la calidad de servicio para el usuario de la EPIS – UNA – PUNO 2011, así mismo se logró estudiar y analizar los requerimientos como su arquitectura y protocolos de señalización para la convergencia de servicios que es posible con la implementación de la tecnología *MPLS* en el *backbone* de la red ya que permite unificar la rapidez del reenvío del tráfico con las funciones de enrutamiento además de brindar Calidad de Servicio con la utilización de *DiffServ*, mejorando la transmisión y priorizando el tráfico de las aplicaciones de voz, datos y video.

Menedez (2012) tesis titulada "ESTUDIO DEL DESEMPEÑO E IMPLEMENTACIÓN DE UNA SOLUCIÓN *MPLS-VPN* SOBRE MÚLTIPLES SISTEMAS AUTÓNOMOS*"* trabajo realizado en la Pontificia Universidad Católica del Perú el año 2012, Lima – Perú, tuvo como problema: A medida que las empresas crecen, los requerimientos de sus *VPNs* aumentan, se hace necesario abarcar diferentes áreas geográficas, muchas veces cruzando más de un país. Inclusive, algunas *VPNs* necesitan extenderse a través de múltiples proveedores de servicios *VPN*. El objetivo de la tesis consistió en realizar el estudio de cuatro tipos de implementación de la solución multi-AS-*VPN*. La arquitectura *Multi Protocol Label Switching* (*MPLS*) proporciona alta escalabilidad y rapidez en el reenvío de paquetes, siendo su aplicación más empleada las *VPNs*. Sin embargo, esta arquitectura implica que los clientes de servicios *VPN* estén conectados a un solo proveedor. Como resultado llego a las siguientes conclusiones: Se logró identificar al modelo de implementación "M*ulti Protocol eBGP Multisalto entre Route Reflectors*" como el más adecuado y también se realizó la propuesta técnica en la cual se describe el escenario general al que se enfrenta un proveedor de servicio para brindar servicios *VPN* a grandes distancias.

2.1.3. Local

Revisado los catálogos, ficheros y la base de datos con las cuales cuenta la Biblioteca Central de la Universidad Nacional de Huancavelica, no se encontró ningún trabajo de investigación a fin al tema, razón por el cual la investigación a realizar; expresa su originalidad y se constituirá en un precedente para la ejecución de otros proyectos.

2.2. Bases teóricas

2.2.1. Modelo de red

Según Santos (2014) define: "Los modelos en capas, como el modelo TCP/IP, se utilizan para ayudar a visualizar la interacción entre los diversos protocolos". Se clasifican en dos tipos de modelos de redes:

a) **Modelo de protocolo:** La arquitectura TCP/IP propone la existencia de cinco niveles: físico, enlace, red, transporte y aplicación. Como se observa, la diferencia más obvia es que en este modelo no aparecen los niveles de sesión y presentación. Lo que ocurre es que cualquier función por encima del nivel de transporte en TCP/IP se implementa en el nivel de aplicación. Los niveles con más similitudes entre el modelo OSI y el modelo TCP/IP son los de red y de transporte (Santos, 2014, pág. 110).

b) **Modelo de referencia:** OSI es una arquitectura basada en niveles para el diseño de sistemas de red. Este modelo además permite la interconexión de sistemas abiertos, o lo que es lo mismo, permite que dos sistemas diferentes se puedan comunicar independientemente de su arquitectura. Es importante resaltar que OSI es un modelo, no un protocolo. Además, el modelo OSI no especifica los servicios ni los protocolos que forman parte de cada nivel (Santos, 2014, pág. 103).

Las infraestructuras de red pueden variar en gran medida en función del ámbito o alcance geográfico de la red, y en función de este factor podemos distinguir entre tres tipos de redes: *LAN*, *MAN* y *WAN*.

- **Red de área local (*LAN*). -** El término *LAN* (*Local Area Network*) se aplica a una red de datos cuando los dispositivos unidos en dicha red se encuentran ubicados en un área geográfica limitada. Las distancias entre dispositivos conectados a una red de área local pueden variar entre unos pocos metros hasta varios cientos de metros o incluso kilómetros (Santos, 2014, pág. 20).

- **Red de área metropolitana (MAN). -** El término MAN (Metropolitana Area Network) se aplica a redes que unen redes *LAN* o dispositivos dispersos en varias ubicaciones dentro de un núcleo de población, o de varios núcleos cercanos entre sí (Santos, 2014, pág. 21)

- **Red de área extensa (*WAN*). -** El término *WAN* (Wide Area Network) se aplica realmente a la infraestructura que permite la conexión de redes o dispositivos ubicados en diferentes zonas geográficas con una distancia lo suficientemente grande como para no considerarse una red MAN (Santos, 2014, pág. 21).

2.2.2. *Multiprotocol Label Switching* (*MPLS*)

2.2.2.1. Introducción a las redes *MPLS*

MPLS (*Multiprotocol Label Switching*) es una tecnología *Wan* que está definida en la RFC 3031. Para poder saber cómo funciona esta nueva tecnología, así como las ventajas que introduce, es necesario saber cómo funcionaban sus antecesores. Las conexiones *WAN* tradicionales son conexiones de capa 2 que se pueden clasificar como punto a punto o multipunto. Estas redes no entienden de calidad de servicio de capa 3 (*QoS*). En algunos casos muy específicos se pueden priorizar circuitos en los dispositivos frontera (Ariganello & Enrique , 2013, pág. 563).

A través de las redes *WAN* existe muy poco o casi nada de protección del tráfico. Las *WAN* tradicionalmente existen en un número limitado de arquitecturas según cada empresa y también dependen del ancho de banda de cada uno de dichos sitios (Ariganello & Enrique , 2013, pág. 563).

Los modelos de arquitectura más comunes son los siguientes:

- *Hub-and-spoke*
- Malla parcial
- Malla completa
- Hub-and-spoke redundante

2.2.2.2. Elementos de *MPLS*

a) *FEC* (*Forwarding Equivalence Class*)

Una Clase de Equivalencia de Reenvío (*FEC*) es un grupo o flujo de paquetes que se reenvían a lo largo de la misma ruta y se tratan de la misma manera con respecto al tratamiento de reenvío. Todos los paquetes que pertenecen a la misma FEC tienen la misma etiqueta. Sin embargo, no todos los paquetes que tienen la misma etiqueta pertenecen a el mismo *FEC*, porque sus valores de EXP pueden diferir; El tratamiento de reenvío podría ser diferente y podrían pertenecer a una *FEC* diferente (Luc, 2007, pág. 30).

b) *LSP* (*Label Switched Path*)

Una ruta de conmutación de etiquetas (*LSP*) es una secuencia de LSR que cambian un paquete etiquetado a través de una red *MPLS* o parte de una red *MPLS*, que básicamente, el LSP es la ruta a través de la red *MPLS* o una parte de ella que

toman los paquetes. El primer LSR de un LSP es el LSR de ingreso, mientras que el último LSR del LSP es el LSR de egreso. Todos los LSR entre los LSR de ingreso y egreso son los LSR intermedios (Luc, 2007, pág. 29)

c) *LSR* (*Label Switch Router*)

Un enrutador de conmutador de etiquetas (*LSR*) es un enrutador que admite *MPLS*. Es capaz de comprender las etiquetas *MPLS*, de recibir y transmitir un paquete etiquetado en un enlace de datos (Luc, 2007, pág. 29). Existen tres tipos de LSR en una red *MPLS*:

***LSRs* de ingreso. -** Los *LSR* de ingreso reciben un paquete que aún no está etiquetado, inserta una etiqueta (pila) frente al paquete y lo envía en un enlace de datos.

***LSRs* de salida. -** Los LSR de egreso reciben paquetes etiquetados, eliminan las etiquetas y los envían a través de un enlace de datos. Los LSR de ingreso y egreso son LSR de borde.

***LSRs* intermedios. -** Los LSR intermedios reciben un paquete etiquetado entrante, luego realizan una operación en él, cambian la etiqueta y lo envían el paquete en el enlace de datos correcto.

d) *LDP* (*Label Distribution Protocol*).- Es el protocolo que utilizan los LSR para asignar las etiquetas (Luc, 2007, pág. 66).

e) *LIB (Label Information Base*). - La tabla de etiquetas que manejan los LSR. Relaciona el par (interfaz de entrada - etiqueta de entrada) con (interfaz de salida - etiqueta de salida) (Luc, 2007, pág. 36)

2.2.2.3. Mecanismos de conmutación

El mecanismo de *MPLS* en los routers Cisco está basado en

CEF (Cisco Express Forwarding) y es un mecanismo necesario para el funcionamiento de *MPLS*. Existen dos mecanismos de conmutación dentro de un router: *Process switching*, *Cactae-driven switching y topology-driven switching,* la FIB. (Ariganello & Enrique , 2013, pág. 570)

a) Conmutación *IP* estándar

Para definir el concepto de Conmutación IP estándar se ha tomado como referencia de Cisco, que manifiesta dentro de la red corporativa se utiliza un IGP y un EGP para conectar a un sistema autónomo externo, que en la mayoría de los casos suele ser *BGP* (Ariganello & Enrique , 2013, pág. 570).

Para anunciar las redes internas de la empresa las rutas son redistribuidas entre estas dos entidades. Las rutas deben ser consideradas públicamente enrutables en el supuesto caso de que sean enviadas hacia Internet. (Ariganello & Enrique , 2013, pág. 570)

b) Conmutación *CEF*

La definición de conmutación de CEF (Cisco Express Forwarding) según Cisco; es una tecnología que utiliza la FIB (Forwarding Information Base) y que es una imagen de la tabla de enrutamiento. (Ariganello & Enrique , 2013, pág. 571)

Cuando existe algún cambio en la topología la FIB se actualiza basándose en los cambios de dicha tabla. La FIB mantiene un listado de rutas y una dirección de próximo salto provistas por el protocolo de enrutamiento de capa 3. CEF simplemente copia dicha información. (Ariganello & Enrique , 2013, pág. 571).

2.2.2.4. Arquitectura *MPLS*

La arquitectura *MPLS* está compuesto de dos componentes que son: plano de control y plano de datos.

a) Plano de control

Es aquella que lleva las tareas destinadas a determinar la disponibilidad del acceso hacia una red destino, el plano de control contiene toda la información de direccionamiento de la capa 3 (Zapata, 2016, pág. 28).

Por otro lado, la función del plano de control es cuando se hace el intercambio de información por parte de dos protocolos de enrutamiento como *OSPF* y *BGP*, adicionalmente se encarga del valor que llevan las etiquetas (Zapata, 2016, pág. 28).

b) Plano de datos

Es aquella que está relacionada con el *forwarding* (envío de paquetes), los mismos que pueden ser paquetes IP o paquetes IP etiquetados (Zapata, 2016, pág. 28).

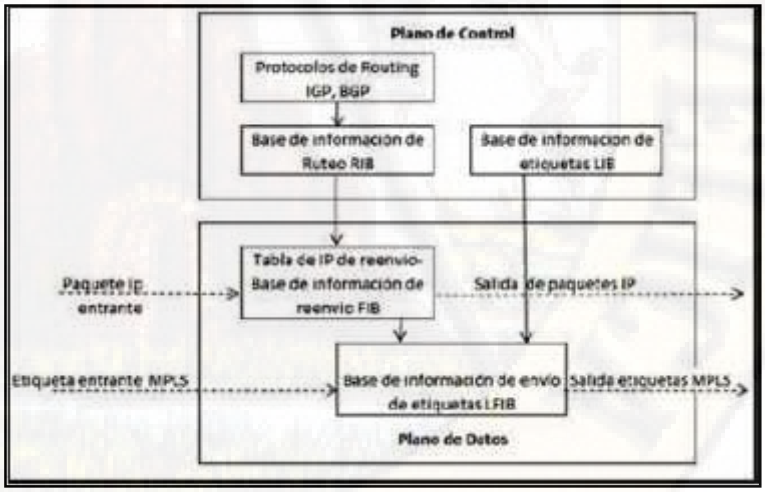


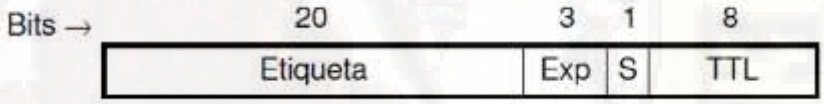
Figura Nº 2.1: Bloques de la red *MPLS*.
Fuente: Miroslava Zapata Rodríguez.

2.2.2.5. Distribución de etiquetas

MPLS, tal cual ocurre en el enrutamiento tradicional, se basa en los destinos. Las funciones de las etiquetas *MPLS* son separar las operaciones de envío desde los destinos de capa 3 contenidos en la cabecera de los paquetes asociando una etiqueta con una FEC (*Forwarding Equivalence Class*). Siendo éste un mecanismo altamente eficiente para el envío de información. (Uba, 2016)

Las etiquetas *MPLS* proporcionan un mecanismo por el cual los paquetes pueden ser ordenados en varios FEC sin la necesidad de examinar la cabecera de capa 3. Cada LSP a lo largo del camino utiliza la etiqueta para tomar decisiones de envío para cada paquete. Dicha etiqueta es insertada entre la cabecera de capa 2 y la cabecera de capa 3. Este mecanismo se llama *frame mode MPLS*. (Uba, 2016)

Formato de la etiqueta *MPLS* tiene 32 bits que se encuentra en el siguiente esquema:



Cuadro Nº 2.1: Descripción de la cabecera *MPLS*.
Fuente: Diapositivas UBA.

Según Alarcón y Martinez (2008) define la cabecera *MPLS*:

a) Etiqueta (20): Campo de 20 bits que acarrea el valor de la etiqueta *MPLS*.

b) EXP (3): Antes se llamaba CoS (*Class of Service)*, ahora se considera un rango experimental. Este campo se considera para consideraciones *QoS* (*Quality of Service*).

c) **S (1):** Se usa para indicar si está presente una pila de etiquetas (*label stack*), entonces su valor será uno. Si la etiqueta es la única presente en la pila, entonces el valor será 0.

d) **TTL (8):** El campo Time To Live provee funcionalidad IP TTL. Se usa para indicar el número de nodos *MPLS* por los que el paquete ha viajado hasta alcanzar su destino. El valor es copiado del encabezado del paquete cuando se ingresa a la LSP, y copiado de vuelta al encabezado del paquete IP cuando sale de la misma.

2.2.2.6. Aplicaciones de *MPLS*

Según Santos (2014) define las principales aplicaciones de *MPLS*, que son los siguientes:

a) **Ingeniería de Tráfico**

La ingeniería de tráfico (o dimensionado de tráfico como algunos autores prefieren traducir la expresión *inglesa Traffic Engineering*) puede ser definida como el proceso de controlar los flujos de datos a través de una red. Es decir, el proceso de optimizar la utilización de los recursos disponibles por parte de los distintos flujos y, por tanto, optimizar el uso global de los recursos y las prestaciones de la red (Santos, 2014, pág. 354).

b) **Redes privadas virtuales (*VPN*)**

Una red privada virtual (*VPN*) es un modo de permitir a los usuarios el extender sus redes privadas sobre la infraestructura de la red pública de forma segura. Básicamente una red privada virtual (*VPN*) se construye utilizando conexiones realizadas sobre una infraestructura compartida con

funcionalidades de encaminamiento y de seguridad similares a las que existen en una red privada (Santos, 2014, pág. 352).

c) Calidad de servicio (*QoS*)

Es posible asignar a un cliente o a un tipo de tráfico una FEC a la que se asocie una conexión virtual (LSP) que discurra por enlaces con bajo nivel de carga (Cujae, 2011).

d) Soporte a las clases de servicios

Estos nuevos tipos de servicios añaden requisitos adicionales a la red de transporte (por ejemplo, el tráfico de voz es muy sensible al retardo y a su variación, mientras que las comunicaciones de video suelen ser muy exigentes desde el punto de vista del ancho de banda que necesitan) y los usuarios de las mismas quieren garantías de que las prestaciones de la red son suficientes para que los servicios finales no sufran degradación (Santos, 2014, pág. 352).

e) Soporte multiprotocolo

Los *LSPs* son válidos para múltiples protocolos, ya que el encaminamiento de los paquetes se realiza en base a la etiqueta *MPLS* estándar, no a la cabecera de nivel de red (Cujae, 2011).

2.2.2.7. *MPLS* con tecnología *VPN*

Según Cisco define que las *VPN* permiten el uso de infraestructura compartida ofrecida por un ISP para implementar redes privadas. El uso de seguridad está sujeto a negociación, los ISP ofrecen servicios adicionales tales como firewall para filtrar tráfico indeseado. (Ariganello & Enrique , 2013, pág. 592)

Desde un punto de vista de implementación de *VPN* existen dos tipos de modelos:

- ***Overlay VPN***, o tradicionales, incluye tecnologías como X.25, *Frame- Relay*, ATM (*Asynchronous Transfer Mode*) para *VPN* de capa 2 y túneles GRE e IPsec para *VPN* de nivel 3 (Ariganello & Enrique , 2013, pág. 592).

- ***Peer to peer VPN*,** son implementadas con ISP compartidos y las infraestructuras son realizadas con ACL para separar a los distintos clientes (Ariganello & Enrique , 2013, pág. 592).

a) *VPN* tradicionales

Las *VPN* tradicionales han sido utilizadas durante mucho tiempo y se basan en el modelo de capa 2 en el que el ISP ofrece una cantidad de circuitos virtuales. Como muchas otras tecnologías de red las conexiones *VPN* van evolucionando desde capa 1 hasta las capas superiores (Ariganello & Enrique , 2013, pág. 593).

El concepto de *VPN* comenzó años atrás cuando se utilizaban circuitos TDM (Time-División Multiplex); la evolución fue constante hasta alcanzar la capa 2 y la capa 3 (Ariganello & Enrique , 2013, pág. 593).

b) *VPN* peer to peer

Las *VPN* peer to peer hacen que el ISP tenga un papel más activo en las operaciones de enrutamiento de cada cliente. El ISP mantendrá información de instancias de enrutamiento separadas dentro de su red (Ariganello & Enrique , 2013, pág. 594).

El router CE (*Customer Edge*) comparte información sólo con el router PE (*Provider Edge*) a través del circuito del ISP. Esta conexión e intercambio de información con el ISP facilita el concepto de *VPN* peer to peer (Ariganello & Enrique , 2013, pág. 594).

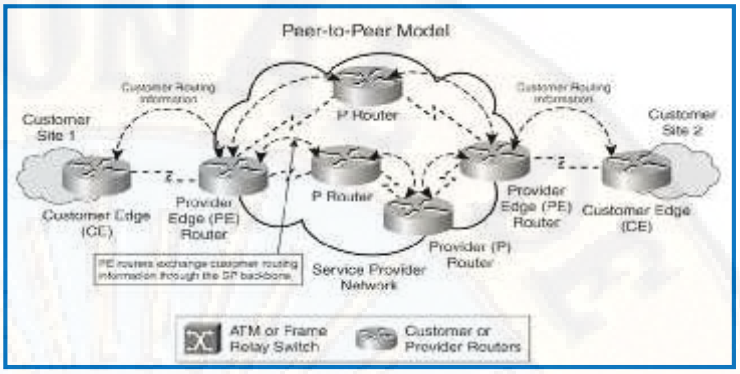


Figura Nº 2.2: *VPN* peer to peer

Fuente: *wordpresslvyang* 2010

La ventaja de la *VPN* como tecnología de acceso avanzada ofrece múltiples posibilidades. Las opciones para la conectividad se adaptan a los requisitos de cada empresa. Los beneficios de las *VPN* son conocidos y además útiles para pequeñas y grandes empresas (Ariganello & Enrique , 2013, pág. 595).

- Las *VPN* tradicionales son fáciles de implementar tanto del lado del ISP como por el del cliente. El proveedor no participa en los procesos de enrutamiento.
- Las *VPN* peer to peer proporcionan una solución óptima en los procesos de enrutamiento empleando topologías de malla completa proporcionando redundancias entre todos los sitios, sin necesidad de implementar cambios desde el punto de vista del cliente.
- Agregar sitios nuevos es tan simple como el agregado de nuevos routers e interconectarlos a un nuevo bucle local. La configuración no requiere múltiples circuitos para proporcionar capacidades de malla completa.

Las desventajas de las *VPN* es el coste y las tareas administrativas asociadas en grandes empresas con las topologías de malla completa pueden ser enormes. Para la reducción de número de circuitos virtuales requeridos se deben sacrificar posibles rutas redundantes. (Ariganello & Enrique , 2013, pág. 596)

Esto requiere un control administrativo permanente de los circuitos virtuales para mantener la conectividad necesaria. (Ariganello & Enrique , 2013, pág. 596)

Las *VPN* tradicionales también tienen problemas de sobrecarga cuando se utiliza IPsec o GRE. Los principales beneficios de las *VPN* peer to peer pueden ser también su principal desventaja, como por ejemplo en la participación del enrutamiento del cliente. (Ariganello & Enrique , 2013, pág. 596)

La información de enrutamiento de las distintas redes es redistribuida entre el CE y el PE. Deben aplicarse filtros de enrutamiento en las interfaces de los routers para proteger ambas partes de flujos de rutas no deseadas. El cliente debe confiar en la capacidad del ISP para configurar y mantener la infraestructura de enrutamiento. (Ariganello & Enrique , 2013, pág. 596)

En sitios críticos con routers redundantes y varias conexiones a distintos ISP, se deben tener consideraciones tales como la diversificación de los circuitos de manera que no todos éstos terminen en el mismo PE. El objetivo final es tratar de eliminar en lo posible puntos comunes de fallos. (Ariganello & Enrique , 2013, pág. 596)

2.2.3. Protocolos de Enrutamiento

2.2.3.1. *OSPF*

Open Shortest Path First (*OSPF*), es un Protocolo de Gateway interior que se usa para distribuir información de enrutamiento dentro de un sistema autónomo único. El protocolo *OSPF* se basa en tecnología de estado de enlace, la cual es una desviación del algoritmo basado en el vector *Bellman-Ford* que se usa en los protocolos tradicionales de enrutamiento de Internet (Crow, 2016, pág. 11).

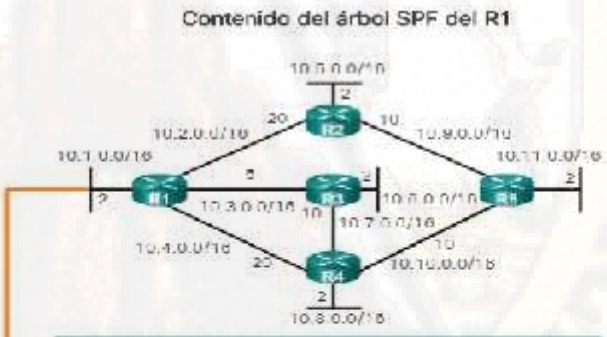
OSPF soporta los enlaces punto a punto y las redes de difusión (la mayoría de las *LAN*). En realidad, es capaz de soportar redes con múltiples enrutadores, cada uno de los cuales se puede comunicar en forma directa con los demás (a éstas se les conoce como redes multiacceso) incluso aunque no tengan capacidad de difusión. (Tanenbaum, 2012, pág. 407).

a) Funcionamiento de estado de enlace

Según Crow (2016) afirma: "*OSPF* usa un algoritmo de estado de enlace para generar y calcular el trayecto más corto a todos los destinos conocidos y el algoritmo en sí mismo es bastante complicado". A continuación, se ofrece una forma simplificada de nivel muy elevado para analizar los diversos pasos del algoritmo:

- Durante la inicialización, o bien cuando se produce algún cambio en la información de enrutamiento, un router generará un anuncio de estado de enlace. Este anuncio representará la agrupación de todos estos estados de enlace en dicho router.

- Todos los routers intercambiarán estados de enlace mediante la inundación. Cada router que recibe una actualización de estado de enlace debe almacenar una copia de su base de datos de estados de enlace y luego propagar la actualización a otros routers.
- Una vez que la base de datos de cada router está completa, el router calculará un árbol de trayecto más corto a todos los destinos. Para ello, el router utiliza el algoritmo *Dijkstra*. Los destinos, el costo asociado y el siguiente salto (*next hop*) para alcanzar dichos destinos formarán la tabla de IP *Routing*.
- En caso de que no se produzcan cambios en la red *OSPF*, por ejemplo, el costo de un enlace o bien la adición o eliminación de una red, *OSPF* debería permanecer muy tranquilo. Los cambios que se produzcan se comunicarán a través de paquetes de estado de enlace y se volverá a calcular el algoritmo Dijkstra para encontrar el trayecto más corto.



Destino	Ruta más corta	Costo
10.5.0.0/16	R1 → R2	22
10.6.0.0/16	R1 → R3	7
10.7.0.0/16	R1 → R3	15
10.8.0.0/16	R1 → R3 → R1	17
10.9.0.0/16	R1 → R2	30
10.10.0.0/16	R1 → R3 → R4	25
10.11.0.0/16	R1 → R3 → R4 → R5	27

Figura Nº 2.3: Árbol del router en *OSPF*.

Fuente: Cisco CCNA

b) *OSPF* de área única y *OSPF* multiárea

Cisco Ccna (2017), el *OSPF* se puede implementar de dos formas:

***OSPF* de área única:** En la figura siguiente se observa, todos los routers se encuentran en una sola área "área *backbone*" (área 0).

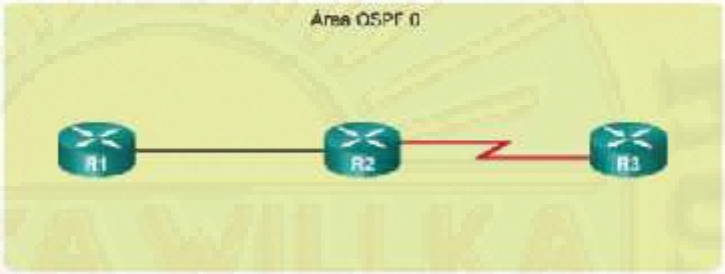


Figura Nº 2.4: Área única de *OSPF*

Fuente: Cisco CCNA

***OSPF* multiárea:** En la figura siguiente se observa, el *OSPF* multiárea está formado por varias áreas, de manera jerárquica, que todas las áreas deben conectarse al área 0 (*backbone*) y los routers que interconectan las áreas se denominan "routers fronterizos de área" (ABR), por otro lado, con *OSPF* multiárea, puede dividir un sistema autónomo (AS) grande en áreas más pequeñas.

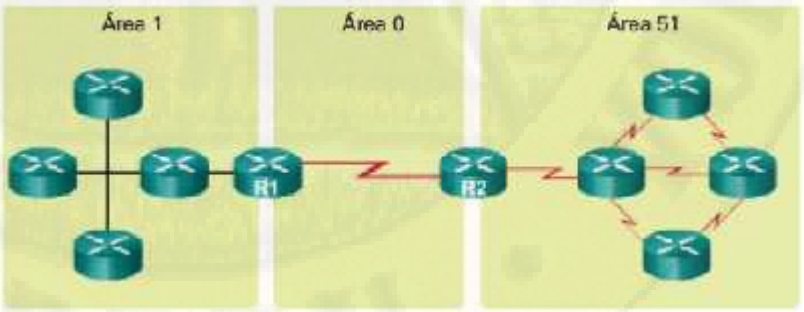


Figura Nº 2.5: Área multiárea de *OSPF*

Fuente: Cisco 2017

c) DR y BDR OSPF

Según Ariganello y Enrique (2013), las redes de accesos múltiples pueden crear dos retos para *OSPF*:

Router DR

El DR recibe actualizaciones y las distribuye a todos los demás routers del segmento asegurándose con acuses de recibo de que éstos han recibido correctamente dichas actualizaciones y que poseen una copia sincronizada de la LSDB (Ariganello & Enrique , 2013, pág. 73).

Router BDR

El BDR escucha pasivamente y mantiene una tabla de relación con todos los demás routers, en el caso de que el DR deje de enviar helio el BDR tomará el papel del DR (Ariganello & Enrique , 2013, pág. 74).

2.2.3.2. Enrutamiento virtual y reenvío (*VRF*)

Según Rouse (2012) afirma: "el Enrutamiento Virtual y Reenvío llamado *VRF* es una tecnología incluida en routers de red IP que permite a varias instancias de una tabla de enrutamiento existir en un router y trabajar al simultáneamente". Esto aumenta la funcionalidad al permitir que las rutas de red sean segmentadas sin usar varios dispositivos. Dado que el tráfico es automáticamente segregado, *VRF* también aumenta la seguridad de la red y puede eliminar la necesidad de cifrado y autenticación.

Según Cano (2018) afirma: "Una *VRF* es una instancia de enrutamiento y reenvío en la *VPN*, es el nombre que recibe la combinación de la tabla de *routing* de la *VPN*, la CEF de la *VRF* y los protocolos de routing IP asociados en el router PE" (pág. 79). Un nodo PE tiene una instancia de *VRF* para cada *VPN* asociada.

En la figura siguiente, podemos observar como un nodo PE tiene su tabla de rutas global IP y también una tabla de enrutamiento *VRF* por cada *VPN* conectada al router PE.

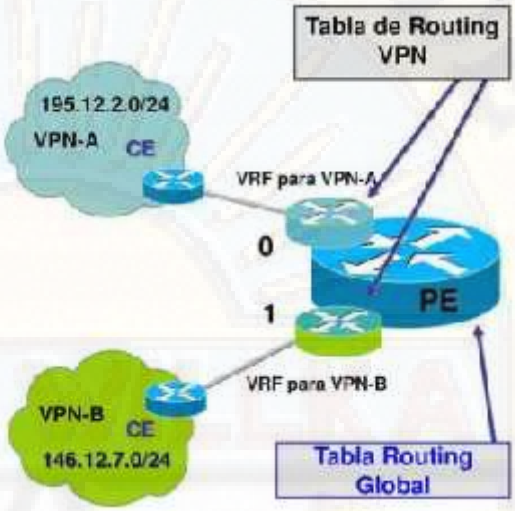


Figura Nº 2.6: *VRFs* en el nodo PE.
Fuente: José Cano Sáez.

La tabla de rutas debe estar separada y ser privada para cada cliente dentro de un nodo PE, cada *VPN* debe tener su propia tabla de rutas y esta tabla de rutas privada se llama tabla de rutas *VRF*. El interfaz del PE que conecta con el CE puede pertenecer solo a una *VRF* por lo que todos los paquetes recibidos en la interfaz de esa *VRF* se identifican inequívocamente como pertenecientes a esa *VRF* (Cano, 2018, pág. 80).

2.2.3.3. *BGP* (*Border Gateway Protocol*)

BGP es un protocolo de enrutamiento moderno diseñado para ser escalable y poder utilizarse en grandes redes creando rutas estables entre las organizaciones. *BGP* soporta VLSM (Variable *Length Subnet Mask*), CIDR (*Classless Interdomain Routing*) y sumarización. (Ariganello & Enrique , 2013, pág. 201)

Para Cisco CCNP el *BGP* es un protocolo de enrutamiento extremadamente complejo, usado entre organizaciones

multinacionales y en Internet. El principal propósito de *BGP* es conectar grandes redes o sistemas autónomos. Las grandes organizaciones utilizan *BGP* como el vínculo entre diferentes divisiones empresariales. *BGP* se utiliza en Internet para conectar diferentes organizaciones entre sí.

Es el único protocolo que actualmente soporta enrutamiento entre dominios. Los dispositivos, equipos y redes controlados por una organización son llamados sistemas autónomos, AS. Esto significa independencia, es decir, que cada organización es independiente de elegir la forma de conducir el tráfico y no se los puede forzar a cambiar dicho mecanismo. Por lo tanto, *BGP* comunica los AS con independencia de los sistemas que utilice cada organización. (Ariganello & Enrique , 2013, pág. 201)

a) Funcionamiento básico de *BGP*

BGP asocia redes con sistemas autónomos de tal manera que otros router envían tráfico hacia el destino a través de un sistema autónomo. Cuando el tráfico llega a los routers frontera de *BGP*, es trabajo de los routers del IGP encontrar el mejor camino interno. (Ariganello & Enrique , 2013)

Para Ariganello y Enrique (2013), *BGP* es un protocolo *path-vector*, aunque mantiene muchas características comunes con los de vector-distancia. Las rutas son registradas de acuerdo con los sistemas autónomos por donde está pasando y los bucles son evitados rechazando aquellas rutas que tienen el mismo número de sistema autónomo al cual están llegando. La idea de cómo *BGP* evita los bucles se ilustra en la siguiente figura:

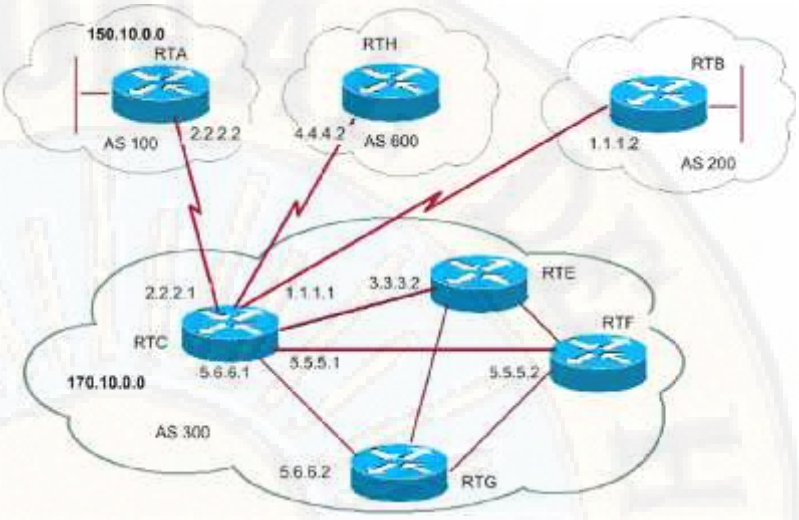


Figura Nº 2.7: Topología de red con *BGP*

Fuente: Cisco 2013

Los vecinos *BGP* son los llamados *peers*, éstos no son automáticamente descubiertos, sino que deben estar predefinidos. Existen cuatro tipos de mensajes en *BGP* para que la relación sea construida y posteriormente mantenida:

- *Open*
- *Keepalive*
- *Update*
- *Notifícation*

b) Jerarquías *BGP*

Otros protocolos de enrutamiento han sido creados de tal manera que soporten sumarizaciones y para que se pueda organizar la red de manera jerárquica. (Ariganello & Enrique , 2013)

Las organizaciones no están distribuidas jerárquicamente, por lo tanto, *BGP* debe trabajar con cualquier topología que le sea dada. *BGP* se beneficia de la sumarización de la misma manera que los demás protocolos de enrutamiento, es decir, menos

consumo de recursos de memoria y CPU, y tablas de enrutamiento más pequeñas. (Ariganello & Enrique , 2013)

Una red *BGP* optimizada será altamente sumarizada, pero no necesariamente de manera jerárquica. *BGP* por naturaleza proporciona un resumen de las rutas claves identificando los posibles caminos entre sistemas autónomos. (Ariganello & Enrique , 2013)

Debido a que los AS no están bien organizados, las redes *BGP* reflejan esa falta de organización. *BGP* puede ser implementado entre redes o dentro de una red. *BGP* detecta los bucles mirando las rutas de los AS-Path. (Ariganello & Enrique , 2013)

c) Tablas de *BGP*

Según Ariganello y Enrique (2013), el enrutamiento a través de *BGP* involucra tres tipos de tablas:

- Tabla de vecinos
- Tabla de *BGP*
- Tabla de enrutamiento IP

Las rutas de *BGP* son mantenidas en una tabla de *BGP* separada y las mejores rutas son pasadas a la tabla de enrutamiento. A diferencia de los protocolos detallados en los capítulos anteriores, *BGP* no utiliza una métrica. En su lugar *BGP* emplea un proceso de 10 pasos para seleccionar las rutas dependiendo de una serie de propiedades. (Ariganello & Enrique , 2013)

En suma, *BGP* soporta herramientas como *route-maps* y listas de distribución que permiten al administrador cambiar el flujo de tráfico basado en los atributos de este protocolo. (Ariganello & Enrique , 2013)

d) Estados de *BGP*

Para Ariganello y Enrique (2013), los estados que toma *BGP* son los siguientes:

- ***Idle,*** durante este estado el router está buscando a los vecinos, técnicamente *BGP* espera una fase llamada *start*. Este evento puede ser iniciado por un administrador o por el sistema *BGP*. Un administrador estableciendo una sesión *BGP* o reseteando una sesión que ya existe causa un evento start.

- ***Connect, BGP*** espera que se complete la conexión del protocolo de transporte, en este caso TCP puerto 179. Si la conexión de TCP se realiza satisfactoriamente, el estado pasa a la fase *open sent*. En el caso de que no sea satisfactoria el estado cambiará a active.

- ***Active,*** intenta establecer una vecindad iniciando la conexión a través del protocolo de transporte. En caso de que lo consiga pasará al siguiente estado, open sent. Cuando el temporizador *connect retray* expira *BGP* lo reinicia y vuelve al estado connect. Si un router permanece entre los estados connect y active revela que la conexión TCP no se puede establecer. El estado active indica que el router está intentando iniciar la sesión TCP.

- ***Open Sent,*** en este estado *BGP* espera los mensajes open del vecino, estos mensajes son chequeados para verificar que los datos son correctos, que las versiones de *BGP* sean las debidas como así también el número del sistema autónomo.

- ***Open Confirma,*** *BGP* espera los mensajes *keepalive,* si recibe estos mensajes de su vecino entonces la sesión pasa al siguiente estado.

- ***Established,*** es el estado final y el necesario para que *BGP* comience a funcionar, se intercambien rutas, actualizaciones o *keepalives*.

2.2.4. Calidad de servicio (*QoS*)

El efecto global de la calidad de funcionamiento de un servicio que determina el grado de satisfacción de un usuario de un servicio. (Itu-I, 2002)

La necesidad de cada flujo se puede caracterizar por cuatro parámetros principales: confiabilidad, retardo, fluctuación y ancho de banda. Estos parámetros en conjunto determinan la *QoS* (calidad del servicio) que el flujo requiere. En el cuadro siguiente se listan varias aplicaciones y el nivel de sus requerimientos de aplicación. (Tanenbaum, 2012, pág. 347)

Aplicación	Confiabilidad	Retardo	Fluctuación	Ancho de banda
Correo electrónico	Alta	Bajo	Baja	Bajo
Transferencia de archivos	Alta	Bajo	Baja	Medio
Acceso a Web	Alta	Medio	Baja	Medio
Inicio de sesión remoto	Alta	Medio	Media	Bajo
Audio bajo demanda	Baja	Bajo	Alta	Medio
Vídeo bajo demanda	Baja	Bajo	Alta	Alto
Telefonía	Baja	Alto	Alta	Bajo
Videoconferencia	Baja	Alto	Alta	Alto

Cuadro Nº 2.2: Nivel de los requerimientos de calidad del servicio de la aplicación.

Fuente: ANDREW S. TANENBAUM

El modelado de tráfico es una técnica para regular la tasa promedio y las ráfagas de un flujo de datos que entra a la red. (Tanenbaum, 2012, pág. 349)

La programación de paquetes es tener la capacidad de regular la forma del tráfico ofrecido, sin embargo, para ofrecer una garantía de desempeño debemos reservar suficientes recursos a lo largo de la ruta que toman los paquetes a través de la red. (Tanenbaum, 2012, pág. 353)

El control de admisión es la garantía de *QoS* se establecen por medio del proceso de control de admisión para controlar la congestión, lo cual es una garantía de desempeño, aunque algo débil. (Tanenbaum, 2012, pág. 356)

2.2.4.1. Modelos de calidad de servicio (*QoS*)

a) Modelo *Best-Effort*

El modelo Best-Effort significa que no hay *QoS* aplicado, de manera que todos los paquetes dentro de la red independientemente del tipo que sean reciben el mismo trato. Como beneficio de este sistema está la facilidad de implementación, ya que no hay que hacer nada para ponerlo en funcionamiento, pero tiene como desventaja que no es posible garantizar ningún tipo de servicio a ninguna aplicación (Ariganello & Enrique , 2013, pág. 729)

b) Servicios integrados

En la actualidad, la tecnología permite disponer de estaciones de trabajo equipados con los últimos procesadores, técnicas de codificación para señales de audio y vídeo, programas de aplicación multimedia y transmisión multicast en la Internet. Aplicaciones en tiempo real es hoy en día uno de mayor demanda. A partir de 1994, la comunidad de Internet inicia los estudios para proponer una nueva arquitectura que modifique a la actual Internet y que satisfaga a las nuevas aplicaciones de tiempo real. En esta arquitectura, tanto los usuarios como los administradores de la red, deberán de disponer del ancho de banda de los enlaces para asignar adecuadamente a las diferentes aplicaciones tanto convencional como de tiempo real. Es aquí donde de define en el término Servicios Integrados (IS) para un modelo de servicio de la Internet que incluye tanto servicio

de mejor esfuerzo o *best effort* y servicio de tiempo real. El modelo de servicio fundamental de la actual Internet, el servicio de envío con el mejor esfuerza, ha ido cambiando desde sus inicios; ahora con los servicios integrados lo que se pretende es extender la arquitectura original, ya que proponer una nueva arquitectura sería una meta casi imposible. La arquitectura extendida está constituida por dos partes: el modelo de servicios entendidos (extended service model) llamado modelo IS y la referencia de la estructura de implantación (*reference implementación framework*). La razón principal de estas dos partes, es separar el comportamiento del servicio integrado de la manera como se implanta este servicio, ya que éste último puede ir cambiando según se estabilice el modelo" (Díaz Ataucuri , 2001, pág. 1)

RSVP: el protocolo de reservación de recursos

A decir de ANDREW S. TANENBAUM el protocolo de reservación de recursos vienen a ser: "La parte principal de la arquitectura de servicios integrados visible para los usuarios de la red es RSVP. Se describe en los RFC 2205-2210. Este protocolo se utiliza para hacer las reservaciones; se usan otros protocolos para enviar los datos. RSVP brinda la posibilidad de que varios emisores transmitan a múltiples grupos de receptores, permite que receptores individuales cambien de canal libremente, optimiza el uso de ancho de banda y al mismo tiempo elimina la congestión. En su forma más simple, el protocolo usa enrutamiento de multidifusión con árboles de expansión, como vimos antes. A cada grupo se le asigna una dirección. Para enviar a un grupo, un emisor pone la dirección asignada en sus paquetes. El algoritmo estándar de enrutamiento multidifusión construye entonces un árbol de expansión que cubre a todos los miembros del grupo. El

algoritmo de enrutamiento no es parte de RSVP. La única diferencia con la multidifusión normal es un poco de información adicional que se transmite por multidifusión al grupo en forma periódica, para indicarle a los enrutadores a lo largo del árbol que mantengan ciertas estructuras de datos en sus memorias" (Tanenbaum, 2012, pág. 359)

c) Servicios diferenciados

A decir de ANDREW S. TANENBAUM los servicios diferenciados vienen a ser: "Los algoritmos basados en flujo tienen el potencial de ofrecer buena calidad de servicio a uno o más flujos, debido a que reservan los recursos necesarios a lo largo de la ruta. Sin embargo, también tienen una desventaja. Requieren una configuración avanzada para establecer cada flujo, algo que no se escala bien cuando hay miles o millones de flujos. Además, mantienen el estado por flujo interno en los enrutadores, lo cual los hace vulnerables a las fallas de éstos. Por último, los cambios requeridos al código de enrutador son considerables e involucran intercambios complejos de enrutador a enrutador para establecer los flujos. Como consecuencia, aunque el trabajo continúa para mejorar los servicios integrados, existen pocas implementaciones de RSVP o algo parecido" (Tanenbaum, 2012, pág. 361).

2.2.4.2. Modelos de tunelización aplicados a *MPLS* con *QoS*

A través de la utilización de etiquetas se configura los túneles de esta manera, un túnel comienza donde se coloca una etiqueta al paquete y finaliza donde se la extrae, normalmente esto ocurre en los router de borde denominados *Label Switch Router* PE (LSR) (Luc, 2007, pág. 466). Los modos de tunelización o formas de transmitir los datos a través de la red son:

- Modo Uniforme
- Modo Tubería
- Modo Tubería corta

a) Modo Uniforme

En el modo de tunelización uniforme solamente se considera una capa de calidad de servicio, es decir, los paquetes son tratados uniformemente en las redes IP y *MPLS*, tanto el valor de la IP como el valor EXP de *MPLS* son idénticos. Sin embargo, un router puede cambiar o reescribir el valor de PHB de un paquete, este cambio debe ser reflejado tanto en el campo del paquete IP como del paquete *MPLS* (Luc, 2007, pág. 468).

Este modo de tunelización funciona de la siguiente manera:

- El valor de PHB es copiado en una nueva capa superior o en el campo del DSCP, esto ocurre tanto en las redes *MPLS-MPLS* como en las *MPLS-IP*.
- El campo del PHB es de 3 bits (8 posibles tipos de PHB)
- Si el campo PHB sobrepasa los 3 bits se debe realizar una tabla de mapeo desde el valor DSCP a *MPLS* justo a la entrada de la red *MPLS*
- De la misma manera, cuando el paquete sale de la red *MPLS* se debe volver a mapear el campo PHB para volver a tener el valor del campo DSCP en lugar del valor del EXP.

b) Modo Tubería

El modo tubería brinda una *QoS* en la interfaz de salida del LER de egreso, basada en el campo EXP de la cabecera *MPLS* recibida, aun cuando una o más etiquetas *MPLS* hayan

sido removidas. El sub campo precedencia del paquete IP, los bits del campo EXP y el sub campo DSCP no son alterados cuando el paquete es transmitido por la red *MPLS* (Luc, 2007, pág. 467).

Cualquier cambio en el marcado de los paquetes en el interior de la red *MPLS* no es permanente ni propagado cuando el paquete deja la red. El LER de egreso usa el marcado que fue usado por los LSRs. Sin embargo, este LER debe remover las etiquetas impuestas al paquete original, después de guardar una copia interna del marcado para clasificar el paquete en la interfaz de salida. La figura indica un ejemplo del comportamiento de los *routers* configurados con el modo tubería (Luc, 2007, pág. 467).

c) Modo de Tubería Corta

Posee la misma funcionalidad que un modelo de tubería normal con la única diferencia que las políticas de calidad de servicio, son aplicadas basándose en el valor del campo DSCP con el que llegue al destino el paquete (Luc, 2007, pág. 467).

La transmisión del paquete es similar a un modelo de túnel, en la trayectoria hacia el destino los valores del campo EXP de las etiquetas pueden ser cambiadas, pero al final de la transmisión se utiliza el campo del DSCP para aplicar las políticas de QoS (Luc, 2007, pág. 467).

2.2.4.3. Mecanismo de Gestión de Colas

El control de congestión involucra la creación de colas, asignación de paquetes a dichas colas basándose en la clasificación de los paquetes y la planificación de los paquetes en la cola para su transmisión (Chacha, 2019, pág. 30).

a) FIFO (First-In, First-Out)

Es el tipo más simple de encolamiento, se basa en el concepto de que el primer paquete en entrar a la interfaz es el primero en salir, como se indica en la Figura siguiente. La ventaja clave de FIFO es que requiere la menor cantidad de recursos del *router*. Sin embargo, su naturaleza simplista es también su desventaja principal, ya que como los paquetes salen por la interfaz en su orden de llegada, no es posible asignar prioridades al tráfico, ni evitar que una aplicación o usuario utilice en exceso el ancho de banda disponible (Chacha, 2019, pág. 30).

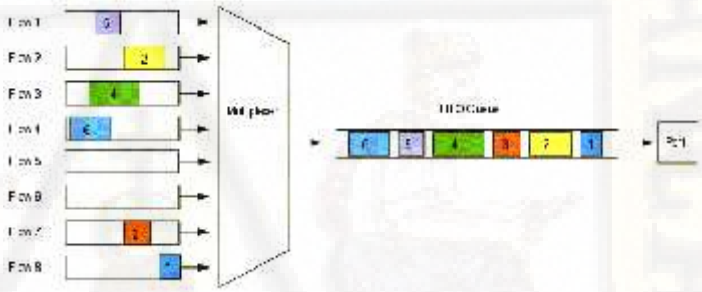


Figura Nº 2.8: Encolamiento de FIFO.

Fuente: Cisco 2017

b) WFQ (Weighted Fair Queueing)

WFQ es un algoritmo de encolamiento basado en flujos, que realiza dos cosas simultáneamente, programar el tráfico interactivo al frente de la cola para la reducción de tiempo de respuesta y compartir equitativamente el ancho de banda remanente entre flujos de gran ancho de banda. En la Figura 2.9 se observa un esquema del encolamiento del método WFQ (Chacha, 2019, pág. 31).

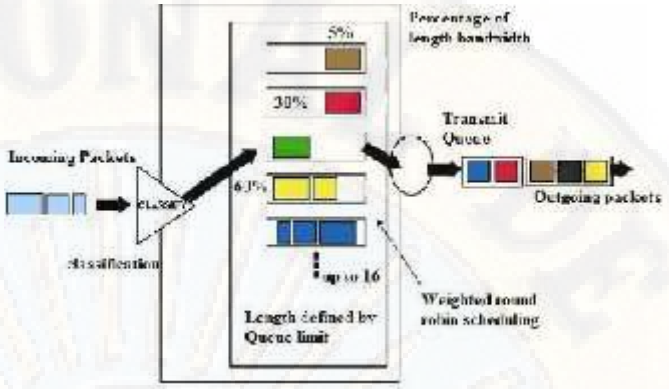


Figura Nº 2.9: Encolamiento de WFQ.

Fuente: Cisco 2017

c) *CBWFQ (*WFQ basado en clases*)*

CBWFQ permite la creación de clases definidas por el usuario, que permiten un mayor control sobre las colas de tráfico y asignación del ancho de banda.

Cada clase posee una cola separada y todos los paquetes que cumplen el criterio definido para una clase en particular son asignados a dicha cola. Una vez que se establecen los criterios para las clases, es posible determinar cómo los paquetes pertenecientes a dicha clase serán manejados. Si una clase no utiliza su porción de ancho de banda, otras pueden hacerlo. El peso asignado a la cola de la clase es determinado mediante el ancho de banda asignado a dicha clase (Chacha, 2019, pág. 31).

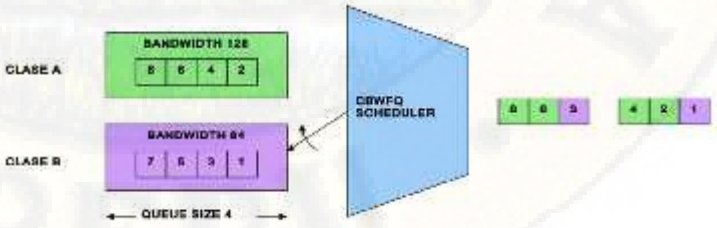


Figura Nº 2.10: Encolamiento de CBWFQ

Fuente: Cisco 2017

d) CQ (Custom Queueing)

En CQ, el ancho de banda es asignado proporcionalmente para cada clase de tráfico diferente. CQ permite especificar el número de bytes o paquetes que serán sacados de la cola. Se pueden crear hasta 16 colas para categorizar el tráfico, donde cada cola es atendida al estilo *round-robin*. Se utiliza CQ para proveer a tráficos particulares de un ancho de banda garantizado en un punto de posible congestión, asegurando para este tráfico una porción fija del ancho de banda y permitiendo al resto del tráfico utilizar los recursos disponibles. La gestión de colas CQ permite especificar qué porcentaje de ancho de banda se dedica a cada tipo de tráfico (Chacha, 2019, pág. 33).

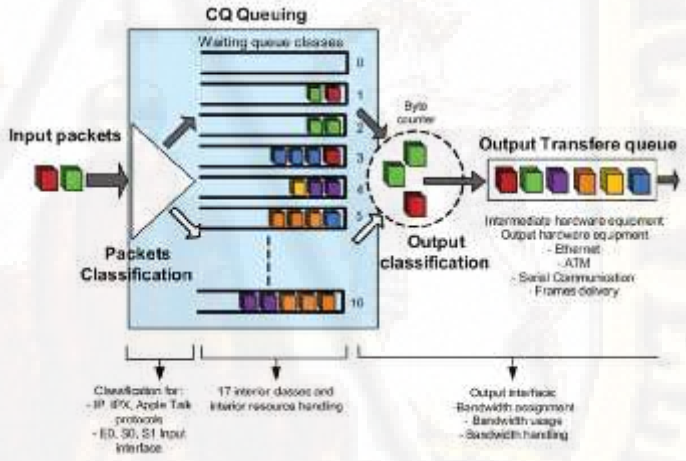


Figura Nº 2.11: Encolamiento de CQ.

Fuente: Cisco 2017

e) PQ (Priority Queueing)

PQ consiste en un conjunto de cuatro colas, clasificadas desde alta, hasta baja prioridad. Cada paquete es asignado a una de estas colas, las cuales son servidas en estricto orden de prioridad. Las colas de mayor prioridad son siempre atendidas primero, luego la siguiente de menor prioridad y así. Si una cola

de menor prioridad está siendo atendida, y un paquete ingresa a una cola de mayor prioridad, ésta es atendida inmediatamente (Nieto, 2010, p. 82). En la Figura 2.12, se observa el esquema de encolamiento PQ (Chacha, 2019, pág. 34).

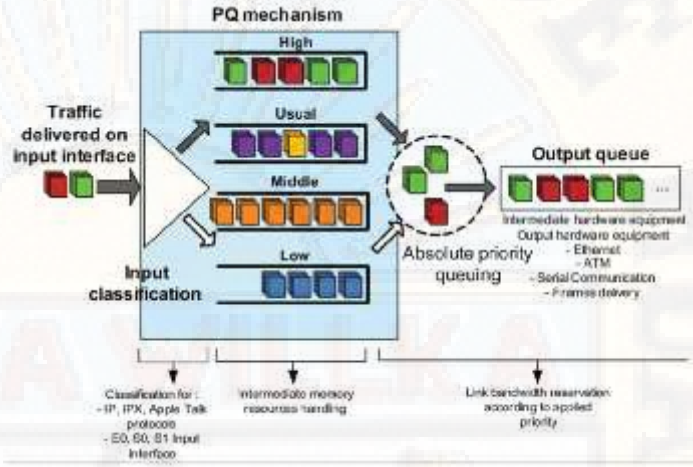


Figura Nº 2.12: Encolamiento de PQ.

Fuente: Cisco 2017

f) LLQ (Low Latency Queueing)

LLQ es una mezcla entre los métodos PQ y CBWFQ y es actualmente el método de encolamiento recomendado para VoIP y telefonía IP, por lo que también trabajará apropiadamente con tráfico de videoconferencia. LLQ consta de colas de prioridad personalizadas, basadas en clases de tráfico, en conjunto con una cola de prioridad, la cual tiene preferencia absoluta sobre las otras colas. Si existe tráfico en la cola de prioridad, ésta es atendida antes que las otras colas de prioridad personalizadas. Si la cola de prioridad no está encolando paquetes, se procede a atender las otras colas según su prioridad. Debido a este comportamiento es necesario configurar un ancho de banda límite reservado para la cola de prioridad (Chacha, 2019, pág. 34).

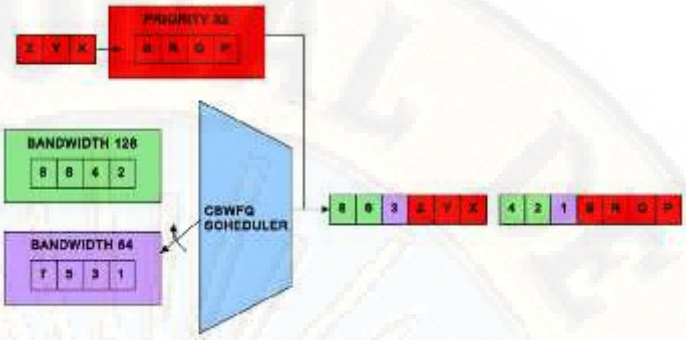


Figura Nº 2.13: Encolamiento de LLQ.
Fuente: Cisco 2017

2.2.4.4. Parámetros de calidad de servicio

Son las definiciones que caracterizan la calidad de servicio que se le va a brindar. Son acordados por contrato y establecen los valores máximos y/o mínimos (SLO) que pueden tener ciertos parámetros de performance. (Uba, 2016)

Parámetros a tener en cuenta para SLA

a) Throughput

Balakrishnan (2014) considera el flujo de tráfico de H1 a H3 a través de TrafficPath13, suponiendo que todos los recursos de red en la ruta están disponibles para el flujo de tráfico, el flujo de tráfico está sujeto por los siguientes recursos:

- La velocidad a la que H1 puede transmitir.
- El ancho de banda de L1.
- La velocidad a la que N1 puede recibir tráfico que llega a través de L1.
- La velocidad a la que N1 puede reenviar tráfico en su núcleo.
- La velocidad a la que N1 puede transmitir a través de L3.
- El ancho de banda de L3.

- La velocidad a la que H3 puede recibir tráfico que llega a través de H3.

El rendimiento del tráfico es la velocidad a la que el tráfico puede fluir a través del segmento más restringido en su camino. Dada la naturaleza dinámica del flujo de tráfico a través de una red, ya que diferentes recursos pueden convertirse en cuellos de botella en diferentes momentos (Balakrishnan, 2014, pág. 12).

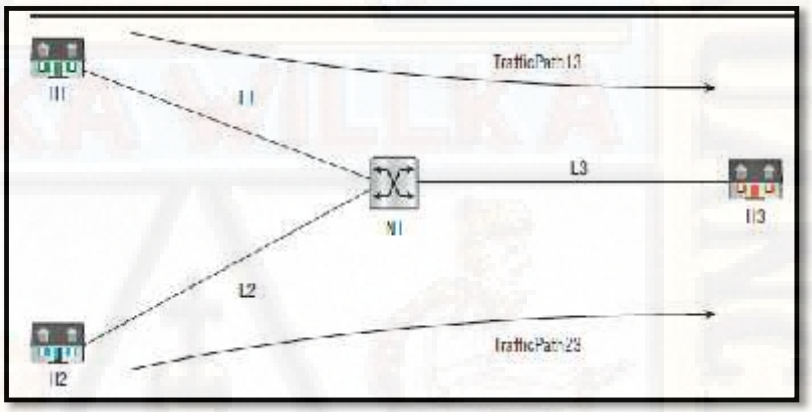


Figura Nº 2.14: Diagrama de red simple.

Fuente: ***Balakrishnan***

b) Delay

En general se especifica como el *Round-Trip Delay*, y es el tiempo en que la comunicación extremo a extremo tarda en ir y volver. También puede están discriminado en *delay source-destination y dest-source.*

RFC 2679 define una métrica para medir el retraso unidireccional como la diferencia en el tiempo en que el datagrama cruza dos puntos de referencia. El retraso de un datagrama experimentado dentro de una red de proveedor de servicios se define como la diferencia en la hora a la que el datagrama ingresa a la red y la hora a la que sale de la red, el

retraso también se conoce comúnmente como latencia (Ariganello & Enrique , 2013, pág. 13).

Cada elemento a través del cual fluye un datagrama en una ruta de tráfico aumentará el retraso experimentado por el datagrama. Por ejemplo, en TrafficPath13 dentro de la red ilustrada en la Figura anterior, los enlaces L1 y L3 impondrán un retraso de propagación, y el nodo N1 impondrá un retraso de procesamiento al tráfico que fluye a través de ellos (Balakrishnan, 2014, pág. 13).

Desde una perspectiva de SLA, el retraso es el retraso fijo promedio que experimentará el tráfico de una aplicación dentro de la red del proveedor de servicios (Balakrishnan, 2014, pág. 13).

c) *Jitter*

Es la reducción de *delay* entre paquetes, celdas de información o *Frames*. (También llamado *Delay variation*) *Jitter* positivo y *Jitter* negativo.

RFC 3393 ha definido una métrica para medir la fluctuación unidireccional, el Jitter es la variación en el retraso de la red que experimentan los datagramas, más específicamente, se mide como la reducción de retraso entre dos datagramas consecutivos que pertenecen a un flujo de tráfico (Balakrishnan, 2014, pág. 13).

En el ejemplo que se muestra en la Figura anterior, suponga que el tráfico de fondo fluye a través de TrafficPath23. El tráfico de fondo está en ráfaga y satura la capacidad del enlace L3 frecuentemente, en este escenario, cuando el puerto L3 está congestionado en N1, si los datagramas llegan a través de TrafficPath13, los datagramas se descartarán. Para evitar

soltar datagramas cuando un recurso se congestiona temporalmente, se crea espacio de almacenamiento intermedio disponible en nodos de red y los datagramas están en cola, hacer cola dentro de una red El nodo introduce la reducción de retraso entre diferentes datagramas de un flujo de tráfico (Balakrishnan, 2014, pág. 13).

Aunque la cola es la causa principal de la fluctuación de fase del tráfico, los largos retrasos de propagación de redireccionamiento y las demoras de procesamiento adicionales también pueden afectar la fluctuación de fase del tráfico.

d) Packet Loss

Pérdida de paquetes (también puede ser *CellLoss* para el tráfico de celdas o *FrameLoss* para el de tramas).

RFC2680 y RFC3357 tienen métricas definidas para medir la pérdida de tráfico unidireccional, la pérdida de tráfico caracteriza las caídas del datagrama que ocurren en la ruta de un flujo de tráfico unidireccional entre dos puntos de referencia: uno al principio cuando el tráfico ingresa a una red y el otro al final cuando el tráfico sale de la red. Aunque tener espacio de búfer para poner en cola temporalmente datagramas en nodos de red ayuda a la reducción de pérdida de datagramas, no se puede eliminar por completo (Balakrishnan, 2014, pág. 14). Algunos de los factores que contribuyen a la pérdida de datagramas según Balakrishnan (2014) son:

- Congestión: el tráfico en ráfagas puede causar desbordamientos de la cola y provocar la pérdida de datagramas.
- Limitación de la velocidad del tráfico: para garantizar que el tráfico de los clientes se ajuste a un SLA negociado, los

proveedores de servicios pueden limitar la velocidad del tráfico entrante y descartar datagramas no conformes.

- Errores de la capa física: el ruido en las capas físicas (como los enlaces satelitales) puede causar errores de bit. Como resultado, los protocolos de la capa superior pueden descartar datagramas.
- Fallos en los elementos de la red: los fallos en los elementos de la red pueden hacer que los datagramas se caigan hasta que se detecte el fallo y se restablezca la conectividad.

Como se especifica en RFC3357, para algunas aplicaciones en tiempo real (como la transmisión de tráfico de video), ciertas características de pérdida de datagramas son más importantes que la cantidad real de datagramas perdidos según Balakrishnan (2014) son:

- Distancia de pérdida: la diferencia en el número de secuencia entre dos sucesivamente paquetes perdidos (que pueden o no estar separados por paquetes recibidos con éxito).
- Período de pérdida: la duración de un evento de pérdida o error una vez que comienza. En otras palabras, el período de pérdida se define como la frecuencia con la que ocurre la pérdida y el número de paquetes consecutivos descartados cada vez que ocurre la pérdida.

2.2.4.5. Calidad de funcionamiento para diferentes aplicaciones o servicios

Según la Unión Internacional de Telecomunicaciones UIT-T G.1010 (2008) los tipos de servicios se clasifican de acuerdo al tipo de tráfico que genera, que a continuación se tiene:

a) Servicio de audio o Voz

Se tiene una clasificación general del audio en cinco niveles de calidad y los niveles de calidad de audio necesarios para diversos servicios. A continuación, se menciona algunas aplicaciones de audio.

- Voz en conversación.
- Mensajería vocal
- Audio en tiempo real

b) Servicio de Vídeo

El servicio de video tiene una clasificación general del vídeo en seis niveles de calidad y los niveles de calidad de vídeo necesarios para diversos servicios. A continuación, se menciona algunas aplicaciones de video.

- Videoteléfono
- Vídeo en un sentido

c) Servicio de Datos

Desde el punto de vista del usuario, el requisito principal para cualquier aplicación de transferencia de datos es garantizar, en la medida de lo posible, una pérdida de información nula. Al mismo tiempo, el usuario casi nunca percibe la variación de retardos, si bien en una sesión multimedios tiene que haber un cierto grado de sincronización entre los trenes de los medios. Por consiguiente, un criterio para distinguir entre las aplicaciones es el retardo que puede tolerar el usuario extremo desde el momento en que el contenido fuente se solicita hasta el momento en que se le presenta al usuario.

- Navegación en la Web
- Gran volumen de datos

- Servicios de transacciones de alta prioridad (comercio electrónico)
- Modo dirigido/control
- Juegos interactivos
- Telnet

2.3. Formulación de hipótesis

2.3.1. Hipótesis general

Un modelo de red con tecnología *MPLS* influirá significativamente en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

2.3.2. Hipótesis específico

a) Un modelo de red con tecnología *MPLS* influirá significativamente en el ***delay*** en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

b) Un modelo red con tecnología *MPLS* influirá significativamente en el ***jitter*** en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

c) Un modelo red con tecnología *MPLS* influirá significativamente en la ***packet loss*** en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

2.4. Definición de términos

a) ***Backbone*.-** Un sistema de transmisión utilizado para interconectar redes de distribución de menor velocidad (González , 2011, pág. 221).

b) Calidad. - La totalidad de las características de una entidad que determinan su capacidad para satisfacer las necesidades explícitas e implícitas. (Itu, 2008, pág. 03)

c) *CIDR*. - Enrutamiento Interdominio sin Clases que consiste en asignar bloques de direcciones IP de manera que las direcciones se utilicen con eficiencia, de todas formas, hay un problema presente: la explosión de las tablas de enrutamiento (Tanenbaum, 2012, pág. 382).

d) *Diff-Serv*.- Los Servicios Diferenciados (*DiffServ o DS*) proporcionan un método que intenta garantizar la calidad de servicio en redes de gran tamaño, como puede ser Internet (Uit, 2003, pág. 14)

e) Emulador.- Software que permite ejecutar programas de ordenador en una plataforma hardware o software diferente de aquella para la cual fueron escritos originalmente (Cisco Ccna, 2017).

f) *Int-Serv*.- Servicios Integrados o *IntServ* constituyen una arquitectura cuyo cometido es gestionar los recursos necesarios para garantizar calidad de servicio (*QoS*) en una red de computadores. (Uit, 2003, pág. 13)

g) IP. – Provienes de las siglas de inglés (*Internet Protocol*) es parte del conjunto de protocolos TCP/IP y es el protocolo de interconexión de redes más utilizado, como con cualquier protocolo estándar, IP (Stallings, 2012, pág. 608).

h) Modelo.- Representación simplificada de un objeto o proceso en la que se representan algunas de sus propiedades. (Felicisimo, 2012, pág. 07)

i) *MPLS*. – Proviene de las siglas de inglés (Multiprotocolo Rabel Switching) traducido al español significa la conmutación de etiquetas multiprotocolo, es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031 que opera entre la capa de enlace de datos y la capa de red del modelo OSI. (Rfc, 2001, pág. 03)

j) Nodo. - Una estación de trabajo en red o cualquier otro dispositivo unido a la red. Un nodo, término derivado de la palabra nódulo, es de hecho el punto de referencia que utiliza la red para identificar lo que esté unido a la red. (Rodriguez, 2007, pág. 10)

k) Red. - Sistema de comunicación de datos que conecta entre sí sistemas

informáticos situados en lugares más o menos próximos. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes. En inglés se le conoce como Network. El internet está compuesto de miles de redes, por lo tanto al internet también se le conoce como "la red" (Cisco Ccna, 2017)

l) Servicio. - El conjunto de funciones ofrecidas al usuario por una organización constituye un servicio. (Itu, 2008, pág. 04)

m)TCP. - Protocolo de la capa de transporte orientado a conexión que proporciona una transmisión confiable de datos de full dúplex, TCP es parte de la pila de protocolo TCP/IP (Rodriguez, 2007, pág. 12).

n) Tecnología. - Con frecuencia conocimiento científico, pero también conocimiento organizado en otra forma, aplicado sistemáticamente a la producción y distribución de bienes y servicios. (Lemarchand, 2008, pág. 23)

o) Topología: Organización física de la red de bus, de anillo y de estrella son las topologías más comunes de las redes. (Rodriguez, 2007, pág. 12)

p) Transporte. - Trasladar una composición de un tono a otro. (Real Academia Española, 2001)

q) *UDP*. – Proviene de las siglas de inglés (*User Datagram Protocol*) es un protocolo que utiliza un esquema de datagramas sobre IP, que no garantiza la comunicación, es decir, los paquetes pueden no llegar, llegar correctamente, duplicados o fuera de orden (Postel, Crocker , & Cerf, 2009, pág. 29).

r) UIT-T.- La Unión Internacional de Telecomunicaciones (UIT) es una organización internacional perteneciente a las Naciones Unidas en la que los gobiernos y el sector privado coordinan las redes y los servicios globales de telecomunicación. El Sector para la Normalización de las Telecomunicaciones (UIT-T) es uno de los tres sectores de la UIT. Su misión es la especificación de normas en el campo de las telecomunicaciones. (Stallings, 2012, pág. 5)

s) *VPN*. – Provienes de las siglas de inglés (*Virtual Private Network*) Red Virtual Privada que permite que varios sitios conectados uno al otro para contactarse

con cada uno sin marcar todos los once dígitos. (Icmas, 2001, pág. 29)

t) ***WAN*.-** Red que interconecta dos o más *LAN* utilizando alguna forma de línea de telecomunicaciones, como las líneas telefónicas o dedicadas de alta velocidad (Rodriguez, 2007, pág. 13).

2.5. Identificación de variables

a) Variable independiente (Causa)

- Modelo de red con tecnología *MPLS*. (independiente)

b) Variable dependiente (Efecto)

- Calidad de servicio (dependiente)

2.6. Operacionalización de variables

VARIABLES	DEFINICION OPERATIVA DE VARIABLES	DIMENSIONES	INDICADORES
Variable independiente Modelo de red con tecnología *MPLS*.	El *MPLS* es una tecnología que permite transportar diferentes tipos de tráfico.	Modelo de red con *MPLS*.	• La conmutación de paquetes por etiquetas.
Variable dependiente Calidad de servicio.	La calidad de servicios comprende requerimientos en todos los aspectos de una conexión.	*Delay*	• Datos • Voz • Video
		Jitter	• Datos • Voz • Video
		Packet Los	• Datos • Voz • Video

Cuadro Nº 2.3: Operacionalización de variables

Fuente: Elaboración propia.

CAPÍTULO III
METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Tipo de investigación

El proyecto de investigación desarrollado por la naturaleza de las variables de estudio se ubicó dentro del tipo de investigación aplicada, llamado también utilitaria o tecnológica, porque tuvo como objetivo: Determinar la influencia del modelo de red con tecnología *MPLS* en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018. Es decir, tal como manifestó José Lozada "la investigación aplicada tiene por objetivo la generación de conocimiento con aplicación directa y a mediano plazo en la sociedad o en el sector productivo, este tipo de estudios presenta un gran valor agregado por la utilización del conocimiento que proviene de la investigación básica" (Sanchez & Reyes, 2017, pág. 44)

3.2. Nivel de investigación

Según Sanchez y Reyes (2017) el presente trabajo de investigación desarrollado se ubicó en el nivel de la investigación explicativa debido a que; "nos permitirá explicar tentativamente la ocurrencia de un fenómeno"; el objetivo a lograr ha sido: Determinar la influencia del modelo de red con tecnología *MPLS*

en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018. Se justifica lo expuesto anteriormente porque: se tomó en cuenta la información proveniente de las distintas facultades que generan tráfico en la red, asimismo se realizó el análisis de tráfico de los distintos servicios en un pre y post análisis con lo que se implementó la tecnología *MPLS* para mejorar la calidad de servicio.

3.3. Métodos de investigación:

3.3.1. Método general

El método general que reguló todo el proceso de la investigación fue: el método científico o dialéctico cuyos procedimientos son: identificación del problema; selección y revisión bibliográfica y hemerografía; construcción de las bases teóricas; formulación de hipótesis; contrastación de hipótesis; análisis y discusión de resultados y comunicación de resultados de la investigación.

3.3.2. Métodos particulares

Los métodos particulares que se utilizaron en el desarrollo teórico práctico de la investigación fueron:

3.3.2.1. Método Experimental

Según Sánchez y Reyes (2017) debido a que se organiza deliberadamente las condiciones, “con el fin de investigar las posibles relaciones causa-efecto del problema en estudio” exponiendo a un grupo experimental la acción de una variable experimental que es la tecnología *MPLS* y “contrastando sus resultados con grupos de control o de comparación” (Sanchez & Reyes, 2017, pág. 67).

3.3.2.2. Método Bibliográfico

El método bibliográfico fue un recurso que nos permitirá recolectar, sistematizar y organizar la información bibliográfica relacionado con las variables de estudio, apoyado por la técnica del fichaje.

3.3.2.3. Método de Observación

Procedimiento que fue útil para percibir las características de los parámetros de calidad de servicio en la transmisión de voz, video y datos, en una topología definida a nivel de simulación de la red de datos de la Universidad Nacional de Huancavelica.

3.3.2.4. Método Descriptivo

El método descriptivo nos permitió enumerar las características técnicas de transmisión de los diferentes tipos de servicios a través de la red de datos de la Universidad Nacional de Huancavelica.

3.4. Diseño de la investigación

El diseño para la contratación de la hipótesis fue el diseño experimental con un solo grupo con Pretest y Postest, cuyo esquema es el siguiente:

$$M: \quad O_1 \quad X \quad O_2$$

Donde:

M = muestra

O_1: Calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica (Estado actual – Prestest)

O_2: Calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica (Estado posterior-Postest)

X: Modelo de red con tecnología *MPLS*

3.5. Población, muestra y muestreo

3.5.1. Población. - La población de estudio estuvo constituido por todas las redes *WAN* de la Universidad nacional de Huancavelica que tiene conexión con las Facultades, que a través de esta red fluye todo los servicios o aplicaciones que generan los tres tipos de tráfico de voz, video y datos que provienen de las distintas áreas o unidades, lo cual es producido por los usuarios que acceden a los distintos servicios a través de la red.

3.5.2. Muestra. - La muestra de estudio para el presente trabajo de investigación se consideró las diez redes *WAN* que hace la conexión entre la Casa Rosada (Local administrativo) y los cinco campus universitarios, a través de estas redes se hará la prueba de tres tipos de servicio que requieren mayor ancho de banda y la vez generan mayor tráfico que son: VoIP, Video Streaming y FTP, desde la sala de videoconferencia de la Universidad Nacional de Huancavelica.

3.5.3. Muestreo. - En la investigación realizada el muestreo fue de manera no probabilística, por lo que se optó las diez redes *WAN*, para inyectar los tres tipos de tráfico de mayor representatividad.

3.6. Técnicas e instrumentos de recolección de datos

Las técnicas e instrumentos de recolección de datos que se utilizó en la ejecución del presente proyecto de investigación son:

3.6.1. Técnicas de recolección de datos

a. Simulación. – La técnica que sirvió para realizar el modelamiento de la red de datos con diferentes tipos de tráfico.

b. Medición. – La técnica que sirvió para evaluar la calidad de servicio de la red de transporte de datos**.**

c. Observación directa. – La técnica que sirvió para la recopilación de datos del estado de la infraestructura de la red de transporte y la calidad de servicios para los servicios de VoIP, video Streaming y datos.

3.6.2. Instrumento de recolección de datos

Los instrumentos que se utilizaron para recolección de datos son tres, la primera y segunda son reconocidas por la UIT-T G.1010 y la tercera es validada por los especialistas en el área de electrónica y telecomunicaciones.

a. *GNS3*.- Es una herramienta que se utilizó para realizar la simulación de la topología de la red de datos.

b. *D-ITG*. - El software que se utilizó para analizar los datos de los parámetros de la calidad de servicio (*delay*, *jitter* y packet loss) de una red, que fluye los diferentes tipos de tráfico.

c. Ficha de observación. - Instrumento que se utilizó para registrar los datos de observación con respectos a las pruebas realizadas a través de la red de datos en presencia de tráfico.

Configuración de *D-IGT*

Para la recolección de datos del escenario establecido, se utilizó el software *D-ITG*, a través de este instrumento se ha obtenido los datos de los diferentes tipos de servicios, para lo cual se realizó el siguiente procedimiento:

- Instalación del software *D-ITG* en el servidor y cliente, para el sistema operativo Windows de 32 bits.
- Configuración del emisor de acuerdo al tipo de tráfico que se va enviar hacia el receptor de extremo a extremo a través de la topología de la red.

Configuración del emisor

En el diagrama abajo se muestra la configuración de *D-ITG*, de la opción de *Define Flow*, para definir el tipo de tráfico o servicio que se va enviar hacia el receptor.

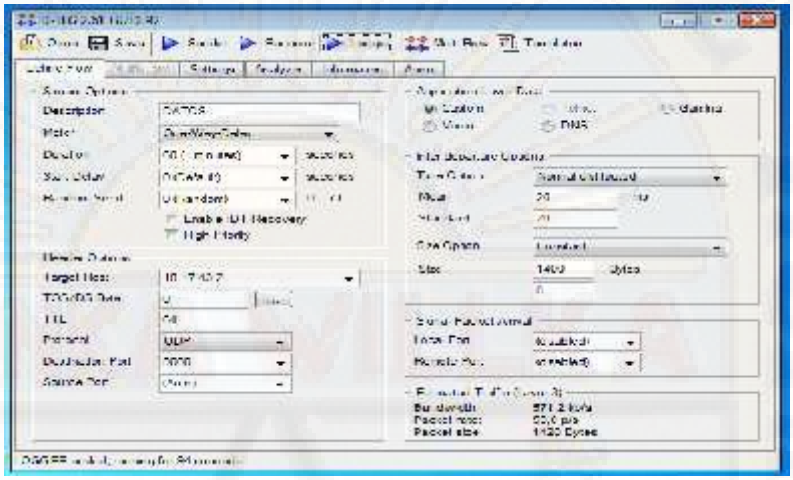


Figura Nº 3.1: Configuración de Define Flow del emisor.

Fuente: Elaboración Propia.

En el diagrama abajo se muestra la configuración de *D-ITG*, de la opción de *Setings*, para definir el host como servidor en el emisor.

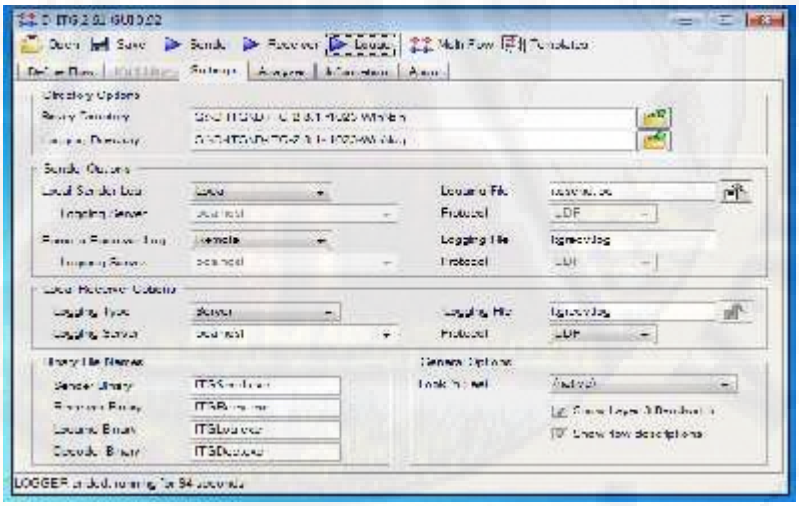


Figura Nº 3.2: Configuración de Setings del emisor.

Fuente: Elaboración Propia.

En el diagrama abajo se muestra la configuración de *D-ITG*, de la opción de *Analyzer*, para definir el tipo de archivo a generar en el emisor.

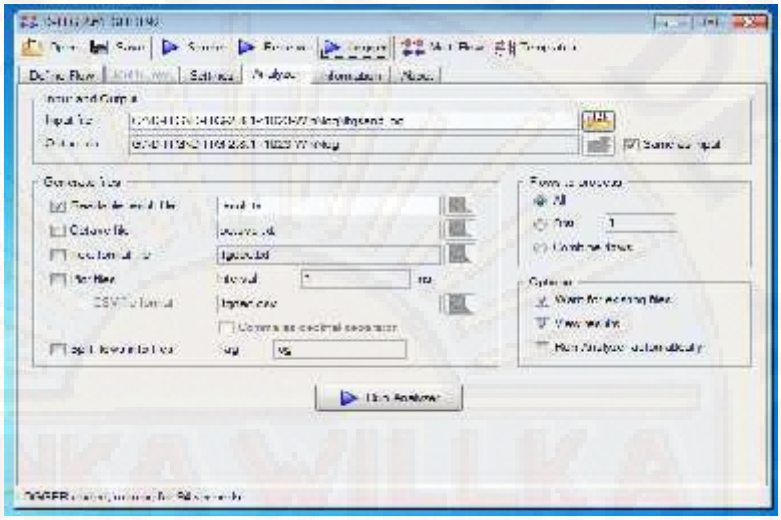


Figura Nº 3.3: Configuración de Analyzer del emisor.

Fuente: Elaboración Propia.

Configuración del receptor.

En el diagrama abajo se muestra la configuración de *D-ITG*, de la opción de Define Flow, para definir el tipo de tráfico de recepción.

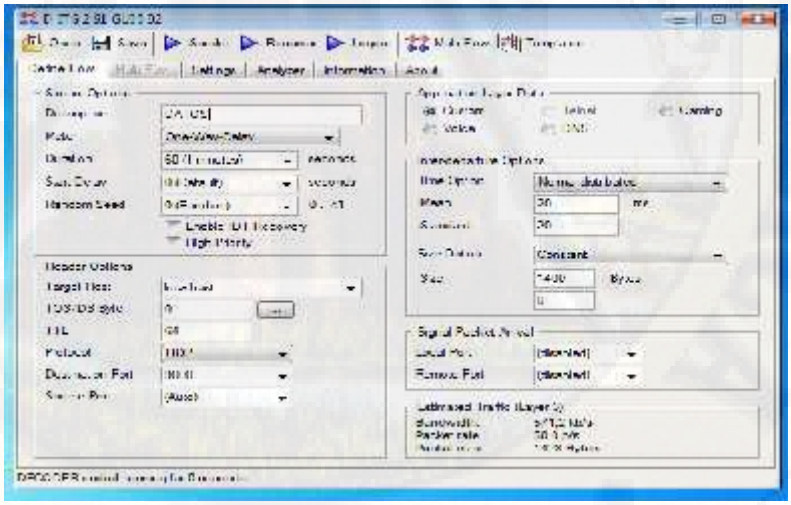


Figura Nº 3.4: Configuración de Define Flow del receptor.

Fuente: Elaboración Propia.

En el diagrama abajo se muestra la configuración de *D-ITG*, de la opción de Setings, para definir como cliente.

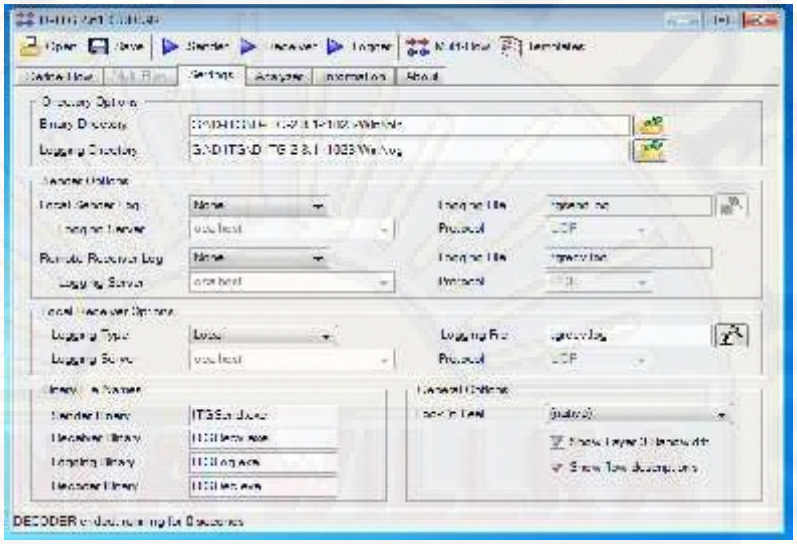


Figura Nº 3.5: Configuración de Setings del receptor

Fuente: Elaboración Propia.

En el diagrama abajo se muestra la configuración de *D-ITG*, de la opción de *Analyzer*, para definir el tipo de archivo a generar en el receptor de resultado.

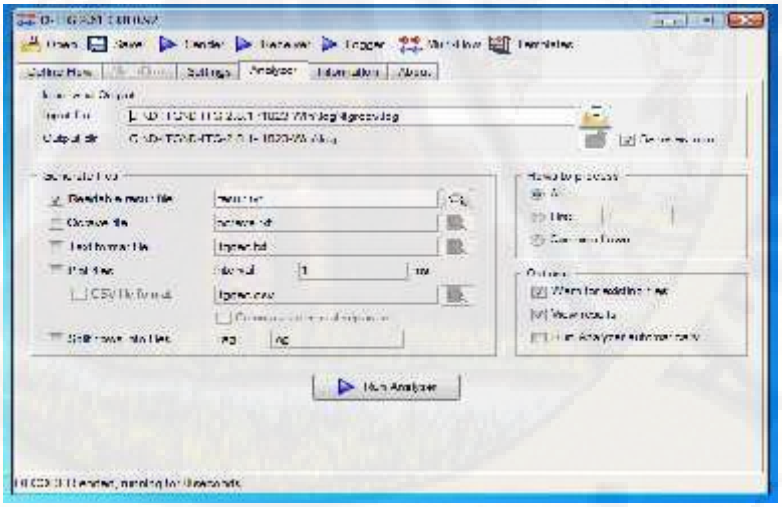


Figura Nº 3.6: Configuración de Analyzer del receptor

Fuente: Elaboración Propia.

Resultados obtenidos

En el receptor se obtiene los resultados del tipo de tráfico enviado desde del emisor al receptor de extremo a extremo, obteniendo el resultado con *D-ITG*, los parámetros de calidad de servicio (*QoS*) de la red *WAN*.

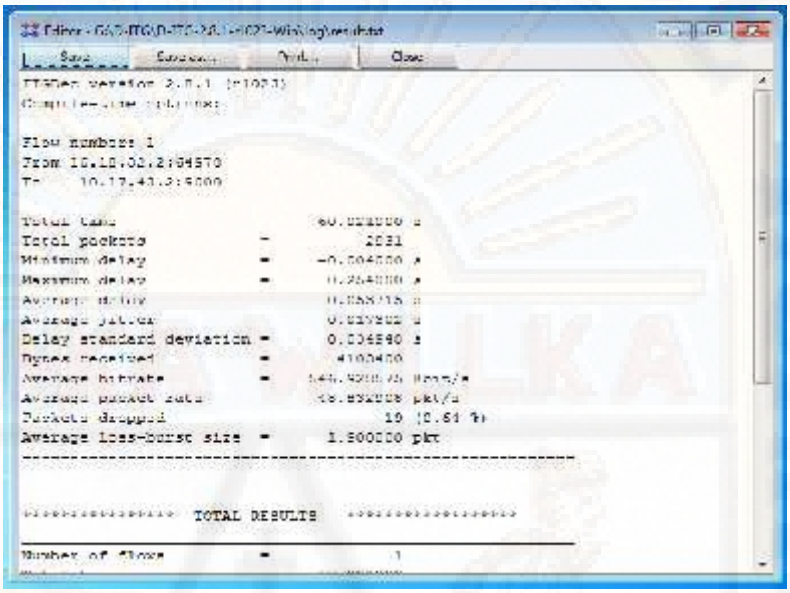


Figura Nº 3.7: Generación del resultado en el receptor.

Fuente: Elaboración Propia.

3.6.3. Actividades realizadas para la recolección de datos

- Diagnóstico de la red *Wan* de la Universidad Nacional de Huancavelica.
- Levantamiento de datos de la topología de la red *Wan* de la Universidad Nacional de Huancavelica.
- Elaboración de la topología de la red *Wan* en *GNS3* de la Universidad Nacional de Huancavelica.
- Configuración de la tecnología IP en los routers que conforma la topología de la red *Wan* de la universidad nacional de Huancavelica.
- Instalación de máquinas virtuales y sistemas operativos en *virtualbox*.
- Prueba de interconexión de host mediante el comando ping.
- Instalación y Configuración de *D-ITG* en cada host.
- Prueba de inyección del tipo de tráfico en la red de transporte.

- Evaluación e análisis de los parámetros de a calidad de servicio con DI-TG.
- Configuración de la tecnología *MPLS* en los routers que conforma la topología de la red *Wan* de la universidad nacional de Huancavelica.
- Evaluación e análisis de los parámetros de a calidad de servicio con *MPLS*.
- Prueba de inyección del tipo de tráfico en la red de transporte con *MPLS*.
- Comparación de los resultados obtenidos con ambas tecnologías IP y *MPLS*.

3.6.4. La red *WAN* de la Universidad Nacional de Huancavelica

Para el diseño de la red *WAN* de la universidad Nacional de Huancavelica se realizó el análisis de la infraestructura de la red de transporte, a través del cual, se realiza la comunicación con las cinco sedes o campos universitario ubicado en distintas provincias de la región Huancavelica.

En la siguiente tabla se presenta el sistema de coordenadas geográficas de cada campus universitario que está ubicado en distintas provincias, desde allí se tiene acceso a todos los servicios internos que se encuentra en la sede central.

Tabla Nº 3.1: Coordenadas geográficas

Campos Universitario	Coordenadas geográficas		
	Longitud	Latitud	Altitud
Facultad de ingeniería Electrónica y Sistemas - Pampas	-74.872528°	-12.395550°	3250 msnm
Escuela Profesional de Ingeniería de Sistemas - Pampas	-74.859440°	-12.389109°	3250 msnm

Facultad de ingeniería Electrónica Minas - civil - Lircay	-74.721832°	-12.996457°	3283 msnm
Facultad de Ciencias Agrarias - Acobamba	-74.562509°	-12.843306°	3401 msnm
Ciudad Universitaria - Paturpampa	-74.960932°	-12.777741°	3730 msnm
Local Administrativo – Casa Rosada.	-74.974416°	-12.786252°	3683 msnm

Fuente: Elaboración Propia – Google *Earth*.

En la figura siguiente se presenta la ubicación de cada campus universitario de la Universidad Nacional de Huancavelica, tal como son: La ciudad Universitaria de Paturpampa, Local administrativo (Casa rosada), Sede Acobamba, Sede Lircay, Sede Pampas y Sede Daniel Hernández.

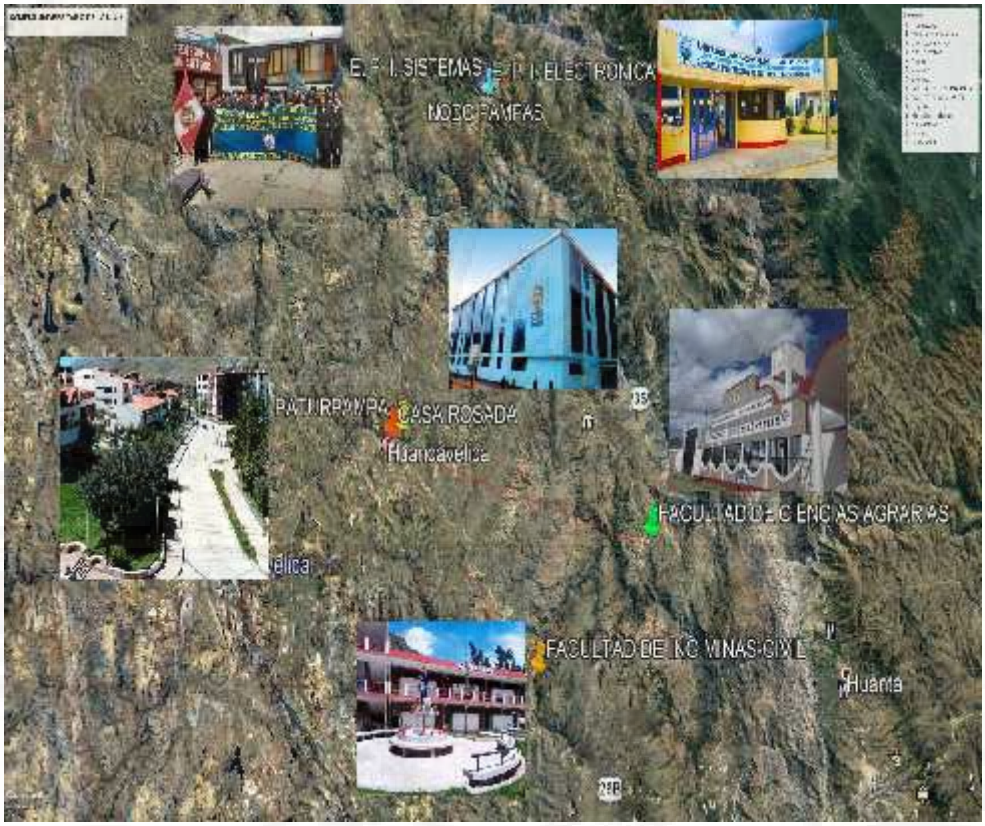


Figura Nº 3.8: Campus universitario de la Universidad Nacional de Huancavelica.
Fuente: Elaboración propia – Google Earth.

Topología de la red *WAN*

En el diagrama siguiente se tiene la topología de la red de transporte de la Universidad Nacional de Huancavelica, que está constituido por los siguientes partes: la red *WAN* y la red *LAN*. La tecnología *MPLS* se implementó en el router Cisco de 7200, que forma parte de la red de *Backbone* o en la red de área amplia (*WAN*), para mejorar la calidad de servicio de transporte de datos y de conexión, mediante la tecnología *MPLS*/*VPN*. En la figura siguiente se observa la comunicación a través de la red privada virtual (*VPN*) entre la sede central y las Sedes correspondientes que se encuentran en distintas provincias de la región Huancavelica.

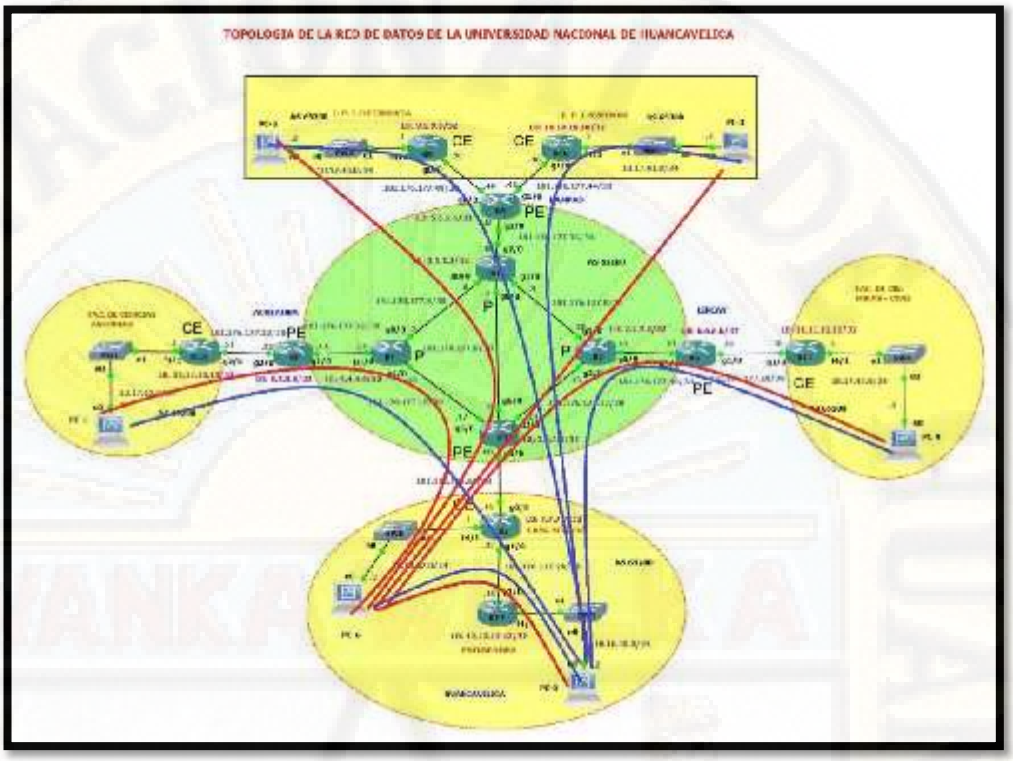


Figura Nº 3.9: Topología de la red *WAN* de la Universidad Nacional de Huancavelica.

Fuente: Elaboración propia.

Enlace WAN

Enlace 1: Casa Rosada (PC6) –Acobamba (PC1)

Enlace 2: Casa Rosada (PC6) -Pampas (E)(PC2)

Enlace 3: Casa Rosada (PC6) –Pampas (s)(PC3)

Enlace 4: Casa Rosada (PC6)-Lircay (PC4)

Enlace 5: Casa Rosada (PC6) –Paturpampa (PC5)

Enlace 5: Paturpampa (PC5) –Acobamba (PC1)

Enlace 7: Paturpampa (PC5) –Pampas (E)(PC2)

Enlace 8: Paturpampa (PC5) –Pampas (S)(PC3)

Enlace 9: Paturpampa (PC5) –Lircay (PC4)

Enlace 10: Paturpampa (PC5) -Casa Rosada (PC6)

Direccionamiento IP

En el siguiente cuadro se tiene la dirección IP de los equipos que componen la red de área amplia (*WAN*).

Tabla Nº 3.2: Direccionamiento IP de los equipos.

DIRECCIONAMIENTO IP DE LA RED *WAN* DE LA UNIVERSIDAD NACIONAL DE HUANCAVELICA					
LUGAR (ROUTER)	**DIRECCION IP**	**ROUTER**	**INTERFACES**	**IP**	**PROTOCOLO**
ROUTER PAMPAS ELECTRÓNICA CE	10.17.40.0	R9	F4/1	10.17.40.1	*BGP*
			G0/0	181.176.177.50	*BGP VRF*
ROUTER PAMPAS SISTEMAS CE	10.17.41.0	R10	F4/1	10.17.41.1	*BGP*
			G1/0	181.176.177.46	*BGP VRF*
ROUTER LIRCAY MINAS-CIVIL CE	10.17.43.0	R11	F4/1	10.17.43.1	*BGP*
			G1/0	181.176.177.30	*BGP VRF*
ROUTER PATURPAMPA CE	10.16.30.0	R12	F4/1	10.16.30.1	*OSPF*
			G1/0	181.176.177.26	*OSPF*
LOCAL ADMINISTRATIVO CE	10.18.32.2	R7	F4/1	10.18.32.1	*BGP*
			G1/0	181.176.177.25	*OSPF*
			G0/0	181.176.181.65	*BGP VRF*
ROUTER ACOBAMBA AGRONOMIA	10.17.42.0	R13	F4/1	10.17.42.1	*BGP*
			G2/0	181.176.177.21	*BGP VRF*

AGROINDUSTRIAL CE					
BACKBONE	P	R1	G0/0	181.176.177.6	*OSPF*
			G1/0	181.176.177.9	*OSPF*
			G2/0	181.176.177.38	*OSPF*
			G6/0	181.176.177.2	*OSPF*
BACKBONE	P	R2	G1/0	181.176.177.10	*OSPF*
			G2/0	181.176.177.13	*OSPF*
			G5/0	181.176.177.42	*OSPF*
BACKBONE	PE	R3	G0/0	181.176.181.66	*BGP VRF*
			G2/0	181.176.177.14	*OSP*
			G5/0	181.176.177.17	*OSPF*
			G6/0	181.176.177.1	*OSPF*
BACKBONE	P	R4	G0/0	181.176.177.5	*OSPF*
			G1/0	181.176.177.34	*OSPF*
			G5/0	181.176.177.18	*OSPF*
BACKBONE	PE	R5	G0/0	181.176.177.49	*BGP VRF*
			G1/0	181.176.177.45	*BGP VRF*
			G2/0	181.176.177.37	*OSPF*
BACKBONE	PE	R6	G1/0	181.176.177.29	*BGP VRF*
			G5/0	181.176.177.41	*OSPF*
BACKBONE	PE	R8	G1/0	181.176.177.33	*OSPF*

			G2/0	181.176.177.22	*BGP VRF*

Fuente: Elaboración Propia – Universidad Nacional de Huancavelica.

3.7. Técnicas de procesamiento y análisis de datos

3.7.1. Simbólica. - Las técnicas de procesamiento y análisis de datos que se utilizaron en el desarrollo de la investigación fueron la estadística descriptiva, con la cual se hallarán las medidas de tendencia central (media aritmética, mediana y moda) y las medidas de dispersión (desviación estándar, rango y varianza), seguidamente se diseñaron las tablas de frecuencias y los gráficos correspondientes. Así mismo, se utilizó la estadística inferencial para hallar los parámetros correspondientes y se utilizó el paquete estadístico SPSS y Excel.

3.7.2. Hermenéutica. - Los datos procesados y analizados estadísticamente se procedieron a interpretar mediante el uso de un lenguaje literal accesible a la comunidad científica interesada por el trabajo de investigación.

3.8. Descripción de la prueba de hipótesis

Para el contraste de la hipótesis se utilizó el software *GNS3* consta de un paquete de protocolos y tecnologías con un sofisticado entorno de desarrollo, que permite probar y demostrar diseños tecnológicos antes de la producción o implementación. GSN3 es uno de los softwares al igual que el *Opnet Modeler*, lo más utilizado en la actualidad para realizar la investigación y desarrollo de redes complejas.

Para la presente investigación se utilizó la prueba t, es una prueba de hipótesis basada en el estadístico *T-Student*, que sigue la distribución normal estándar bajo la hipótesis nula.

CAPÍTULO IV

PRESENTACIÓN DE RESULTADOS

4.1. Presentación e interpretación de datos

Para la presentación e interpretación de los datos se utilizó distintos softwares para su mayor confiabilidad tales como: *GNS3*, *D-ITG*, Excel y *SPSS*. Los datos se han obtenido a través de la prueba realizada en las redes *WAN* de la Universidad Nacional de Huancavelica, la prueba se realizó desde la sede central hacia las sucursales, que consistió en medir los parámetros de calidad de servicio(*QoS*) establecidas por la Unión Internacional de Telecomunicaciones (ITU) en los tres tipos de servicios: servicio de datos, servicio de VoIP y servicio de video streaming. A continuación, se detalla los datos de cada uno de estos servicios y la estructura de la red.

4.1.1. Resultados de la prueba de parámetros de calidad de servicio en la red *WAN*.

Los resultados de calidad de servicio, se obtuvieron para los tres tipos de servicios (Datos, VoIP y *Streaming*), para lo cual, se realizaron las pruebas en cada red *Wan*, de los siguientes parámetros: *delay*, *jitter y packet loss*. Para el servicio de datos la prueba se realizó enviando el tamaño de

paquetes de 1400 bytes de extremo a extremo, para el servicio de VoIP la prueba se realizó enviando el tráfico de voz con una codificación de G.711 de extremo a extremo y para el servicio de *streaming* la prueba se realizó enviando el tráfico de video streaming con el tamaño trama de 1500 bytes de extremo a extremo.

4.1.1.1. Resultados de la calidad de servicio - *Delay*

En las siguientes tablas se presenta los datos obtenidos de la prueba con respecto al *delay*, de cada enlace, desde el Local Administrativo (casa rosada) hacia las sucursales y desde la ciudad universitaria de Parturpampa hacia las sedes de la Universidad Nacional de Huancavelica, para la generación de tráfico y la medición de los parámetros de calidad de servicio (*QoS*), se hizo con la ayuda del software *D-ITG*.

a) Resultados de *delay* con el servicio de datos

Tabla Nº 4.1: Resultados de *delay* con el servicio de datos.

ENLACE DE RED *WAN*	SERVICIO DE DATOS	
	PARAMETROS DE CALIDAD DE SERVICIO	
	DELAY (S)	*DELAY (S)*
	TECNOLOGIA IP PRETEST	TECNOLOGIA *MPLS* POSTEST
CASA ROSADA(PC6) - ACOBAMBA(PC1)	0.0705	0.0236
CASA ROSADA(PC6) - PAMPAS (E)(PC2)	0.1638	0.0996
CASA ROSADA(PC6) - PAMPAS(S)(PC3)	0.0469	0.0462
CASA ROSADA(PC6)- LIRCAY(PC4)	0.0964	0.0018
CASA ROSADA(PC6) - PATURPAMPA(PC5)	0.1942	0.0587

PATURPAMPA(PC5) - ACOBAMBA(PC1)	0.3061	0.1100
PATURPAMPA(PC5) -PAMPAS (E)(PC2)	0.4239	0.1536
PATURPAMPA(PC5) - PAMPAS(S)(PC3)	0.1427	0.1269
PATURPAMPA(PC5) - LIRCAY(PC4)	0.0518	0.0452
PATURPAMPA(PC5) -CASA ROSADA(PC6)	0.1497	0.0747

Fuente: Elaboración Propia – Ficha técnica.

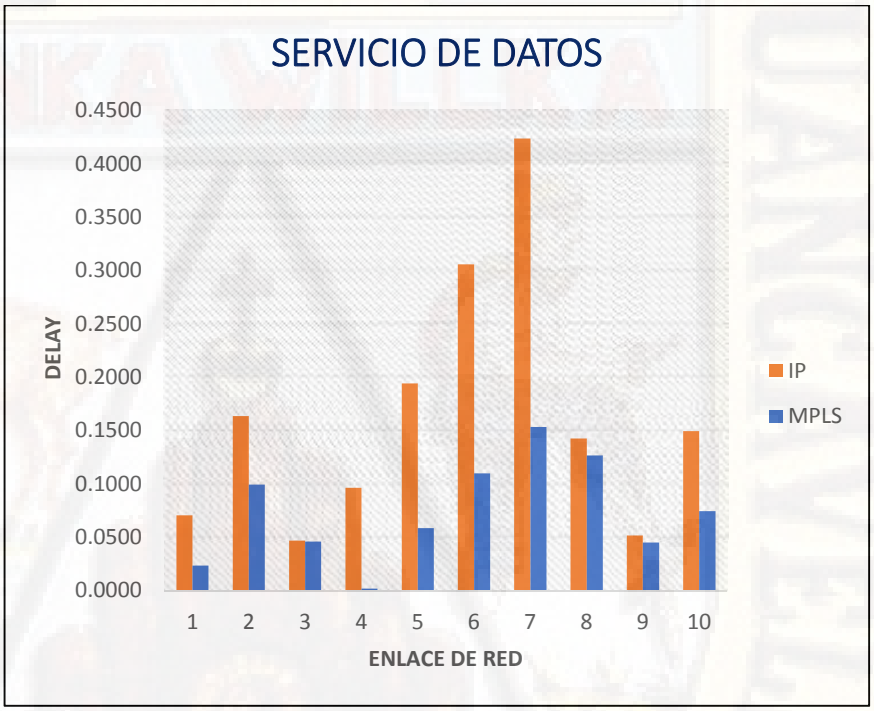


Figura Nº 4.1: *Delay* generado por el servicio de datos en la red de transporte.

Fuente: Elaboración Propia – Ficha técnica.

Interpretación:

En la tabla Nº 4.1 y figura Nº 4.1, se observa los resultados de la prueba de *delay* con la tecnología IP y *MPLS* (*Multiprotocol Label Switching),* de cada una de los enlaces de conexión desde el local administrativo y de Paturpampa con las sedes respectivas de

la Universidad Nacional de Huancavelica, en este resultado se observa, con la tecnología *MPLS* disminuye el *delay* en comparación que la tecnología IP, siendo un *delay* máxima de 153.6m segundos con la tecnología *MPLS* y un *delay* máxima de 423.9 m segundos con la tecnología IP(*Internet Protocol*).

b) Resultados de *delay* con el servicio de Voz (VoIP)

Tabla Nº 4.2: Resultados de *delay* con el servicio de VoIP.

ENLACE DE RED *WAN*	SERVICIO DE VoIP	
	PARAMETROS DE CALIDAD DE SERVICIO	
	DELAY (S)	*DELAY (S)*
	TECNOLOGIA IP PRETEST	TECNOLOGIA *MPLS* POSTEST
CASA ROSADA(PC6) - ACOBAMBA(PC1)	0.1501	0.0299
CASA ROSADA(PC6) - PAMPAS (E)(PC2)	0.4779	0.1197
CASA ROSADA(PC6) - PAMPAS(S)(PC3)	0.0889	0.0399
CASA ROSADA(PC6)- LIRCAY(PC4)	0.1158	0.0310
CASA ROSADA(PC6) - PATURPAMPA(PC5)	0.1267	0.0490
PATURPAMPA(PC5) - ACOBAMBA(PC1)	0.1465	0.0299
PATURPAMPA(PC5) -PAMPAS (E)(PC2)	0.1726	0.1647
PATURPAMPA(PC5) - PAMPAS(S)(PC3)	0.2261	0.1044
PATURPAMPA(PC5) - LIRCAY(PC4)	0.2874	0.0497
PATURPAMPA(PC5) -CASA ROSADA(PC6)	0.1947	0.0166

Fuente: Elaboración Propia – Ficha técnica.

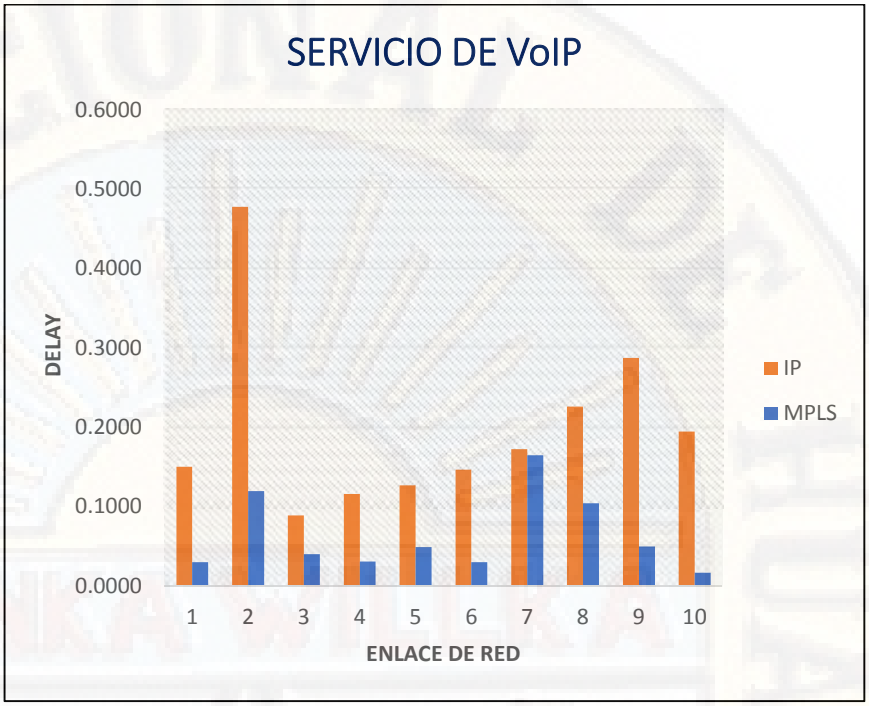


Figura Nº 4.2: *Delay* generado por el servicio de VoIP en la red de transporte.

Fuente: Elaboración Propia – Ficha técnica.

Interpretación:

En la tabla Nº 4.2 y figura Nº 4.2, se observa los resultados de la prueba de *delay* con la tecnología IP (*Internet Protocol*) y *MPLS*(*Multiprotocol Label Switching*), en cada una de los enlaces de conexión desde el local administrativo y de Paturpampa con las sedes respectivas de la Universidad Nacional de Huancavelica, en este resultado se observa con la tecnología *MPLS* disminuye el *delay* en comparación que la tecnología IP, siendo el *delay* máxima de 164.7m segundos con la tecnología *MPLS* y un *delay* máxima de 477.9m segundos con la tecnología IP.

c) Resultados de *delay* con el servicio de Video (streaming)

Tabla Nº 4.3: Resultados de *delay* con el servicio de *streaming*.

ENLACE DE RED *WAN*	SERVICIO DE *STREAMING*	
	PARAMETROS DE CALIDAD DE SERVICIO	
	DELAY (S)	*DELAY (S)*
	TECNOLOGIA IP PRETEST	TECNOLOGIA *MPLS* POSTEST
CASA ROSADA(PC6) - ACOBAMBA(PC1)	0.1059	0.0435
CASA ROSADA(PC6) - PAMPAS (E)(PC2)	0.1349	0.1325
CASA ROSADA(PC6) - PAMPAS(S)(PC3)	0.0967	0.0442
CASA ROSADA(PC6)- LIRCAY(PC4)	0.1272	0.0075
CASA ROSADA(PC6) - PATURPAMPA(PC5)	0.1952	0.0521
PATURPAMPA(PC5) - ACOBAMBA(PC1)	0.1106	0.0865
PATURPAMPA(PC5) -PAMPAS (E)(PC2)	0.2800	0.1536
PATURPAMPA(PC5) - PAMPAS(S)(PC3)	0.2345	0.1172
PATURPAMPA(PC5) - LIRCAY(PC4)	0.3024	0.0478
PATURPAMPA(PC5) -CASA ROSADA(PC6)	0.1466	0.0124

Fuente: Elaboración Propia – Ficha técnica.

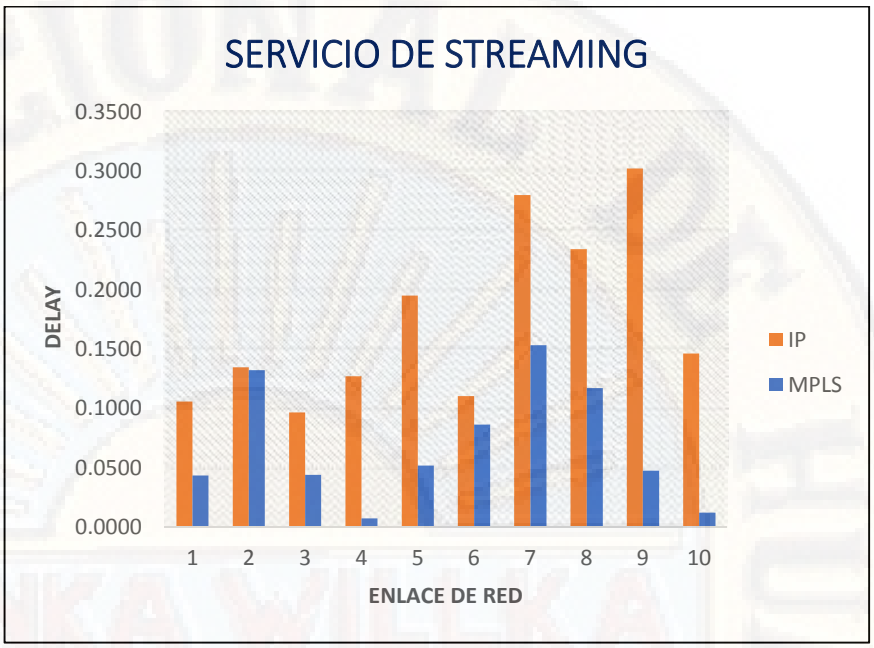


Figura Nº 4.3: *Delay* generado por el servicio de *streaming* en la red de transporte.

Fuente: Elaboración Propia – Ficha técnica.

Interpretación:

En la tabla Nº 4.3 y figura Nº 4.3, se observa los resultados de la prueba de *delay* con la tecnología IP(*Internet Protocol*) y *MPLS* (*Multiprotocol Label Switching*), en cada una de los enlaces de conexión desde el local administrativo y de Paturpampa con las sedes respectivas de la Universidad Nacional de Huancavelica, en este resultado se observa con la tecnología *MPLS* disminuye el *delay* en comparación que la tecnología IP, siendo un *delay* máxima de 153.6m segundos con la tecnología *MPLS* y un *delay* máxima de 302.4m segundos con la tecnología IP.

d) Resultado de *delay* promedio de los tres tipos de servicio

Tabla Nº 4.4: Resultados de *delay* promedio.

ENLACE DE RED *WAN*	PARAMETROS DE CALIDAD DE SERVICIO	
	DELAY PROMEDIO	
	DELAY (S)	*DELAY (S)*
	TECNOLOGIA IP	TECNOLOGIA *MPLS*
	PRETEST	POSTEST
CASA ROSADA(PC6) -ACOBAMBA(PC1)	0.1088	0.0323
CASA ROSADA(PC6) -PAMPAS (E)(PC2)	0.2589	0.1173
CASA ROSADA(PC6) -PAMPAS(S)(PC3)	0.0775	0.0434
CASA ROSADA(PC6)-LIRCAY(PC4)	0.1131	0.0134
CASA ROSADA(PC6) -PATURPAMPA(PC5)	0.1720	0.0533
PATURPAMPA(PC5) -ACOBAMBA(PC1)	0.1877	0.0755
PATURPAMPA(PC5) -PAMPAS (E)(PC2)	0.2922	0.1573
PATURPAMPA(PC5) -PAMPAS(S)(PC3)	0.2011	0.1162
PATURPAMPA(PC5) -LIRCAY(PC4)	0.2139	0.0476
PATURPAMPA(PC5) -CASA ROSADA(PC6)	0.1637	0.0346

Fuente: Elaboración Propia – Ficha técnica.

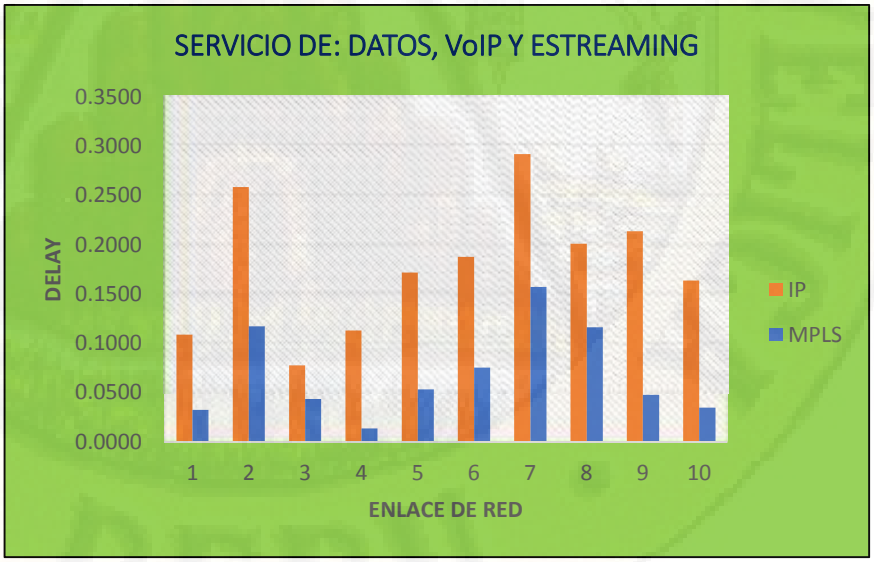


Figura Nº 4.4: *Delay* promedio de los tres servicios.

Fuente: Elaboración Propia – Ficha técnica.

Interpretación:

En la tabla Nº 4.4 y figura Nº 4.4, se observa los resultados de la prueba de *delay* promedio con la tecnología IP(*Internet Protocol)* y *MPLS* (*Multiprotocol Label Switching*), de cada una de los enlaces de conexión desde el local administrativo y de Paturpampa con las sedes respectivas de la Universidad Nacional de Huancavelica, en este resultado se observa con la tecnología *MPLS* disminuye el *delay* en comparación que la tecnología IP, siendo un *delay* máxima de 157.3m segundos con la tecnología *MPLS* y un *delay* máxima de 292.2m segundos con la tecnología IP.

4.1.1.2. Resultados de la calidad de servicio – *jitter*

En las siguientes tablas se presenta los datos obtenidos de la prueba con respecto al *jitter*, de cada enlace, desde el Local Administrativo (casa rosada) hacia las sucursales y desde la ciudad universitaria de Parturpampa hacia las sedes de la Universidad Nacional de Huancavelica, para la generación de tráfico y la medición de los parámetros de calidad de servicio (*QoS*), se hizo con la ayuda de software *D-ITG*.

a) Resultados de *jitter* con el servicio de datos

Tabla Nº 4.5: Resultados de *jitter* con el servicio de datos.

ENLACE DE RED *WAN*	SERVICIO DE DATOS	
	PARAMETROS DE CALIDAD DE SERVICIO	
	JITTER (S)	*JITTER (S)*
	TECNOLOGIA IP PRETEST	TECNOLOGIA *MPLS* POSTEST
CASA ROSADA(PC6) - ACOBAMBA(PC1)	0.0085	0.0078

CASA ROSADA(PC6) - PAMPAS (E)(PC2)	0.0086	0.0079
CASA ROSADA(PC6) - PAMPAS(S)(PC3)	0.0082	0.0082
CASA ROSADA(PC6)- LIRCAY(PC4)	0.0089	0.0082
CASA ROSADA(PC6) - PATURPAMPA(PC5)	0.0055	0.0054
PATURPAMPA(PC5) - ACOBAMBA(PC1)	0.0098	0.0094
PATURPAMPA(PC5) -PAMPAS (E)(PC2)	0.0093	0.0090
PATURPAMPA(PC5) - PAMPAS(S)(PC3)	0.0086	0.0082
PATURPAMPA(PC5) - LIRCAY(PC4)	0.0097	0.0090
PATURPAMPA(PC5) -CASA ROSADA(PC6)	0.0054	0.0053

Fuente: Elaboración Propia – Ficha técnica.

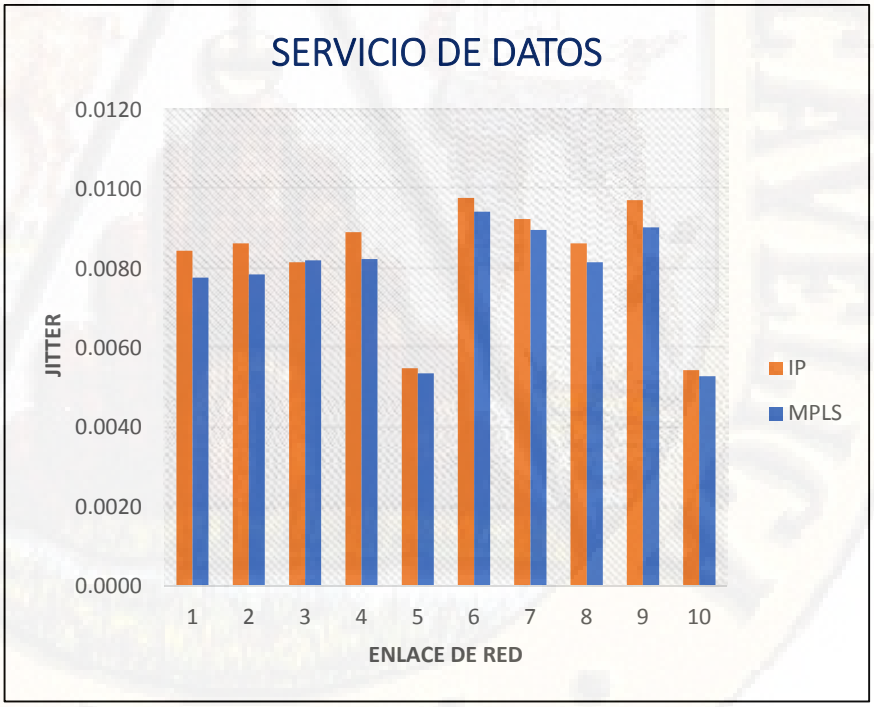


Figura Nº 4.5: *Jitter* generado por el servicio de datos en la red de transporte.

Fuente: Elaboración Propia – Ficha técnica.

Interpretación:

En la tabla Nº 4.5 y figura Nº 4.5, se observa los resultados de la prueba de *jitter* con la tecnología IP y *MPLS* (*Multiprotocol Label Switching*), de cada una de los enlaces de conexión desde el local administrativo y de Paturpampa con las sedes respectivas de la Universidad Nacional de Huancavelica, en este resultado se observa con la tecnología *MPLS* disminuye el *Jitter* en comparación que la tecnología IP, siendo el *Jitter* máxima de 9.4m segundos con la tecnología *MPLS* y el *Jitter* máxima de 9.8 m segundos con la tecnología IP(*Internet Protocol*).

b) Resultados de *jitter* con el servicio de Voz (VoIP)

Tabla Nº 4.6: Resultados de *jitter* con el servicio de VoIP.

ENLACE DE RED *WAN*	SERVICIO DE VoIP	
	PARAMETROS DE CALIDAD DE SERVICIO	
	JITTER (S)	*JITTER (S)*
	TECNOLOGIA IP PRETEST	TECNOLOGIA *MPLS* POSTEST
CASA ROSADA(PC6) - ACOBAMBA(PC1)	0.0091	0.0089
CASA ROSADA(PC6) - PAMPAS (E)(PC2)	0.0076	0.0064
CASA ROSADA(PC6) - PAMPAS(S)(PC3)	0.0077	0.0072
CASA ROSADA(PC6)- LIRCAY(PC4)	0.0094	0.0091
CASA ROSADA(PC6) - PATURPAMPA(PC5)	0.0062	0.0049
PATURPAMPA(PC5) - ACOBAMBA(PC1)	0.0085	0.0082
PATURPAMPA(PC5) -PAMPAS (E)(PC2)	0.0100	0.0093
PATURPAMPA(PC5) - PAMPAS(S)(PC3)	0.0092	0.0077
PATURPAMPA(PC5) - LIRCAY(PC4)	0.0086	0.0072

PATURPAMPA(PC5) -CASA ROSADA(PC6)	0.0062	0.0054

Fuente: Elaboración Propia – Ficha técnica.

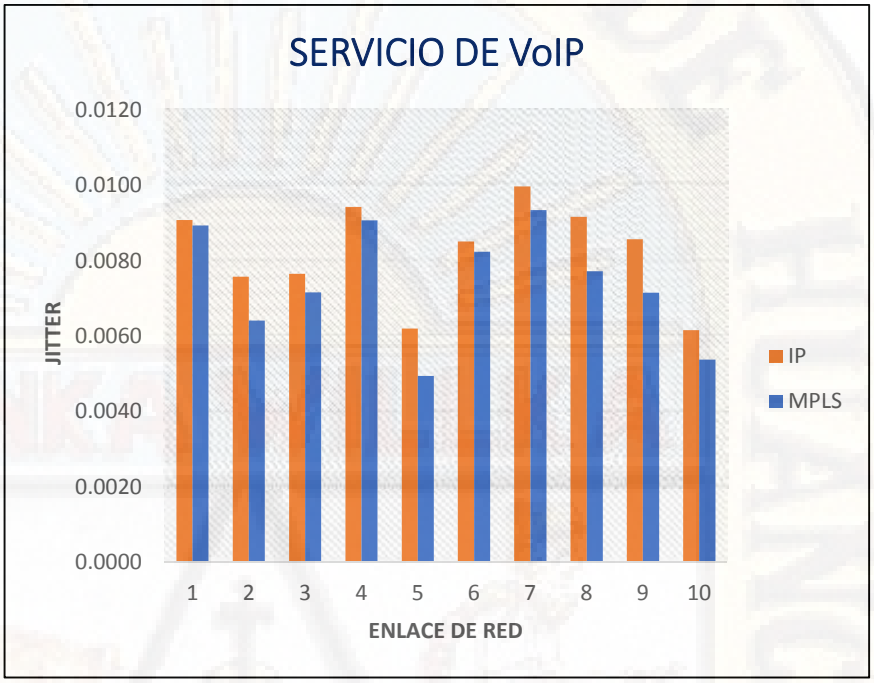


Figura Nº 4.6: *Jitter* generado por el servicio de VoIP en la red de transporte

Fuente: Elaboración Propia – Ficha técnica.

Interpretación:

En la tabla Nº 4.6 y figura Nº 4.6, se observa los resultados de la prueba de *jitter* con la tecnología IP y *MPLS* (*Multiprotocol Label Switching*), de cada una de los enlaces de conexión desde el local administrativo y de Paturpampa con las sedes respectivas de la Universidad Nacional de Huancavelica, en los resultados se observa con la tecnología *MPLS* disminuye el *Jitter* en comparación que la tecnología IP, siendo el *Jitter* máxima de 9.3m segundos con la tecnología *MPLS* y el *Jitter* máxima de 10m segundos con la tecnología IP (*Internet Protocol*).

c) Resultados de *jitter* con el servicio de video (*streaming)*

Tabla Nº 4.7: Resultados de *jitter* con el servicio de *streaming*.

ENLACE DE RED *WAN*	SERVICIO DE STREAMING	
	PARAMETROS DE CALIDAD DE SERVICIO	
	JITTER (S)	*JITTER (S)*
	TECNOLOGIA IP PRETEST	TECNOLOGIA *MPLS* POSTEST
CASA ROSADA(PC6) - ACOBAMBA(PC1)	0.0223	0.0198
CASA ROSADA(PC6) - PAMPAS (E)(PC2)	0.0192	0.0130
CASA ROSADA(PC6) - PAMPAS(S)(PC3)	0.0127	0.0120
CASA ROSADA(PC6)- LIRCAY(PC4)	0.0137	0.0111
CASA ROSADA(PC6) - PATURPAMPA(PC5)	0.0086	0.0075
PATURPAMPA(PC5) - ACOBAMBA(PC1)	0.0109	0.0108
PATURPAMPA(PC5) -PAMPAS (E)(PC2)	0.0157	0.0135
PATURPAMPA(PC5) - PAMPAS(S)(PC3)	0.0171	0.0139
PATURPAMPA(PC5) - LIRCAY(PC4)	0.0121	0.0116
PATURPAMPA(PC5) -CASA ROSADA(PC6)	0.0091	0.0071

Fuente: Elaboración Propia – Ficha técnica.

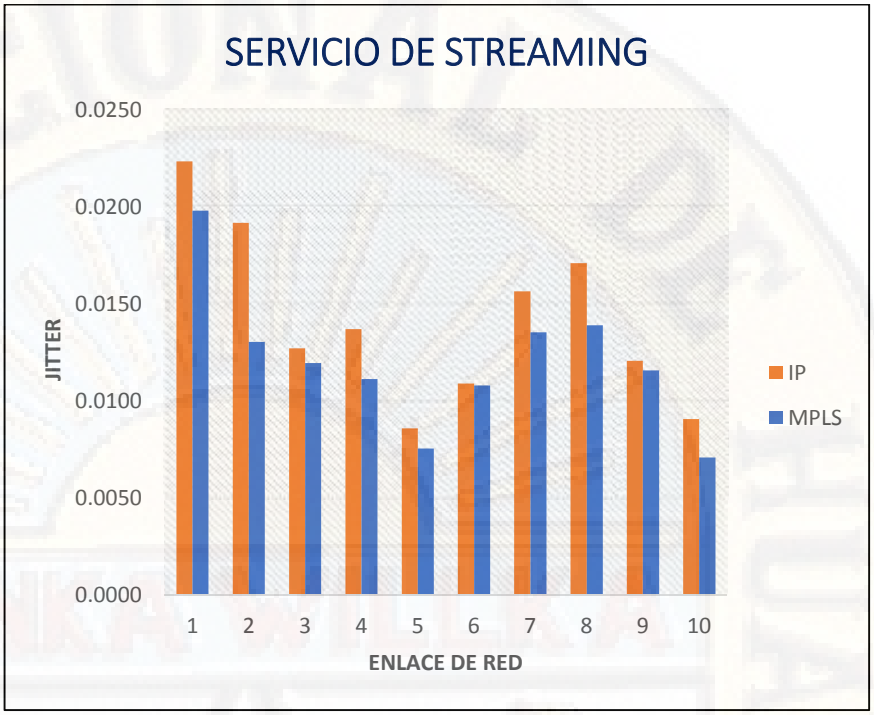


Figura Nº 4.7: *Jitter* generado por el servicio de streaming en la red de transporte

Fuente: Elaboración Propia – Ficha técnica.

Interpretación:

En la tabla Nº 4.7 y figura Nº 4.7, se observa los resultados de la prueba de *Jitter* con la tecnología IP y *MPLS* (*Multiprotocol Label Switching*), en cada una de los enlaces de conexión desde el local administrativo y de Paturpampa con las sedes respectivas de la Universidad Nacional de Huancavelica, en este resultado se observa con la tecnología *MPLS* disminuye el *Jitter* en comparación que la tecnología IP, siendo el *Jitter* máxima de 19.8m segundos con la tecnología *MPLS* y el *Jitter* máxima de 22.3m segundos con la tecnología IP (*Internet Protocol*).

d) Resultado de *jitter* promedio de los tres tipos de servicio

Tabla Nº 4.8: Resultados de *jitter* promedio.

ENLACE DE RED *WAN*	PARAMETROS DE CALIDAD DE SERVICIO	
	JITTER PROMEDIO	
	JITTER (S)	*JITTER (S)*
	TECNOLOGIA IP	TECNOLOGIA *MPLS*
	PRETEST	POSTEST
CASA ROSADA(PC6) -ACOBAMBA(PC1)	0.0133	0.0122
CASA ROSADA(PC6) -PAMPAS (E)(PC2)	0.0118	0.0091
CASA ROSADA(PC6) -PAMPAS(S)(PC3)	0.0095	0.0091
CASA ROSADA(PC6)-LIRCAY(PC4)	0.0107	0.0095
CASA ROSADA(PC6) -PATURPAMPA(PC5)	0.0068	0.0059
PATURPAMPA(PC5) -ACOBAMBA(PC1)	0.0097	0.0095
PATURPAMPA(PC5) -PAMPAS (E)(PC2)	0.0117	0.0106
PATURPAMPA(PC5) -PAMPAS(S)(PC3)	0.0116	0.0099
PATURPAMPA(PC5) -LIRCAY(PC4)	0.0101	0.0093
PATURPAMPA(PC5) -CASA ROSADA(PC6)	0.0069	0.0059

Fuente: Elaboración Propia – Ficha técnica.

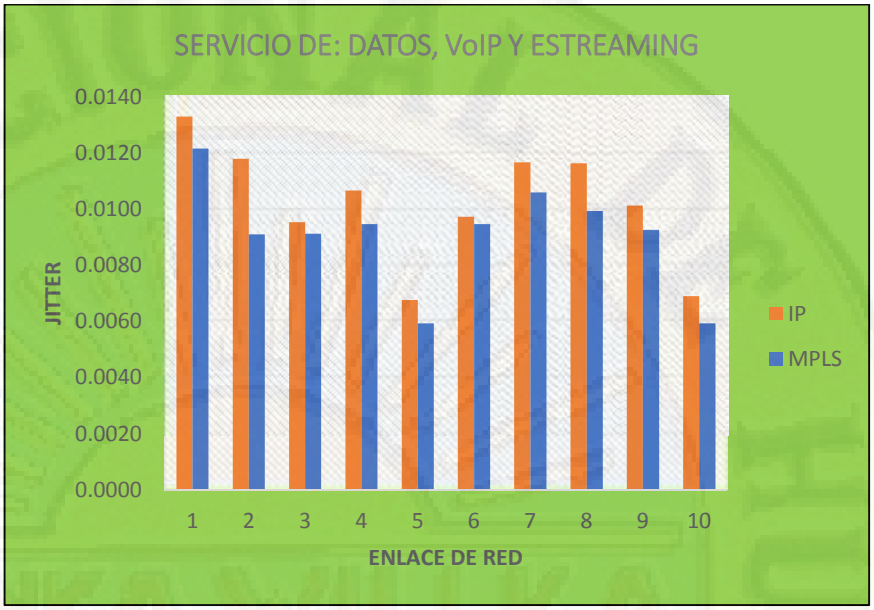


Figura Nº 4.8: *Jitter* promedio de los tres servicios.

Fuente: Elaboración Propia – Ficha técnica.

Interpretación:

En la tabla Nº 4.8 y figura Nº 4.8, se observa los resultados de la prueba de *Jitter* promedio con la tecnología IP y *MPLS* (*Multiprotocol Label Switching*), en cada una de los enlaces de conexión desde el local administrativo y de Paturpampa con las sedes respectivas de la Universidad Nacional de Huancavelica, en este resultado se observa con la tecnología *MPLS* disminuye el *Jitter* en comparación que la tecnología IP, siendo el *Jitter* máxima de 12.2m segundos con la tecnología *MPLS* y el *Jitter* máxima de 13.3m segundos con la tecnología IP (*Internet Protocol*).

4.1.1.3. Resultados de la calidad de servicio – *packet loss*

En las siguientes tablas se presenta los datos obtenidos de la prueba con respecto a la *packet loss*, de cada enlace, desde el Local Administrativo (casa rosada) hacia las sucursales y desde la ciudad universitaria de Parturpampa hacia las sedes de la Universidad Nacional de Huancavelica, para la generación de tráfico y la

medición de los parámetros de calidad de servicio (*QoS*), se hizo con la ayuda de software *D-ITG*.

a) Resultados de *packet loss* con el servicio de datos

Tabla Nº 4.9: Resultados de *packet loss* con el servicio de datos.

ENLACE DE RED *WAN*	SERVICIO DE DATOS	
	PARAMETROS DE CALIDAD DE SERVICIO	
	PACKET LOSS (%)	*PACKET LOSS (%)*
	TECNOLOGIA IP PRETEST	TECNOLOGIA *MPLS* POSTEST
CASA ROSADA(PC6) - ACOBAMBA(PC1)	0.0000	0.0000
CASA ROSADA(PC6) - PAMPAS (E)(PC2)	0.0000	0.0000
CASA ROSADA(PC6) - PAMPAS(S)(PC3)	0.0000	0.0000
CASA ROSADA(PC6)- LIRCAY(PC4)	0.0000	0.0000
CASA ROSADA(PC6) - PATURPAMPA(PC5)	0.0000	0.0000
PATURPAMPA(PC5) - ACOBAMBA(PC1)	0.0000	0.0000
PATURPAMPA(PC5) -PAMPAS (E)(PC2)	0.0000	0.0000
PATURPAMPA(PC5) - PAMPAS(S)(PC3)	0.0000	0.0000
PATURPAMPA(PC5) - LIRCAY(PC4)	0.0000	0.0000
PATURPAMPA(PC5) -CASA ROSADA(PC6)	0.0000	0.0000

Fuente: Elaboración Propia – Ficha técnica.

Interpretación:

En la tabla Nº 4.9 se observa los resultados obtenidos de la prueba de calidad de servicio de cada red *Wan* de la Universidad Nacional de Huancavelica, con respecto al *packet loss*, que no hubo ninguna variación de resultados con la implementación de la

tecnología *MPLS* con tráfico de datos, por lo tanto, los resultados con ambas tecnologías es el 0% de *packet loss.*

b) Resultados de *packet loss* con el servicio de Voz (VoIP)

Tabla Nº 4.10: Resultados de *packet loss* con el servicio de VoIP.

ENLACE DE RED *WAN*	SERVICIO DE VoIP	
	PARAMETROS DE CALIDAD DE SERVICIO	
	PACKET LOSS (%)	*PACKET LOSS (%)*
	TECNOLOGIA IP PRETEST	TECNOLOGIA *MPLS* POSTEST
CASA ROSADA(PC6) - ACOBAMBA(PC1)	0.0000	0.0000
CASA ROSADA(PC6) - PAMPAS (E)(PC2)	0.0000	0.0000
CASA ROSADA(PC6) - PAMPAS(S)(PC3)	0.0000	0.0000
CASA ROSADA(PC6)- LIRCAY(PC4)	0.0000	0.0000
CASA ROSADA(PC6) - PATURPAMPA(PC5)	0.0000	0.0000
PATURPAMPA(PC5) - ACOBAMBA(PC1)	0.0000	0.0000
PATURPAMPA(PC5) -PAMPAS (E)(PC2)	0.0000	0.0000
PATURPAMPA(PC5) - PAMPAS(S)(PC3)	0.0000	0.0000
PATURPAMPA(PC5) - LIRCAY(PC4)	0.0000	0.0000
PATURPAMPA(PC5) -CASA ROSADA(PC6)	0.0000	0.0000

Fuente: Elaboración Propia – Ficha técnica.

Interpretación:

En la tabla Nº 4.10 se observa los resultados obtenidos de la prueba de calidad de servicio de cada red *Wan* de la Universidad Nacional de Huancavelica, con respecto al *packet loss*, que no hubo ninguna variación de resultados con la implementación de la

tecnología *MPLS* con tráfico de voz, por lo tanto, los resultados con ambas tecnologías es el 0% de *packet loss*.

c) Resultados de *packet loss* con el servicio de video (*streaming)*

Tabla Nº 4.11: Resultados de *packet loss* con el servicio de *streaming*.

ENLACE DE RED *WAN*	SERVICIO DE STREAMING	
	PARAMETROS DE CALIDAD DE SERVICIO	
	PACKET LOSS (%)	*PACKET LOSS (%)*
	TECNOLOGIA IP PRETEST	TECNOLOGIA *MPLS* POSTEST
CASA ROSADA(PC6) - ACOBAMBA(PC1)	0.0000	0.0000
CASA ROSADA(PC6) - PAMPAS (E)(PC2)	0.0000	0.0000
CASA ROSADA(PC6) - PAMPAS(S)(PC3)	0.0000	0.0000
CASA ROSADA(PC6)- LIRCAY(PC4)	0.0000	0.0000
CASA ROSADA(PC6) - PATURPAMPA(PC5)	0.0000	0.0000
PATURPAMPA(PC5) - ACOBAMBA(PC1)	0.0000	0.0000
PATURPAMPA(PC5) -PAMPAS (E)(PC2)	0.0000	0.0000
PATURPAMPA(PC5) - PAMPAS(S)(PC3)	0.0000	0.0000
PATURPAMPA(PC5) - LIRCAY(PC4)	0.0000	0.0000
PATURPAMPA(PC5) -CASA ROSADA(PC6)	0.0000	0.0000

Fuente: Elaboración Propia – Ficha técnica.

Interpretación:

En la tabla Nº 4.11 se observa los resultados obtenidos de la prueba de calidad de servicio de cada red *Wan* de la Universidad Nacional de Huancavelica, con respecto al *packet loss*, que no hubo ninguna variación de resultados con la implementación de la

tecnología *MPLS* con tráfico de streaming, por lo tanto, los resultados con ambas tecnologías es el 0% de *packet loss*.

d) Resultado de la *packet loss* promedio de los tres tipos de servicio

Tabla Nº 4.12: Resultados de *packet loss* promedio.

ENLACE DE RED *WAN*	PARAMETROS DE CALIDAD DE SERVICIO	
	PACKET LOSS PROMEDIO	
	PACKET LOSS (%)	*PACKET LOSS (%)*
	TECNOLOGIA IP	TECNOLOGIA *MPLS*
	PRETEST	POSTEST
CASA ROSADA(PC6) -ACOBAMBA(PC1)	0.0000	0.0000
CASA ROSADA(PC6) -PAMPAS (E)(PC2)	0.0000	0.0000
CASA ROSADA(PC6) -PAMPAS(S)(PC3)	0.0000	0.0000
CASA ROSADA(PC6)-LIRCAY(PC4)	0.0000	0.0000
CASA ROSADA (PC6) –PATURPAMPA (PC5)	0.0000	0.0000
PATURPAMPA(PC5) -ACOBAMBA(PC1)	0.0000	0.0000
PATURPAMPA(PC5) -PAMPAS (E)(PC2)	0.0000	0.0000
PATURPAMPA(PC5) -PAMPAS(S)(PC3)	0.0000	0.0000
PATURPAMPA(PC5) -LIRCAY(PC4)	0.0000	0.0000
PATURPAMPA(PC5) -CASA ROSADA(PC6)	0.0000	0.0000

Fuente: Elaboración Propia – Ficha técnica.

Interpretación:

En la tabla Nº 4.12 se observa los resultados obtenidos de la prueba de calidad de servicio en cada red *Wan* de la Universidad Nacional de Huancavelica, con respecto a la *packet loss* promedio,

que no hubo ninguna variación de resultados con la implementación de la tecnología *MPLS* con tráfico de datos, por lo tanto, los resultados con ambas tecnologías es el 0% de *packet loss*.

4.2. Discusión de resultados

El análisis y la contrastación de hipótesis del tema de investigación ha sido demostrado y aceptado estadísticamente, tanto la hipótesis general y las hipótesis específicas, que se realizó las prueba paramétrica de T-*Student*, con la finalidad de validar los resultados obtenidos, de los parámetros de calidad de servicio (*QoS*) en la red *WAN* antes y después de aplicación de la tecnología *MPLS*, en donde se puede observar con la tecnología *MPLS* se obtiene mejores resultados en los indicadores del parámetro de calidad de servicio *QoS*, entonces se puede afirmar que la tecnología *MPLS* es mucho mejor en el rendimiento en la red de transporte en comparación que la tecnología IP: Datos (*Delay*: 164.60ms y 74.04ms. *Jitter*: 8.26ms y 7.84ms. *Packet loss*: 0%-0%), VoIP (*Delay*: 198.68ms y 63.49ms. *Jitter*: 8.24ms y 7.44ms. *Packet loss*: 0%-0%) y *Streaming* (*Delay*: 173.38ms y 69.73ms. *Jitter*: 14.13ms y 12.04ms. *Packet loss*: 0%-0%) y por lo tanto se llega a la siguiente conclusión: un modelo de red con tecnología *MPLS* influye de manera significativa en la calidad de servicio de transporte de paquetes en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

Los resultados han sido obtenidos de una prueba de laboratorio a nivel de simulación con el software *GNS3*, que es uno de los softwares más utilizados en el tema de investigación a nivel mundial, en el área de redes y comunicaciones, por lo que tiene mayor credibilidad en los resultados, así mismo se coincide en la conclusión del trabajo realizado por Emileni Solange (2015) donde llega a la siguiente conclusión de la hipótesis, que la tecnología *MPLS* es actualmente mejor opción para empresas medianas y grandes que proveen el servicio de voz, datos y Tv, puesto que su servicio de calidad y su ingeniería de tráfico disminuye notablemente el tráfico en la red, por lo tanto mejora la calidad de servicio.

En el estudio que se desarrolló sobre la tecnología *MPLS* para mejorar la calidad de servicio en la red de transporte del tráfico de los servicios, en donde se

ha obtenido resultados positivos en la mejora de *delay, jitter y packet loss*, coincidiendo el resultado con Miroslava Zapata (2016) quien evaluó los parámetros de calidad de servicio *QoS* en una red *VPN*/*MPLS* a nivel de simulación, utilizando el software *GNS3* y *D-ITG*, este último para la generación de tráfico y llegando a la conclusión, la implementación de la tecnología *VPN*/*MPLS* en el *Backbone* de una red, ofrece garantías de calidad de servicio para los diferentes tipos de tráfico que IP como son: VoIP (*Delay*: 430.52ms y 13.83ms. *Jitter*: 7.24ms y 5.3 ms. *Packet loss*: 0%-0%), Datos (*Delay*:121.50ms y 73.86ms. *Jitter*: 13.24msy 7.8 ms. *Packet loss*: 0%-0%) y *Streaming* (*Delay*: 82.67ms y 27.42ms. *Jitter*: 9.3ms y 10ms. *Packet loss*: 0%-0%), es más Gladys Oña (2016), quien estudió el Diseño y comparación de redes de acceso *MPLS* y metro Ethernet integrada a un *Backbone MPLS* para un proveedor de servicio y realización de un prototipo base, lo cual llega a una conclusión, los proveedores del servicios de internet con el fin de mejorar el rendimiento en la entrega de servicios a los usuarios y su infraestructura, han optado por la redes *MPLS* y Metro Ethernet que acceso *MPLS* y *Backbone MPLS* (*Delay*: Video: 2.8ms a 2.7 ms. VoIP: 8.1ms a 7.0 ms), dos de las tecnologías que actualmente ofrecen mayor escalabilidad, eficiencia en la entrega de servicios y tiempos de conmutación bajos.

Los estudios realizado y publicado en la IEEE por *Samiullah Mehraban, Komil. B. Vora y Darshan Upadhyay* en India (2018) sobre la Implementación para la conmutación de etiquetas de protocolo múltiple (*MPLS*) mediante enrutamiento y reenvío virtual (*VRF*), que llega a la conclusión: El cambio de etiqueta multiprotocolo (*MPLS*) que introdujo el IETF (Grupo de trabajo de ingeniería de Internet) se usa básicamente para redes de comunicación que atraen a todas las redes de proveedores de servicios con sus brillantes y excelentes futuros que brindan garantías para el tráfico y brindan calidad de servicios que transporta datos desde fuente a destino directamente a través de pequeñas etiquetas.

Según los estudios mencionados con relación a la tecnología *MPLS* (*Multiprotocol Label Switching*), y su aplicación en diferentes escenarios, siempre

está basado en la mejora de la calidad de servicio en la red de trasporte de los diferentes tipos de tráfico, utilizando los diferentes protocolos de enrutamiento.

4.3. Proceso de prueba de hipótesis

4.3.1. Contraste de hipótesis específica 1

a) Prueba de normalidad de los datos de *delay*

En el grafico siguiente se tiene los datos de *delay*, para determinar si tiene una distribución normal.

	Enlace	dimension	pretest	postest
1	CASA ROSADA(PC6) -ACOBAMBA(PC1)	Delay	,1088	,0323
2	CASA ROSADA(PC6) -PAMPAS (E)(PC2)	Delay	,2589	,1173
3	CASA ROSADA(PC6) -PAMPAS(S)(PC3)	Delay	,0770	,0434
4	CASA ROSADA(PC6)-LIRCAY(PC4)	Delay	,1131	,0134
5	CASA ROSADA(PC6) -PATURPAMPA(PC5)	Delay	,1720	,0533
6	PATURPAMPA(PC5) -ACOBAMBA(PC1)	Delay	,1877	,0755
7	PATURPAMPA(PC5) - PAMPAS (E)(PC2)	Delay	,2922	,1573
8	PATURPAMPA(PC5) -PAMPAS(S)(PC3)	Delay	,2011	,1162
9	PATURPAMPA(PC5) -LIRCAY(PC4)	Delay	,2139	,0476
10	PATURPAMPA(PC5) -CASA ROSADA(PC6)	Delay	,1637	,0346
11				

Cuadro Nº 4.1: Datos de *delay* por cada enlace.

Fuente: Elaboración Propia – Ficha técnica.

Determinación de alfa

$\alpha = 5\% = 0.05$ Es el grado de error o significancia.

Planteamiento de hipótesis

H_0 = La dimensión de *delay* de la calidad de servicio, tiene una distribución normal.

H_1 = La dimensión de *delay* de la calidad de servicio, no tiene una distribución normal.

Estadígrafo de prueba más apropiado

Para la demostración de la hipótesis se realizó la prueba de normalidad con los datos obtenidos de *delay*, utilizando la estadística de *Shapiro-Wilk* por ser una muestra menor a 30 datos.

Regla de decisión

- Cuando P – valor ≥α Se acepta la hipótesis nula H_0
- Cuando P – valor ≤α Se acepta la hipótesis alternativa H_1

Calculo de valores de la prueba estadística

Tabla Nº 4.13: Prueba de normalidad de *delay*.

Pruebas de normalidad – ***Delay***							
	Dimensión	Kolmogorov-Smirnov[a]			**Shapiro-Wilk**		
		Estadístico	gl	Sig.	Estadístico	Gl	Sig.
pretest	*Delay*	,136	10	,200*	,973	10	,921
postest	*Delay*	,233	10	,132	,901	10	,227

Fuente: Elaboración propia- Resultados de SPSS

Conclusión

En la tabla Nº 4.13 se observa la dimensión *delay*, que tiene una distribución normal, porque el valor de alfa es mayor a 0.05 o 5%, con esto queda demostrado la distribución de normalidad de los datos.

b) Prueba de hipótesis

- Formular la hipótesis nula y alterna de acuerdo al problema.

  H_0 = Un modelo de red con tecnología *MPLS* no influirá significativamente en el *delay* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

H1 = Un modelo de red con tecnología *MPLS* influirá significativamente en el *delay* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

- Escoger un nivel de significancia o riesgo α.

  α = 5% = 0.05 Es el grado de error o significancia.

  $1 - \alpha = 1 - 0.05 = 0.95 = 95\%$ Nivel de confianza.

- Escoger el estadígrafo de prueba más apropiado.

  La prueba de estadística paramétrica para datos con distribución normal menores a 30 datos**,** se consideró la prueba de T-*Stuntend*.

- Establecer la región crítica.

  Cuando P – valor ≥α Se acepta la hipótesis nula H_0

  Cuando P – valor ≤α Se acepta la hipótesis alternativa H_1

- Calcular los valores de la prueba estadística de una muestra de tamaño "n".

Tabla Nº 4.14: Estadísticos de muestras relacionadas de *delay*.

Estadísticos de muestras relacionadas					
		Media	N	Desviación típ.	Error típ. de la media
Par 1	pretest	,178890	10	,0673601	,0213011
	postest	,069090	10	,0464055	,0146747

Fuente: Elaboración propia- Resultados de SPSS

Tabla Nº 4.15: Correlaciones de muestras relacionadas de *delay*.

Correlaciones de muestras relacionadas				
		N	Correlación	Sig.
Par 1	pretest y postest	10	,842	,002

Fuente: Elaboración propia- Resultados de SPSS

Tabla Nº 4.16: La prueba de T-*Student* para muestras relacionadas.

Prueba de muestras relacionadas									
		Diferencias relacionadas					t	gl	Sig. (bilateral)
		Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia				
					Inferior	Superior			
Par 1	pretest - postest	,1098000	,0377894	,0119501	,0827671	,1368329	9,188	9	,000

Fuente: Elaboración propia- Resultados de SPSS

- Rechazar la hipótesis nula (H_o) si el estadígrafo tiene un valor en la región crítica y no rechazar (aceptar) en el otro caso.

Tabla Nº 4.17: Comparación entre de nivel de significancia y valor de p.

Indicadores	Nivel de significancia α	Comparación de signo	valor de P
pretest - postest	0.05	>	0.000

Fuente: Elaboración propia- Resultados de SPSS.

- Conclusión de hipótesis especifica

De la tabla Nº 4.17 se puede observar el valor P es menor al valor de nivel de significancia α que es 5%, por lo tanto rechazamos la hipótesis nula y lo tomamos la hipótesis alterna o de investigación: Un modelo de red con tecnología *MPLS* influirá significativamente en el *delay* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

4.3.2. Contraste de hipótesis específica 2

a) Prueba de normalidad de los datos de *jitter*

En el grafico siguiente se tiene los datos de *jitter*, para determinar si tiene una distribución normal.

	Enlace	dimension	pretest	postest
1	CASA ROSADA(PC6) -ACOBAMBA(PC1)	Jitter	,0133	,0122
2	CASA ROSADA(PC6) -PAMPAS (E)(PC2)	Jitter	,0118	,0091
3	CASA ROSADA(PC6) -PAMPAS(S)(PC3)	Jitter	,0095	,0091
4	CASA ROSADA(PC6) LIRCAY(PC4)	Jitter	,0107	,0096
5	CASA ROSADA(PC6) -PATURPAMPA(PC5)	Jitter	,0068	,0059
6	PATURPAMPA(PC5) -ACOBAMBA(PC1)	Jitter	,0097	,0096
7	PATURPAMPA(PC5) -PAMPAS (E)(PC2)	Jitter	,0117	,0106
8	PATURPAMPA(PC5) -PAMPAS(S)(PC3)	Jitter	,0116	,0099
9	PATURPAMPA(PC5) -LIRCAY(PC4)	Jitter	,0101	,0093
10	PATURPAMPA(PC5) -CASA ROSADA(PC6)	Jitter	,0069	,0059
11				

Cuadro Nº 4.2: Datos de *jitter* por cada enlace.

Fuente: Elaboración Propia – Ficha técnica

Determinación de alfa

$\alpha = 5\% = 0.05$ Es el grado de error o significancia.

Planteamiento de hipótesis

H_0 = La dimensión de *jitter* de la calidad de servicio, tiene una distribución normal.

H_1 = La dimensión de *jitter* de la calidad de servicio, no tiene una distribución normal.

Estadígrafo de prueba más apropiado

Para la demostración de la hipótesis se realizó la prueba de normalidad con los datos obtenidos de *jitter*, utilizando la estadística de *Shapiro-Wilk* por ser una muestra menor a 30 datos.

Regla de decisión

- Cuando P – valor $\geq \alpha$ Se acepta la hipótesis nula H_0
- Cuando P – valor $\leq \alpha$ Se acepta la hipótesis alternativa H_1

Calculo de valores de la prueba estadística

Tabla Nº 4.18: Pruebas de normalidad de *Jitter*.

Pruebas de normalidad – *Jitter*							
	Dimensión	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
		Estadístico	gl	Sig.	Estadístico	Gl	Sig.
pretest	*jitter*	,168	10	,200*	,925	10	,401
postest	*jitter*	,300	10	,011	,871	10	,103

Fuente: Elaboración propia- Resultados de SPSS

Conclusión

En la tabla Nº 4.18 se observa la dimensión *jitter*, tiene una distribución normal, porque el valor de alfa es mayor a 0.05 o 5%, con esto queda demostrado la distribución de normalidad de los datos.

b) Prueba de hipótesis

- Formular la hipótesis nula y alterna de acuerdo al problema.

  H_0 = Un modelo de red con tecnología *MPLS* no influirá significativamente en el *jitter* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

  H1 = Un modelo de red con tecnología *MPLS* influirá significativamente en el *jitter* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

- Escoger un nivel de significancia o riesgo α.

  α = 5% = 0.05 Es el grado de error o significancia.

  $1 - \alpha = 1 - 0.05 = 0.95 = 95\%$ Nivel de confianza.

- Escoger el estadígrafo de prueba más apropiado.

La prueba de estadística paramétrica para datos con distribución normal menores a 30 datos**,** se consideró la prueba de T-*Stutend*.

- Establecer la región crítica.

  Cuando P – valor ≥α Se acepta la hipótesis nula H_0

  Cuando P – valor ≤α Se acepta la hipótesis alternativa H_1

- Calcular los valores de la prueba estadística de una muestra de tamaño "n".

Tabla Nº 4.19: Estadísticos de muestras relacionadas de *jitter*.

Estadísticos de muestras relacionadas					
		Media	N	Desviación típ.	Error típ. de la media
Par 1	pretest	,010210	10	,0021037	,0006652
	postest	,009100	10	,0019247	,0006086

Fuente: Elaboración propia- Resultados de SPSS

Tabla Nº 4.20: Correlaciones de muestras relacionadas de *jitter*.

Correlaciones de muestras relacionadas				
		N	Correlación	Sig.
Par 1	pretest y postest	10	,944	,000

Fuente: Elaboración propia- Resultados de SPSS

Tabla Nº 4.21: La prueba de T-*Student* para muestras relacionadas.

Prueba de muestras relacionadas								
	Diferencias relacionadas					t	gl	Sig. (bilateral)
	Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia				
				Inferior	Superior			

Par 1	pretest - postest	,0011100	,0006967	,0002203	,0006116	,0016084	5,038	9	,001

Fuente: Elaboración propia- Resultados de SPSS

- Rechazar la hipótesis nula (H_o) si el estadígrafo tiene un valor en la región crítica y no rechazar (aceptar) en el otro caso.

Tabla Nº 4.22: Comparación entre de nivel de significancia y valor de p.

Indicadores	Nivel de significancia α	Comparación de signo	valor de P
pretest - postest	0.05	>	0.001

Fuente: Elaboración propia- Resultados de SPSS.

- Conclusión de hipótesis especifica

De la tabla Nº 4.22 se puede observar el valor P es menor al valor de nivel de significancia α que es 5%, por lo tanto rechazamos la hipótesis nula y lo tomamos la hipótesis alterna o de investigación: Un modelo de red con tecnología *MPLS* influirá significativamente en el *jitter* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

4.3.3. Contraste de hipótesis específica 3

a) Prueba de normalidad de los datos de *packet loss*

En el grafico siguiente se tiene los datos de *packet loss*, para determinar si tiene una distribución normal o no.

	Enlace	dimension	pretest	postest
1	CASA ROSADA(PC6) -ACOBAMBA(PC1)	PacketLoss	,0000	,0000
2	CASA ROSADA(PC6) -PAMPAS (E)(PC2)	PacketLoss	,0000	,0000
3	CASA ROSADA(PC6) -PAMPAS(S)(PC3)	PacketLoss	,0000	,0000
4	CASA ROSADA(PC6)-URCAY(PC4)	PacketLoss	,0000	,0000
5	CASA ROSADA(PC6) -PATURPAMPA(PC5)	PacketLoss	,0000	,0000
6	PATURPAMPA(PC5) -ACOBAMBA(PC1)	PacketLoss	,0000	,0000
7	PATURPAMPA(PC5) -PAMPAS (E)(PC2)	PacketLoss	,0000	,0000
8	PATURPAMPA(PC5) -PAMPAS(S)(PC3)	PacketLoss	,0000	,0000
9	PATURPAMPA(PC5) -URCAY(PC4)	PacketLoss	,0000	,0000
10	PATURPAMPA(PC5) -CASA ROSADA(PC6)	PacketLoss	,0000	,0000
11				

Cuadro Nº 4.3: Datos de *packet loss* por cada enlace.

Fuente: Elaboración Propia – Ficha técnica

Conclusión

En la figura anterior se observa que todos los datos de pretest y postes son cero, por lo tanto, no es necesario de realizarlo la prueba de normalidad.

b) Prueba de hipótesis

- Formular la hipótesis nula y alterna de acuerdo al problema.

  H_0 = Un modelo de red con tecnología *MPLS* no influirá significativamente en el *packet loss* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

  H1 = Un modelo de red con tecnología *MPLS* influirá significativamente en el *packet loss* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

- Escoger un nivel de significancia o riesgo α.

  α = 5% = 0.05 Es el grado de error o significancia.

  $1 - \alpha = 1 - 0.05 = 0.95 = 95\%$ Nivel de confianza.

- Escoger el estadígrafo de prueba más apropiado.

  La prueba de estadística paramétrica para datos con distribución normal menores a 30 datos**,** se consideró la prueba de T-*Stutend*.

- Establecer la región crítica.

  Cuando P – valor ≥α Se acepta la hipótesis nula H_0

  Cuando P – valor ≤α Se acepta la hipótesis alternativa H_1

- Calcular los valores de la prueba estadística de una muestra de tamaño "n".

Tabla Nº 4.23: Estadísticos de muestras relacionadas de *packet loss*.

Estadísticos de muestras relacionadas					
		Media	N	Desviación típ.	Error típ. de la media
Par 1	pretest	,000000a	10	,0000000	,0000000
	postest	,000000a	10	,0000000	,0000000
a. No se puede calcular la correlación y T porque el error típico de la diferencia es 0.					

Fuente: Elaboración propia- Resultados de *SPSS*

- Conclusión de hipótesis especifica

  De la tabla Nº 4.23 se puede observar que no se puede calcular la correlación, ni tampoco la prueba de T, entonces podemos decir: Un modelo de red con tecnología *MPLS* no influye significativamente en el *packet loss* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018, porque los valores son los mismo.

4.3.4. Contraste de hipótesis general

a) Prueba de normalidad de los datos

En el grafico siguiente se tiene los datos de la calidad de servicio, para determinar si tiene una distribución normal.

	Enlace	dimension	pretest	postest
1	CASA ROSADA(PC6) -ACOBAMBA(PC1)	Delay	,1088	,0323
2	CASA ROSADA(PC6) -PAVPAS (E)(PC2)	Delay	,2589	,1173
3	CASA ROSADA(PC6) -PAVPAS(S)(PC3)	Delay	,0775	,0434
4	CASA ROSADA(PC6)-LIRCAY(PC4)	Delay	,1131	,0134
5	CASA ROSADA(PC6) -PATURPAMPA(PC5)	Delay	,1720	,0631
6	PATURPAMPA(PC5) -ACOBAMBA(PC1)	Delay	,1877	,0755
7	PATURPAMPA(PC5) -PAMPAS (E)(PC2)	Delay	,2922	,1573
8	PATURPAMPA(PC5) -PAMPAS(S)(PC3)	Delay	,2011	,1152
9	PATURPAMPA(PC5) -LIRCAY(PC4)	Delay	,2139	,0478
10	PATURPAMPA(PC5) -CASA ROSADA(PC6)	Delay	,1637	,0346
11	CASA ROSADA(PC6) -ACOBAMBA(PC1)	Jitter	,0130	,0122
12	CASA ROSADA(PC6) -PAVPAS (E)(PC2)	Jitter	,0118	,0091
13	CASA ROSADA(PC6) -PAVPAS(S)(PC3)	Jitter	,0095	,0031
14	CASA ROSADA(PC6)-LIRCAY(PC4)	Jitter	,0107	,0091
15	CASA ROSADA(PC6) -PATURPAMPA(PC5)	Jitter	,0068	,0059
16	PATURPAMPA(PC5) -ACOBAMBA(PC1)	Jitter	,0097	,0035
17	PATURPAMPA(PC5) -PAMPAS (E)(PC2)	Jitter	,0117	,0106
18	PATURPAMPA(PC5) -PAMPAS(S)(PC3)	Jitter	,0116	,0099
19	PATURPAMPA(PC5) -LIRCAY(PC4)	Jitter	,0101	,0093
20	PATURPAMPA(PC5) -CASA ROSADA(PC6)	Jitter	,0069	,0059
21				

Cuadro Nº 4.4: Datos de *delay* y *jitter* por cada enlace.

Fuente: Elaboración Propia – Ficha técnica

Determinación de alfa

$\alpha = 5\% = 0.05$ Es el grado de error o significancia.

Planteamiento de hipótesis

H_0 = La variable de parámetros de calidad de servicio, tiene una distribución normal.

H_1 = La variable de parámetros de calidad de servicio, no tiene una distribución normal.

Estadígrafo de prueba más apropiado

Para la demostración de la hipótesis se realizó la prueba de normalidad con los datos obtenidos de la calidad de servicio, utilizando la estadística de *Shapiro-Wilk* por ser una muestra menor a 30 datos.

Regla de decisión

- Cuando P – valor ≥α Se acepta la hipótesis nula H_0
- Cuando P – valor ≤α Se acepta la hipótesis alternativa H_1

Calculo de valores de la prueba estadística

Tabla Nº 4.24: Pruebas de normalidad – *Delay* y *Jitter*.

Pruebas de normalidad – *Delay* y *Jitter*						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
pretest	,296	20	,000	,820	20	,020
postest	,269	20	,001	,749	20	,015

Fuente: Elaboración propia- Resultados de *SPSS*

Conclusión

En la tabla Nº 4.24 se observa la variable de la calidad de servicio, tiene una distribución normal, porque el valor de alfa es mayor a 0.05 o 5%, con esto queda demostrado la distribución de normalidad de los datos.

b) Prueba de hipótesis

- Formular la hipótesis nula y alterna de acuerdo al problema.

  H_0 = Un modelo de red con tecnología *MPLS* no influirá significativamente en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

  H1 = Un modelo de red con tecnología *MPLS* influirá significativamente en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

- Escoger un nivel de significancia o riesgo α.

α = 5% = 0.05 Es el grado de error o significancia.

$1 - \alpha = 1 - 0.05 = 0.95 = 95\%$ Nivel de confianza.

- Escoger el estadígrafo de prueba más apropiado.

  La prueba de estadística paramétrica para datos con distribución normal menores a 30 datos**,** se consideró la prueba de T-*Stutend*.

- Establecer la región crítica.

  Cuando P – valor ≥α Se acepta la hipótesis nula H_0

  Cuando P – valor ≤α Se acepta la hipótesis alternativa H_1

- Calcular los valores de la prueba estadística de una muestra de tamaño "n".

Tabla Nº 4.25: Estadísticos de muestras relacionadas *Delay* + *Jitter*.

Estadísticos de muestras relacionadas ***Delay* + *Jitter***					
		Media	N	Desviación típ.	Error típ. de la media
Par 1	pretest	,094550	20	,0981784	,0219534
	postest	,039095	20	,0443720	,0099219

Fuente: Elaboración propia- Resultados de *SPSS*

Tabla Nº 4.26: Correlaciones de muestras relacionadas.

Correlaciones de muestras relacionadas				
		N	Correlación	Sig.
Par 1	pretest y postest	20	,898	,000

Fuente: Elaboración propia- Resultados de *SPSS*

Tabla Nº 4.27: La prueba de T-*Student* para muestras relacionadas.

Prueba de muestras relacionadas *Delay* + *Jitter*									
		Diferencias relacionadas					t	gl	Sig. (bilateral)
		Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia				
					Inferior	Superior			
Par 1	pretest - postest	,0554550	,0615263	,0137577	,0266598	,0842502	4,031	19	,001

Fuente: Elaboración propia- Resultados de *SPSS*

- Rechazar la hipótesis nula (H_o) si el estadígrafo tiene un valor en la región crítica y no rechazar (aceptar) en el otro caso.

Tabla Nº 4.28: Comparación entre de nivel de significancia y valor de p.

Indicadores	Nivel de significancia α	Comparación de signo	valor de P
pretest - postest	0.05	>	0.001

Fuente: Elaboración propia- Resultados de *SPSS*.

- Conclusión de hipótesis general

De la tabla Nº 4.28 se puede observar el valor P es menor al valor de nivel de significancia α que es 5%, por lo tanto rechazamos la hipótesis nula y lo tomamos la hipótesis alterna o de investigación: Un modelo de red con tecnología *MPLS* influirá significativamente en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.

CONCLUSIONES

1. Un modelo de red con tecnología *MPLS* influye en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018. Porque el valor de P es mayor a 0.05 del nivel de significancia, en cado uno de los indicadores, por tanto, la tecnología *MPLS* influye de manera significativa en la calidad de servicio en comparación a la tecnología IP.

2. Los parámetros de calidad de servicio que influye en la red *WAN* son la *delay* y el *jitter*, en donde cada uno de estos indicadores ha sido medido antes y después de la implementación de la tecnología *MPLS*; en donde se comprobó los resultados de *delay* y *jitter* con la tecnología *MPLS* es considerablemente mucho menor que la de tecnología IP.

3. En cuanto al parámetro de la calidad de servicio de *packet loss* en la red *WAN*, se evaluó este parámetro antes y después de la implementación de la tecnología *MPLS* en la topología de la red *WAN* de la Universidad Nacional de Huancavelica, dando como resultado de que no hubo ninguna pérdida de porcentaje de paquetes con la tecnología *MPLS* y como también con la tecnología IP, por tanto, ambas tecnologías IP y *MPLS* soportan de manera significativa en la mejora de la calidad de servicio de conexión.

4. Con el software *D-ITG* se generó los distintos tipos de tráfico a través de la topología de la red *WAN* de la Universidad de Nacional de Huancavelica, en donde se logró a observar los distintos parámetros de calidad de servicio como son: *delay*, el *jitter* y *packet loss*, obteniendo los resultados con el mismo software *D-ITG*.

5. En el software *GNS3* se logró implementar la topología de la red *WAN* de la Universidad Nacional de Huancavelica, en donde se utilizó los siguientes equipos para la implementación: el IOS del router cisco, máquinas virtuales, maquinas reales, con todos estos equipos se realizó la simulación y luego la obtención de resultados de manera exitosa.

RECOMENDACIONES

1. A las Empresas, Instituciones u organizaciones de la región Huancavelica: Optar por la implementación de las nuevas tecnologías en su infraestructura de la red de datos a fin de mejorar el rendimiento de la red, con mayores velocidades de transferencia de información entre sus diversas sucursales, lo cual mejora el servicio de comunicación tales como VoIP, Videoconferencia, internet y otras aplicaciones.

2. Al Centro de investigación de la Universidad Nacional de Huancavelica: Promover programas de investigación en ciencia y tecnología de acuerdo al avance de las nuevas tecnologías, específicamente en el área de telemática en el análisis, estudio y evaluación de las tecnologías de redes como la conmutación de etiquetas multiprotocolo (*MPLS*) y red privada virtual (*VPN*), que actualmente sigue siendo uno de las tecnologías más optativas en las empresas u organizaciones en el mundo.

3. A la Facultad de Ingeniería Electrónica y Sistemas de la Universidad Nacional de Huancavelica: Constituir una red de investigación con otras Universidades del país o con universidades extranjeras para contribuir nuevos conocimientos en el campo de redes, a fin de dar nuevas soluciones a las necesidades de las empresas u organizaciones, y de igual forma compartir las investigaciones en conjuntos con otras universidades o instituciones vinculadas al tema.

4. A los investigadores en el área de redes de comunicaciones: realizar un estudio, análisis y modelamiento de la calidad de servicio y la seguridad en redes de conmutación de etiquetas multiprotocolo (*MPLS*) para garantizar el eficiente rendimiento y la integridad de la información en la red de datos de las instituciones u organizaciones, quienes desean migrar su infraestructura a la red *MPLS*/*VPN* como alternativa de solución a sus requerimientos.

REFERENCIAS BIBLIOGRÁFICAS

Abad, L. (2014). Estudio y diseño de QoS para una red de internet, datos y VoIP. *(Tesis de Titulación).* Universidad Tecnológica Israel, Quito, Ecuador. Recuperado el 25 de 05 de 2017, de http://repositorio.uisrael.edu.ec/handle/47000/899

Alarcon, V., & Martinez, J. (2008). *Introduccion a rede MPLS* (Vol. 1). Mexico, Mexico: El Cid Editor.

Ariganello, E., & Enrique , B. (2013). *Redes Cisco Ccnp a fondo.* Mexico, Mexico: Alfaomega Grupo Editor, S.A. de C.V.

Balakrishnan, R. (2014). *Advanced QoS for Multi-Service IP/MPLS Networks.* Indianápolis, United States of America: Wiley Publishing, Inc.

Calcina , Y. (2011). Diseño de Red *Lan* Utilizando el Protocolo *Mpls* para la Transmisión de Voz, Dato y Video en la Epis – UNA – Puno 2011. *(Tesis de grado).* Universidad Nacional del Altiplano, Puno, Perú. Recuperado el 18 de 10 de 2017, de http://repositorio.unap.edu.pe/handle/UNAP/1853

Cano, J. (2018). Configuración de servicios *VPN* en entorno *MPLS*. *(Tesis de maestria).* Universidad Politecnica de Valencia, Valencia, España.

Castro, E. (2015). Diseño y Simulacion de una red *MPLS* para interconectar estaciones remotas utilizando el emulador GNS3. *(tesis de grado).* Universidad Politecnica Salesiana, Guauaquil, Ecuador .

Chacha, P. (2019). Evaluación de una red *Mpls* usando Diffserv para mejorar el rendimiento en aplicaciones con Qos. *(Tesis de maestria).* Escuela Superior Politécnica de Chimborazo, Riobamba, Ecuador.

Cisco Ccna. (14 de 12 de 2017). *Campus Virtual: "Netacad"*. Recuperado el 28 de 06 de 2018, de Networking Academy: https://www.netacad.com/es

Crow, W. (2016). Análisis de calidad de servicio en transferencia de voz y video en una red de tecnología *mpls*. *(Tesis de Pregrado).* Escuela Superior Politécnica de Chimborazo, Riobamba, Ecuador. Recuperado el 12 de 01 de 2019, de http://dspace.espoch.edu.ec/bitstream/123456789/6428/1/98T00124.pdf

Cujae. (21 de 06 de 2011). *Diapositivas: MPLS*. Recuperado el 01 de 10 de 2017, de Moodle: http://moodle.cujae.edu.cu/pluginfile.php/7423/mod_resource/content/1/Tema_4/Epig._4.5_*MPLS*.pdf

Díaz Ataucuri , D. (27 de 10 de 2001). Calidad de servicio en la internet. *Revista de investigación*. Obtenido de: http://sisbib.unmsm.edu.pe/m_recursos/repositorios.html

Felicisimo, A. M. (23 de 10 de 2012). Modelos de distribución de especies y potencialidad con tecnolgia. *Reduca, 5*, 137-153. Recuperado el 22 de 09 de 2017, de Repositorio: http://revistareduca.es/index.php/biologia/article/viewFile/881/1030

González , Á. (2011). Integración y optimización de redes *MPLS*. *(Tesis de grado).* Universidad Carlos III de Madrid, Madrid, España.

Grajales Bartolo, M. (2011). ANÁLISIS DE TRÁFICO PARA LA RED DE DATOS DE LAS INSTITUCIONES. *(Tesis de grado).* Universidad Tecnológica de Pereira, Pereira, Colombia. Recuperado el 22 de 05 de 2017, de http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4700/6213821G743.pdf?sequence=1

Icmas. (26 de 10 de 2001). *Terminos tecnicos de Telecomunicaciones*. Recuperado el 28 de 11 de 2017, de Repositorio: http://bear.warrington.ufl.edu/centers/purc/docs/papers/sp_02.pdf

Itu. (2008). *Téminos y definiciones: Union Internacional de Telecomunicaciones.* Recuperado el 14 de 12 de 2017, de https://www.itu.int/dms_pubrec/itu-r/rec/v/R-REC-V.662-2-199304-S!!PDF-S.pdf

Itu-I. (2002). *Norma: Unión Internacional de Telecomunicaciones.* Recuperado el 2017 de 09 de 30, de www.itu.int/itudoc/itu-t/workshop/standard/3-02_pp7-es.ppt

Lemarchand, G. A. (20 de 10 de 2008). *Definicion de terminos*. Recuperado el 22 de 11 de 2017, de Tecnologia y Innovacion:

http://www.unesco.org.uy/politicacientifica/budapest+10/fileadmin/templates/cienciasNaturales/pcyds/Budapest10/archivos/Doc%2012-Glosario%20de%20t%C3%A9rminos%20sobre%20ciencia.pdf

Luc, G. (2007). *MPLS Fundamentals.* Indianapolis, USA: Cisco Press.

Mehraban, S., Vora, K., & Upadhyay, D. (2018). Deploy Multi Protocol Label Switching (*MPLS*) Using Virtual Routing and Forwarding (*VRF*). *IEEE*.

Menedez, R. (2012). Estudio del desempeño e implementación de una solución *MPLS-VPN* sobre múltiples sistemas autónomos. *(Tesis de grado).* Pontificia Universidad Católica del Perú, Lima, Perú.

Oña, G. (2016). Diseño y comparación de redes de acceso *MPLS* y metro Ethernet integradas a un *backbone MPLS* para un proveedor de servicio y realizacion de un prototipo base. *(Tesis de grado).* Escuela Politecnica Nacional, Quito, Ecuador.

Peña, G., Sanatana, S., & Contreras, V. (2014). Diseño e implementación de una red *mpls* para el sistema de comunicación de editorial Oceano Dominicana, en Santo Domingo y zona metropolitana de Santiago, agosto-diciembre 2014. *(Tesis de Grado).* Universidad del Caribe, Santo Domingo, República Dominicana. Recuperado el 20 de 02 de 2018, de https://es.slideshare.net/vanessajcontreras16/informe-final-modificado

Postel, J., Crocker , S., & Cerf, V. (2009). *Redes de comunicaciones.* Madrid, España: Guimi.

Pozueco, L. (2014). Diseño y evaluación de sistemas de estimación de ancho de banda disponible para servicios adaptativos de vídeo streaming. *(Tesis Dotoral).* Universidad Nacional de Educación a Distancia, Madrid, España. Recuperado el 30 de 05 de 2017, de http://e-spacio.uned.es/fez/eserv/tesisuned:IngInd-Lpozueco/POZUECO_ALVAREZ_Laura_Tesis.pdf

Real Academia Española. (12 de 15 de 2001). *Diccionario de la lengua española*. Recuperado el 28 de 12 de 2017, de Repositorio: http://dle.rae.es/

Rfc. (12 de 05 de 2001). *Norma: "RFC 3031 - Multiprotocol Label Switching Architecture - IETF Tools"*. Recuperado el 28 de 10 de 2017, de Documentos: https://tools.ietf.org/html/rfc3031

Rodriguez, R. (15 de 09 de 2007). *Cátedra: "Redes de Computadoras"*. Recuperado el 20 de 01 de 2018, de Campus virtual: https://rodrigorodriguez.files.wordpress.com/2009/02/glosario_redes.pdf

Rouse, M. (02 de 11 de 2012). *Articulo:"Redes empresariales"*. Recuperado el 27 de 12 de 2018, de Datca Center: https://searchdatacenter.techtarget.com/es/definicion/Enrutamiento-virtual-y-reenvio-*VRF*

Sanchez, H., & Reyes, C. (2017). *METODOLOGÍA Y DISEÑO DE LA INVESTIGACIÓN CIENTÍFICA.* Lima, Perú: Universidad Ricardo Palma.

Santos, M. (2014). *Diseño de Redes Telematicas.* Madrid, España: RA-MA S.A.

Stallings, W. (2012). *Comunicaciones y Redes de computadores.* Madrid, España: Pearson Educación, S. A.

Tanenbaum, A. S. (2012). *Redes de computadoras.* Mexico, Mexico: Pearson Educación de México, S.A. de C.V.

Uba. (20 de 09 de 2016). *Guia de clases: "Redes IP"*. Recuperado el 20 de 10 de 2017, de Campus Virtual: http://campus.fi.uba.ar/

Uit. (2003). *Glosario de términos: Union Internacional de Telecomunicaciones.* Recuperado el 25 de 12 de 2017, de https://www.itu.int/rec/T-REC-Z.341-198811-I/es

Velurtas, F. (2009). En redes de datos. *(Tesis de Maestria).* Universidad Nacional de la Plata, La Plata, Argentina. Recuperado el 30 de 05 de 2017, de http://postgrado.info.unlp.edu.ar/Carreras/Magisters/Redes_de_Datos/Tesis/Velurtas_Facundo.pdf

Victoria, L., & Igor , J. (2009). MEDICIÓN Y ANÁLISIS DE TRÁFICO EN REDES *MPLS. (Tesis de grado).* Pontificia Universidad Católica del Perú, Lima, Perú.

Yadav, S., & Jeyakumar, A. (15 de 09 de 2016). Design of traffic engineered *MPLS VPN* for protected traffic using GNS simulator. *IEEE*, 405 - 409. Recuperado el 10 de 02 de 2017, de http://ieeexplore.ieee.org/document/7566165/

Zapata , M. (2016). Evaluación de parámetros de calidad de servicio (QOS) para el diseño de una red *VPN* con *MPLS*. *(Tesis de Maestria).* Pontificia Universidad Católica del Ecuador, Quito, Ecuador. Recuperado el 12 de 06 de 2017, de DSpace is a digital service: http://repositorio.puce.edu.ec/bitstream/handle

ANEXOS

ANEXO Nº 01: MATRIZ DE CONSISTENCIA

PROBLEMA	OBJETIVO	HIPOTESIS	VARIABLES Y DIMENSIONES	METODOLOGIA
Problema general: ¿Cómo influye un modelo de red con tecnología *MPLS* en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018? **Problemas específicos** ¿Cómo influye un modelo de red con tecnología *MPLS* en el *delay* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018? ¿Cómo influye un modelo de red con tecnología *MPLS* en el *jitter* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018? ¿Cómo influye un modelo de red con tecnología *MPLS* en la *packet loss* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018?	**Objetivo general** • Determinar la influencia del modelo de red con tecnología *MPLS* en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018. **Objetivos específicos** • Determinar la influencia del modelo de red con tecnología *MPLS* en el *delay* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018. • Determinar la influencia del modelo de red con tecnología *MPLS* en el *jitter* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018. • Determinar la influencia del modelo de red con tecnología *MPLS* en la *packet loss* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.	**Hipótesis general** • Un modelo de red con tecnología *MPLS* influirá significativamente en la calidad de servicio en la red *WAN* de la Universidad Nacional de Huancavelica, 2018. **Hipótesis específicos** • Un modelo de red con tecnología *MPLS* influirá significativamente en el *delay* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018. • Un modelo red con tecnología *MPLS* influirá significativamente en el *jitter* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018. • Un modelo red con tecnología *MPLS* influirá significativamente en la *packet loss* en la red *WAN* de la Universidad Nacional de Huancavelica, 2018.	**Variable independiente** • Modelo de red con tecnología *MPLS*. **Dimensiones** • Modelo de red con MPLS **Variable dependiente** • La calidad de servicio. **Dimensiones** • *Delay*. • *Jitter* • *Packet loss* **Indicadores** • Datos • Voz • Video	**Tipo:** Aplicada **Nivel:** Explicativa **Métodos:** • General: científico •Particulares: Experimental, observación, bibliográfico y descriptivo. **Diseño:** Experimental pre y post test. **M: O_1 X O_2** **Población:** Todas las redes *WAN* de la Universidad Nacional de Huancavelica. **Muestra:** Los diez redes *WAN* de la Universidad Nacional de Huancavelica. **Muestreo:** No probabilística. **Técnicas de recolección de datos:** • Simulación • Medición • Observación **Instrumentos de recolección de datos:** •*GNS3* •*D-ITG* •Ficha de observación. **Técnicas de procesamiento y análisis de datos:** • Estadística descriptiva • Estadística inferencial • SPSS v.24

ANEXO Nº 02

INSTRUMENTO DE RECOLECCIÓN DE DATOS

FICHA DE OBSERVACIÓN

EVALUACIÓN DE PARÁMETROS DE CALIDAD DE SERVICIO (*QoS*) EN LA RED *WAN* DE LA UNIVERISDAD NACIONAL DE HUANCAVELICA

Observador: ……

Tipo de tecnología: ……..……..

Indicación: Anotar en el siguiente cuadro los resultados obtenidos de los parámetros de calidad de servicio (*QoS*) de cada enlace de red.

ENLACE DE RED *WAN*: ……..			
Tipos de tráfico	**Parámetros de calidad de servicio**		
	***Delay* (ms)**	***Jitter* (ms)**	**Pérdida de paquetes (%)**
Datos			
VoIP			
Video Streaming			
ENLACE DE RED *WAN*: ……..			
Tipos de tráfico	**Parámetros de calidad de servicio**		
	***Delay* (ms)**	***Jitter* (ms)**	**Pérdida de paquetes (%)**
Datos			
VoIP			
Video Streaming			
ENLACE DE RED *WAN*: ……..			
Tipos de tráfico	**Parámetros de calidad de servicio**		
	***Delay* (ms)**	***Jitter* (ms)**	**Pérdida de paquetes (%)**
Datos			
VoIP			
Video Streaming			

Fuente: Elaboración propia.

ANEXO Nº 03: BASE DE DATOS

ENLACE DE RED *WAN*	SERVICIO DE DATOS					
	PARAMETROS DE CALIDAD DE SERVICIO					
	DELAY (S)		*JITTER* (S)		*PACKET LOSS* (%)	
	TECNOLOGIA IP	TECNOLOGIA *MPLS*	TECNOLOGIA IP	TECNOLOGIA *MPLS*	TECNOLOGIA IP	TECNOLOGIA *MPLS*
CASA ROSADA(PC6) - ACOBAMBA(PC1)	0.0705	0.0236	0.0085	0.0078	0.0000	0.0000
CASA ROSADA(PC6) - PAMPAS (E)(PC2)	0.1638	0.0996	0.0086	0.0079	0.0000	0.0000
CASA ROSADA(PC6) - PAMPAS(S)(PC3)	0.0469	0.0462	0.0082	0.0082	0.0000	0.0000
CASA ROSADA(PC6)- LIRCAY(PC4)	0.0964	0.0018	0.0089	0.0082	0.0000	0.0000
CASA ROSADA(PC6) - PATURPAMPA(PC5)	0.1942	0.0587	0.0055	0.0054	0.0000	0.0000
PATURPAMPA(PC5) - ACOBAMBA(PC1)	0.3061	0.1100	0.0098	0.0094	0.0000	0.0000
PATURPAMPA(PC5) - PAMPAS (E)(PC2)	0.4239	0.1536	0.0093	0.0090	0.0000	0.0000
PATURPAMPA(PC5) - PAMPAS(S)(PC3)	0.1427	0.1269	0.0086	0.0082	0.0000	0.0000
PATURPAMPA(PC5) - LIRCAY(PC4)	0.0518	0.0452	0.0097	0.0090	0.0000	0.0000
PATURPAMPA(PC5) - CASA ROSADA(PC6)	0.1497	0.0747	0.0054	0.0053	0.0000	0.0000

ENLACE DE RED *WAN*	SERVICIO DE VoIP					
	PARAMETROS DE CALIDAD DE SERVICIO					
	DELAY (S)		*JITTER* (S)		*PACKET LOSS* (%)	
	TECNOLOGIA IP	TECNOLOGIA *MPLS*	TECNOLOGIA IP	TECNOLOGIA *MPLS*	TECNOLOGIA IP	TECNOLOGIA *MPLS*
CASA ROSADA(PC6) - ACOBAMBA(PC1)	0.1501	0.0299	0.0091	0.0089	0.0000	0.0000
CASA ROSADA(PC6) - PAMPAS (E)(PC2)	0.4779	0.1197	0.0076	0.0064	0.0000	0.0000
CASA ROSADA(PC6) - PAMPAS(S)(PC3)	0.0889	0.0399	0.0077	0.0072	0.0000	0.0000
CASA ROSADA(PC6)- LIRCAY(PC4)	0.1158	0.0310	0.0094	0.0091	0.0000	0.0000
CASA ROSADA(PC6) - PATURPAMPA(PC5)	0.1267	0.0490	0.0062	0.0049	0.0000	0.0000
PATURPAMPA(PC5) - ACOBAMBA(PC1)	0.1465	0.0299	0.0085	0.0082	0.0000	0.0000
PATURPAMPA(PC5) - PAMPAS (E)(PC2)	0.1726	0.1647	0.0100	0.0093	0.0000	0.0000
PATURPAMPA(PC5) - PAMPAS(S)(PC3)	0.2261	0.1044	0.0092	0.0077	0.0000	0.0000
PATURPAMPA(PC5) - LIRCAY(PC4)	0.2874	0.0497	0.0086	0.0072	0.0000	0.0000
PATURPAMPA(PC5) - CASA ROSADA(PC6)	0.1947	0.0166	0.0062	0.0054	0.0000	0.0000

ENLACE DE RED *WAN*	SERVICIO DE STREAMING					
	PARAMETROS DE CALIDAD DE SERVICIO					
	DELAY (S)		*JITTER* (S)		*PACKET LOSS* (%)	
	TECNOLOGIA IP	TECNOLOGIA *MPLS*	TECNOLOGIA IP	TECNOLOGIA *MPLS*	TECNOLOGIA IP	TECNOLOGIA *MPLS*
CASA ROSADA(PC6) - ACOBAMBA(PC1)	0.1059	0.0435	0.0223	0.0198	0.0000	0.0000
CASA ROSADA(PC6) - PAMPAS (E)(PC2)	0.1349	0.1325	0.0192	0.0130	0.0000	0.0000
CASA ROSADA(PC6) - PAMPAS(S)(PC3)	0.0967	0.0442	0.0127	0.0120	0.0000	0.0000
CASA ROSADA(PC6)- LIRCAY(PC4)	0.1272	0.0075	0.0137	0.0111	0.0000	0.0000
CASA ROSADA(PC6) - PATURPAMPA(PC5)	0.1952	0.0521	0.0086	0.0075	0.0000	0.0000
PATURPAMPA(PC5) - ACOBAMBA(PC1)	0.1106	0.0865	0.0109	0.0108	0.0000	0.0000
PATURPAMPA(PC5) - PAMPAS (E)(PC2)	0.2800	0.1536	0.0157	0.0135	0.0000	0.0000
PATURPAMPA(PC5) - PAMPAS(S)(PC3)	0.2345	0.1172	0.0171	0.0139	0.0000	0.0000
PATURPAMPA(PC5) - LIRCAY(PC4)	0.3024	0.0478	0.0121	0.0116	0.0000	0.0000
PATURPAMPA(PC5) - CASA ROSADA(PC6)	0.1466	0.0124	0.0091	0.0071	0.0000	0.0000

ANEXO Nº 04

VALIDACIÓN DE INSTRUMENTOS POR JUICIO DE EXPERTOS

UNIVERSIDAD NACIONAL DE HUANCAVELICA
(Creada por Ley N° 25265)
ESCUELA DE POSGRADO

FICHA DE VALIDACIÓN

INFORME DE OPINIÓN DEL JUICIO DE EXPERTOS

1. **DATOS GENERALES**
   - 1.1. **Apellidos y nombres:** Almidón Elescano Angel
   - 1.2. **Grado académico:** Maestro en docencia superior
   - 1.3. **Mención:** Docencia superior.
   - 1.4. **DNI/Teléfono:** 23715269 / 990866060
   - 1.5. **Institución donde labora:** Universidad Nacional de Huancavelica
   - 1.6. **Lugar y fecha** Pampas
   - 1.7. **Título de la investigación:** MODELO DE RED CON TECNOLOGÍA MPLS PARA LA MEJORA DE LA CALIDAD DE SERVICIO EN LA RED WAN DE LA UNIVERSIDAD NACIONAL DE HUANCAVELICA
   - 1.8. **Instrumento de evaluación:** Ficha de observación para la evaluación de los parámetros de calidad de servicio (QoS) en la red de transporte (WAN).
   - 1.9. ***Tesista:*** *WILLIAM DANTY RAMOS PAUCAR*
   - 1.10. **Maestría:** CIENCIAS DE INGENIERÍA
   - 1.11. **Mención:** PLANEACIÓN ESTRATÉGICA Y GESTIÓN EN INGENIERÍA DE PROYECTOS

2. **ASPECTOS DE EVALUACIÓN**

CRITERIOS	*DEFICIENTE*	*BAJA*	*REGULAR*	*BUENA*	*MUY BUENA*
	1	2	3	4	5
CONTENIDO					X
OBJETIVIDAD				X	
ACTUALIDAD					X
CRITERIO					X
CLARIDAD Y PRESICIÓN					X
PUNTAJE PARCIAL				4	20
PUNTAJE TOTAL	24				

3. **OPINIÓN DE LA APLICABILIDAD:** (Marque con un aspa en el circulo asociado)

CATEGORIA		INTERVALO
No valido, reformular	○	[5-16]
No valido, modificar	○	[17-18]
Valido, mejorar	○	[19-21]
Valido, aplicar	⊗	[22-25]

4. **RECOMENDACIONES**

Firma

UNIVERSIDAD NACIONAL DE HUANCAVELICA
(Creada por Ley N° 25265)
ESCUELA DE POSGRADO

FICHA DE VALIDACIÓN

INFORME DE OPINIÓN DEL JUICIO DE EXPERTOS

1. **DATOS GENERALES**
   - 1.1. **Apellidos y nombres:** HERRERA MORALES JAVIER ALFREDO
   - 1.2. **Grado académico:** MAESTRO
   - 1.3. **Mención:** PLANEACIÓN ESTRATÉGICA Y GESTIÓN DE INGENIERÍA DE PROYECTOS
   - 1.4. **DNI/Teléfono:** 10198612 / 930605443
   - 1.5. **Institución donde labora:** UNIVERSIDAD NACIONAL DE HUANCAVELICA
   - 1.6. **Lugar y fecha:** HUANCAVELICA
   - 1.7. **Título de la investigación:** MODELO DE RED CON TECNOLOGÍA MPLS PARA LA MEJORA DE LA CALIDAD DE SERVICIO EN LA RED WAN DE LA UNIVERSIDAD NACIONAL DE HUANCAVELICA
   - 1.8. **Instrumento de evaluación:** Ficha de observación para la evaluación de los parámetros de calidad de servicio (QoS) en la red de transporte (WAN)
   - 1.9. **Tesista:** WILLIAM DANTY RAMOS PAUCAR
   - 1.10. **Maestría:** CIENCIAS DE INGENIERÍA
   - 1.11. **Mención:** PLANEACIÓN ESTRATÉGICA Y GESTIÓN EN INGENIERÍA DE PROYECTOS

2. **ASPECTOS DE EVALUACIÓN**

CRITERIOS	DEFICIENTE	BAJA	REGULAR	BUENA	MUY BUENA
	1	2	3	4	5
CONTENIDO				X	
OBJETIVIDAD					X
ACTUALIDAD					X
CRITERIO				X	
CLARIDAD Y PRESICIÓN					X
PUNTAJE PARCIAL				8	15
PUNTAJE TOTAL	23				

3. **OPINIÓN DE LA APLICABILIDAD:** (Marque con un aspa en el circulo asociado)

CATEGORIA		INTERVALO
No valido, reformular	○	[5-16]
No valido, modificar	○	[17-18]
Valido, mejorar	○	[19-21]
Valido, aplicar	⊗	[22-25]

4. **RECOMENDACIONES:**

Firma

UNIVERSIDAD NACIONAL DE HUANCAVELICA
(Creada por Ley N° 25265)
ESCUELA DE POSGRADO

FICHA DE VALIDACIÓN

INFORME DE OPINIÓN DEL JUICIO DE EXPERTOS

1. **DATOS GENERALES**
   - 1.1. **Apellidos y nombres:** MARQUEZ COMARENA JAVIER FRANCISCO
   - 1.2. **Grado académico:** DOCTOR
   - 1.3. **Mención:** INGENIERÍA DE SISTEMAS
   - 1.4. **DNI/Teléfono:** 19930942 / 985320392
   - 1.5. **Institución donde labora:** UNIVERSIDAD NACIONAL DE HUANCAVELICA
   - 1.6. **Lugar y fecha:** PAMPAS
   - 1.7. **Titulo de la investigación:** MODELO DE RED CON TECNOLOGÍA MPLS PARA LA MEJORA DE LA CALIDAD DE SERVICIO EN LA RED WAN DE LA UNIVERSIDAD NACIONAL DE HUANCAVELICA
   - 1.8. **Instrumento de evaluación:** Ficha de observación para la evaluación de los parámetros de calidad de servicio (QoS) en la red de transporte (WAN).
   - 1.9. **Tesista:** WILLIAM DANTY RAMOS PAUCAR
   - 1.10. **Maestría:** CIENCIAS DE INGENIERÍA
   - 1.11. **Mención:** PLANEACIÓN ESTRATÉGICA Y GESTIÓN EN INGENIERÍA DE PROYECTOS

2. **ASPECTOS DE EVALUACIÓN**

CRITERIOS	DEFICIENTE	BAJA	REGULAR	BUENA	MUY BUENA
	1	2	3	4	5
CONTENIDO					X
OBJETIVIDAD					X
ACTUALIDAD					X
CRITERIO				X	
CLARIDAD Y PRESICIÓN				X	
PUNTAJE PARCIAL				8	15
PUNTAJE TOTAL	23				

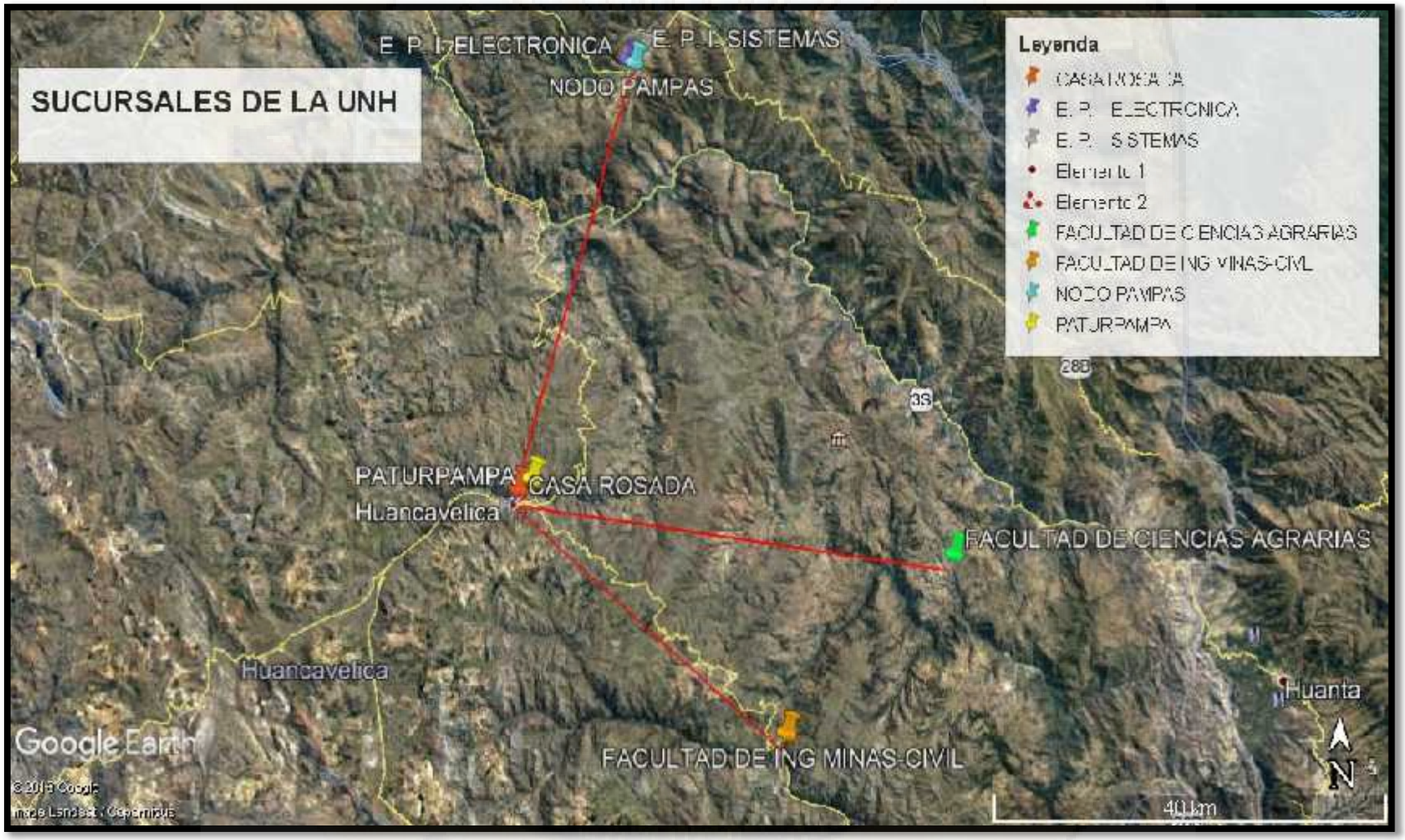
3. **OPINIÓN DE LA APLICABILIDAD:** (Marque con un aspa en el circulo asociado)

CATEGORIA		INTERVALO
No valido, reformular	○	[5-16]
No valido, modificar	○	[17-18]
Valido, mejorar	○	[19-21]
Valido, aplicar	⊗	[22-25]

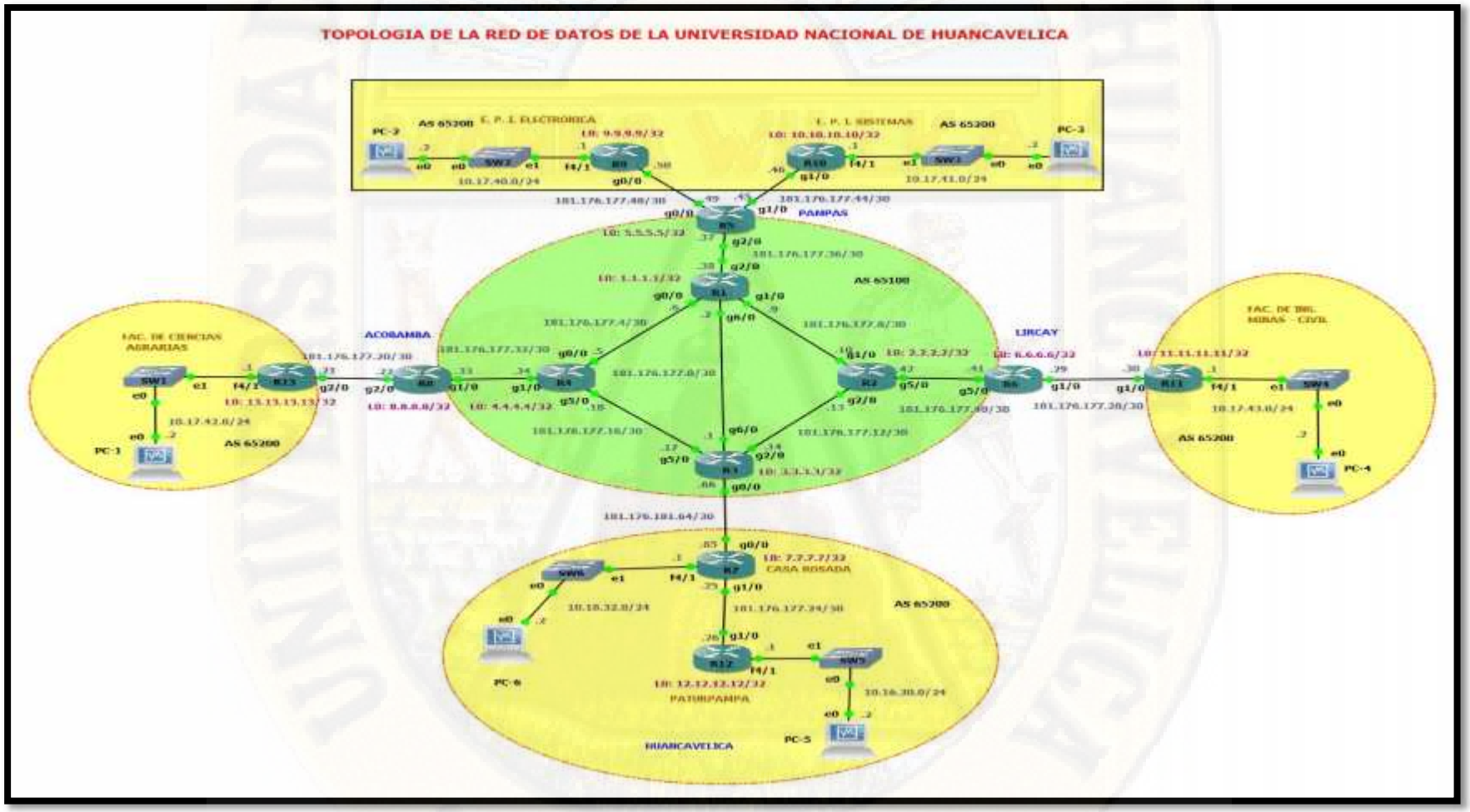
4. **RECOMENDACIONES:**

Firma

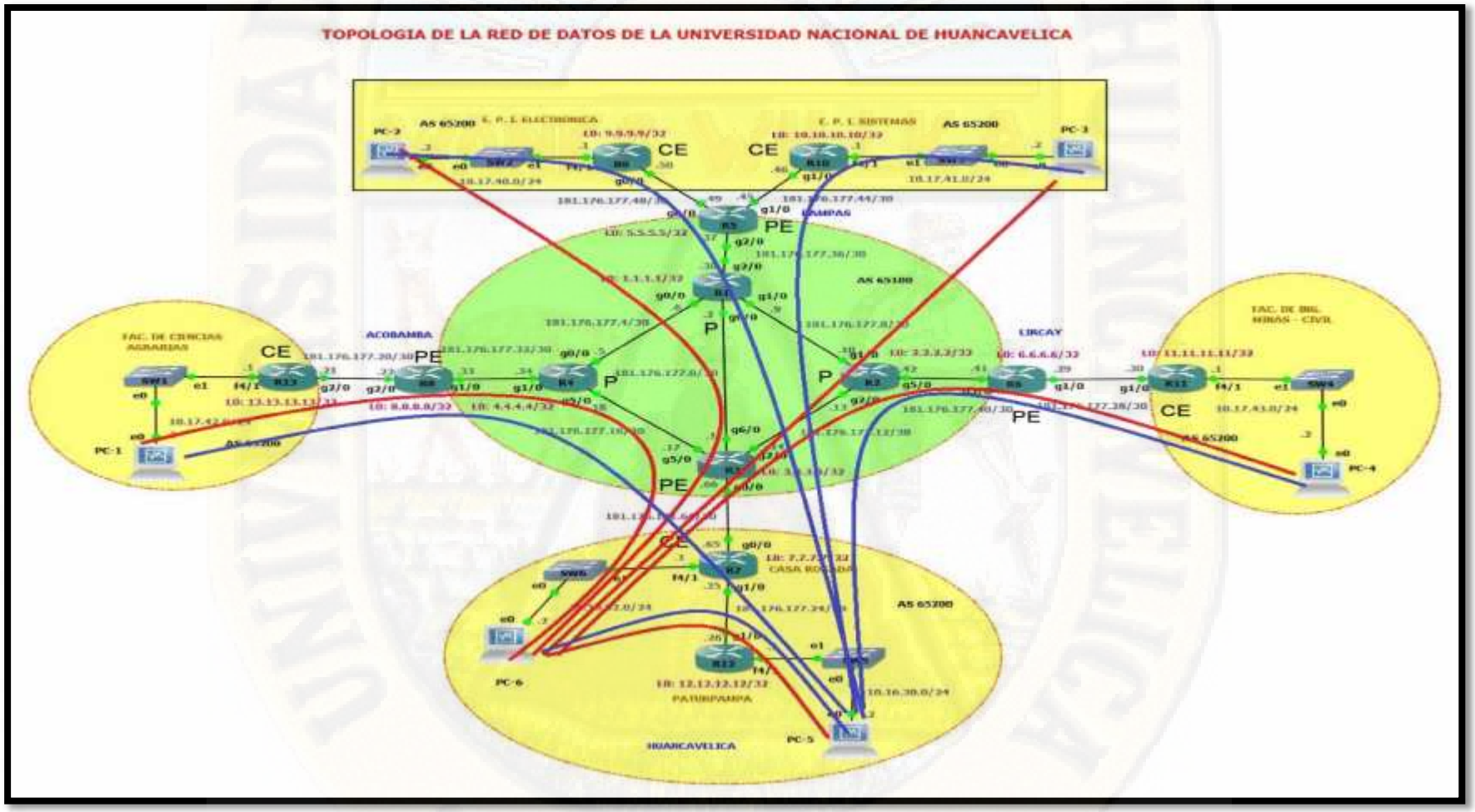
ANEXO Nº 05: SUCURSALES DE LA UNIVERSIDAD NACIONAL DE HUANCAVELICA



ANEXO Nº 06: TOPOLOGÍA DE LA RED DE DATOS DE LA UNIVERSIDAD NACIONAL DE HUANCAVELICA



ANEXO Nº 07: DIAGRAMA DE COMUNICACIONES DE LA RED WAN DE LA UNIVERSIDAD NACIONAL DE HUANCAVELICA



ANEXO Nº 08

GALERÍA DE FOTOS

ANEXO Nº 09

CONFIGURACIÓN DE LA TOPOLOGÍA

CONFIGURACIÓN DE LA TECNOLOGÍA MPLS/L3VPN

(MPLS – OSPF –VRF – MG – BGP)

1) CONFIGURACION DE OSPF

LA RED CORE

R1

R1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#router ospf 1

R1(config-router)#network 181.176.177.4 0.0.0.3 area 0

R1(config-router)#network 181.176.177.0 0.0.0.3 area 0

R1(config-router)#network 181.176.177.8 0.0.0.3 area 0

R1(config-router)#exit

R1(config)#exit

R1#wr

Building configuration...

[OK]

R1#

R2

R2#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#router ospf 1

R2(config-router)#network 181.176.177.12 0.0.0.3 area 0

R2(config-router)#network 181.176.177.8 0.0.0.3 area 0

R2(config-router)#exit

R2(config)#exit

R2#wr

Building configuration...

[OK]

R2#

R3

R3#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#router ospf 1

R3(config-router)#network 181.176.177.12 0.0.0.3 area 0

R3(config-router)#network 181.176.177.16 0.0.0.3 area 0

R3(config-router)#network 181.176.177.0 0.0.0.3 area 0

R3(config-router)#exit

R3(config)#exit

R3#wr

Building configuration...

[OK]

R4

R4#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R4(config)#router ospf 1

R4(config-router)#network 181.176.177.16 0.0.0.3 area 0

R4(config-router)#network 181.176.177.4 0.0.0.3 area 0

R4(config-router)#exit

R4(config)#exit

R4#wr

Building configuration...

[OK]

R4#

R5

R5#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R5(config)#router ospf 1

R5(config-router)#network 181.176.177.36 0.0.0.3 area 0

R5(config-router)#exit

R5(config)#exit

R5#wr

Building configuration...

[OK]

R5#

R6

R6#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R6(config)#router ospf 1

R6(config-router)#network 181.176.177.40 0.0.0.3 area 0

R6(config-router)#exit

R6(config)#exit

R6#wr

Building configuration...

[OK]

R6#

R8

R8#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R8(config)#router ospf 1

R8(config-router)#network 181.176.177.32 0.0.0.3 area 0

R8(config-router)#exit

R8(config)#exit

R8#wr

Building configuration...

[OK]

R8#

LA RED CLIENTE

R7

R7#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R7(config)#router ospf 1

R7(config-router)#network 10.18.32.0 0.0.0.255 area 0

R7(config-router)#exit

R7(config)#exit

R7#wr

Building configuration...

[OK]

R7#

R12

R12#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R12(config)#router ospf 1

R12(config-router)#network 181.176.177.24 0.0.0.3 area 0

R12(config-router)#network 10.16.30.0 0.0.0.255 area 0

R12(config-router)#exit

R12(config)#exit

R12#wr

Building configuration...

[OK]

R12#

2) **CONFIGURACION DE MPLS + LDP**

LA RED CORE

R1

R1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#mpls ip

R1(config)#mpls ldp router-id loopback 0

R1(config)#interface g0/0

R1(config-if)#mpls ip

R1(config-if)#exit

R1(config)#interface g6/0

R1(config-if)#mpls ip

R1(config-if)#exit

R1(config)#interface g1/0

R1(config-if)#mpls ip

R1(config-if)#exit

R1(config)#interface g2/0

R1(config-if)#mpls ip

R1(config-if)#exit

R1(config)#exit

R1#wr

R1#wr

Building configuration...

[OK]

R1#

R2

R2#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#mpls ip

R2(config)#mpls ldp router-id loopback 0

R2(config)#interface g1/0

R2(config-if)#mpls ip

R2(config-if)#exit

R2(config)#

R2(config)#interface g5/0

R2(config-if)#mpls ip

R2(config-if)#exit

R2(config)#interface g2/0

R2(config-if)#mpls ip

R2(config-if)#exit

R2(config)#exit

R2#wr

Building configuration...

[OK]

R2#

R3

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#mpls ip
R3(config)#mpls ldp router-id loopback 0
R3(config)#interface g5/0
R3(config-if)#mpls ip
R3(config-if)#exit
R3(config)#interface g6/0
R3(config-if)#mpls ip
R3(config-if)#exit
R3(config)#interface g2/0
R3(config-if)#mpls ip
R3(config)#exit
R3#
R3#wr
Building configuration...
[OK]
R3#
```

R4

```
R4#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#mpls ip
R4(config)#mpls ldp router-id loopback 0
R4(config)#interface g0/0
R4(config-if)#mpls ip
R4(config-if)#exit
```

R4(config)#interface g1/0

R4(config-if)#mpls ip

R4(config-if)#exit

R4(config)#interface g5/0

R4(config-if)#mpls ip

R4(config-if)#exit

R4(config)#exit

R4#wr

Building configuration...

[OK]

R4#

R5

R5#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R5(config)#mpls ip

R5(config)#mpls ldp router-id loopback 0

R5(config)#interface g2/0

R5(config-if)#mpls ip

R5(config-if)#exit

R5#wr

Building configuration...

[OK]

R5#

R6

R6#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R6(config)#mpls ip

R6(config)#mpls ldp router-id loopback 0

R6(config)#interface g5/0

R6(config-if)#mpls ip

R6(config-if)#exit

R6(config)#exit

R6#wr

Building configuration...

[OK]

R6#

R8

R8#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R8(config)#mpls ip

R8(config)#mpls ldp router-id loopback 0

R8(config)#interface g1/0

R8(config-if)#mpls ip

R8(config-if)#exit

R8(config)#exit

R8#wr

Building configuration...

[OK]

R8#

3) **CONFIGURACION DE VRF**

R3

R3#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#ip vrf ADMINISTRATIVO-HVCA

R3(config-vrf)#rd 65200:1

R3(config-vrf)#route-target export 65200:1

R3(config-vrf)#route-target import 65200:2

R3(config-vrf)#route-target import 65200:3

R3(config-vrf)#route-target import 65200:4

R3(config-vrf)#route-target import 65200:5

R3(config-vrf)#interface g0/0

R3(config-if)#ip vrf forwarding ADMINISTRATIVO-HVCA

% Interface GigabitEthernet0/0 IP address 181.176.181.66 removed due to enabling VRF ADMINISTRATIVO-HVCA

R3(config-if)#ip address 181.176.181.66 255.255.255.252

R3(config-if)#exit

R3(config)#exit

R3#w

*Feb 3 10:36:41.887: %SYS-5-CONFIG_I: Configured from console by console

R3#wr

Building configuration...

[OK]

R3#

R5

R5#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R5(config)#ip vrf PAMPAS-E

R5(config-vrf)#rd 65200:4

R5(config-vrf)#route-target export 65200:4

```
R5(config-vrf)#route-target import 65200:1
R5(config-vrf)#interface g0/0
R5(config-if)#ip vrf forwarding PAMPAS-E
% Interface GigabitEthernet0/0 IP address 181.176.177.49 removed due to enabling VRF PAMPAS-E
R5(config-if)#ip address 181.176.177.49 255.255.255.252
R5(config-if)#exit
R5(config)#exit
R5#wr
*Feb  3 10:16:48.043: %SYS-5-CONFIG_I: Configured from console by console
R5#wr
Building configuration...
[OK]
R5#
R5#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R5(config)#ip vrf PAMPAS-S
R5(config-vrf)#rd 65200:3
R5(config-vrf)#route-target export 65200:3
R5(config-vrf)#route-target import 65200:1
R5(config-vrf)#interface g1/0
R5(config-if)#ip vrf forwarding PAMPAS-S
% Interface GigabitEthernet1/0 IP address 181.176.177.45 removed due to enabling VRF PAMPAS-S
R5(config-if)#ip address 181.176.177.45 255.255.255.252
R5(config-if)#exit
R5(config)#exit
R5#wr
```

*Feb 3 10:21:00.151: %SYS-5-CONFIG_I: Configured from console by console

R5#wr

Building configuration...

[OK]

R5#

R6

R6#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R6(config)#ip vrf LIRCAY

R6(config-vrf)#rd 65200:2

R6(config-vrf)#route-target export 65200:2

R6(config-vrf)#route-target import 65200:1

R6(config-vrf)#interface g1/0

R6(config-if)#ip vrf forwarding LIRCAY

% Interface GigabitEthernet1/0 IP address 181.176.177.29 removed due to enabling VRF LIRCAY

R6(config-if)#ip address 181.176.177.29 255.255.255.252

R6(config-if)#exit

R6(config)#exit

R6#wr

Building configuration...

[OK]

R6#

R8

R8#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

R8(config)#ip vrf ACOBAMBA

R8(config-vrf)#rd 65200:5

R8(config-vrf)#route-target export 65200:5

R8(config-vrf)#route-target import 65200:1

R8(config-vrf)#interface g2/0

R8(config-if)#ip vrf forwarding ACOBAMBA

R8(config-if)#ip address 181.176.177.22 255.255.255.252

R8(config-if)#exit

R8(config)#exit

R8#wr

Building configuration...

[OK]

R8#

4) **CONFIGURACION MP-BGP**

LA RED CORE

R3

R3#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#router bgp 65100

R3(config-router)#bgp router-id 3.3.3.3

R3(config-router)#neighbor 5.5.5.5 remote-as 65100

*Feb 3 16:50:00.539: %BGP-5-ADJCHANGE: neighbor 5.5.5.5 Up

R3(config-router)#neighbor 6.6.6.6 remote-as 65100

*Feb 3 16:50:50.775: %BGP-5-ADJCHANGE: neighbor 6.6.6.6 Up

R3(config-router)#neighbor 8.8.8.8 remote-as 65100

*Feb 3 16:51:13.871: %BGP-5-ADJCHANGE: neighbor 8.8.8.8 Up

R3(config-router)#neighbor 5.5.5.5 update-source loopback 0

R3(config-router)#neighbor 6.6.6.6 update-source loopback 0

R3(config-router)#neighbor 8.8.8.8 update-source loopback 0

R3(config-router)#address-family vpnv4 unicast

R3(config-router-af)#neighbor 5.5.5.5 activate

*Feb 3 16:53:58.839: %BGP-5-ADJCHANGE: neighbor 5.5.5.5 Down Address family activated

*Feb 3 16:54:00.907: %BGP-5-ADJCHANGE: neighbor 5.5.5.5 Up

R3(config-router-af)#neighbor 6.6.6.6 activate

*Feb 3 16:54:32.023: %BGP-5-ADJCHANGE: neighbor 6.6.6.6 Down Address family activated

*Feb 3 16:54:34.123: %BGP-5-ADJCHANGE: neighbor 6.6.6.6 Up

R3(config-router-af)#neighbor 8.8.8.8 activate

*Feb 3 16:54:56.271: %BGP-5-ADJCHANGE: neighbor 8.8.8.8 Down Address family activated

*Feb 3 16:54:58.391: %BGP-5-ADJCHANGE: neighbor 8.8.8.8 Up

R3(config-router-af)#exit

R3(config-router)#exit

R3(config)#exit

R3#wr

Building configuration...

[OK]

R3#

R5

R5#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R5(config)#router bgp 65100

R5(config-router)#bgp router-id 5.5.5.5

R5(config-router)#neighbor 3.3.3.3 remote-as 65100

R5(config-router)#neighbor 3.3.3.3 update-source loopback 0

R5(config-router)#address-family vpnv4 unicast

R5(config-router-af)#neighbor 3.3.3.3 activate

R5(config-router-af)#exit

R5(config-router)#exit

R5(config)#exit

R5#wr

Building configuration...

[OK]

R5#

R6

R6#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R6(config)#router bgp 65100

R6(config-router)#bgp router-id 6.6.6.6

R6(config-router)#neighbor 3.3.3.3 remote-as 65100

R6(config-router)#neighbor 3.3.3.3 update-source loopback 0

R6(config-router)#address-family vpnv4 unicast

R6(config-router-af)#neighbor 3.3.3.3 activate

R6(config-router-af)#exit

R6(config-router)#exit

R6(config)#exit

R6#wr

Building configuration...

[OK]

R6#

R8

```
R8#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R8(config)#router bgp 65100
R8(config-router)#bgp router-id 8.8.8.8
R8(config-router)#neighbor 3.3.3.3 remote-as 65100
R8(config-router)#neighbor 3.3.3.3 update-source loopback 0
R8(config-router)#address-family vpnv4 unicast
R8(config-router-af)#neighbor 3.3.3.3 activate
R8(config-router-af)#exit
R8(config-router)#exit
R8(config)#exit
R8#wr
Building configuration...
[OK]
R8#
```

5) **CONFIGURACION DE SESIONES DE LA RED DE CLIENTES EN EL COORE**

R3

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router bgp 65100
R3(config-router)#address-family ipv4 unicast vrf ADMINISTRATIVO-HVCA
R3(config-router-af)#neighbor 181.176.181.65 remote-as 65200
R3(config-router-af)#neighbor 181.176.181.65 activate
R3(config-router-af)#exit
R3(config-router)#exit
```

R3(config)#exit

*Feb 4 09:19:56.039: %SYS-5-CONFIG_I: Configured from console by console[OK]

R3#wr

Building configuration...

[OK]

R3#

R5

R5#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R5(config)#router bgp 65100

R5(config-router)#address-family ipv4 unicast vrf PAMPAS-E

R5(config-router-af)#neighbor 181.176.177.50 remote-as 65200

R5(config-router-af)#neighbor 181.176.177.50 activate

R5(config-router-af)#exit

R5(config-router)#address-family ipv4 unicast vrf PAMPAS-S

R5(config-router-af)#neighbor 181.176.177.46 remote-as 65200

R5(config-router-af)#neighbor 181.176.177.46 activate

R5(config-router-af)#exit

R5(config-router)#exit

R5(config)#exit

R5#

*Feb 4 09:11:32.239: %SYS-5-CONFIG_I: Configured from console by console

R5#wr

Building configuration...

[OK]

R5#

R6

```
R6#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R6(config)#router bgp 65100
R6(config-router)#address-family ipv4 unicast vrf LIRCAY
R6(config-router-af)#neighbor 181.176.177.30 remote-as 65200
R6(config-router-af)#neighbor 181.176.177.30 activate
R6(config-router-af)#exit
R6(config-router)#exit
R6(config)#exit
R6#wr
*Feb  4 09:06:21.883: %SYS-5-CONFIG_I: Configured from console by console
R6#wr
Building configuration...
[OK]
R6#
```

R8

```
R8#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R8(config)#router bgp 65100
R8(config-router)#address-family ipv4 unicast vrf ACOBAMBA
R8(config-router-af)#neighbor 181.176.177.21 remote-as 65200
R8(config-router-af)#neighbor 181.176.177.21 activate
R8(config-router-af)#exit
R8(config-router)#exit
R8(config)#exit
R8#w
```

*Feb 4 09:14:58.131: %SYS-5-CONFIG_I: Configured from console by console

R8#wr

Building configuration...

[OK]

R8#

EN LOS CLIENTES

R7

R7#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R7(config)#router bgp 65200

R7(config-router)#neighbor 181.176.181.66 remote-as 65100

*Feb 4 09:57:09.687: %BGP-5-ADJCHANGE: neighbor 181.176.181.66 Up

R7(config-router)#network 7.7.7.7 mask 255.255.255.255

R7(config-router)#neighbor 181.176.181.66 allowas-in

R7(config-router)#exit

R7(config)#exit

*Feb 4 09:57:51.259: %SYS-5-CONFIG_I: Configured from console by console

R7#wr

Building configuration...

[OK]

R7#

R9

R9#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R9(config)#router bgp 65200

R9(config-router)#neighbor 181.176.177.49 remote-as 65100

R9(config-router)#

*Feb 4 09:20:26.499: %BGP-5-ADJCHANGE: neighbor 181.176.177.49 Up

R9(config-router)#network 9.9.9.9 mask 255.255.255.255

R9(config-router)#neighbor 181.176.177.49 allowas-in

R9(config-router)#exit

R9(config)#exit

R9#

*Feb 4 09:21:24.191: %SYS-5-CONFIG_I: Configured from console by console

R9#wr

Building configuration...

[OK]

R9#

R10

R10#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R10(config)#router bgp 65200

R10(config-router)#neighbor 181.176.177.45 remote-as 65100

*Feb 4 09:16:23.963: %BGP-5-ADJCHANGE: neighbor 181.176.177.45 Up

R10(config-router)#network 10.10.10.10 mask 255.255.255.255

R10(config-router)#neighbor 181.176.177.45 allowas-in

R10(config-router)#exit

R10(config)#exit

*Feb 4 09:19:00.739: %SYS-5-CONFIG_I: Configured from console by console

R10#wr

Building configuration...

[OK]

R10#

R11

```
R11#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R11(config)#router bgp 65200
R11(config-router)#neighbor 181.176.177.29 remote-as 65100
*Feb  4 09:14:19.347: %BGP-5-ADJCHANGE: neighbor 181.176.177.29 Up
R11(config-router)#network 11.11.11.11 mask 255.255.255.255
R11(config-router)#neighbor 181.176.177.29 allowas-in
R11(config-router)#exit
R11(config)#exit
*Feb  4 09:16:04.463: %SYS-5-CONFIG_I: Configured from console by console
R11#wr
Building configuration...
[OK]
R11#
```

R13

```
R13#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R13(config)#router bgp 65200
R13(config-router)#neighbor 181.176.177.22 remote-as 65100
R13(config-router)#network
*Feb  4 09:12:45.219: %BGP-5-ADJCHANGE: neighbor 181.176.177.22 Up
R13(config-router)#network 13.13.13.13 mask 255.255.255.255
R13(config-router)#neighbor 181.176.177.22 allowas-in
R13(config-router)#exit
R13(config)#exit
R13#wr
```

*Feb 4 09:16:41.139: %SYS-5-CONFIG_I: Configured from console by console

R13#wr

Building configuration...

[OK]

R13#

PRUEBA DE VERIFICACIÓN DE LA CONFIGURACIÓN

R7#ping 13.13.13.13 source loopback 0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 13.13.13.13, timeout is 2 seconds:

Packet sent with a source address of 7.7.7.7

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 80/125/156 ms

R7#

R7#ping 9.9.9.9 source loopback 0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 9.9.9.9, timeout is 2 seconds:

Packet sent with a source address of 7.7.7.7

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 112/122/140 ms

R7#

R7#ping 10.10.10.10 source loopback 0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:

Packet sent with a source address of 7.7.7.7

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 92/116/156 ms

R7#

R7#ping 11.11.11.11 source loopback 0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 11.11.11.11, timeout is 2 seconds:

Packet sent with a source address of 7.7.7.7

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 60/128/156 ms

R7#

PRUEBA DE TRACEROUTE

R7#trace 13.13.13.13 source loopback 0

Type escape sequence to abort.

Tracing the route to 13.13.13.13

1 181.176.181.66 64 msec 80 msec 80 msec

2 181.176.177.18 120 msec 76 msec 92 msec

3 181.176.177.22 92 msec 128 msec 128 msec

4 181.176.177.21 172 msec 128 msec 156 msec

R7#

R7#trace 9.9.9.9 source loopback 0

Type escape sequence to abort.

Tracing the route to 9.9.9.9

1 181.176.181.66 44 msec 12 msec 48 msec

2 181.176.177.2 80 msec 108 msec 108 msec

3 181.176.177.49 108 msec 136 msec 76 msec

4 181.176.177.50 140 msec 196 msec 148 msec

R7#

R7#trace 10.10.10.10 source loopback 0

Type escape sequence to abort.

Tracing the route to 10.10.10.10

1 181.176.181.66 40 msec 64 msec 32 msec

2 181.176.177.2 140 msec 124 msec 124 msec

3 181.176.177.45 124 msec 92 msec 92 msec

4 181.176.177.46 140 msec 124 msec 132 msec

R7#

R7#trace 11.11.11.11 source loopback 0

Type escape sequence to abort.

Tracing the route to 11.11.11.11

1 181.176.181.66 40 msec 80 msec 80 msec

2 181.176.177.13 124 msec 148 msec 136 msec

3 181.176.177.29 104 msec 80 msec 140 msec

4 181.176.177.30 156 msec 120 msec 204 msec

R7#