UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE TELECOMUNICACIONES

TEMA:

Diseño y emulación de una red IP/MPLS para interconectar las facultades de la UCSG con el centro de cómputo y rectorado como site alterno

AUTOR:

Cortés Hincapié, Marco Joel

Trabajo de Titulación previo a la obtención del título de

INGENIERO EN TELECOMUNICACIONES

TUTOR:

Ing. Suárez Murillo, Efraín Oswaldo

Guayaquil, Ecuador

10 de Marzo del 2021

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE TELECOMUNICACIONES

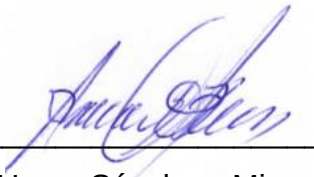
CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Sr. **Cortés Hincapié, Marco Joel** como requerimiento para la obtención del título de **INGENIERO EN TELECOMUNICACIONES**.

TUTOR

Ing. Suárez Murillo, Efraín Oswaldo

DIRECTOR DE CARRERA



M. Sc. Heras Sánchez, Miguel Armando

Guayaquil, a los 10 días del mes de marzo del año 2021

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Cortés Hincapié, Marco Joel**

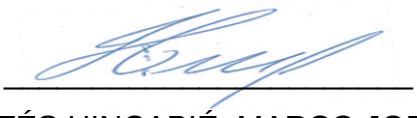
DECLARÓ QUE:

El trabajo de titulación **"Diseño y emulación de una red IP/MPLS para interconectar las facultades de la UCSG con el centro de cómputo y rectorado como site alterno"** previo a la obtención del Título de **Ingeniero en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 10 días del mes de marzo del año 2021

EL AUTOR



CORTÉS HINCAPIÉ, MARCO JOEL

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE TELECOMUNICACIONES

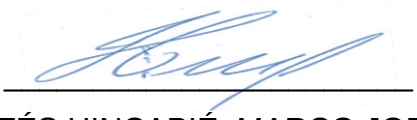
AUTORIZACIÓN

Yo, **Cortés Hincapié, Marco Joel**

Autorizó a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación: **"Diseño y emulación de una red IP/MPLS para interconectar las facultades de la UCSG con el centro de cómputo y rectorado como site alterno"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

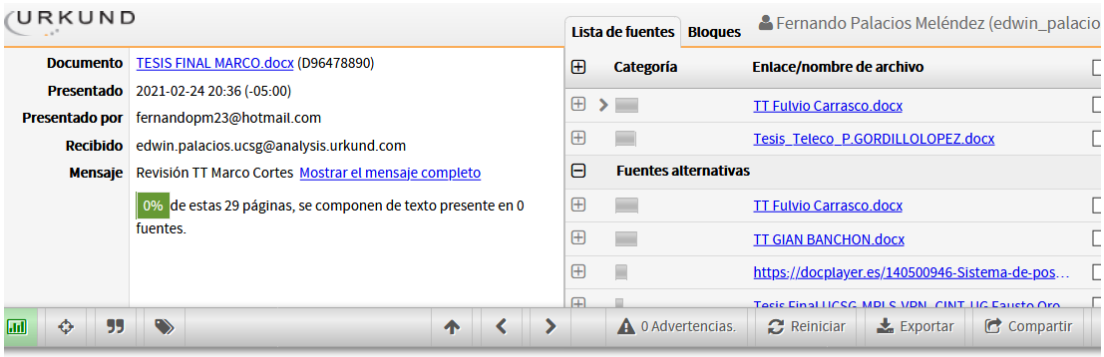
Guayaquil, a los 10 días del mes de marzo del año 2021

EL AUTOR



CORTÉS HINCAPIÉ, MARCO JOEL

REPORTE DE URKUND



UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA: Diseño y emulación de una red IP/MPLS para interconectar las facultades de la UCSG con el centro de cómputo y rectorado como site alterno

AUTOR: Cortés Hincapié, Marco Joel

Trabajo de Titulación previo a la obtención del título de INGENIERO EN TELECOMUNICACIONES

TUTOR: Ing. Suárez Murillo, Efraín Oswaldo

Guayaquil, Ecuador

20 de Febrero del 2021

UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO CARRERA DE INGENIERÍA EN

TUTOR

Ing. Suárez Murillo, Efraín Oswaldo

DEDICATORIA

Este trabajo está dedicado a:

A mis padres Marco e Inés quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de sacrificio y valentía, de no temer a las adversidades porque Dios está conmigo en todo momento.

A mis hermanos Anya y Yanni por su cariño y apoyo incondicional durante todo este proceso, por estar conmigo en cada momento, gracias. A toda mi familia porque con sus oraciones, consejos y palabras de aliento hicieron de mí una mejor persona y de una u otra manera me acompañan en todos mis sueños y metas.

EL AUTOR

CORTÉS HINCAPIÉ, MARCO JOEL

AGRADECIMIENTO

A Dios por ser la luz incondicional que ha guiado mi camino.

A la Universidad Católica de Santiago de Guayaquil por ser la sede de todo el conocimiento adquirido estos años.

A mis catedráticos, en especial al Ing. Efraín Suárez, asesor de tesis, quien estuvo guiándome académicamente con su experiencia y profesionalismo.

Al Ing. Raúl Suárez por bridarme sus conocimientos sobre Networking, que fue un motivo por la cual decidí hacer mi proyecto de tesis.

A todos mis amigos y futuros colegas que e ayudaron de una manera desinteresada, gracias infinitas por toda su ayuda y buena voluntad.

EL AUTOR

CORTÉS HINCAPIÉ, MARCO JOEL

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

M. Sc. ROMERO PAZ, MANUEL DE JESUS

DECANO

f. _____

M. Sc. PALACIOS MELÉNDEZ, EDWIN FERNANDO

COORDINADOR DEL ÁREA

f. _____

M. Sc. PHILCO ASQUI, LUIS ORLANDO

OPONENTE

Índice General

Índice de Figuras

Capítulo 2

Capítulo 3

Índice de Tablas

Capítulo 2

Resumen

Para el desarrollo de la presente optimización de red, se optó por la tecnología MPLS L3VPN muy utilizada para ambientes, en el cual, se requiere optimizar la conmutación de paquetes y aislar el tráfico entre diferentes tipos de fuentes como datos, telefonía y vídeo. Lo que permite que MPLS se ajuste a las redes modernas es el uso de etiquetas para la conmutación del tráfico y uso en conjunto de MP – BGP para garantizar que no exista superposición en los prefijos que se transportan dentro de una red. La potencia que aporta MPLS no es eficaz sino se trabaja con una pila de protocolos como OSPF, BGP, MP – BGP. Se emuló una red prototipo campus universitario para demostrar la eficacia que MPLS y su pila de protocolos aportan para brindar alta disponibilidad a nivel WAN y en incrementar la disponibilidad de los servicios en el datacenter de la UCSG hacia las facultades.

Palabras claves: MPLS, NETWORK, ROUTING, OSPF, GNS3, HSRP

Capítulo 1: Descripción General del Trabajo de Titulación

1.1. Introducción.

Hoy en día las redes de datos se enfrentan a un reto que es garantizar la continuidad de los servicios y el tratamiento de la diversidad de tráficos que fluyen a través de una red, por ende, se vuelve indispensable implementar un protocolo que garantice el aislamiento de los diferentes tipos de tráficos e incrementar el nivel de disponibilidad en la red.

Los protocolos tradicionales de capa 3 no cumplen con los niveles que exigen las redes modernas por la velocidad en la conmutación de paquetes entre los routers de la red, por lo cual, las redes requieren trabajar con un protocolo que sea veloz como MPLS el cual trabaja en la capa 2.5 del modelo OSI, este protocolo realiza la conmutación del tráfico basado en etiquetas y no en la información que contiene dentro del paquete IP. Esto logra incrementar la velocidad en la transmisión ya que, no tiene que estar encapsulando o desencapsulando los paquetes IP, sino que solo extrae etiquetas o labels y los conmuta hacia el router destino.

Una red de campus universitaria dispone de un centro de datos el cual provee de servicios internos a las facultades, dicho tráfico transporta consultas hacia bases de datos desde las facultades hacia el datacenter, igualmente tráfico telefónico hacia centrales IP y salida de Internet seguro mediante un firewall centralizado, por ende, se debe implementar un protocolo a nivel WAN y LAN de alta disponibilidad como MPLS y HSRP para en conjunto incrementar la disponibilidad de los recursos lógicos en la red,

1.2. Antecedentes.

Las redes de campus universitarios requieren cumplir con un nivel de SLA muy elevado ya que, se debe garantizar el nivel de disponibilidad de acceso a servicios centralizados desde el centro de datos, por lo cual, se enfrenta a un reto que es incrementar las conexiones a través de un protocolo que pueda reconverger sin presentar problemas como latencia, jitter, packet loss, etc.

Las conexiones actuales carecen de un protocolo a nivel de transporte que en conjunto con un protocolo FHRP incrementan el nivel de disponibilidad de los recursos hacia el centro de datos. Por ende, el presente estudio logrará mitigar las falencias de una red plana.

1.3. Definición del Problema.

La Universidad Católica de Santiago de Guayaquil dispone de un Centro de Computo el cual aloja servidores de base de datos y aplicativos para almacenar y visualizar la información académica y administrativa de las facultades de la UCSG, dicho centro de cómputo no cuenta con un esquema de alta disponibilidad a nivel de conectividad de datos para la réplica o backup de la información en caso de una perdida de conexión parcial o total.

Al existir un único punto de conexión central (Hub and Spokes), el nivel de disponibilidad para acceso a servicios centralizado desde las facultades se decrementa, por lo cual es necesario diseñar un mecanismo para incrementar el nivel de disponibilidad hacia los recursos centralizados.

Las Facultades de la UCSG deben consultar y enviar información frecuentemente a la base de datos alojado en el Centro de Computo a través de conexiones de datos internas por fibra óptica, dichas conexiones suelen ser a nivel de capa 2 o capa 3 dependiendo del arquitecto de red, sin embargo dichas conexiones no siempre suelen ser óptimas para brindar rutas de respaldo hacia un punto central, lo cual impacta drásticamente en la disponibilidad de los servicios y aplicativos que se desean consultar.

Una arquitectura de red que disponga de 2 puntos centrales (Centro de cómputo y Rectorado), que trabaje con un protocolo en la capa 2.5 (MPLS) el cual brinda una conmutación veloz y utilice conexiones de fibra óptica redundantes con un protocolo FHRP incrementara el nivel de disponibilidad a un 99.9% lo cual nos garantizará que solo 4.3 horas al año existirá desconexión desde las Facultades hacia el centro de cómputo.

1.4. Justificación del Problema.

Las facultades del campus de la UCSG realizan consultas a bases de datos y direccionan tráfico hacia diferentes servicios localizados en el centro de datos, por lo cual, resulta indispensable diseñar un esquema de alta disponibilidad a través de protocolos WAN y LAN que garanticen la continuidad del servicio hacia el centro de datos.

Las conexiones entre el datacenter y las facultades deben tener doble redundancia a nivel de enlaces físicos en una arquitectura Hub and Spokes con dos Hubs a fin de incrementar el nivel de disponibilidad en las conexiones WAN. Las conexiones tipo lineal desde una facultad hacia un datacenter están propensas a sufrir algún daño físico en la red, por lo que, en el diseño se debe mallar la red hacia dos sitios con un protocolo MPLS a nivel WAN y HSRP a nivel LAN para que el centro de cómputo sea el site principal y en caso de una desconexión o desastre se disponga de un site secundario el cual reconverja con el tráfico para todas las facultades.

1.5. Objetivos del Problema de Investigación.

1.5.1. Objetivo General.

Diseñar y emular una red IP/MPLS para brindar alta disponibilidad y eficiencia para el transporte de tráfico de voz y datos entre las facultades de la Universidad Católica de Santiago de Guayaquil y el Centro de Cómputo con site alterno Rectorado.

1.5.2. Objetivos Específicos.

- Diseñar una solución para ofrecer alta disponibilidad en el transporte de tráfico de voz y datos que fluye entre las facultades de la UCSG y Centro de Cómputo.
- Emular una red IP/MPLS en base al diseño propuesto para optimizar el tráfico de voz y datos entre las facultades y centro de cómputo.
- Aplicar técnicas y protocolos de alta disponibilidad que permitan tener un esquema de redundancia física y lógica entre las facultades y el centro de cómputo.

- Estudiar los protocolos de enrutamientos dinámicos y de etiquetas que se implementarán en el diseño propuesto.

1.6. Hipótesis.

El diseño y emulación de una red de alta disponibilidad a través de una arquitectura MPLS permitirá tener una visión más clara para garantizar la continuidad de los servicios hacia el centro de datos de la UCSG.

1.7. Metodología de Investigación.

Las metodologías que se implementaron en el trabajo de titulación fueron las siguientes:

El proyecto es investigativo y explicativo ya que, consiste en indagar sobre la manera de cómo funcionan los distintos tipos de protocolos, además, de la importancia ventajas y desventajas y, la definición de cada uno de ellos.

También es demostrativo porque se empleará un emulador, llamado GNS3, que nos brindará la facilidad de observar cómo interactúan los protocolos sobre una red IP/MPLS para su correcto funcionamiento.

Capítulo 2: Fundamentación Teórica

2.1. Introducción de las redes MPLS.

Actualmente, los consumidores de telecomunicaciones son rigurosos y apegado a modificar de distribuidor de servicios. El mercado de las telecomunicaciones estimula a los oponentes a dar opciones a los consumidores. La gloria de los operarios de telecomunicaciones depende totalmente de la amplitud del operador para crear nuevos servicios apoyándose en las exigencias del usuario y para obtener una máxima calidad de servicio y experiencia. (Ramadaa et al., 2015)

MPLS (Multiprotocol Label Switching) se ha fundado como la tecnología de transporte autoritario de elección en las redes centrales cimentada en paquetes. La tecnología MPLS ha posibilitado el aumento de una cadena de mecanismos a través los cuales se puede incrementar el nivel de disponibilidad, fiabilidad y optimización de la red. El Multiprotocol Label Switching también se emplea para la ingeniería de tráfico para examinar el control de flujos de información mediante una red, optimizando así el manejo de recursos y la rentabilidad de la red. (Ramadaa et al., 2015)

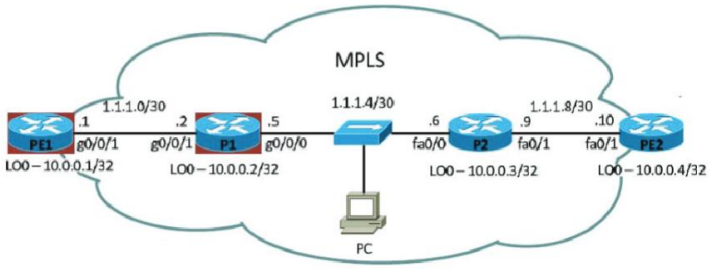


Figura 2. 1: Topología de red usando tecnología MPLS.
Fuente: (Hlozak et al., 2014)

En la red central del distribuidor de servicios, LDP (Label Distribution Protocol) repartirá las etiquetas entre los enrutadores que cada etiqueta está agregado con la dirección IP del próximo salto y el primer enrutador detallará y mostrará el camino a seguir. Absolutamente cada uno de los paquetes que entrarán a la red MPLS reciben una etiqueta según su función, ese enrutador reenvía la procedencia del paquete en la etiqueta de entrada. (Mehraban et al., 2018)

2.2. Tecnología MPLS.

MPLS es un protocolo que se utiliza para aligerar y distribuir el flujo de tráfico de red sobre las redes troncales. MPLS adquirió su nombre porque funciona con IP (Protocolo de Internet), ATM (Modo de transporte asíncrono) y con los protocolos de red de retransmisión de tramas. La palabra multiprotocolo denota a que se aceptan diversos protocolos de la capa 3, p. ej: IPv4, IPv6, IPX. Además, protocolos de capa 2, p. ej: Ethernet, HDLC, Frame-Relay y ATM. (Hlozak et al., 2014)

MPLS consta de un circuito que se denomina ruta de etiqueta conmutada (LSP) que enlaza los nodos conocidos como enrutador de etiqueta conmutada (LSR). Cada LSP está ligado con un tipo de equivalencia de reenvío, conocido como FEC, que es un conjunto de paquetes en un enrutador de etiqueta conmutada. La equivalencia de reenvío (FEC) se describe con la etiqueta de instalación. (Soewito et al., 2017)

La ingeniería de tráfico MPLS tiene como finalidad el envío de paquetes entre dos puntos, denominados origen y destino. El funcionamiento de los protocolos de encaminamiento es hallar el camino más corto para transferir la información. (Imran et al., 2018)

2.2.1. Características MPLS

MPLS tiene las siguientes características, p.ej: posee un mejor rendimiento en transmisión, es fundamental en los proveedores de servicios, tienen mejoras en los protocolos en lo que es el trazado de paquetes y que el flujo de la red sea más ágil y eficiente, posee direccionamiento que está apoyado en limitaciones, tiene la capacidad de adaptarse automáticamente y de manera fácil si existe una falla a nivel de nodos o servidores, se ejecuta entre la capa 2 (enlace físico) y nivel 3 (datos). (Imran et al., 2018)

2.2.2. Enrutadores de conmutación de etiquetas

Los Providers End (PE), también llamados como enrutadores de entrada y salida. Además, los PE son dominados enrutadores de borde de etiquetas o en inglés, Label Edge Routers (LER). (Fathima, 2018)

Los enrutadores de conmutación de etiquetas (LSR) son llamados así, debido a que, los enrutadores subsiguientes en la ruta realizan la función de conmutación de etiquetas. (Fathima, 2018)

Los routers de entrada da una etiqueta para los paquetes, por lo que, cogen el camino de las etiquetas del protocolo MPLS que se les fue asignado. Y el router de salida se encarga de retirar dicha etiqueta previamente asignada y redirige el paquete hacia el destinatario final. (Fathima, 2018)

Una vez que los enrutadores de conmutación de etiquetas (LSR) acogen un paquete, puede ejecutar una o varias de las siguientes acciones. (Fathima, 2018)

- Empuje o push: Normalmente, esta acción lo ejecuta el router de entrada y, se encarga de añadir etiquetas.
- Intercambio o swap: Los ejecutan los LSRs, entre los routers de entrada y salida. Su función en la de intercambiar etiquetas.
- Remover o pop: Remueve etiquetas, con frecuencia está función es realizada por el router de salida.

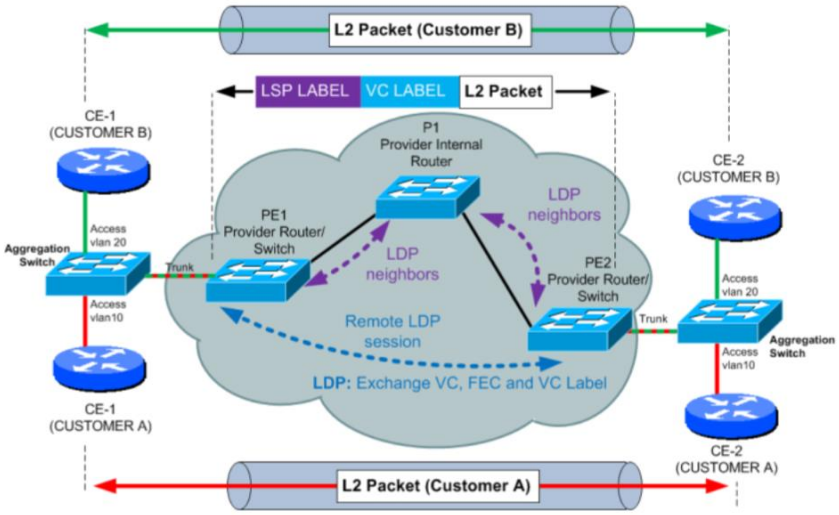


Figura 2. 2: Diagrama de una red usando protocolo MPLS con VPN.
Fuente: (Fathima, 2018)

2.3. Routing

Se le conoce como routing al procedimiento del reenvío de paquetes de datos que va desde la red origen hasta el destino, este proceso es ejecutado

por enrutadores conforme con la información que se halla en el router, tal como la tabla de direccionamiento. La tabla de encaminamiento es una herramienta para coger decisiones en el direccionamiento de paquetes de información que viene del enrutador. (Soewito et al., 2017)

2.4. Emulador GNS3

El software GNS3 (Grapical Network Simulator), es un emulador de origen Cisco y posee una gran variedad de ventajas a comparación de otros programas de emulación de red. (Liu et al., 2019)

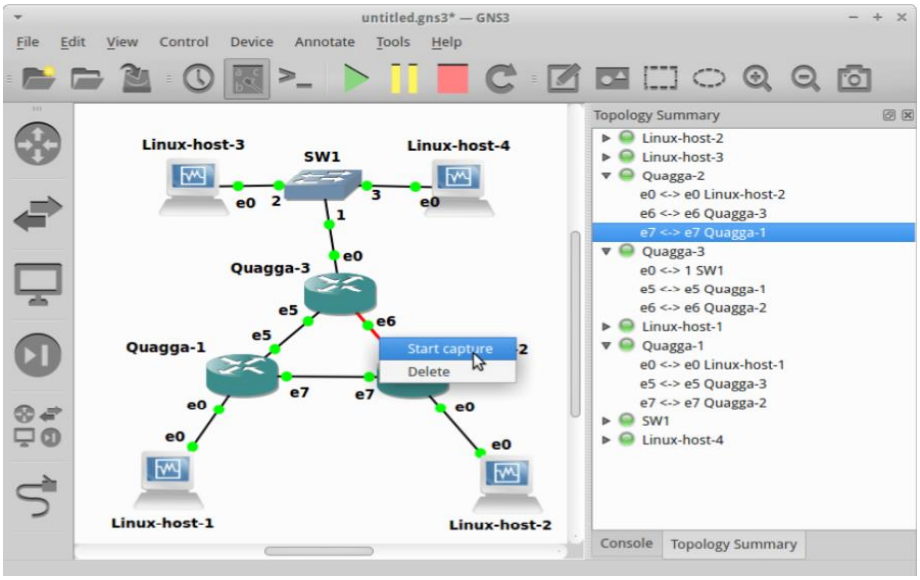


Figura 2. 3: Programa de emulación GNS3.
Fuente: (Imran et al., 2018)

2.4.1. Ventajas del emulador GNS3.

- El emulador GNS3 puede acoger mayor número de comandos y parámetros. El software Grapical Network Simulator efectúa de manera directa el IOS de los equipos Cisco disponibles de red. (Liu et al., 2019)
- Se vincula con dispositivos reales: Es decir, con cualquier dispositivo se puede enlazar el GNS3 en la red real. P. ej: routers, PC's, conmutador, entre otros dispositivos., mediante la interfaz de la tarjeta de la red. (Liu et al., 2019)
- Se puede permitir un gran número de equipos de red en el GNS3. Además, el emulador ofrece IDS (Intrusion Detection Systems)

firewalls como PIX y ASA, conmutadores de retransmisión de tramas, incluyendo el equipo de red básico. (Liu et al., 2019)

2.4.2. Desventaja del emulador GNS3

- Requiere de mucha memoria: Porque al tener demasiados equipos y sistemas de redes virtuales simulando en una computadora, eso hará que la computadora no sea efectiva en su totalidad. (Liu et al., 2019)

2.5. Open Shortest Path First (OSPF)

Según (Robbins, 2018), el OSPF pertenece al conjunto de protocolos IGPs (Interior Gateway Protocols) aplicados más veces en los sistemas independientes de Internet. Puesto que, OSPF es la finalidad de los consumidores malignos ya que, la inseguridad de adulteración de LSA (Link State Advertisement) para los OSPFs es la debilidad más alta y aplica el riesgo de denegación de servicio (DoS) en los sistemas de red OSPF.

El Open Shortest Path First es uno de los protocolos de direccionamiento de estado de enlace, por lo tanto, algunos routers que trabajan con OSPF poseen un panorama más específico y preciso sobre todos los links de direccionamiento de un sistema OSPF. (Robbins, 2018)

Ya que, para esto, los routers OSPF ocupan las informaciones para calcular los caminos posibles para enviar los datos, por tal motivo las ejecuciones del protocolo Open Shortest Path First poseen un inmenso campo de agresiones que ocasionan la intoxicación de las rutas y por ende, sus infiltraciones malignas tienen efectos positivos ante la usurpación del Link State Advertisement (LSA). (Robbins, 2018)

2.6. Protocolo de Puerta de enlace Fronteriza (BGP)

Se encarga del sostenimiento de la información que se va actualizando en los routers en los caminos que se ha elegido a diferentes prefijos de encaminamiento seleccionado. (Fonseca et al., 2019)

Durante su normal funcionamiento, el protocolo BGP era usado solamente por Ases y conmutar las informaciones que equivalía a palpables modificaciones tanto en la base entre los dominios y las políticas del administrador de la red en la parte de las aplicaciones. Entonces, si están de manera equitativa ambas partes, la cantidad del tráfico del Border Gateway Protocol será bajo. Pero, los estudios que se hicieron sobre la manera de actuar del protocolo BGP demostraron que el tráfico de este protocolo posee demasiada dinámica, mal comportamiento bajo ciertas condiciones y desequilibrio. (Fonseca et al., 2019)

El mal funcionamiento del protocolo a gran escala se debe a las actualizaciones múltiples del BGP que dan lugar a una significativa desorientación de la repartición dinámica que maneja BGP normalmente, esto tiene repercusiones en diversos Ases en un lapso de tiempo, por la cual, después el BGP regresa a su estado inicial con normalidad. (Fonseca et al., 2019)

Las irregularidades del protocolo de enlace de puerta fronteriza tienen cuatro clases que son: fallas indirectas, fallas de red, fallas con intención directa y fallas sin intención directa. (Fonseca et al., 2019)

2.6.1. Falla de red

La conformación de la Internet por diversos tipos de equipos y entidades de red, por ejemplo: routers, ASes, operadores, etc. Estos equipos y entidades poseen un porcentaje a fallar, por ende, tener un impacto negativo sobre la Internet. (Fonseca et al., 2019)

2.6.2. Fallas indirectas

La falla indirecta más frecuente que se presente en el BGP, son los accesos sin permisos que representan una gran cantidad de tráfico y resultan en el embotellamiento y ausencia de contestación rápida del encaminador AS. Esto puede provocar la agitación en las rutas si los mensajes de KEEPALIVE no son respondidos en un lapso corto de tiempo. (Fonseca et al., 2019)

2.6.3. Falla de intención directa

Los más frecuentes a las irregularidades a las fallas de intención directa son las agresiones de rapto del protocolo BGP que se produce en el momento cuando un agresor asegura en tener ya sea un prefijo o sub-fijo que es correspondida a otro AS para cambiar la ruta desde el AS hasta al agresor. Con la finalidad de que el tráfico sea cortado hacia el AS que está siendo atacado. (Fonseca et al., 2019)

2.6.4. Falla sin intención directa

Dado a las formas erróneas que se produce a nivel de la configuración del BGP, los routers tienen la probabilidad de dar aviso ya sea, prefijos o sub-fijos malignos ya que, los AS autorizados ya están siendo divulgados al mismo o por la razón de que son privados y/o no se los emplean. Aunque dichas irregularidades pueden ser transitorio debido a que todas las partes, que van desde el comienzo AS y los pares perjudicados, están empeñadas en contar las irregularidades de manera rápida. (Fonseca et al., 2019)

2.7. Características de BGP

En el Border Gateway Protocol los mensajes del plano de control son los que se realizan con más frecuencia en la detección de irregularidades. El alto nivel de detalle, la granularidad fina temporal y la disponibilidad que va desde varias perspectivas mediante la Internet. (Fonseca et al., 2019)

Según (Fonseca et al., 2019), los mensajes del protocolo BGP simbolizan solamente modificaciones incrementales, aunque esto no proporcione información que no sean ni de estados pesados ni de alteraciones de proceder que exceda de los diferentes sistemas autónomos. Y para disponer de importante información de los mensajes de control plano hay que utilizar y ejecutar un proceso de extracción de peculiaridad del BGP y actualizaciones de este.

2.8. Clasificación de las características de extracción de BGP

Según (Fonseca et al., 2019), por lo general, casi todos los Border Gateway Protocol, las resoluciones de la detección de irregularidades

obtienen singularidades como las series de tiempo y examinan los tipos de desviación y dan señal si existe o no una conducta irregular.

2.8.1. Características de volumen

Como muestra en la Figura 2.8., en el BGP, la clasificación en las actualizaciones de mensajes es de la siguiente manera:

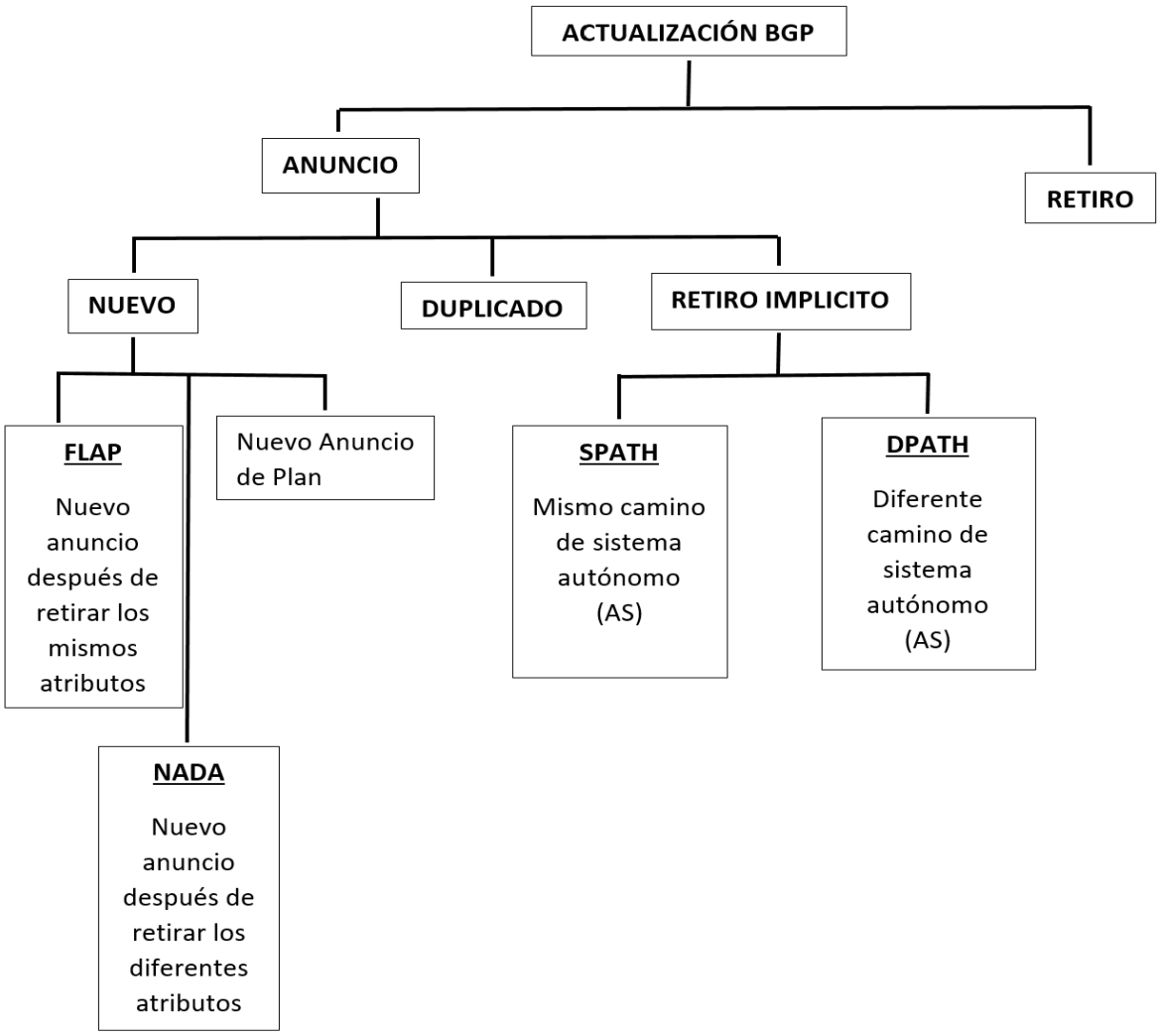


Figura 2. 4: Clasificación de los diferentes mensajes BGP
Fuente: (Fonseca et al., 2019)

2.8.2. Multiprotocolo de Puerta de enlace Fronteriza (MP-BGP)

El MP-BGP proviene del protocolo BGP, es decir, si el usuario logra una conexión de red con dos proveedores de servicios de Internet (ISP), significa que es un usuario de doble hogar. Además, el MP-BGP se lo efectúa entre el borde del proveedor (PE, Provider Edge) de dos ASes (Autonomous Systems). Su función es la de intercambiar rutas de las redes privadas

virtuales (VPNv4), entre los proveedores de servicios de Internet (ISP) con características de comunidad de envío. (Fathima, 2018)

2.8.3. Calidad de Servicio (QoS)

Las pérdidas de paquetes, demora, variaciones, desempeño y la latencia son indicadores del QoS que pueden mejorar con el MP-BGP. (Fathima, 2018)

El Acuerdo de Nivel de Servicio (SLA, sus siglas en inglés) tiene por objetivo, identificar el pacto entre el proveedor de servicio de Internet y el usuario. Esto quiere decir que, cuando el usuario solicita el mayor rendimiento de tiempo de actividad, pero sin pérdidas en los paquetes, el MP-BGP interviene para que dicha petición se cumpla, la cual, a veces en el mapa de ruta se usa un tráfico personalizado desde el origen hasta el destinatario final. (Fathima, 2018)

Determinados paquetes se los distinguen con un seguimiento y resaltándolos. Si hay una congestión de tráfico y red, la dirección IP tiene que anteponer el tráfico que identificó. (Fathima, 2018)

2.9. Virtual Local Area Network (VLAN)

Según (Haiyan, 2018), la Virtual Local Area Network, la principal función de las VLAN es implementar dominios de broadcast lógicos que permitan la comunicación entre cualquier cliente en la misma red de área local virtual, sin intervenir la infraestructura física de la red. Antiguamente para poder definir un dominio de broadcast se debían utilizar enrutadores, lo que resultaba muy costoso.

La red de área local virtual, sus siglas en inglés (VLAN), de manera lógica es un mecanismo, que no tendrá prohibiciones por su localización de forma física, por lo contrario, logrará adecuarse en relación con los factores que son como departamento, rol y aplicación. (Haiyan, 2018)

Tabla 2. 1: Tipos de diseños de una VLAN.

VLAN ID	VLAN NAME	SUBNET	IP INTERFACE
1	DEV – Manage	172.20.1.0/24	172.20.1.1
5	WAP – Manage	172.20.5.0/24	172.20.5.1
L3	NET – Gateway	172.20.10.0/24	172.20.10.1
12	SKRU - 802.1X	172.20.12.0/24	172.20.12.1
16	SKRU – WiFi	172.20.16.0/24	172.20.16.1
20	Eduroam	172.20.20.0/24	172.20.20.1
21	Admin-Build-F1	172.20.21.0/24	172.20.21.1
22	Admin-Build-F2	172.20.22.0/24	172.20.22.1
23	Admin-Build-F3	172.20.23.0/24	172.20.23.1
24	Library	172.20.24.0/24	172.20.24.1
31	Versatile – Building	172.20.31.0/24	172.20.31.1
41	Hotel – Building	172.20.41.0/24	172.20.41.1
51	Hostal – Building	172.20.51.0/24	172.20.51.1
61	VoIP	172.20.61.0/24	172.20.61.1
71	CCTV	172.20.71.0/24	172.20.71.1
100	ServerFarm	172.20.100.0/24	172.20.100.1

Fuente: (Tongkaw & Tongkaw, 2018)

2.9.1. Lista de acceso de LAN virtual

Son conocidas como VLAN Access List (VACL) que funcionan como pequeños filtradores, las cuales se dedican a la parte de los conmutadores a nivel de red o capa 3 y, esto ocasionaría un fallo en la configuración de cómo se estén dirigiendo los paquetes de datos en la red de área local virtual, como se muestra en la siguiente figura. (Lehocine & Batouche, 2017)

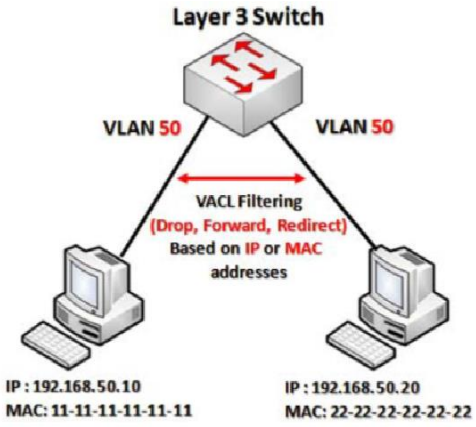


Figura 2. 5: Esquema de la VACL
Fuente: (Lehocine & Batouche, 2017)

Tiene como función excluir paquetes concurrentes, enviarlo y dirigirlo nuevamente a una interfaz distinta a la que se está utilizando. La lista de acceso de una LAN virtual se modela como un tipo de mapa de acceso de las redes de área local virtual que se caracterizan con un sin número de entradas que portan una mezcla de cláusulas y comandos de acción. (Lehocine & Batouche, 2017)

Las estipulaciones de concurrencia, que permiten la detección del tráfico que se va a filtrar, son operadas con apoyo de las listas de accesos IP o MAC. (Lehocine & Batouche, 2017)

2.9.2. Red de Área Local Virtual Privada

Las VLAN privadas son empleadas para la segmentación una VLAN a varias porciones aisladas, a través de la construcción lógica de VLAN's anexada dentro de otra VLAN. (Lehocine & Batouche, 2017)

Los conceptos son utilizados en el contexto de coubicación NSP, debido a que muchos usuarios se comparten y se comunican a la misma subred IP. Esto da una mejoría a la dirección y dialogo de los espacios de direcciones IP, garantizando totalmente el aislamiento entre ellos. Además, las VLAN privadas también excluye servidores que se encuentran en una sola VLAN. (Lehocine & Batouche, 2017)

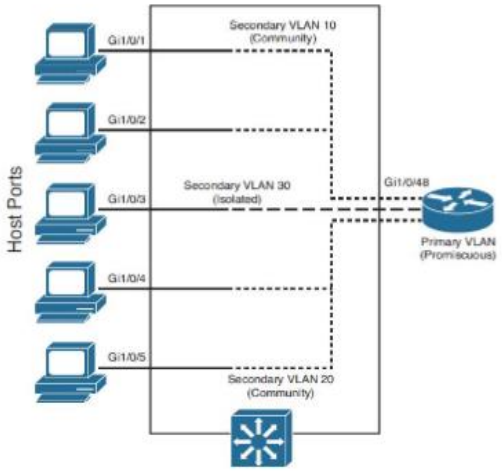


Figura 2. 6: Diagrama de una VLAN privada
Fuente: (Lehocine & Batouche, 2017)

2.10. Red Privada Virtual

La VPN es la tecnología que permite crear redes a través de redes públicas, pero de forma más segura y eficaz. (Tongkaw & Tongkaw, 2018)

En las redes privadas virtuales, las formas más comunes son: VPN de sitio a sitio y la VPN de acceso remoto. Ciertas redes privadas virtuales disponen de un acceso a nivel de los enlaces de datos a la red que fue destinada. Para esto, se necesita un protocolo de tunneling punto a punto o el protocolo de tunneling de la capa 2 que se realiza mediante una conexión base IPsec. (Tongkaw & Tongkaw, 2018)

Como ventaja, la VPN es económica y puede conectarse a un campus remoto de manera segura, una vez descifrado los datos a través del protocolo tunneling entre los destinatarios. (Tongkaw & Tongkaw, 2018)

Según (Tongkaw & Tongkaw, 2018), el protocolo más fiable para garantizar una conexión de redes es el IPsec. Además, IPsec es un protocolo de la red privada virtual más conveniente en la conectividad entre un campo principal y uno remoto.

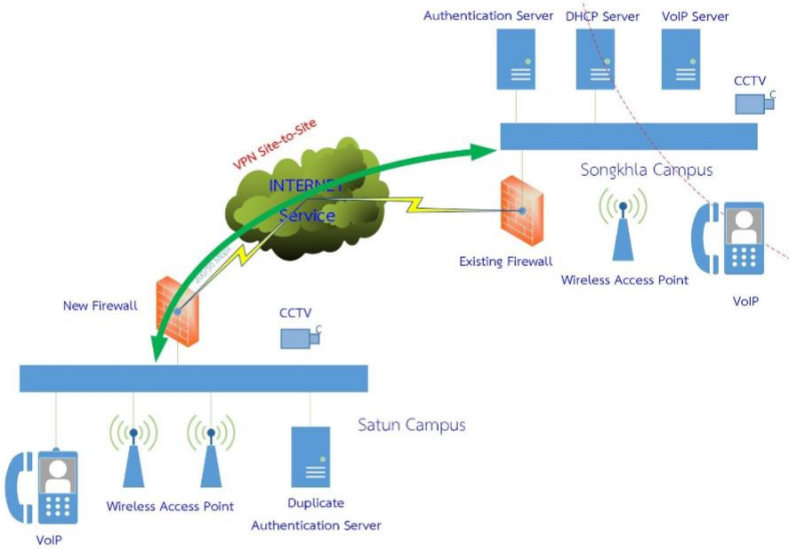


Figura 2. 7: Campo de la VPN
Fuente: (Tongkaw & Tongkaw, 2018)

2.11. Internet Protocol Security (IPsec)

Internet Protocol Security es una agrupación de protocolos que se usan principalmente para la protección y confidencialidad de la información, por ejemplo: autenticación, cifrado de información. Incluso, es considerado como la solución más ejecutada para las VPN. (Tongkaw & Tongkaw, 2018)

IPsec trabaja en la capa 3, es decir, en la capa de red. Su función es la elaboración y encriptación una nueva cabecera. En la parte de su configuración, el modelo algorítmico se lo usa para el cifrado y verificación de la autenticidad de la información que pasan por el protocolo de tunneling. (Tongkaw & Tongkaw, 2018)

Los hosts son los encargados de crear la VPN IPsec sin importar el dispositivo que se esté utilizando. Los hosts que pertenecen a la red de destino que se encuentran dentro de la red tiene la capacidad de utilizar las direcciones IP de dicha red para la conectividad con la red de destinatario. (Tongkaw & Tongkaw, 2018)

2.12. Servicios de tunelización y seguridad

La red privada virtual funciona únicamente en Internet, donde podrá simular el sistema de la Internet, siempre y cuando se considere pública. Los elementos más cruciales en la tecnología VPN está formada por los servicios de tunneling y de seguridad. (Tongkaw & Tongkaw, 2018)

2.12.1. Tunelización

Los túneles es lo esencial en lo que representa la tecnología VPN. Ya que, al momento en que se crea un túnel virtual, se va elaborando una conexión virtual en Internet de la VPN. Además, existen dos maneras de hacer la tunelización: extremo a extremo y nodo a nodo. (Tongkaw & Tongkaw, 2018)

2.12.2. Servicios de seguridad

La seguridad es la encargada del buen funcionamiento de la tecnología de la red privada virtual. En los sistemas de seguridad existen diversos

modelos como autenticidad, encriptación de la información y firewall. (Tongkaw & Tongkaw, 2018)

2.13. Tunelización de extremo a extremo

La forma de extremo a extremo es una operación de tunelización donde en ambos lados de una conexión VPN, los puntos finales son los encargados de administrar las conexiones de tunneling, codificación y descodificación de la información ya sea entrante o saliente entre dos tecnologías VPN. (Tongkaw & Tongkaw, 2018)

2.14. Tunelización de nodo a nodo

En este caso, el enrutador o router, gestiona la conectividad de la tecnología VPN de lado a lado. Además, para la tunelización de nodo a nodo, la elaboración y terminación de la misma integra el cifrado y descifrado. (Tongkaw & Tongkaw, 2018)

2.15. Encriptación o confidencialidad de la información

La encriptación de datos es un método que permite proteger la información ante una amenaza. La función que realiza la confidencialidad de datos es cifrar un código o llave para así enviar la información de manera segura y, una vez enviada la información, el dispositivo del destinatario tendrá que descifrar la información, para esto empleará una llave de descodificación que está ligada a la llave que se utilizó para encriptar los datos. (Tongkaw & Tongkaw, 2018)

Esto hace que sea muy difícil para los hackers plagiar la información ya que, no cuentan con las respectivas llaves para descodificar la información nueva a la información maestra. (Tongkaw & Tongkaw, 2018)

2.16. Muro de fuego

Los muros de fuego (Firewall) se encargan de la protección de la red de clientes no autorizados. Además, proporciona que el usuario o cliente obtenga un total acceso a los elementos de la red en la que está interactuando. (Tongkaw & Tongkaw, 2018)

Hoy en día, el firewall o control de acceso se clasifica en tres tipos de sistemas: Control de acceso de filtrado de paquetes, control de acceso de puerta de enlace de aplicaciones y control de acceso de inspección de estado. (Tongkaw & Tongkaw, 2018)

2.16.1. Firewall de filtrado de acceso

Los filtrados de acceso o de capa de red son los tipos de firewalls más frecuentes. Se trata cuando un cortafuego sin estado maneja cada trama o paquete de red por separado. (Krit & Haimoud, 2017)

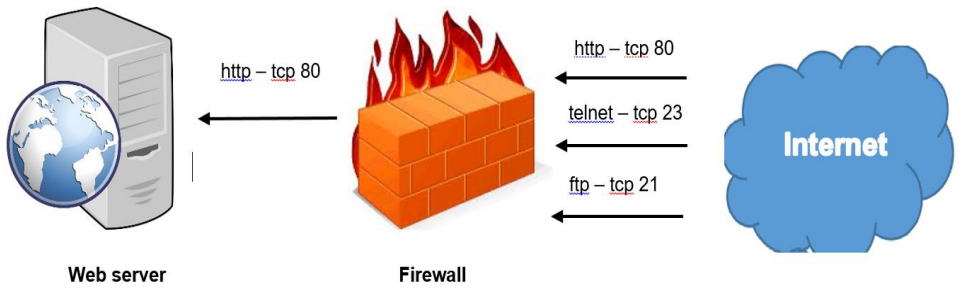


Figura 2. 8: Diseño de un servidor de Web protegido por un muro de fuego de tipo filtrado de acceso
Fuente: (Krit & Haimoud, 2017)

El firewall de filtrado de acceso tiene ventajas lo siguiente: una configuración sencilla, tiene transparencia para los usuarios y, es de muy alta velocidad. Sin embargo, también posee desventajas como, falta de legitimidad y, además de que, es sensible a diferentes tipos de ataques, por ej: Plagio de las direcciones IP, ataque DOS, ataques de fragmentos pequeños, entre otros. (Krit & Haimoud, 2017)

2.16.2. Puertas a nivel de circuitos

Se encarga del monitoreo del protocolo de control de transmisión (TCP) que está ubicado entre los hosts locales y remotos, la cual decide si la sesión que se está iniciando es legítima y, se establece como confiable sólo si el sistema remoto lo considera así. (Krit & Haimoud, 2017)

Aunque este tipo de firewall, no chequean los paquetes por sí mismos. Para la revisión de paquetes, se ejecutan procesos de seguridad al momento en que se realiza una conexión UDP o TCP. Una vez ejecutada la conexión, dichos paquetes circularán sin más verificación entre los hosts. (Krit & Haimoud, 2017)

2.16.3. Filtros con estado

Su función es la de mantener los registros de las conexiones que pasan a través de él. De esta manera, puede decidir si el paquete es el inicio de una conexión, parte de una conexión que ya existe o simplemente se trate de un paquete inválido. Para que el firewall pueda realizar esto, debe de tener una entrada para cada flujo que esté abierto y, cuando el firewall detecte el primer paquete de un flujo nuevo, éste procede a la comparación en los registros de las conexiones. (Krit & Haimoud, 2017)

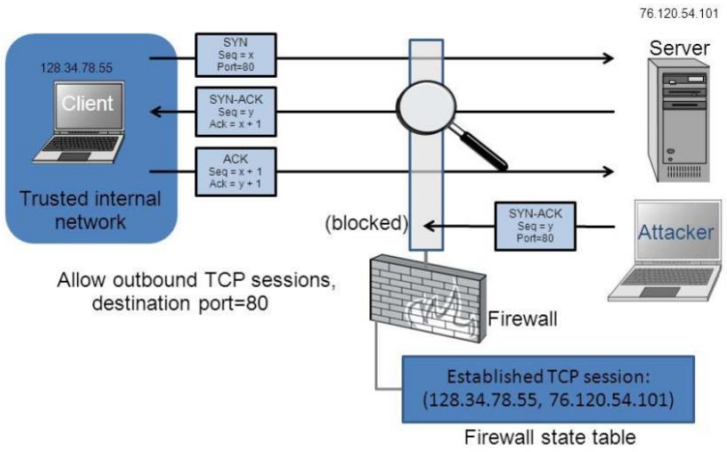


Figura 2. 9: Esquema de una red usando cortafuego con filtro de estado
Fuente: (Krit & Haimoud, 2017)

2.16.4. Firewall de capa o nivel de aplicación

El cortafuego de nivel de aplicación, también conocido como un cortafuego de proxy de aplicación, se refiere a un mecanismo de protección de red ya que, otorga seguridad a los recursos que se encuentran en la red a través del filtrado de mensajería en el nivel aplicación. (Krit & Haimoud, 2017)

El proxy de aplicación posee un funcionamiento más complejo que el firewall de filtrado de paquetes. De hecho, este firewall asimila el protocolo y

datos de la aplicación y obstruye información ya sea de cualquier índole que este destinada a la aplicación. (Krit & Haimoud, 2017)

El firewall de nivel de aplicación realiza el reconocimiento y validación de los usuarios ya que, juzga y decide si uno de los paquetes representa una amenaza. Aunque esto, puede conllevar a que los clientes tengan que reconfigurarlo más seguido, por lo que, ocasiona una pérdida de transparencia por la complejidad de su proceso. (Krit & Haimoud, 2017)

Los hosts efectúan los servicios de proxy como gateways de aplicación. Esto mezcla ciertas características del firewall de filtrado de paquetes con los de puertas de enlace a nivel de circuitos. (Krit & Haimoud, 2017)

Además, estos filtran los paquetes con el servicio a la cual fueron destinados sino también con la cadena de solicitud HTTP, debido a otras características que tienen los servicios de proxy. Aunque las puertas de enlace a nivel de aplicación ofrecen una protección considerable a los datos, también puede afectar de manera drástica el rendimiento de la red. (Krit & Haimoud, 2017)

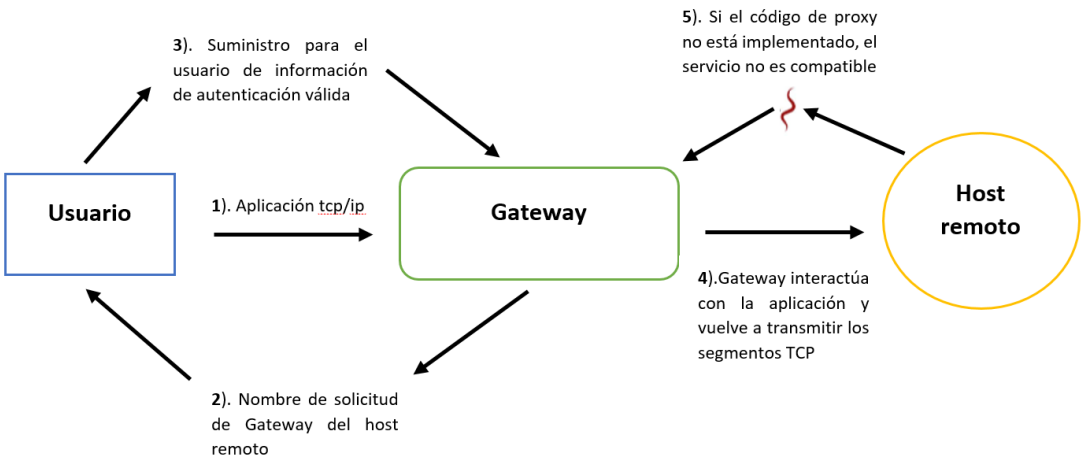


Figura 2. 10: Procedimiento del gateway de aplicación
Fuente: (Krit & Haimoud, 2017)

2.16.5. Firewall de revisión multinivel

Este tipo de firewall realiza la función de mantener el estado que se le otorgo a un paquete a cada uno de los componentes del firewall la cual transita por el camino hacia una multitud de protocolos. (Krit & Haimoud, 2017)

Permitiendo que el usuario tenga el control máximo y absoluto sobre los paquetes que pueden llegar a su destinatario final. Sin embargo, esto afecta el rendimiento de la red de una manera no tan drástica como lo es el proxy. (Krit & Haimoud, 2017)

2.17. Políticas de los firewalls

Las políticas de los firewalls son aquellas definiciones de mayor rango sobre el tráfico que debe o no debe permitirse.

Tabla 2. 2: Tipos de normas de los firewalls.

Políticas	Descripción	Ventajas
Modelado de políticas	Formaliza las reglas de firewall	Define la lista de reglas para la filtración de paquetes
Detección de anomalías	Detecta las incongruencias de la secuencia de reglas de filtrado	Proporciona diferentes métodos para la detección de anomalías en el firewall
Corrección automatizada de fallas de políticas	Corrección automatizada de la corrección de fallas de políticas	Proporciona recursos de generación de paquetes al azar
Localización de fallas	Define la ubicación de la falla	Proporciona enfoques para reducir el costo de prueba y depuración (RFC y RDC)
Editor de políticas de firewall	Ayuda al cliente a disponer el orden correcto para una nueva regla o modificación en la política	Proporciona métodos de inserción y de eliminación en la secuencia de reglas de filtrado
Herramientas de firewall	Ayuda al administrador a resolver tareas complejas que requieran de mucho tiempo	Proporciona la herramienta de detección de anomalías de políticas

Fuente: (Krit & Haimoud, 2017)

2.18. Protocolo de Enrutamiento en Espera Activa

El HSRP (Hot Standby Routing Protocol), es un protocolo que permite utilizar el 100% de tiempo sobre la actividad de la red ya que, otorga la reincidencia de red hacia los sistemas de Internet Protocol, la cual, asegura que la tarea del usuario pueda recuperarse de forma eficaz y fácil debido a las consecuencias del primer salto por el orden de los aparatos periféricos o de circuitos de acceso. (Alam et al., 2018)

El HSRP, Protocolo de Encaminamiento de Espera Activa, es un protocolo de Cisco que facilita una puerta de enlace redundante para un host en una subred de área local (Alam et al., 2018). Este protocolo HSRP, facilita un procedimiento elaborado para aceptar la conmutación por errores no conservadoras del tráfico IP en circunstancias determinadas. (Alam et al., 2018)

Hot Sandby Routing Protocol, otorga una puerta de enlace predeterminada. También, facilita a la configuración de dos o más routers en un agrupamiento de espera ya que, reparten una dirección IP y una dirección MAC y, además, con recursos de red (Alam et al., 2018). El mecanismo de HSRP mantiene un router activo, mientras tanto, los otros solamente están en modo espera y no tendrán una reacción hasta que el router principal, es decir, el router activo presente una falla. (Alam et al., 2018)

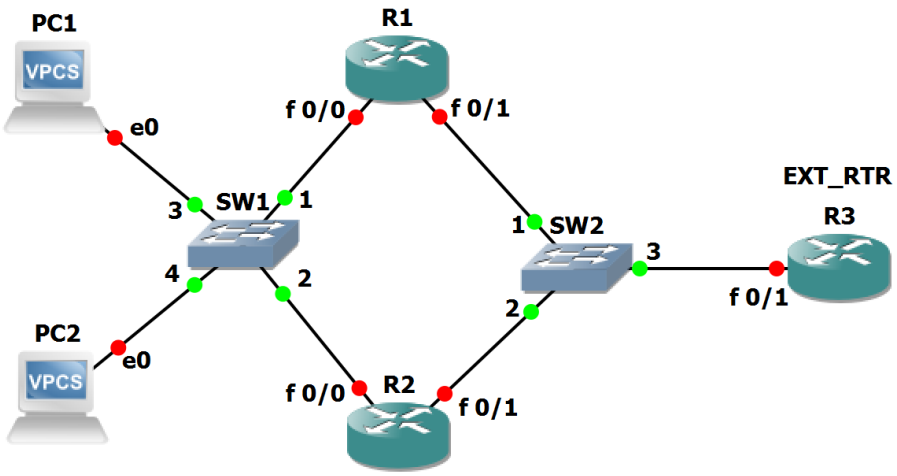


Figura 2. 11: Diagrama usando protocolo HSRP
Fuente: (Anwar et al., 2019)

2.19. Protocolo de Redundancia de Primer Salto

Este protocolo de red lo que hace es robustecer la dirección IP del gateway primario, siempre y cuando, consiga dos o más enrutadores para así ofrecer una protección. Además, brinda una redundancia en las redes y ayuda a eliminar el único punto de error a través del uso de un algoritmo de elección. (Anwar et al., 2019)

2.20. Protocolo de Redundancia de Enrutador Virtual

El protocolo VRRP es un tipo estándar abierto que elabora un router virtual la cual tienen muchos routers que sirven para incrementar los servicios de un gateway por default. (Anwar et al., 2019)

El VRRP se utiliza extensamente en las redes LAN para confrontar cualquier error en los gateways. Aunque, fue prohibido su utilización para las primeras configuraciones ya que, no albergaban la estabilidad de carga entre routers de Gateway primarios con los de apoyo. (Anwar et al., 2019)

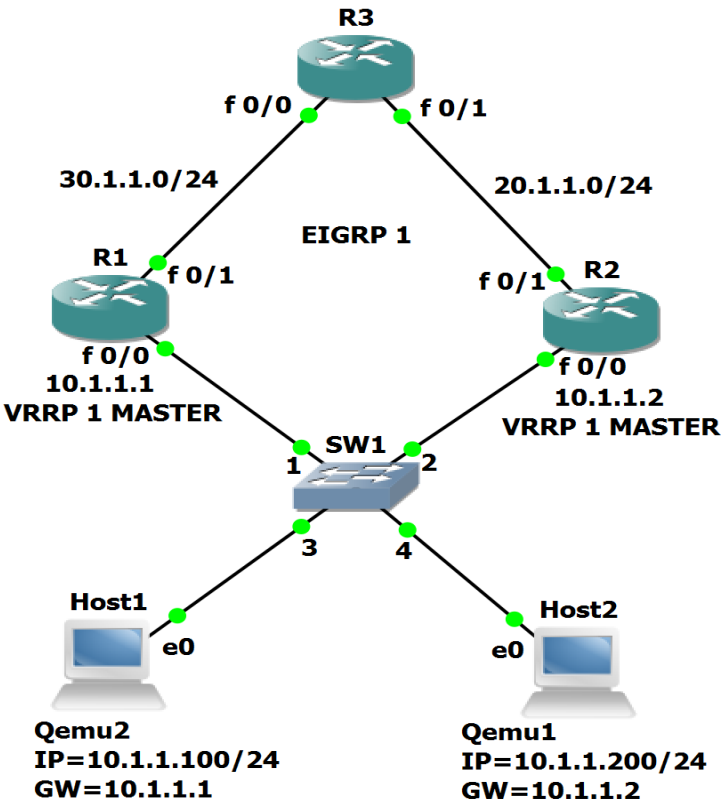


Figura 2. 12: Diagrama usando el protocolo VRRP
Fuente: (Anwar et al., 2019)

Existen dos clases de routers para este protocolo que son, el router principal y el router de apoyo. El router principal es el responsable de las funciones para la transmisión de datos, por lo que, manda un mensaje al router secundario para demostrar su estado activo. Por otro lado, el router secundario opera únicamente cuando el router principal tiene una falla operacional y en ese lapso de tiempo que el router de apoyo no opera, se convierte en un despojo de recursos. (Anwar et al., 2019)

Capítulo 3: Diseño, Implementación y resultados

3.1. Antecedentes del proyecto

El presente proyecto tiene por finalidad diseñar y emular una red IP/MPLS para proveer alta disponibilidad y eficiencia para el transporte de tráfico de voz y datos entre las facultades de la UCSG y Centro de Cómputo.

Las facultades del campus universitario realizan constantemente consultas a bases de datos centralizados en el Data Center de la Universidad Católica de Santiago de Guayaquil, por lo que se vuelve imprescindible disponer de conexiones con alta capacidad y disponibilidad para el transporte de dicho tráfico. De igual forma el tráfico telefónico generado entre las terminales IP y las centrales SIP debe ser diferenciado y viajar a través de forma aislada al tráfico de datos.

Las facultades de la UCSG disponen de conexiones de fibra óptica lineales hacia el Centro de Cómputo a través de una red IP vlaneada, pero la conmutación sigue siendo de paquetes, por lo que, podría generar retardo en la red de datos y jitter en la red telefónica. La conexión que actualmente disponen las facultades hacia el Centro de Cómputo tiene redundancia a nivel de capa 1 del modelo OSI, rutas redundantes de fibra óptica, pero no poseen una topología con conexiones de fibra y site redundantes, por lo cual, se plantea incrementar la alta disponibilidad a nivel de conexiones físicas, sitio y hardware (routers MPLS).

Para el presente estudio de diseño de una red IP/MPLS para interconectar las facultades de la UCSG y el Centro de Cómputo, es necesario conocer la demanda de servicios, tráficos y estaciones de trabajo promedio que consultan las bases de datos hacia el Centro de Cómputo.

3.1.1. Levantamiento de la infraestructura existente en el centro de cómputo y la facultad técnica

Tabla 3. 1: Infraestructura existente en Centro de Cómputo y F. Técnica

ITEM	Descripción	Cantidad	Tipo de tráfico
1	Estaciones de trabajo	25	Datos
2	Teléfonos IP	10	Telefónico
3	Impresoras	4	Datos
4	Cámaras IP	4	Vídeo

Elaborado por: Autor.

3.1.2. Situación actual de las conexiones hacia el centro de cómputo en el campus de la UCSG

Las conexiones en el campus universitario se componen de una red de fibra óptica lineal entre las facultades y el centro de cómputo. La topología actual es un Hub and Spoke donde no consta con enlaces redundantes para brindar alta disponibilidad o un site Backup para brindar redundancia física en caso de que el centro de cómputo colapse.

Las facultades de la UCSG realizan constantemente consultas a las bases de datos en el centro de cómputo, por lo cual, se torna indispensable tener una arquitectura con conexiones redundantes y un protocolo de transporte con alto rendimiento.

Las conexiones actuales se basan en una solución puramente de capa 3, con lo que, está soportada a través de un protocolo de direccionamiento dinámico cuya convergencia es relativamente lenta en comparación a un protocolo que maneje etiqueta para distribución del tráfico. En una red capa 3 (nivel de red) la diferencia de tráfico de telefonía e Internet se convierte en un reto ya que, no existe un mecanismo que aplique políticas de tráficos con la flexibilidad y desempeño que un protocolo que trabaje en capa 2.5 pueda lograr.

3.2. Consideraciones para el diseño de una red MPLS en el campus de la UCSG

3.2.1. Demanda actual y futura en los servicios internos en la UCSG

La demanda actual y futura a nivel de servicios entre las facultades de la UCSG y el Centro de Cómputo comprende de lo siguiente:

Tabla 3. 2: Demanda actual y futura de los servicios

FACULTAD TÉCNICA PARA EL DESARROLLO

Servicio	Consumo actual	Consumo a futuro
Datos/Internet	15 Mbps	25 Mbps
Telefonía	20 Mbps	25 Mbps
Vídeo	10 Mbps	15 Mbps

Elaborado por: Autor.

3.2.2. Distribución e interconexiones de las facultades de la UCSG hacia el centro de cómputo

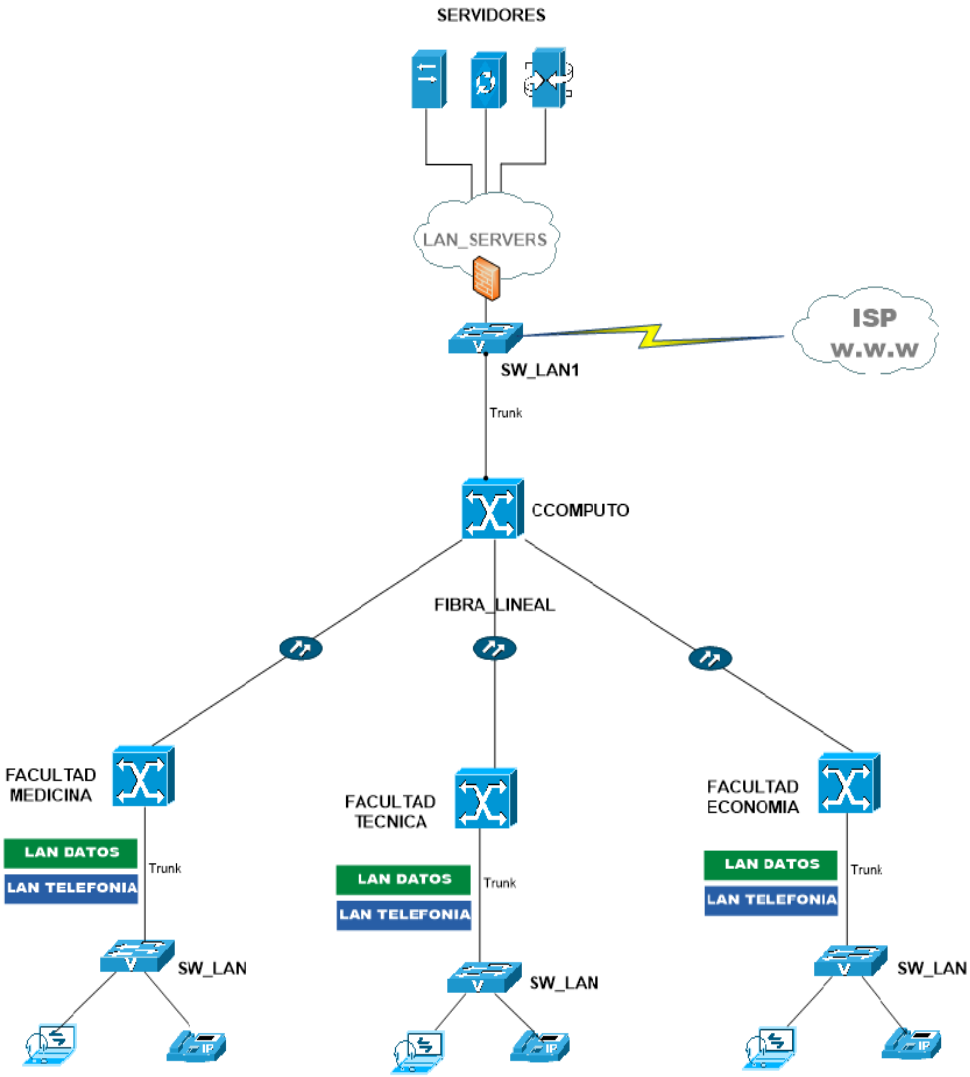


Figura 3. 1: Esquema de la repartición e interconexión de las facultades con Centro de Cómputo
Elaborado por: Autor.

3.2.3. Recursos y recomendaciones a considerar para el diseño de la red MPLS en la UCSG

Dentro de los recursos y recomendaciones que hay que considerar para el diseño e implementación de una red IP/MPLS para interconectar las facultades del campus de la UCSG y en Centro de Cómputo, se citan los siguientes:

- Determinar los tipos de tráficos que transitan entre las facultades de la UCSG y Centro de Cómputo.
- Determinar el consumo de tráfico entre las facultades del campus universitario y Centro de Cómputo.
- La cantidad de estaciones de trabajo dentro de las facultades y edificio principal para determinar la densidad de puertos LAN a considerar.
- Protocolos y equipamiento que actualmente se utilizan a nivel de conectividad para interconectar las facultades, edificios y Rectorado hacia el Centro de Cómputo.
- Utilización de GNS3 como programa para la emulación de la solución a diseñar.
- Utilización de Microsoft Visio para realizar los esquemas de conectividad.
- Determinación del equipamiento y protocolos a usar en el diseño de la red IP/MPLS para interconectar las facultades de la UCSG y el Centro de Cómputo.
- Diseñar una red convergente y con alta disponibilidad para brindar conexiones redundantes en caso de que el Centro de Cómputo quede aislado de la red MPLS.

3.2.4. Definición y características del modelo MPLS a considerar

El modelo MPLS a considerar en el presente estudio, contempla una solución en capa 3 a través del modelo L3VPN, el cual consiste en crear

instancias en capa 3 para cada servicio (tráfico de datos y telefonía) mediante una infraestructura compartida, esto permite aislar los tráficos para que no exista superposición a nivel de direccionamiento.

Una red L3VPN sobre MPLS nos permite aplicar una conmutación de etiqueta, la cual permite una mayor velocidad a nivel de envío de paquetes ya que, la toma de decisión de aprendizaje de prefijos lo hace por medio de labels sin analizar direcciones origen – destino.

3.3. Ingeniería y desarrollo del modelo MPLS propuesto

3.3.1. HLD de la solución propuesta

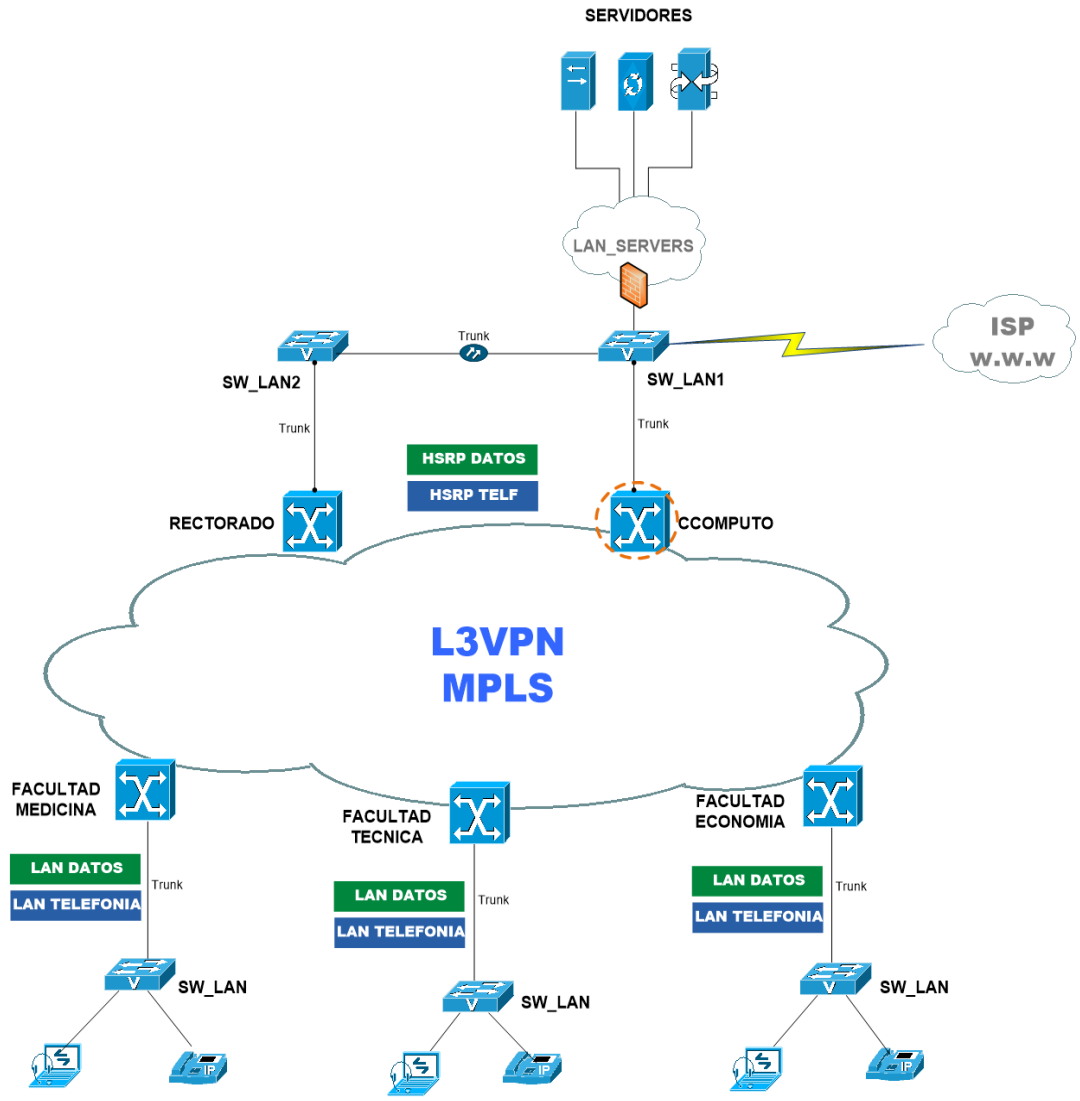


Figura 3. 2: Esquema HLD del modelo IP/MPLS propuesto
Elaborado por: Autor.

3.3.2. DLD de la solución propuesta

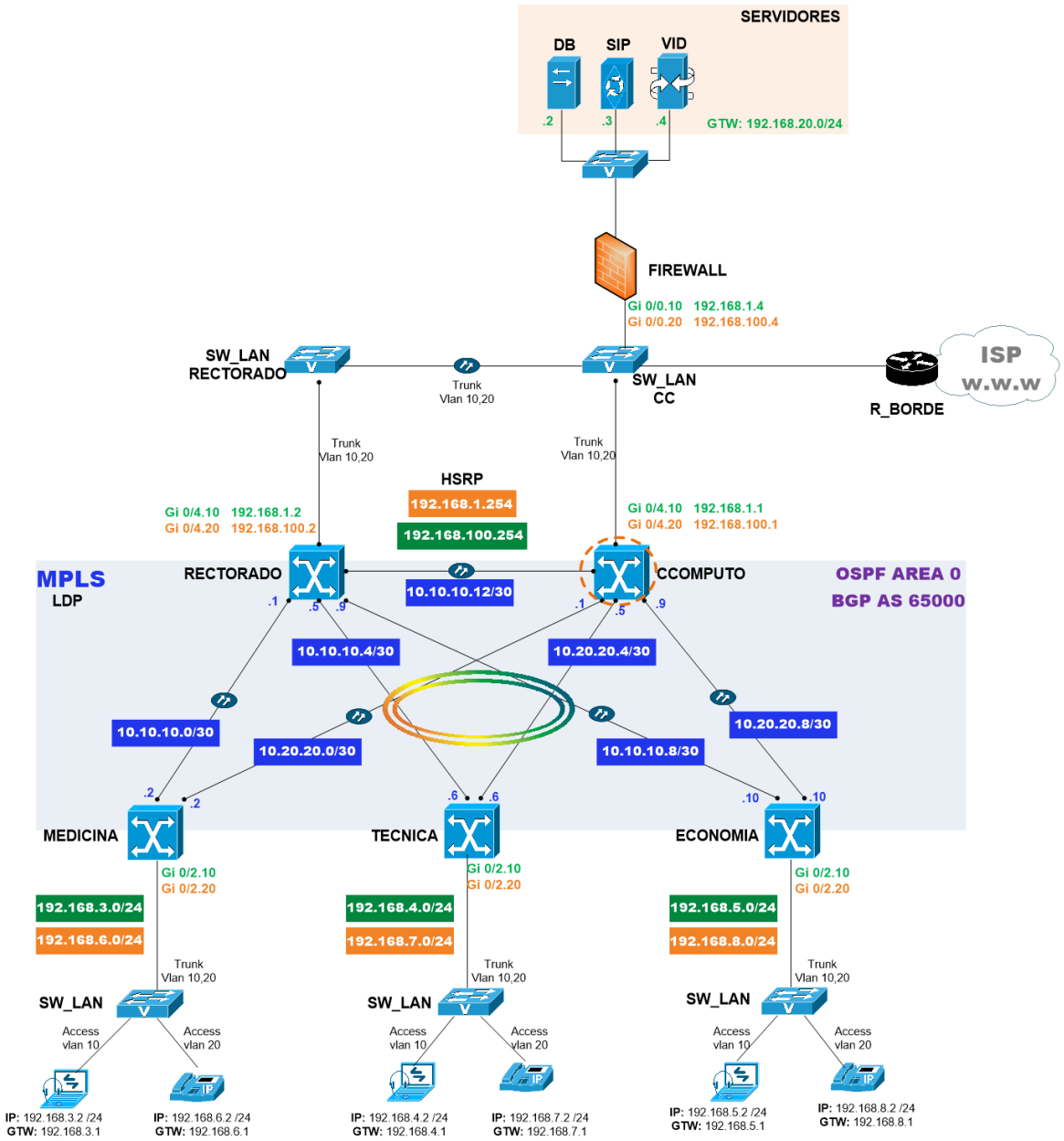


Figura 3. 3: Esquema DLD del modelo IP/MPLS propuesto
Elaborado por: Autor.

3.3.3. Dimensionamiento de dispositivos a usar en la emulación

Tabla 3. 3: Equipos utilizados en el emulador

DIMENSIONAMIENTO DE HARDWARE						
ITEM	**DESCRIPCIÓN**	**MODELO**	**#**	**SISTEMA OPERATIVO**	**INTERFACES**	**THOUTPUT**
1	Router	Cisco ME 3800x	2	Cisco IOS Software	Spare Cisco ME 3800X-	44 Gbps

				Release 15.2(2)S	24FS Ethernet Carrier Ethernet Switch Router	
2	Router	Cisco ME 3600x	3	Cisco IOS Software Release 15.2(2)S	Cisco ME 3600X-24FS Ethernet Access Switch	30 Gbps
3	Switch	Cisco Catalyst 9400	2	Cisco IOS XE	Cisco Catalyst 9400 Series 24-Port Gigabit Ethernet(SFP)	960-Gbps switching capacity
4	Switch	Cisco Catalyst 9200	3	Cisco IOS XE	24 ports full PoE+ | Modular Uplinks	160-Gbps switching capacity
5	Firewall	Fortigate 60E	1	FortiOS	2x GE RJ45 WAN Ports + 7x GE RJ45 Internal Ports	Firewall Throughput: 3 Gbps

Elaborado por: Autor.

3.3.4. IP/PLANNING

- **IP/PLANNING red MPLS**

Tabla 3. 4: Descripción de las IP/PLANNING

IP/PLANNING MPLS			
Device	**Interface**	**IPv4 Address**	**Mask**
Centro de Cómputo	Giga 0/0	10.10.10.13	255.255.255.252
	Giga 0/1	10.20.20.9	255.255.255.252
	Giga 0/2	10.20.20.5	255.255.255.252
	Giga 0/3	10.20.20.1	255.255.255.252
	Loopback 0	1.1.1.1	255.255.255.255
Rectorado	Giga 0/0	10.10.10.14	255.255.255.252
	Giga 0/1	10.10.10.1	255.255.255.252
	Giga 0/2	10.10.10.5	255.255.255.252
	Giga 0/3	10.10.10.9	255.255.255.252
	Loopback 0	2.2.2.2	255.255.255.255
Facultad de Medicina	Giga 0/0	10.20.20.2	255.255.255.252
	Giga 0/1	10.10.10.2	255.255.255.252
	Loopback 0	3.3.3.3	255.255.255.255
	Giga 0/0	10.20.20.6	255.255.255.252

Facultad Técnica	Giga 0/1	10.10.10.6	255.255.255.252
	Loopback 0	4.4.4.4	255.255.255.255
Facultad de Economía	Giga 0/0	10.20.20.10	255.255.255.252
	Giga 0/1	10.10.10.10	255.255.255.252
	Loopback 0	5.5.5.5	255.255.255.255

Elaborado por: Autor.

- **IP - VLAN/PLANNING redes LAN en las facultades**

Tabla 3. 5: IP/PLANNING detallado

IP/PLANNING de redes LAN						
Site	**Interface**	**Tipo**	**VLAN**	**Tipo**	**IPv4 Address**	**Mask**
Centro de Cómputo	Giga 0/2	TRUNK	10	Datos	192.168.1.1	255.255.255.0
			20	Voz	192.168.100.1	255.255.255.0
Rectorado	Giga 0/2	TRUNK	10	Datos	192.168.1.2	255.255.255.0
			20	Voz	192.168.100.2	255.255.255.0
Facultad de Medicina	Giga 0/2	TRUNK	10	Datos	192.168.3.1	255.255.255.0
			20	Voz	192.168.6.1	255.255.255.0
Facultad Técnica	Giga 0/2	TRUNK	10	Datos	192.168.4.1	255.255.255.0
			20	Voz	192.168.7.1	255.255.255.0
Facultad de Economía	Giga 0/2	TRUNK	10	Datos	192.168.5.1	255.255.255.0
			20	Voz	192.168.8.1	255.255.255.0

Elaborado por: Autor.

3.3.5. Definición de RDs y RTs

Tabla 3. 6: VRF de Datos

VRF DATOS												
	Centro de Cómputo			**Rectorado**			**Facultad de Medicina**		**Facultad Técnica**		**Facultad de Economía**	
RT IMPORT	6:6	7:7	8:8	6:6	7:7	8:8	4:4	5:5	4:4	5:5	4:4	5:5
RT EXPORT	4:4			5:5			6:6		7:7		8:8	
RD	RD 2:2			RD 3:3			RD 4:4		RD 5:5		RD 6:6	

Elaborado por: Autor.

Tabla 3. 7: VRF de Voz

	VRF VOZ											
	Centro de Cómputo			Rectorado			Facultad de Medicina		Facultad Técnica		Facultad de Economía	
RT IMPORT	10:10	11:11	12:12	10:10	11:11	12:12	100:100	200:200	100:100	200:200	100:100	200:200
RT EXPORT	100:100			200:200			10:10		11:11		12:12	
RD	RD 3:3			RD 3:3			RD 3:3		RD 3:3		RD 3:3	

Elaborado por: Autor.

3.3.6. Protocolos implementados

Tabla 3. 8: Protocolos que fueron implementados

Protocolos usados	
Protocolo	**Descripción**
OSPF	IGP impartido para obtener conectividad entre las LOOPBACKS para el levantamiento de adyacencias IBGP
LDP – MPLS	Protocolo utilizado para el etiquetado de los prefijos LAN
BGP – MPBGP	Usado para el anunciamiento de prefijos VPNv4 entre las facultades consideradas y el centro de cómputo
HSRP – FHRP	Protocolo de alta disponibilidad LAN para brindar un Gateway virtual
STATIC ROUTES	Rutas declaradas de forma estática para llegar a los servidores del centro de cómputo
TRUNKING DOT1Q	Protocolo para generar un TAG de VLAN hacia los dispositivos de capa 2, p.ej: switches
VRF	Técnica empleada para crear varias instancias en capa 3 con el propósito de segmentar el tráfico de datos y telefonía

Elaborado por: Autor.

3.4. Configuraciones en equipos del Backbone y dispositivos LAN

3.4.1. Configuración del direccionamiento en equipos Backbone

- **PE del Centro de Cómputo**

```
interface GigabitEthernet0/0
 description CONEXION_FO_HACIA_RECTORADO
 ip address 10.10.10.13 255.255.255.252
```

Figura 3. 4: Configuración de la IP address de Centro de Cómputo hacia el Rectorado

Elaborado por: Autor.

Figura 3. 5: Configuración de la IP address de Centro de Cómputo hacia la F. Economía
Elaborado por: Autor.

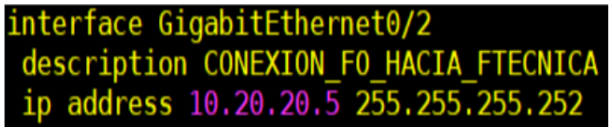


Figura 3. 6: Configuración de la IP address de Centro de Cómputo hacia la F. Técnica
Elaborado por: Autor.

Figura 3. 7: Configuración de la IP address de Centro de Cómputo hacia la F. Medicina
Elaborado por: Autor.

- **PE de Rectorado**

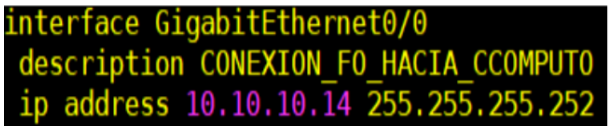


Figura 3. 8: Configuración de la IP address de Rectorado hacia el Centro de Cómputo
Elaborado por: Autor.

Figura 3. 9: Configuración de la IP address de Rectorado hacia la F. Medicina
Elaborado por: Autor.

Figura 3. 10: Configuración de la IP address de Rectorado hacia la F. Técnica
Elaborado por: Autor.

```
interface GigabitEthernet0/3
 description CONEXION_FO_HACIA_FECONOMIA
 ip address 10.10.10.9 255.255.255.252
```

Figura 3. 11: Configuración de la IP address de Rectorado hacia la F. de Economía
Elaborado por: Autor.

- **PE de la Facultad Médica**

```
interface GigabitEthernet0/0
 description CONEXION_FO_HACIA_CCOMPUTO
 ip address 10.20.20.2 255.255.255.252
```

Figura 3. 12: Configuración de la IP address de la F. Médica hacia Centro de Cómputo
Elaborado por: Autor.

```
interface GigabitEthernet0/1
 description CONEXION_FO_HACIA_RECTORADO
 ip address 10.10.10.2 255.255.255.252
```

Figura 3. 13: Configuración de la IP address de la F. Médica hacia Rectorado
Elaborado por: Autor.

- **PE de la Facultad Técnica**

```
interface GigabitEthernet0/0
 description CONEXION_FO_HACIA_CCOMPUTO
 ip address 10.20.20.6 255.255.255.252
```

Figura 3. 14: Configuración de la IP address de la F. Técnica hacia Centro de Cómputo
Elaborado por: Autor.

```
interface GigabitEthernet0/1
 description CONEXION_FO_HACIA_RECTORADO
 ip address 10.10.10.6 255.255.255.252
```

Figura 3. 15: Configuración de la IP address de la F. Técnica hacia Rectorado
Elaborado por: Autor.

- **PE de la Facultad de Economía**

```
interface GigabitEthernet0/0
 description CONEXION_FO_HACIA_CCOMPUNTO
 ip address 10.20.20.10 255.255.255.252
```

Figura 3. 16: Configuración de la IP address de la F. Economía hacia Centro de Cómputo
Elaborado por: Autor.

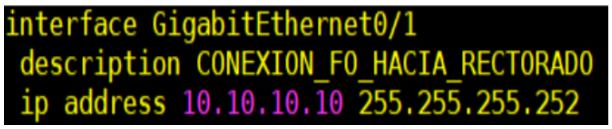


Figura 3. 17: Configuración de la IP address de la F. de Economía hacia Rectorado
Elaborado por: Autor.

3.4.2. Configuración de protocolos en equipos Backbone

Para la implementación de servicios L3VPN en el transporte del tráfico de datos y telefonía entre las facultades de la UCSG y el Centro de Cómputo se requiere del uso de un protocolo IGP underlay como OSPF para las conexiones internas en el Core del campus universitario, dicho protocolo permite el levantamiento de sesiones IBGP entre los enrutadores PE de las facultades y los enrutadores PE del Centro de Cómputo y Rectorado, este último como site backup.

Mediante el protocolo BGP que se transportan los prefijos de las facultades hacia el centro de datos, por lo que, dicho tráfico debe ir debidamente etiquetado a través de labels por medio de un protocolo llamado LDP (Label Distribution Protocol), que permite diferenciar instancias locales en capa 3 VRF's agregando un marcado como el RT (Router Target) para diferenciarlos en otras situaciones.

A continuación, se detallan las configuraciones que se realizaron en los routers PE del centro de datos y facultades para levantar conectividad de voz y datos hacia el Centro de Cómputo.

- **Configuración de OSPF**
  - **PE del Centro de Cómputo**

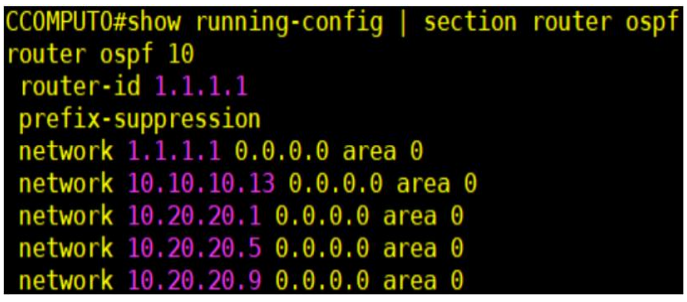


Figura 3. 18: Configuración de OSPF de Centro de Cómputo
Elaborado por: Autor.

- **PE de Rectorado**

```
RECTORADO#show running-config | section router ospf
router ospf 10
 router-id 2.2.2.2
 prefix-suppression
 network 2.2.2.2 0.0.0.0 area 0
 network 10.10.10.1 0.0.0.0 area 0
 network 10.10.10.5 0.0.0.0 area 0
 network 10.10.10.9 0.0.0.0 area 0
 network 10.10.10.14 0.0.0.0 area 0
```

Figura 3. 19: Configuración de OSPF de Rectorado
Elaborado por: Autor.

- **PE de la Facultad Médica**

```
FMEDICINA#sho running-config | section router ospf
router ospf 10
 router-id 3.3.3.3
 prefix-suppression
 network 3.3.3.3 0.0.0.0 area 0
 network 10.10.10.2 0.0.0.0 area 0
 network 10.20.20.2 0.0.0.0 area 0
```

Figura 3. 20: Configuración de OSPF de la Facultad Médica
Elaborado por: Autor.

- **PE de la Facultad Técnica**

```
FTECNICA#show running-config | section router ospf
router ospf 10
 router-id 4.4.4.4
 prefix-suppression
 network 4.4.4.4 0.0.0.0 area 0
 network 10.10.10.6 0.0.0.0 area 0
 network 10.20.20.6 0.0.0.0 area 0
```

Figura 3. 21: Configuración de OSPF de la Facultad Técnica
Elaborado por: Autor.

- **PE de la Facultad de Economía**

```
FECONOMIA#sho running-config | section router ospf
router ospf 10
 router-id 5.5.5.5
 prefix-suppression
 network 5.5.5.5 0.0.0.0 area 0
 network 10.10.10.10 0.0.0.0 area 0
 network 10.20.20.10 0.0.0.0 area 0
```

Figura 3. 22: Configuración de OSPF de la Facultad de Economía
Elaborado por: Autor.

- **Configuración de MPLS – LDP**
  - **PE de Centro de Cómputo**

```
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
mpls label protocol ldp
```

Figura 3. 23: Configuración de MPLS - LDP del Centro de Cómputo
Elaborado por: Autor.

```
interface GigabitEthernet0/0
 description CONEXION_FO_HACIA_RECTORADO
 ip address 10.10.10.13 255.255.255.252
 ip ospf network point-to-point
 duplex auto
 speed auto
 media-type rj45
 mpls label protocol ldp
 mpls ip
!
```

Figura 3. 24: Configuración de MPLS - LDP del Centro de Cómputo hacia Rectorado
Elaborado por: Autor.

```
interface GigabitEthernet0/1
 description CONEXION_FO_HACIA_FECONOMIA
 ip address 10.20.20.9 255.255.255.252
 ip ospf network point-to-point
 duplex auto
 speed auto
 media-type rj45
 mpls label protocol ldp
 mpls ip
end
```

Figura 3. 25: Configuración de MPLS - LDP del Centro de Cómputo con la F. Economía
Elaborado por: Autor.

```
interface GigabitEthernet0/2
 description CONEXION_FO_HACIA_FTECNICA
 ip address 10.20.20.5 255.255.255.252
 ip ospf network point-to-point
 duplex auto
 speed auto
 media-type rj45
 mpls label protocol ldp
 mpls ip
end
```

Figura 3. 26: Configuración de MPLS - LDP del Centro de Cómputo con la F. Técnica
Elaborado por: Autor.

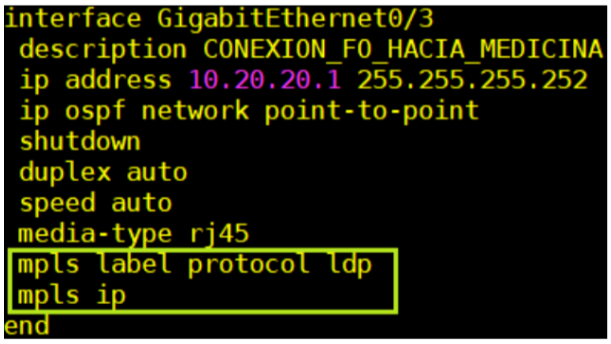


Figura 3. 27: Configuración de MPLS - LDP del Centro de Cómputo con la F. Médica
Elaborado por: Autor.

- **PE de Rectorado**

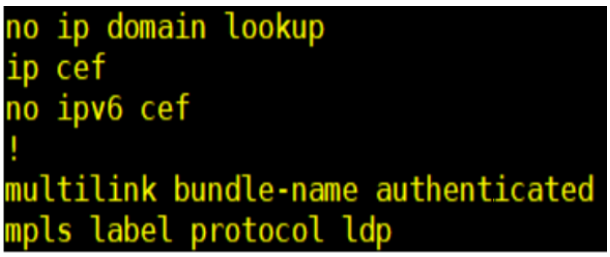


Figura 3. 28: Configuración de MPLS - LDP de Rectorado
Elaborado por: Autor.

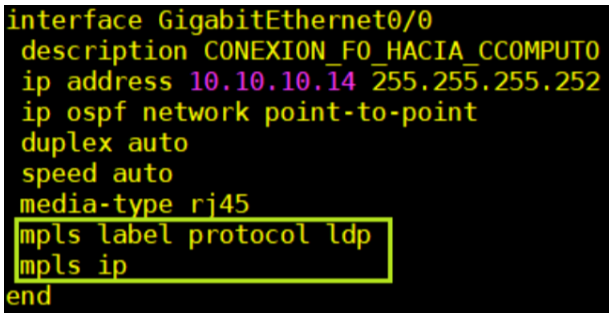


Figura 3. 29: Configuración de MPLS - LDP de Rectorado con Centro de Cómputo
Elaborado por: Autor.

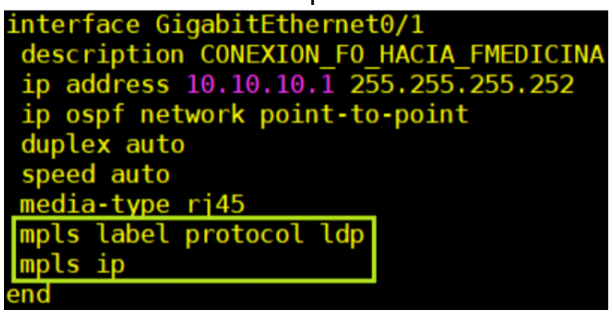


Figura 3. 30: Configuración de MPLS - LDP de Rectorado con la F. Médica
Elaborado por: Autor.

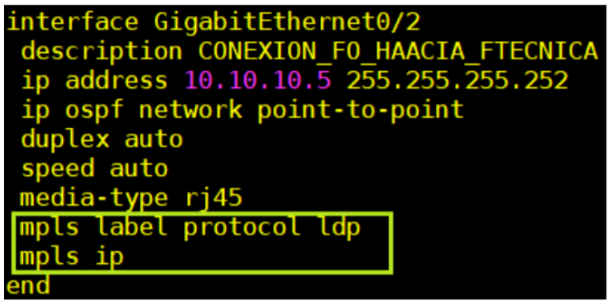


Figura 3. 31: Configuración de MPLS - LDP de Rectorado con la F. Técnica
Elaborado por: Autor.

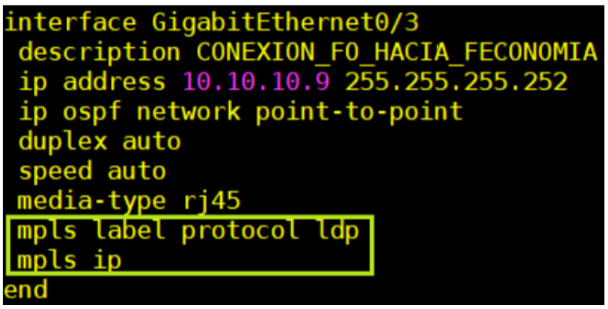


Figura 3. 32: Configuración de MPLS - LDP de Rectorado con la F. de Economía
Elaborado por: Autor.

- **PE de la Facultad de Medicina**

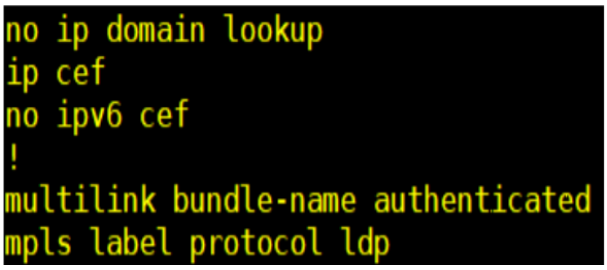


Figura 3. 33: Configuración de MPLS - LDP de la Facultad Médica
Elaborado por: Autor.

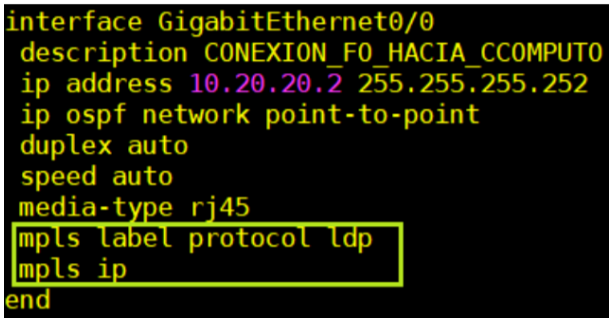


Figura 3. 34: Configuración de MPLS - LDP de la Facultad Médica hacia Centro de Cómputo
Elaborado por: Autor.

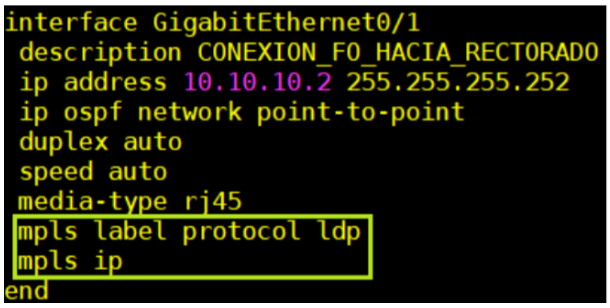


Figura 3. 35: Configuración de MPLS - LDP de la Facultad Médica hacia Rectorado
Elaborado por: Autor.

- **PE de la Facultad Técnica**

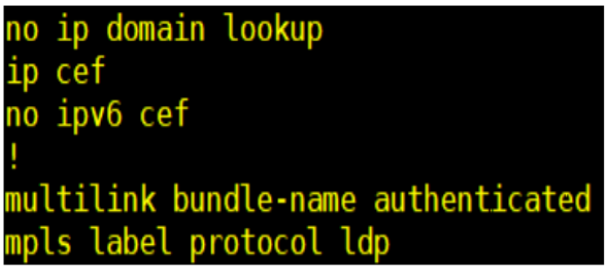


Figura 3. 36: Configuración de MPLS - LDP de la Facultad Técnica
Elaborado por: Autor.

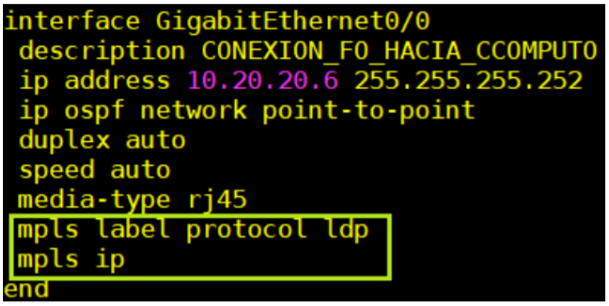


Figura 3. 37: Configuración de MPLS - LDP de la Facultad Técnica con Centro de Cómputo
Elaborado por: Autor.

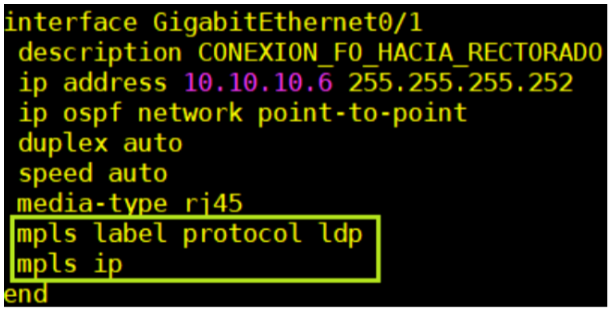


Figura 3. 38: Configuración de MPLS - LDP de la Facultad Técnica hacia Rectorado
Elaborado por: Autor.

- **PE de la Facultad de Economía**

```
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
mpls label protocol ldp
```

Figura 3. 39: Configuración de MPLS - LDP de la Facultad de Economía
Elaborado por: Autor.

```
interface GigabitEthernet0/0
 description CONEXION_FO_HACIA_CCOMPUNTO
 ip address 10.20.20.10 255.255.255.252
 ip ospf network point-to-point
 duplex auto
 speed auto
 media-type rj45
 mpls label protocol ldp
 mpls ip
end
```

Figura 3. 40: Configuración de MPLS - LDP de la Facultad de Economía con Centro de Cómputo
Elaborado por: Autor.

```
interface GigabitEthernet0/1
 description CONEXION_FO_HACIA_RECTORADO
 ip address 10.10.10.10 255.255.255.252
 ip ospf network point-to-point
 duplex auto
 speed auto
 media-type rj45
 mpls label protocol ldp
 mpls ip
end
```

Figura 3. 41: Configuración de MPLS - LDP de la Facultad de Economía con Rectorado
Elaborado por: Autor.

- **Configuración de BGP**
  - **PE de Centro de Cómputo**

```
CCOMPUTO#sho running-config | section router bgp
router bgp 65000
 bgp router-id 1.1.1.1
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 2.2.2.2 remote-as 65000
 neighbor 2.2.2.2 update-source Loopback10
 neighbor 3.3.3.3 remote-as 65000
 neighbor 3.3.3.3 update-source Loopback10
 neighbor 4.4.4.4 remote-as 65000
 neighbor 4.4.4.4 update-source Loopback10
 neighbor 5.5.5.5 remote-as 65000
 neighbor 5.5.5.5 update-source Loopback10
 !
 address-family ipv4
  neighbor 2.2.2.2 activate
  neighbor 3.3.3.3 activate
  neighbor 4.4.4.4 activate
  neighbor 5.5.5.5 activate
 exit-address-family
```

Figura 3. 42: Configuración de BGP de Centro de Cómputo
Elaborado por: Autor.

- **PE de Rectorado**

```
RECTORADO#sho running-config | section router bgp
router bgp 65000
 bgp router-id 2.2.2.2
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 1.1.1.1 remote-as 65000
 neighbor 1.1.1.1 update-source Loopback10
 neighbor 3.3.3.3 remote-as 65000
 neighbor 3.3.3.3 update-source Loopback10
 neighbor 4.4.4.4 remote-as 65000
 neighbor 4.4.4.4 update-source Loopback10
 neighbor 5.5.5.5 remote-as 65000
 neighbor 5.5.5.5 update-source Loopback10
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 3.3.3.3 activate
  neighbor 4.4.4.4 activate
  neighbor 5.5.5.5 activate
 exit-address-family
```

Figura 3. 43: Configuración de BGP de Rectorado
Elaborado por: Autor.

- **PE de la Facultad Médica**

```
FMEDICINA#sho running-config | section router bgp
router bgp 65000
 bgp router-id 3.3.3.3
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 1.1.1.1 remote-as 65000
 neighbor 1.1.1.1 update-source Loopback10
 neighbor 2.2.2.2 remote-as 65000
 neighbor 2.2.2.2 update-source Loopback10
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 2.2.2.2 activate
 exit-address-family
```

Figura 3. 44: Configuración de BGP de la Facultad Médica
Elaborado por: Autor.

- **PE de la Facultad Técnica**

```
FTECNICA#sho running-config | section router bgp
router bgp 65000
 bgp router-id 4.4.4.4
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 1.1.1.1 remote-as 65000
 neighbor 1.1.1.1 update-source Loopback10
 neighbor 2.2.2.2 remote-as 65000
 neighbor 2.2.2.2 update-source Loopback10
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 2.2.2.2 activate
 exit-address-family
```

Figura 3. 45: Configuración de BGP de la Facultad Técnica
Elaborado por: Autor.

- **PE de la Facultad de Economía**

```
FECONOMIA#sho running-config | section router bgp
router bgp 65000
 bgp router-id 5.5.5.5
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 1.1.1.1 remote-as 65000
 neighbor 1.1.1.1 update-source Loopback10
 neighbor 2.2.2.2 remote-as 65000
 neighbor 2.2.2.2 update-source Loopback10
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 2.2.2.2 activate
 exit-address-family
```

Figura 3. 46: Configuración de BGP de la Facultad de Economía
Elaborado por: Autor.

➢ **Configuración del L3VPN**

- **PE de Centro de Cómputo**

```
 address-family vpnv4
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
  neighbor 4.4.4.4 activate
  neighbor 4.4.4.4 send-community extended
  neighbor 5.5.5.5 activate
  neighbor 5.5.5.5 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf DATOS
  redistribute connected
  redistribute static
 exit-address-family
 !
 address-family ipv4 vrf VOIP
  redistribute static
 exit-address-family
CCOMPUTO#
```

Figura 3. 47: Configuración de L3VPN de Centro de Cómputo
Elaborado por: Autor.

- **PE de Rectorado**

```
address-family vpnv4
 neighbor 3.3.3.3 activate
 neighbor 3.3.3.3 send-community extended
 neighbor 4.4.4.4 activate
 neighbor 4.4.4.4 send-community extended
 neighbor 5.5.5.5 activate
 neighbor 5.5.5.5 send-community extended
exit-address-family
!
address-family ipv4 vrf DATOS
 redistribute connected
 redistribute static
exit-address-family
!
address-family ipv4 vrf VOIP
 redistribute static
exit-address-family
RECTORADO#
```

Figura 3. 48: Configuración de L3VPN de Rectorado
Elaborado por: Autor.

- **PE de la Facultad de Medicina**

```
address-family vpnv4
 neighbor 1.1.1.1 activate
 neighbor 1.1.1.1 send-community extended
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 send-community extended
exit-address-family
!
address-family ipv4 vrf DATOS
 redistribute connected
exit-address-family
!
address-family ipv4 vrf VOIP
 redistribute connected
exit-address-family
FMEDICINA#
```

Figura 3. 49: Configuración de L3VPN de la Facultad Médica
Elaborado por: Autor.

- **PE de la Facultad Técnica**

```
address-family vpnv4
 neighbor 1.1.1.1 activate
 neighbor 1.1.1.1 send-community extended
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 send-community extended
exit-address-family
!
address-family ipv4 vrf DATOS
 redistribute connected
exit-address-family
!
address-family ipv4 vrf VOIP
 redistribute connected
exit-address-family
FTECNICA#
```

Figura 3. 50: Configuración de L3VPN de la Facultad Médica
Elaborado por: Autor.

- **PE de la Facultad de Economía**

```
address-family vpnv4
 neighbor 1.1.1.1 activate
 neighbor 1.1.1.1 send-community extended
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 send-community extended
exit-address-family
!
address-family ipv4 vrf DATOS
 redistribute connected
exit-address-family
!
address-family ipv4 vrf VOIP
 redistribute connected
exit-address-family
FECONOMIA#
```

Figura 3. 51: Configuración de L3VPN de la Facultad de Economía
Elaborado por: Autor.

- **Configuración de los VRF's, RD y RT**
  - **PE de Centro de Cómputo**

```
CCOMPUTO#sho running-config | section ip vrf DATOS
ip vrf DATOS
 rd 2:2
 route-target export 4:4
 route-target import 6:6
 route-target import 7:7
 route-target import 8:8
CCOMPUTO#
CCOMPUTO#
CCOMPUTO#sho running-config | section ip vrf VOIP
ip vrf VOIP
 rd 3:3
 route-target export 100:100
 route-target import 10:10
 route-target import 11:11
 route-target import 12:12
```

Figura 3. 52: Configuración de las VRF's, RD y RT de Centro de Cómputo
Elaborado por: Autor.

  - **PE de Rectorado**

```
RECTORADO#sho running-config | section ip vrf DATOS
ip vrf DATOS
 rd 2:2
 route-target export 5:5
 route-target import 6:6
 route-target import 7:7
 route-target import 8:8
RECTORADO#
RECTORADO#sho running-config | section ip vrf VOIP
ip vrf VOIP
 rd 3:3
 route-target export 200:200
 route-target import 10:10
 route-target import 11:11
 route-target import 12:12
```

Figura 3. 53: Configuración de las VRF's, RD y RT de Rectorado
Elaborado por: Autor.

  - **PE de la Facultad de Medicina**

```
FMEDICINA#sho running-config | section ip vrf DATOS
ip vrf DATOS
 rd 2:2
 route-target export 6:6
 route-target import 4:4
 route-target import 5:5
FMEDICINA#
FMEDICINA#sho running-config | section ip vrf VOIP
ip vrf VOIP
 rd 3:3
 route-target export 10:10
 route-target import 100:100
 route-target import 200:200
```

Figura 3. 54: Configuración de las VRF's, RD y RT de la Facultad Médica
Elaborado por: Autor.

- **PE de la Facultad Técnica**

```
FTECNICA#sho running-config | section ip vrf DATOS
ip vrf DATOS
 rd 2:2
 route-target export 7:7
 route-target import 4:4
 route-target import 5:5
FTECNICA#
FTECNICA#sho running-config | section ip vrf VOIP
ip vrf VOIP
 rd 3:3
 route-target export 11:11
 route-target import 100:100
 route-target import 200:200
```

Figura 3. 55: Configuración de las VRF's, RD y RT de la Facultad Técnica
Elaborado por: Autor.

- **PE de la Facultad de Economía**

```
FECONOMIA#sho running-config | section ip vrf DATOS
ip vrf DATOS
 rd 2:2
 route-target export 8:8
 route-target import 4:4
 route-target import 5:5
FECONOMIA#
FECONOMIA#sho running-config | section ip vrf VOIP
ip vrf VOIP
 rd 3:3
 route-target export 12:12
 route-target import 100:100
 route-target import 200:200
```

Figura 3. 56: Configuración de las VRF's, RD y RT de la Facultad de Economía
Elaborado por: Autor.

3.4.3. Configuración de protocolos a nivel LAN y de alta disponibilidad con las facultades y Centro de Cómputo

- **Configuración HSRP para dar alta disponibilidad**
  - **Centro de Cómputo**

```
CCOMPUTO#sho running-config interface gigabitEthernet 0/4.10
Building configuration...

Current configuration : 243 bytes
!
interface GigabitEthernet0/4.10
 description LAN_DATOS
 encapsulation dot1Q 10
 ip vrf forwarding DATOS
 ip address 192.168.1.1 255.255.255.0
 standby 1 ip 192.168.1.254
 standby 1 timers 5 15
 standby 1 priority 120
 standby 1 preempt
end
```

Figura 3. 57: Configuración de la HSRP del Centro de Cómputo con GigaEthernet 0/4.10
Elaborado por: Autor.

```
CCOMPUTO#sho running-config interface gigabitEthernet 0/4.20
Building configuration...

Current configuration : 245 bytes
!
interface GigabitEthernet0/4.20
 description LAN_VOIP
 encapsulation dot1Q 20
 ip vrf forwarding VOIP
 ip address 192.168.100.1 255.255.255.0
 standby 2 ip 192.168.100.254
 standby 2 timers 5 15
 standby 2 priority 120
 standby 2 preempt
end
```

Figura 3. 58: Configuración de la HSRP del Centro de Cómputo con GigaEthernet 0/4.20
Elaborado por: Autor.

- **Rectorado**

```
RECTORADO#sho running-config interface gigabitEthernet 0/4.10
Building configuration...

Current configuration : 219 bytes
!
interface GigabitEthernet0/4.10
 description LAN_DATOS
 encapsulation dot1Q 10
 ip vrf forwarding DATOS
 ip address 192.168.1.2 255.255.255.0
 standby 1 ip 192.168.1.254
 standby 1 timers 5 15
 standby 1 preempt
end
```

Figura 3. 59: Configuración de la HSRP de Rectorado con GigaEthernet 0/4.10
Elaborado por: Autor.

```
RECTORADO#sho running-config interface gigabitEthernet 0/4.20
Building configuration...

Current configuration : 221 bytes
!
interface GigabitEthernet0/4.20
 description LAN_VOIP
 encapsulation dot1Q 20
 ip vrf forwarding VOIP
 ip address 192.168.100.2 255.255.255.0
 standby 2 ip 192.168.100.254
 standby 2 timers 5 15
 standby 2 preempt
end
```

Figura 3. 60: Configuración de la HSRP de Rectorado con GigaEthernet 0/4.20
Elaborado por: Autor.

- **Configuración de rutas estáticas en Centro de Cómputo para llegar a los servidores**
  - **Centro de Cómputo**

```
CCOMPUTO#sho running-config | include ip route
ip route vrf DATOS 172.16.20.0 255.255.255.0 192.168.1.4 name HACIA_SERVIDORES_INTERNOS_UCSG
ip route vrf VOIP 172.16.20.0 255.255.255.0 192.168.100.4 name SERVIDORES_INTERNOS_UCGS
```

Figura 3. 61: Configuración Static Route del Centro de Cómputo
Elaborado por: Autor.

  - **Rectorado**

```
RECTORADO#sho running-config | include ip route
ip route vrf DATOS 172.16.20.0 255.255.255.0 192.168.1.4 name RUTA_BCK_HACIA_SERVERS_UCSG
ip route vrf VOIP 172.16.20.0 255.255.255.0 192.168.100.4 name RUTA_BCK_HACIA_SERVERS_UCSG
```

Figura 3. 62: Configuración Static Route de Rectorado
Elaborado por: Autor.

- **Redistribución de las rutas estáticas dentro del MP – BGP**
  - **<u>Centro de Cómputo y Rectorado</u>**

```
address-family ipv4 vrf DATOS
 redistribute connected
 redistribute static
exit-address-family
!
address-family ipv4 vrf VOIP
 redistribute static
exit-address-family
```

Figura 3. 63: Redistribución de las rutas estáticas para datos y voz
Elaborado por: Autor.

- **Configuración en switches capa 2 en las facultades y Centro de Cómputo**
  - **Centro de Cómputo**

```
SW_DC_PRI#sho running-config interface gigabitEthernet 0/0
Building configuration...

Current configuration : 169 bytes
!
interface GigabitEthernet0/0
 switchport trunk allowed vlan 10,20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
end

SW_DC_PRI#sho running-config interface gigabitEthernet 0/1
Building configuration...

Current configuration : 169 bytes
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 10,20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
end
```

Figura 3. 64: Configuración del switch en Centro de Cómputo
Elaborado por: Autor.

- **Rectorado**

```
SW_DC_BCK#sho running-config interface gigabitEthernet 0/0
Building configuration...

Current configuration : 169 bytes
!
interface GigabitEthernet0/0
 switchport trunk allowed vlan 10,20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
end

SW_DC_BCK#sho running-config interface gigabitEthernet 0/1
Building configuration...

Current configuration : 169 bytes
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 10,20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
end
```

Figura 3. 65: Configuración de switch de Rectorado
Elaborado por: Autor.

- **Facultad de Medicina**

```
SW_LAN_M#sho running-config interface gigabitEthernet 0/0
Building configuration...

Current configuration : 216 bytes
!
interface GigabitEthernet0/0
 description UPLINK_HACIA_ROUTER_MPLS_MEDICINA
 switchport trunk allowed vlan 10,20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
end

SW_LAN_M#sho running-config interface gigabitEthernet 0/1
Building configuration...

Current configuration : 143 bytes
!
interface GigabitEthernet0/1
 description LAN_PC1
 switchport access vlan 10
 switchport mode access
 media-type rj45
 negotiation auto
end

SW_LAN_M#sho running-config interface gigabitEthernet 0/2
Building configuration...

Current configuration : 151 bytes
!
interface GigabitEthernet0/2
 description LAN_TELEFONO_IP
 switchport access vlan 20
 switchport mode access
 media-type rj45
 negotiation auto
end
```

Figura 3. 66: Configuración de switch de la Facultad de Medicina
Elaborado por: Autor.

- **Facultad Técnica**

```
SW_LAN_T#sho running-config interface gigabitEthernet 0/0
Building configuration...

Current configuration : 208 bytes
!
interface GigabitEthernet0/0
 description UPLIN_ROUTER_MPLS_TECNICA
 switchport trunk allowed vlan 10,20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
end

SW_LAN_T#sho running-config interface gigabitEthernet 0/1
Building configuration...

Current configuration : 143 bytes
!
interface GigabitEthernet0/1
 description LAN_PC2
 switchport access vlan 10
 switchport mode access
 media-type rj45
 negotiation auto
end

SW_LAN_T#sho running-config interface gigabitEthernet 0/2
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet0/2
 description LAN_TELEFONO_IP1
 switchport access vlan 20
 switchport mode access
 media-type rj45
 negotiation auto
```

Figura 3. 67: Configuración de switch de la Facultad Técnica
Elaborado por: Autor.

- Facultad de Economía

```
SW_LAN_T#sho running-config interface gigabitEthernet 0/0
Building configuration...

Current configuration : 208 bytes
!
interface GigabitEthernet0/0
 description UPLIN_ROUTER_MPLS_TECNICA
 switchport trunk allowed vlan 10,20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
end

SW_LAN_T#sho running-config interface gigabitEthernet 0/1
Building configuration...

Current configuration : 143 bytes
!
interface GigabitEthernet0/1
 description LAN_PC2
 switchport access vlan 10
 switchport mode access
 media-type rj45
 negotiation auto
end

SW_LAN_T#sho running-config interface gigabitEthernet 0/2
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet0/2
 description LAN_TELEFONO_IP1
 switchport access vlan 20
 switchport mode access
 media-type rj45
 negotiation auto
```

Figura 3. 68: Configuración de switch de la Facultad de Economía
Elaborado por: Autor.

3.5. Pruebas de servicio y alta disponibilidad

3.5.1. Pruebas de conectividad de datos entre las facultades de Medicina, Técnica y Economía y el área de Centro de Cómputo

- Host #1 de datos de la Facultad de Medicina

```
PC1> ping 172.16.20.2
84 bytes from 172.16.20.2 icmp_seq=1 ttl=61 time=37.754 ms
84 bytes from 172.16.20.2 icmp_seq=2 ttl=61 time=25.500 ms
84 bytes from 172.16.20.2 icmp_seq=3 ttl=61 time=37.726 ms
84 bytes from 172.16.20.2 icmp_seq=4 ttl=61 time=21.138 ms
84 bytes from 172.16.20.2 icmp_seq=5 ttl=61 time=21.345 ms

PC1> trace 172.16.20.2
trace to 172.16.20.2, 8 hops max, press Ctrl+C to stop
 1   192.168.3.1   13.414 ms  7.884 ms  16.600 ms
 2   192.168.1.1   25.134 ms  17.887 ms  34.193 ms
 3   192.168.1.4   79.938 ms  30.940 ms  26.525 ms
 4   *172.16.20.2   32.913 ms (ICMP type:3, code:3, Destination port unreachable)
```

Figura 3. 69: Verificación de conectividad del Host #1 con Centro de Cómputo mediante PING
Elaborado por: Autor.

- Host #2 de datos de la Facultad Técnica

```
PC2> ping 172.16.20.2
84 bytes from 172.16.20.2 icmp_seq=1 ttl=61 time=23.571 ms
84 bytes from 172.16.20.2 icmp_seq=2 ttl=61 time=18.539 ms
84 bytes from 172.16.20.2 icmp_seq=3 ttl=61 time=33.616 ms
84 bytes from 172.16.20.2 icmp_seq=4 ttl=61 time=27.036 ms
84 bytes from 172.16.20.2 icmp_seq=5 ttl=61 time=25.876 ms

PC2> trace 172.16.20.2
trace to 172.16.20.2, 8 hops max, press Ctrl+C to stop
 1   192.168.4.1   10.482 ms  8.307 ms  13.180 ms
 2   192.168.1.1   26.411 ms  19.200 ms  33.173 ms
 3   192.168.1.4   31.258 ms  27.215 ms  35.015 ms
 4   *172.16.20.2   42.943 ms (ICMP type:3, code:3, Destination port unreachable)
```

Figura 3. 70: Verificación de conectividad del Host #2 con Centro de Cómputo mediante PING
Elaborado por: Autor.

- Host #3 de datos de la Facultad de Economía

```
PC3> ping 172.16.20.2
84 bytes from 172.16.20.2 icmp_seq=1 ttl=61 time=25.521 ms
84 bytes from 172.16.20.2 icmp_seq=2 ttl=61 time=28.081 ms
84 bytes from 172.16.20.2 icmp_seq=3 ttl=61 time=20.720 ms
84 bytes from 172.16.20.2 icmp_seq=4 ttl=61 time=31.045 ms
84 bytes from 172.16.20.2 icmp_seq=5 ttl=61 time=26.801 ms

PC3> trace 172.16.20.2
trace to 172.16.20.2, 8 hops max, press Ctrl+C to stop
 1   192.168.5.1   10.977 ms  10.430 ms  11.621 ms
 2   192.168.1.1   16.857 ms  12.227 ms  13.230 ms
 3   192.168.1.4   36.102 ms  34.639 ms  43.837 ms
 4   *172.16.20.2   24.154 ms (ICMP type:3, code:3, Destination port unreachable)
```

Figura 3. 71: Verificación de conectividad del Host #3 con Centro de Cómputo mediante PING
Elaborado por: Autor.

3.5.2. Pruebas de conectividad de telefonía entre las facultades de Medicina, Técnica, Economía y Centro de Cómputo

- Telefonía IP de la Facultad de Medicina

```
TELEFONO_IP> ping 172.16.20.3
84 bytes from 172.16.20.3 icmp_seq=1 ttl=61 time=42.250 ms
84 bytes from 172.16.20.3 icmp_seq=2 ttl=61 time=47.068 ms
84 bytes from 172.16.20.3 icmp_seq=3 ttl=61 time=28.979 ms
84 bytes from 172.16.20.3 icmp_seq=4 ttl=61 time=62.833 ms
84 bytes from 172.16.20.3 icmp_seq=5 ttl=61 time=57.661 ms

TELEFONO_IP> trace 172.16.20.3
trace to 172.16.20.3, 8 hops max, press Ctrl+C to stop
 1   192.168.6.1   29.832 ms  43.596 ms  17.838 ms
 2   192.168.100.1   32.338 ms  48.075 ms  75.782 ms
 3   192.168.100.4   47.555 ms  56.186 ms  34.732 ms
 4   *172.16.20.3   40.461 ms (ICMP type:3, code:3, Destination port unr
```

Figura 3. 72: Verificación de telefonía IP de la Facultad de Medicina con Centro de Cómputo usando PING
Elaborado por: Autor.

- Telefonía IP1 de la Facultad Técnica

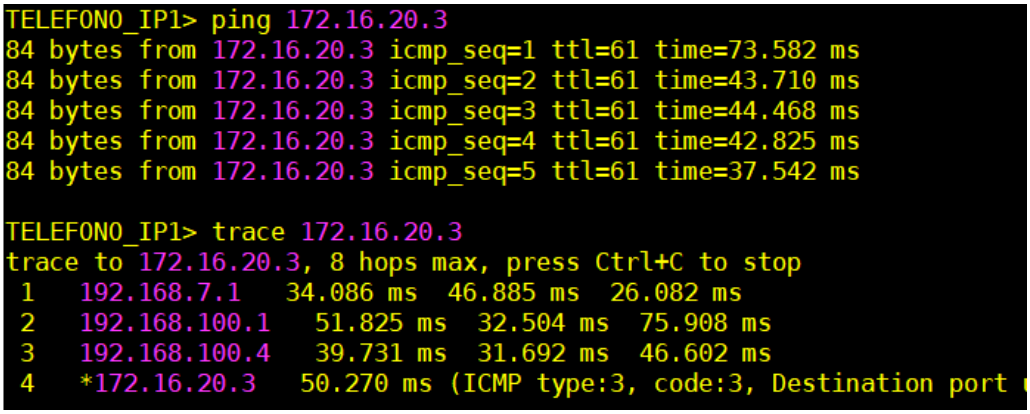


Figura 3. 73: Verificación de telefonía IP de la Facultad Técnica con Centro de Cómputo usando PING
Elaborado por: Autor.

- Telefonía IP2 de la Facultad de Economía

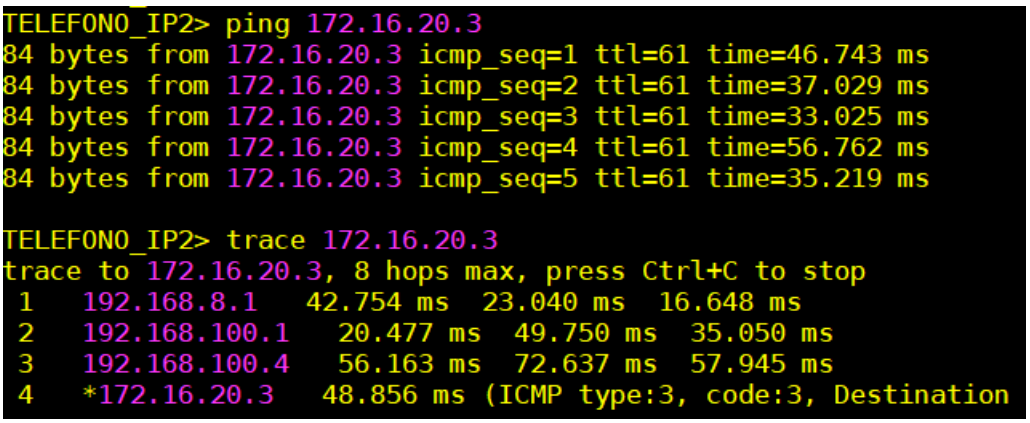


Figura 3. 74: Verificación de telefonía IP de la Facultad de Economía con Centro de Cómputo usando PING
Elaborado por: Autor.

3.5.3. Pruebas de conectividad apagando el router ubicado en el Centro de Cómputo

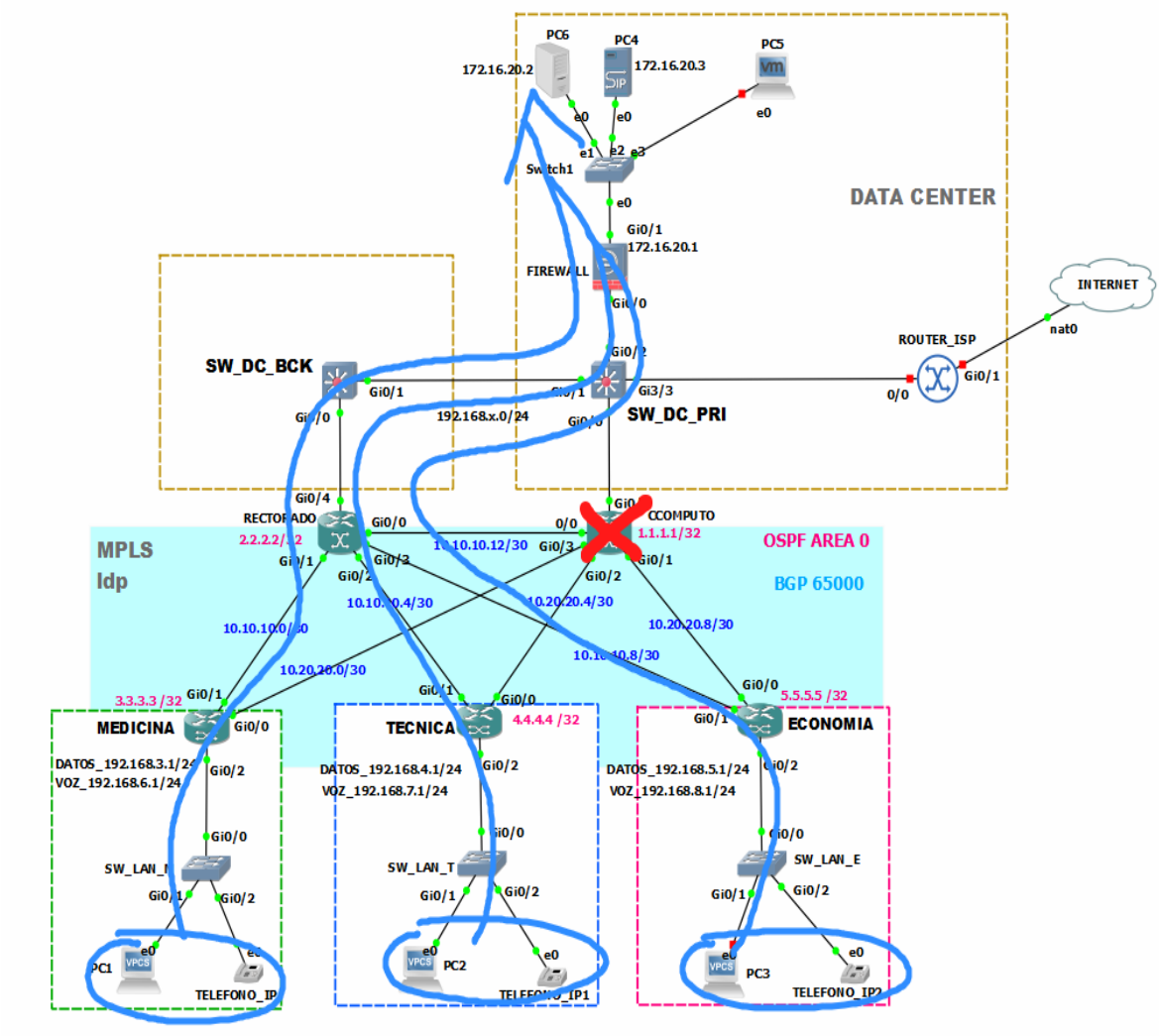


Figura 3. 75: Ruta de los datos de las facultades hacia el servidor 172.16.20.2
Elaborado por: Autor.

- Host #1 de datos de la Facultad de Medicina

```
PC1> ping 172.16.20.2
84 bytes from 172.16.20.2 icmp_seq=1 ttl=61 time=84.451 ms
84 bytes from 172.16.20.2 icmp_seq=2 ttl=61 time=54.903 ms
84 bytes from 172.16.20.2 icmp_seq=3 ttl=61 time=50.520 ms
84 bytes from 172.16.20.2 icmp_seq=4 ttl=61 time=49.378 ms
84 bytes from 172.16.20.2 icmp_seq=5 ttl=61 time=40.846 ms

PC1> trace 172.16.20.2
trace to 172.16.20.2, 8 hops max, press Ctrl+C to stop
 1   192.168.3.1   23.165 ms  27.308 ms  42.177 ms
 2   192.168.1.2   18.438 ms  56.613 ms  25.419 ms
 3   192.168.1.4   60.036 ms  60.146 ms  60.129 ms
 4   *172.16.20.2   56.824 ms (ICMP type:3, code:3, Destination port
```

Figura 3. 76: Verificación de conectividad desde el Host de Medicina usando PING
Elaborado por: Autor.

- Host #2 de datos de la Facultad Técnica

```
PC2> ping 172.16.20.2
84 bytes from 172.16.20.2 icmp_seq=1 ttl=61 time=96.272 ms
84 bytes from 172.16.20.2 icmp_seq=2 ttl=61 time=63.728 ms
84 bytes from 172.16.20.2 icmp_seq=3 ttl=61 time=61.692 ms
84 bytes from 172.16.20.2 icmp_seq=4 ttl=61 time=49.321 ms
84 bytes from 172.16.20.2 icmp_seq=5 ttl=61 time=53.298 ms

PC2> trace 172.16.20.2
trace to 172.16.20.2, 8 hops max, press Ctrl+C to stop
 1   192.168.4.1   27.206 ms  22.544 ms  19.623 ms
 2   192.168.1.2   18.954 ms  32.500 ms  29.656 ms
 3   192.168.1.4   39.930 ms  51.063 ms  54.028 ms
 4   *172.16.20.2   53.322 ms (ICMP type:3, code:3, Destination port
```

Figura 3. 77: Verificación de conectividad desde el Host de la Técnica usando PING
Elaborado por: Autor.

- Host #3 de datos de la Facultad de Economía

```
PC3> ping 172.16.20.2
84 bytes from 172.16.20.2 icmp_seq=1 ttl=61 time=79.944 ms
84 bytes from 172.16.20.2 icmp_seq=2 ttl=61 time=45.823 ms
84 bytes from 172.16.20.2 icmp_seq=3 ttl=61 time=51.002 ms
84 bytes from 172.16.20.2 icmp_seq=4 ttl=61 time=74.557 ms
84 bytes from 172.16.20.2 icmp_seq=5 ttl=61 time=49.714 ms

PC3> trace 172.16.20.2
trace to 172.16.20.2, 8 hops max, press Ctrl+C to stop
 1   192.168.5.1   32.627 ms  21.345 ms  18.323 ms
 2   192.168.1.2   33.520 ms  23.710 ms  30.847 ms
 3   192.168.1.4   73.345 ms  69.791 ms  62.799 ms
 4   *172.16.20.2   57.934 ms (ICMP type:3, code:3, Destination port
```

Figura 3. 78: Verificación de conectividad desde el Host de Economía usando PING
Elaborado por: Autor.

3.5.4. Pruebas de conectividad desconectando la interface WAN del router del Centro de Cómputo que conecta con la Facultad Técnica

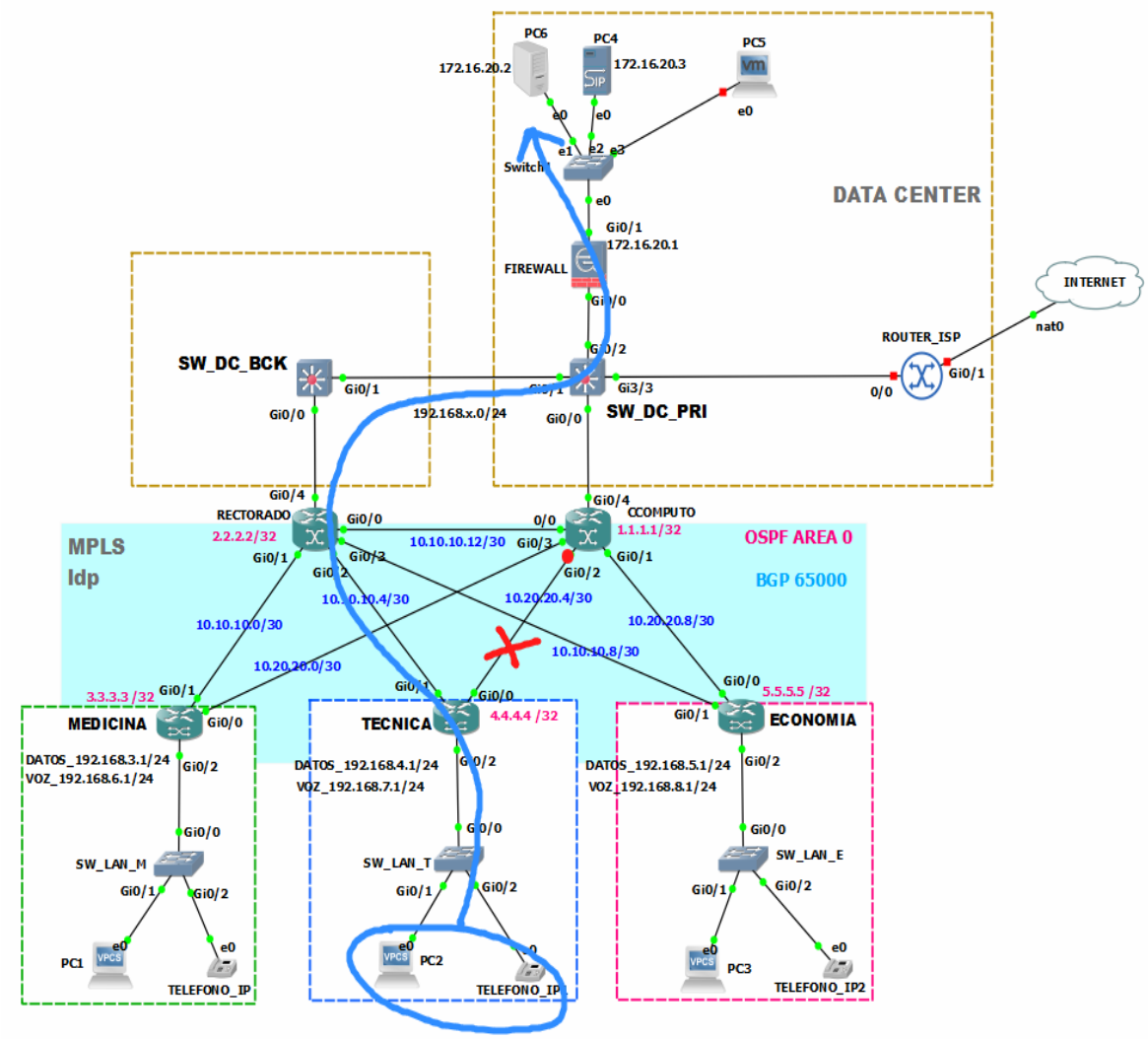


Figura 3. 79: Ruta de la telefonía IP y datos de la Facultad Técnica al servidor 172.16.20.2

Elaborado por: Autor.

- Host #2 de datos de la Facultad Técnica

```
PC2> ping 172.16.20.2
84 bytes from 172.16.20.2 icmp_seq=1 ttl=60 time=70.101 ms
84 bytes from 172.16.20.2 icmp_seq=2 ttl=60 time=37.708 ms
84 bytes from 172.16.20.2 icmp_seq=3 ttl=60 time=45.315 ms
84 bytes from 172.16.20.2 icmp_seq=4 ttl=60 time=45.845 ms
84 bytes from 172.16.20.2 icmp_seq=5 ttl=60 time=42.337 ms

PC2> trace 172.16.20.2
trace to 172.16.20.2, 8 hops max, press Ctrl+C to stop
 1   192.168.4.1   17.317 ms  24.410 ms  31.722 ms
 2   192.168.1.2   41.865 ms  30.265 ms  38.086 ms
 3   192.168.1.4   57.178 ms  62.887 ms  80.531 ms
 4   *172.16.20.2   73.905 ms (ICMP type:3, code:3, Destination
```

Figura 3. 80: Verificación de conectividad desde el Host de la Técnica a través de PING

Elaborado por: Autor.

- Telefonía IP1 de la Facultad Técnica

```
TELEFONO_IP1> ping 172.16.20.3
84 bytes from 172.16.20.3 icmp_seq=1 ttl=60 time=48.713 ms
84 bytes from 172.16.20.3 icmp_seq=2 ttl=60 time=65.691 ms
84 bytes from 172.16.20.3 icmp_seq=3 ttl=60 time=41.374 ms
84 bytes from 172.16.20.3 icmp_seq=4 ttl=60 time=98.567 ms
84 bytes from 172.16.20.3 icmp_seq=5 ttl=60 time=60.507 ms

TELEFONO_IP1> trace 172.16.20.3
trace to 172.16.20.3, 8 hops max, press Ctrl+C to stop
 1   192.168.7.1   11.471 ms  15.028 ms  18.140 ms
 2   192.168.100.2   41.595 ms  20.061 ms  23.809 ms
 3   192.168.100.4   72.062 ms  51.767 ms  70.652 ms
 4   *172.16.20.3   53.689 ms (ICMP type:3, code:3, Destination port
```

Figura 3. 81: Verificación de telefonía IP de la Facultad Técnica con Centro de Cómputo a través de PING
Elaborado por: Autor.

3.5.5. Pruebas de conectividad desconectando la interfaz WAN del router del Centro de Cómputo que conecta con la Facultad Técnica y Rectorado como site alterno

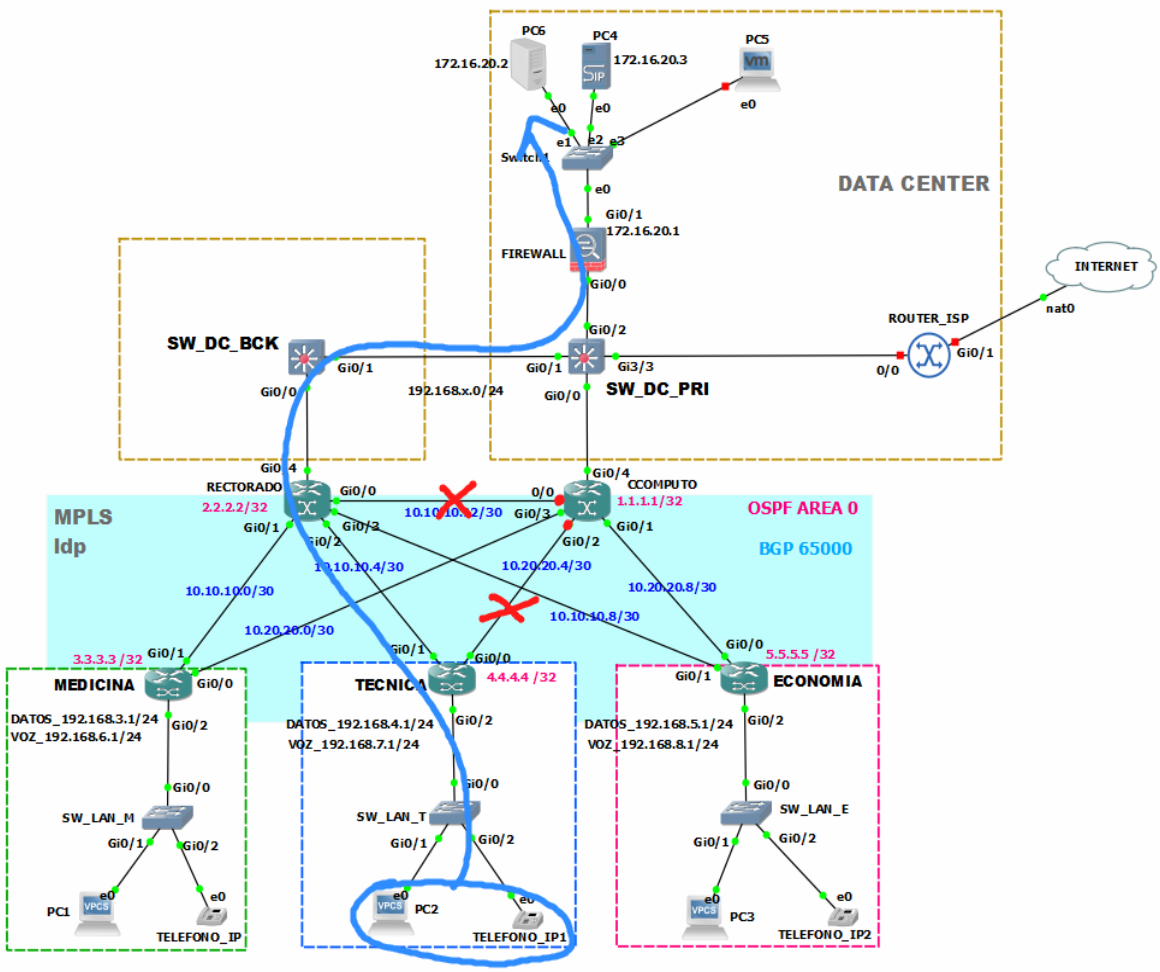


Figura 3. 82: Ruta de la telefonía IP y datos de la Facultad Técnica al servidor 172.16.20.2 pasando por el site alterno
Elaborado por: Autor.

- Host #2 datos de la Facultad Técnica

```
PC2> ping 172.16.20.2
84 bytes from 172.16.20.2 icmp_seq=1 ttl=59 time=63.066 ms
84 bytes from 172.16.20.2 icmp_seq=2 ttl=59 time=68.245 ms
84 bytes from 172.16.20.2 icmp_seq=3 ttl=59 time=70.194 ms
84 bytes from 172.16.20.2 icmp_seq=4 ttl=59 time=63.484 ms
84 bytes from 172.16.20.2 icmp_seq=5 ttl=59 time=63.380 ms

PC2> trace 172.16.20.2
trace to 172.16.20.2, 8 hops max, press Ctrl+C to stop
 1   192.168.4.1   52.275 ms  19.777 ms  35.889 ms
 2   192.168.1.2   33.219 ms  23.779 ms  21.178 ms
 3   192.168.1.4   49.512 ms  68.568 ms  76.167 ms
 4   *172.16.20.2   68.206 ms (ICMP type:3, code:3, Destination port
```

Figura 3. 83: Verificación de conectividad desde el Host de la Técnica a través de PING
Elaborado por: Autor.

- Telefonía IP1 de la Facultad Técnica

```
TELEFONO_IP1> ping 172.16.20.3
84 bytes from 172.16.20.3 icmp_seq=1 ttl=59 time=72.325 ms
84 bytes from 172.16.20.3 icmp_seq=2 ttl=59 time=56.491 ms
84 bytes from 172.16.20.3 icmp_seq=3 ttl=59 time=43.564 ms
84 bytes from 172.16.20.3 icmp_seq=4 ttl=59 time=76.933 ms
84 bytes from 172.16.20.3 icmp_seq=5 ttl=59 time=58.825 ms

TELEFONO_IP1> trace 172.16.20.3
trace to 172.16.20.3, 8 hops max, press Ctrl+C to stop
 1   192.168.7.1   36.448 ms  20.164 ms  31.917 ms
 2   192.168.100.2   25.950 ms  28.542 ms  21.359 ms
 3   192.168.100.4   67.591 ms  58.825 ms  70.473 ms
 4   *172.16.20.3   57.200 ms (ICMP type:3, code:3, Destination port
```

Figura 3. 84: Verificación de telefonía IP de la Facultad Técnica con Centro de Cómputo a través de PING
Elaborado por: Autor.

3.5.6. Pruebas de conectividad normalizando las conexiones deshabilitadas

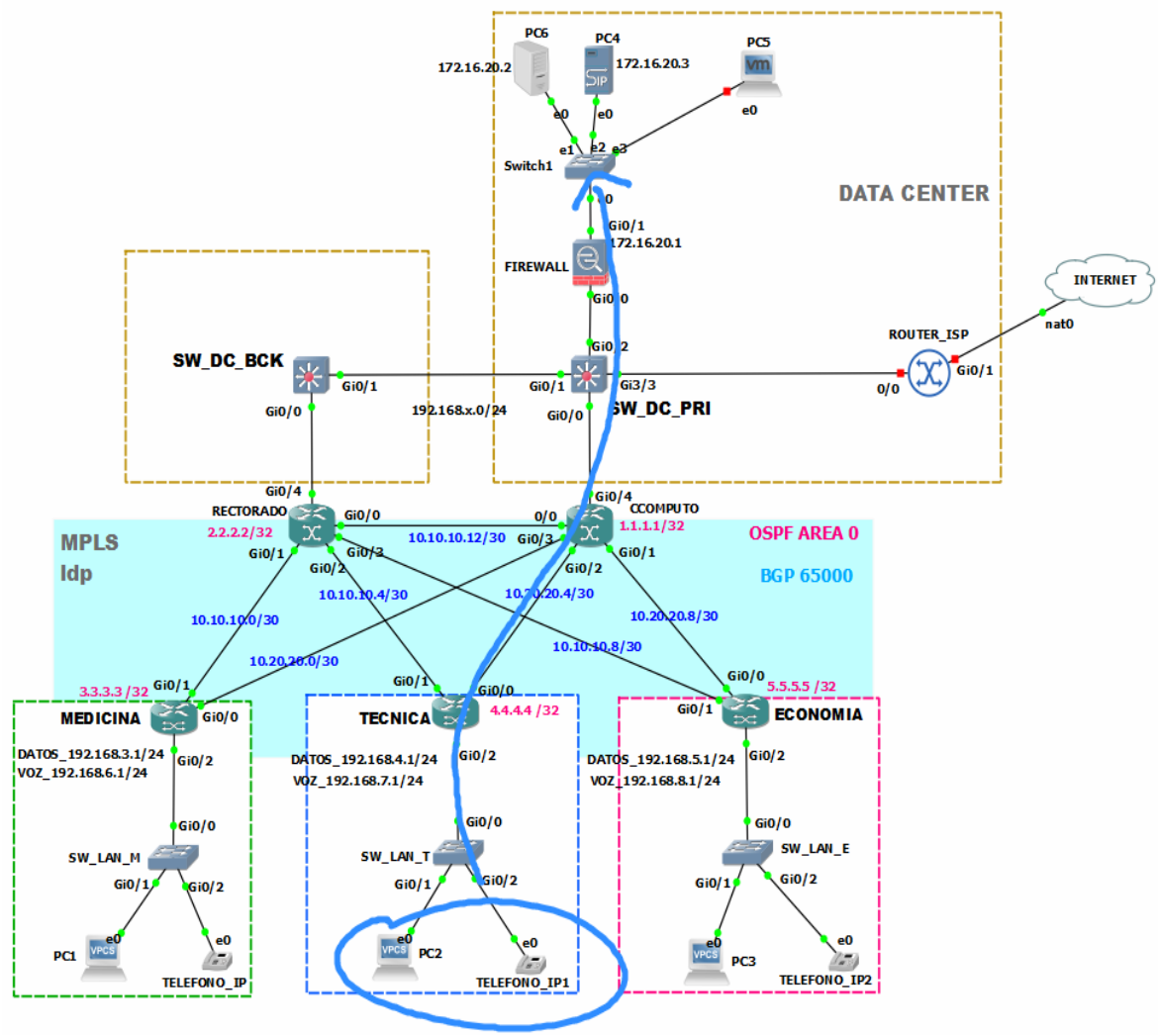


Figura 3. 85: Ruta de la telefonía IP y datos de la Facultad Técnica con la conectividad normal
Elaborado por: Autor.

- Host #2 de datos de la Facultad Técnica

```
PC2> ping 172.16.20.2
84 bytes from 172.16.20.2 icmp_seq=1 ttl=61 time=52.833 ms
84 bytes from 172.16.20.2 icmp_seq=2 ttl=61 time=51.451 ms
84 bytes from 172.16.20.2 icmp_seq=3 ttl=61 time=52.730 ms
84 bytes from 172.16.20.2 icmp_seq=4 ttl=61 time=57.539 ms
84 bytes from 172.16.20.2 icmp_seq=5 ttl=61 time=38.745 ms

PC2> trace 172.16.20.2
trace to 172.16.20.2, 8 hops max, press Ctrl+C to stop
 1   192.168.4.1   24.838 ms  23.640 ms  25.868 ms
 2   192.168.1.1   28.675 ms  27.897 ms  30.347 ms
 3   192.168.1.4   76.758 ms  63.135 ms  46.175 ms
 4   *172.16.20.2   62.106 ms (ICMP type:3, code:3, Destination port
```

Figura 3. 86: Verificación de conectividad desde el Host de la Técnica al switch del Centro de Cómputo a través de PING
Elaborado por: Autor.

- Telefonía IP1 de la Facultad Técnica

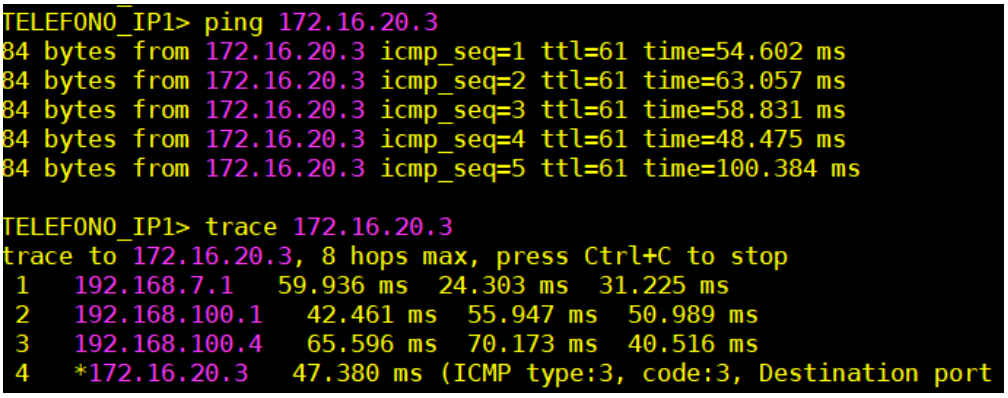


Figura 3. 87: Verificación de telefonía IP de la Facultad Técnica al switch del Centro de Cómputo a través de PING
Elaborado por: Autor.

Conclusiones.

- La red MPLS emulada a través de GNS3 logró cumplir con las exigencias que una red de campus universitaria exige, alcanzando a mantener la continuidad del servicio simulando una caída WAN.
- Se logró segmentar el tráfico de voz y datos mediante una infraestructura de red compartida como MPLS por medio de VRF's.
- Se comprendió el impacto del riesgo en tener una red plana sin un protocolo de conmutación de etiqueta que junto a MP–BGP y HSRP logren incrementar la disponibilidad de los servicios en la red.

Recomendaciones.

- Centralizar en la elaboración de prototipos de emulación de las redes MPLS aplicado en el GNS3 a los estudiantes de la Carrera de Ingeniería en Telecomunicaciones.

Bibliografía

Alam, T., Masum Refat, C. M., Md Imran, A. Z., Rashid, S. Z., Humayun Kabir, M., Tarek, R. H., & Gafur, A. (2018). Design and Implementation of a Secured Enterprise Network using Dynamic Multipoint VPN with HSRP Protocol. *2018 International Conference on Innovations in Science, Engineering and Technology (ICISET)*, 367–371. https://doi.org/10.1109/ICISET.2018.8745601

Anwar, U., Teng, J., Umair, H. A., & Sikander, A. (2019). Performance Analysis and Functionality Comparison of FHRP Protocols. *2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*, 111–115. https://doi.org/10.1109/ICCSN.2019.8905333

Fathima, K. M. M. (2018). A Survey on Multiprotocol Label Switching in Virtual Private Networks. *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on*, 737–740. https://doi.org/10.1109/I-SMAC.2018.8653745

Fonseca, P., Mota, E. S., Bennesby, R., & Passito, A. (2019). BGP Dataset Generation and Feature Extraction for Anomaly Detection. *2019 IEEE Symposium on Computers and Communications (ISCC)*, 1–6. https://doi.org/10.1109/ISCC47284.2019.8969619

Haiyan, Y. (2018). Application of Vlan and HSRP Technology in the Dual Core Campus Network. *2018 International Conference on Smart Grid and Electrical Automation (ICSGEA)*, 332–333. https://doi.org/10.1109/ICSGEA.2018.00088

Hlozak, M., Frnda, J., Chmelikova, Z., & Voznak, M. (2014). Analysis of Cisco and Huawei routers cooperation for MPLS network design. *2014 22nd Telecommunications Forum Telfor (TELFOR)*, 115–118. https://doi.org/10.1109/TELFOR.2014.7034370

Imran, Mohd., Khan, M. A., & Abdul Qadeer, M. (2018). Design and Simulation of Traffic Engineering using MPLS in GNS3 Environment. *2018 Second International Conference on Computing Methodologies and Communication (ICCMC)*, 1026–1030. https://doi.org/10.1109/ICCMC.2018.8487981

Krit, S., & Haimoud, E. (2017). Overview of firewalls: Types and policies: Managing windows embedded firewall programmatically. *2017 International Conference on Engineering & MIS (ICEMIS)*, 1–7. https://doi.org/10.1109/ICEMIS.2017.8273003

Lehocine, M. B., & Batouche, M. (2017). Flexibility of managing VLAN filtering and segmentation in SDN networks. *2017 International Symposium on Networks, Computers and Communications (ISNCC)*, 1–6. https://doi.org/10.1109/ISNCC.2017.8071999

Liu, S., Wang, H., Liu, J., & Xian, M. (2019). Feasibility analysis of network security teaching platform based on KVM and GNS3. *2019 International Conference on Information Technology and Computer Application (ITCA)*, 310–313. https://doi.org/10.1109/ITCA49981.2019.00075

Mehraban, S., Vora, Komil. B., & Upadhyay, D. (2018). Deploy Multi Protocol Label Switching (MPLS) Using Virtual Routing and Forwarding (VRF). *2018 2nd International Conference on Trends in Electronics and*

Informatics (ICOEI), 543–548. https://doi.org/10.1109/ICOEI.2018.8553949

Ramadaa, I., Ozegovic, J., & Pekic, V. (2015). Network performance monitoring within MPLS traffic engineering enabled networks. *2015 23rd International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 315–319. https://doi.org/10.1109/SOFTCOM.2015.7314107

Robbins, D. S. (2018). Using Protocol Redundancy to Enhance OSPF Network System Survivability. *SoutheastCon 2018*, 1–7. https://doi.org/10.1109/SECON.2018.8479134

Soewito, B., Gunawan, F. E., Afdhal, S., & Antonyova, A. (2017). Analysis of quality network using MPLS and non MPLS. *2017 International Seminar on Intelligent Technology and Its Applications (ISITIA)*, 1–4. https://doi.org/10.1109/ISITIA.2017.8124044

Tongkaw, S., & Tongkaw, A. (2018). Multi-VlanDesign Over IPSec VPN for Campus Network. *2018 IEEE Conference on Wireless Sensors (ICWiSe)*, 66–71. https://doi.org/10.1109/ICWISE.2018.8633293

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Cortés Hincapié, Marco Joel** con C.C: # 080281854-2 autor del Trabajo de Titulación: **Diseño y emulación de una red IP/MPLS para interconectar las facultades de la UCSG con el centro de cómputo y rectorado como site alterno** previo a la obtención del título de **INGENIERO EN TELECOMUNICACIONES** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 10 de marzo del 2021

f. _____

Nombre: Cortés Hincapié, Marco Joel

C.C: 080281854-2

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Diseño y emulación de una red IP/MPLS para interconectar las facultades de la UCSG con el centro de cómputo y rectorado como site alterno		
AUTOR(ES)	CORTÉS HINCAPIÉ, MARCO JOEL		
REVISOR(ES)/TUTOR(ES)	M. Sc. Suárez Murillo, Efraín Oswaldo		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Educación Técnica para el Desarrollo		
CARRERA:	De Telecomunicaciones		
TITULO OBTENIDO:	Ingeniero en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	10 de marzo del 2021	**No. DE PÁGINAS:**	68
ÁREAS TEMÁTICAS:	Redes y sistemas telemáticos, Transmisiones		
PALABRAS CLAVES/ KEYWORDS:	MPLS, Network, Routing, OSPF, GNS3, HSRP		

RESUMEN/ABSTRACT (150-250 palabras):

Para el desarrollo de la presente optimización de red, se optó por la tecnología MPLS L3VPN muy utilizada para ambientes, en el cual, se requiere optimizar la conmutación de paquetes y aislar el tráfico entre diferentes tipos de fuentes como datos, telefonía y vídeo. Lo que permite que MPLS se ajuste a las redes modernas es el uso de etiquetas para la conmutación del tráfico y uso en conjunto de MP – BGP para garantizar que no exista superposición en los prefijos que se transportan dentro de una red. La potencia que aporta MPLS no es eficaz sino se trabaja con una pila de protocolos como OSPF, BGP, MP – BGP. Se emuló una red prototipo campus universitario para demostrar la eficacia que MPLS y su pila de protocolos aportan para brindar alta disponibilidad a nivel WAN y en incrementar la disponibilidad de los servicios en el datacenter de la UCSG hacia las facultades.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-9-59653622	E-mail: marcocortesh@outlook.com
CONTACTO CON LA INSTITUCIÓN: COORDINADOR DEL PROCESO DE UTE	**Nombre:** Palacios Meléndez, Edwin Fernando	
	Teléfono: +593-9-67608298	
	E-mail: edwin.palacios@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	