UCLV
Universidad Central
"Marta Abreu" de Las Villas

FIE
Facultad de
Ingeniería Eléctrica

TRABAJO DE DIPLOMA

"Laboratorios para la enseñanza de redes de transporte de banda ancha"

Autor: Yordano Cardenas Santos

Tutor: Ing: Ernesto Pérez Peláez

Santa Clara 2018
Año 60 del Triunfo de la Revolución

UCLV
Universidad Central
"Marta Abreu" de Las Villas

FIE
Facultad de
Ingeniería Eléctrica

TRABAJO DE DIPLOMA

"Laboratorios para la enseñanza de redes de transporte de banda ancha"

Autor: Yordano Cardenas Santos

E-mail: yordanoc@uclv.cu

Tutor: Ing: Ernesto Pérez Peláez

E-mail: eppelaez@uclv.edu.cu

Santa Clara 2018
Año 60 del Triunfo de la Revolución

PENSAMIENTO

"La ciencia se compone de errores, que a su vez son los pasos hacia la verdad"

Jules Verne

DEDICATORIA

A mi madre Olga Lidia, a mi abuela Victoria y a mi abuelo Gertrudis por su apoyo incondicional en todos los momentos de mi vida.

AGRADECIMIENTOS

A mi madre Olga Lidia y mi abuela Victoria por hacer de mi la persona que soy hoy, por su apoyo incondicional en todos los momentos de mi vida y por estar siempre a mi lado.

A mi abuelo Gertrudis Santos por ser mi ejemplo a seguir durante toda mi vida.

A mi novia Mónica por ser la persona que siempre ha estado a mi lado en los momentos más difíciles de la carrera y de mi vida en los últimos años.

A toda mi familia, en especial mi tío Tony, mis tías y mis primos por su apoyo en todos los momentos de mi vida.

A mis suegros Alberto y Tania por su ayuda, apoyo y preocupación en cada momento.

A todos mis amigos que de una forma u otra han estado presente a lo largo de mi carrera.

A mis amigos Elizabeth y Allan por su ayuda y contribución en este trabajo, A Antonio Varona por sus instrucciones en los momentos necesarios.

A todos los profesores de la carrera de Telecomunicaciones y Electrónica que han influido en mi formación profesional.

A mi tutor Ernesto Pérez Peláez que me ha apoyado durante el proceso de la tesis, con consejos oportunos en cada momento.

A todos los que me han ayudado de una forma u otra a llegar hasta aquí.

TAREAS TÉCNICAS

1. Caracterización de las tecnologías de las redes de transporte de banda ancha.
2. Determinación de las herramientas de simulación y emulación en las redes de transporte de banda ancha.
3. Búsqueda de trabajos de simulación y emulación usados en el Simulador de Redes Gráficos, GNS3, en las redes de transporte de banda ancha.
4. Selección de los laboratorios de las redes de transporte de banda ancha.
5. Preparación de las guías de los laboratorios y los escenarios con la ejecución de la simulación con GNS3.
6. Evaluación del comportamiento de las redes de transporte de banda ancha para cada uno de los laboratorios.
7. Análisis de los resultados obtenidos en los diferentes escenarios.
8. Elaboración del informe del trabajo de diploma.

RESUMEN

El presente trabajo de diploma se enfoca en la elaboración de nuevos laboratorios para la disciplina de Sistemas de Telecomunicaciones, enfocados en temas relacionados con las asignaturas de Redes de Comunicaciones. Estos laboratorios han sido elaborados con la herramienta de simulación y emulación GNS3.

Para el desarrollo de este trabajo fue necesario realizar una búsqueda de información que permitió la conformación del marco teórico - conceptual de la investigación y la selección de los nuevos laboratorios de la disciplina.

En este trabajo se adquieren una serie de habilidades importantes en específico en las redes de transporte de banda ancha como MPLS, VPN/MPLS, L2VPN y L3VPN, así como la implementación de protocolos como: OSPF, LDP, RIP, creación de VRF. Se evalúan y analizan los resultados de los laboratorios para cada escenario.

TABLA DE CONTENIDOS

Contenido

INTRODUCCIÓN

El acelerado avance de las técnicas de procesamiento y de las tecnologías para la transmisión de la información; así como de las tecnologías de redes de transporte de banda ancha han provocado que las redes de comunicaciones entren en una era de continuas transformaciones, esto ha llevado a los proveedores de tecnologías, las empresas de telecomunicaciones, y a las universidades, a desarrollar principalmente tres técnicas para evaluar el desempeño de las diferentes tecnologías de red: el análisis, la simulación y la experimentación. Sin embargo, a partir de lo complejas que se hacen las nuevas topologías, los protocolos y el tráfico de las redes, se hace casi imposible construir un modelo analítico que pueda cubrir todos los aspectos técnicos, de esta forma la mayoría de las técnicas analíticas son utilizadas solamente para la evaluación del desempeño de una red en funcionamiento. Por otro lado, construir una red experimental para evaluar el desempeño de la misma generalmente resulta costoso. Por estas razones, los programas computacionales que permiten simular y emular diferentes tecnologías de comunicaciones, son ampliamente utilizados; ya que facilitan el análisis de las redes. Por estos motivos se han creado disimiles herramientas computacionales para la simulación de redes entre las cuales se destacan Cisco Packet Tracer, NCTUns, COMNET III, OPNET Modeler, OMNET ++, Network Simulator, GNS3, entre otros. Estas herramientas son utilizadas por empresas y universidades como medio de apoyo para brindar una mayor calidad en la formación de habilidades en el campo de los Sistemas de Telecomunicaciones y en particular en las redes de banda ancha. Mediante el uso de estas plataformas para la emulación y simulación de redes se pueden desarrollar proyectos que permitan sustituir las carencias de laboratorios de telecomunicaciones los cuales necesitan una gran infraestructura para su creación. Por la importancia que esto tiene, en la Universidad Central de Las Villas se han desarrollado estudios que abordan las diferentes herramientas de simulación y emulación con el paso de los años. Por lo que se han realizado diversos proyectos con el objetivo de actualizar e incorporar nuevos métodos que permitan el aprendizaje y la formación del profesional en correspondencia con los avances tecnológicos actuales. En el desarrollo de laboratorios de redes de banda ancha es importante utilizar una plataforma como GNS3 la cual es un software libre, multiplataforma, con un principio de funcionamiento basado sobre todo

en técnicas de virtualización que permite la emulación de hardware reales, además que trae consigo posibilidades que sugieren su utilización tanto en la enseñanza como en la investigación.

Por otra parte, es de importancia hablar de la actualidad que presentan las tecnologías de redes de transporte de banda ancha, cuando se habla de redes de banda ancha se debe dejar atrás las ya casi obsoletas tecnologías como Frame Relay, ATM y centrarnos en tecnologías actuales como es el caso MPLS, MPLS-TP y de las tendencias más actuales que están encaminada a VPN/MPLS la cual permite utilizar esta infraestructura para crear diferentes tipos de VPN basados en IP, como son, L2VPN, L3PVN, entre otras. Estas permiten a los proveedores utilizar MPLS como medio de transporte para crear túneles entre los sitios privados virtuales, estas tecnologías continúan en constante desarrollo por lo que surge la siguiente interrogante: ¿Cómo encaminar la enseñanza de las tecnologías de redes de transporte de banda ancha?

Por tanto, es necesario tener en cuenta:

- ¿Cuáles son las redes de transporte de banda ancha?
- ¿Qué herramienta se debe implementar para la elaboración de los laboratorios?
- ¿De qué forma se deben organizar y estructurar los laboratorios para desarrollar las habilidades en la enseñanza de las redes de transporte de banda ancha?
- ¿Cuál es la eficacia de los laboratorios de redes de transporte de banda ancha creados?

Por ello el objetivo general de este trabajo es: “Elaborar los laboratorios para la enseñanza de las redes de transporte de banda ancha.”

Del cual se derivan los siguientes objetivos específicos:

- Caracterizar las redes de transporte de banda ancha.
- Seleccionar la herramienta a utilizar para la elaboración de los laboratorios de redes de transporte de banda ancha.
- Elaborar los laboratorios para la enseñanza de redes de transporte de banda ancha.
- Evaluar los laboratorios elaborados en los escenarios seleccionados.

Estructura del informe.

El informe está estructurado de la siguiente forma: introducción, capitulario, conclusiones, recomendaciones, referencias bibliográficas, glosario de términos y anexos. A continuación, se resume brevemente el contenido de los capítulos.

En la introducción queda definida la importancia, actualidad y necesidad del tema que se aborda y se hace alusión a las diferentes tecnologías de redes de transporte de banda ancha y a la necesidad de realizar laboratorios para su enseñanza.

Capítulo 1: Redes de transporte de Banda Ancha.

- Se dedica a la caracterización de la actualidad de las redes de transporte de banda ancha, así como las diferentes herramientas de emulación y simulación de redes.

Capítulo 2: Elaboración de laboratorios para la enseñanza de redes de transporte de banda ancha.

- Se elaboran los laboratorios de redes de transporte de banda ancha, utilizando la herramienta de simulación y emulación seleccionada.

Capítulo 3: Evaluación de los resultados obtenidos de los laboratorios.

- Se evalúan los resultados obtenidos del desarrollo de los laboratorios en los diferentes escenarios

CAPÍTULO 1: REDES DE TRANSPORTE DE BANDA ANCHA

En el presente capítulo se realiza una caracterización de los contenidos relacionados con las redes de transporte de banda ancha. Se define la herramienta a utilizar para la creación de laboratorios para la enseñanza de las mismas.

1.1 Redes de transporte de Banda Ancha.

El concepto de redes de transporte de banda ancha está referido a la capacidad de transmisión cada vez más veloz de datos. Dado el avance de la tecnología y el diferente nivel de desarrollo de las redes de transporte de banda ancha a nivel mundial, no existe consenso respecto a partir de que velocidad se considera banda ancha. De acuerdo con la Unión Internacional de las Telecomunicaciones – UIT, se considera banda ancha a la capacidad de transmisión considerablemente más rápida que la velocidad primaria de la red digital de servicios integrados (RDSI).

La banda ancha no es un concepto estático ya que las velocidades de acceso a Internet se aumentan constantemente. La velocidad mínima para considerarse banda ancha varía entre los países e, incluso, dentro de un país la autoridad puede considerar como banda ancha un valor de velocidad distinto de aquel que el operador estima como banda ancha. Se ha propuesto que una manera para determinar la existencia de banda ancha es aquella basada en los servicios a los que se puede tener acceso (rápida descarga de archivos de Internet, calidad de audio equivalente a un CD, servicios de voz y videos interactivos). La amplia disponibilidad de banda ancha se considera un factor para la innovación, la productividad, el crecimiento económico y la inversión extranjera. Al concepto de banda ancha hay que atribuirle otras características, además de la velocidad, como son la interactividad, digitalización y conexión o capacidad de acceso (función primordial de la banda ancha).[1]

1.1.1 MPLS

MPLS (MultiProtocol Label Switching) es un protocolo de conmutación por etiquetas definido para funcionar sobre múltiples protocolos como Frame Realy, ATM, Ethernet o cualquiera sobre el que pueda funcionar PPP. Las principales motivaciones para su desarrollo son la

ingeniería de tráfico, la diferenciación de clases de servicio, y las redes privadas virtuales (VPN). En un principio, también proporcionaba una mayor velocidad puesto que los enrutadores sólo deben mirar la etiqueta para conmutar y no leer la cabecera de la capa 3 para después decidir por dónde enrutar.

MPLS aprovecha lo mejor de la capa 2, la rápida conmutación, sin perder de vista la capa 3, para no perder sus posibilidades. Esto se consigue separando la función de conmutación de la de enrutamiento. MPLS hace más viable la ingeniería de tráfico, permite enrutamiento rápido (porque en realidad, hace conmutación, pero con información de enrutado), permite que los equipos de reenvío sean más baratos si solo deben entender paquetes etiquetados, permite ofrecer QoS (calidad de servicio) basándose en diferentes CoS (clases de servicio), hace más fáciles y flexibles las VPN, y además parece el primer paso para conseguir redes totalmente ópticas (ya que se decide por dónde enviar el paquete según lo que diga la etiqueta y no hace falta procesar la cabecera de orden 3; es decir, aunque las decisiones del enrutado sean en el dominio eléctrico, la conmutación podría ser óptica).

MPLS utiliza una parte de control, que se encarga de las decisiones de encaminamiento, pero no construye una tabla en la que consultar la dirección IP de los paquetes que lleguen, sino que informa a la parte de reenvío, que construye una tabla con etiquetas; así no es necesario mirar la cabecera de la capa 3, y decidir para cada paquete, porque la decisión ya está tomada para cada etiqueta. El único enrutador que tiene que hacer funciones de enrutamiento es el primero, que tiene que decidir que etiqueta coloca a cada paquete. Todos los paquetes que llevan la misma etiqueta forman un grupo que se denomina Forwarding Equivalent Class (FEC).

1.1.1.1 Arquitectura MPLS.

En general, la diferencia principal entre MPLS y las tecnologías WAN utilizadas tradicionalmente es la forma en la que se asignan las etiquetas y la capacidad de cargar una pila de etiquetas asociadas a un paquete.

El envío de paquetes en MPLS está en un fuerte contraste con los entornos de redes sin conexión actuales, donde se analiza el paquete en cada salto.

Un concepto importante dentro de MPLS es el de LSP (Label Switch Path) que es un camino específico de tráfico a través de la red MPLS, el cual se crea utilizando protocolos de

distribución de etiquetas, tales como RSVP-TE o CR-LDP, si bien el más comúnmente utilizado es el primero de ellos.

El LDP posibilita que los nodos MPLS se descubran y establezcan comunicación entre ellos, a fin de informarse del valor y significado de las etiquetas que serán utilizadas en los enlaces.

Básicamente, la arquitectura del protocolo puede dividirse en dos elementos fundamentales: los componentes de envío, y los componentes de control. Los primeros utilizan una base de datos de etiquetas de envío mantenida por un conmutador de etiquetas para poner en marcha el envío de paquetes de datos basados en etiquetas llevadas por paquetes. Los componentes de control, por su parte, son responsables de crear y mantener la información de envío de etiquetas entre un grupo de switches interconectados.

La diferencia entre un enrutador que no implemente MPLS y uno que sí, es que en el primero se intercambia la información de ruteo con otros enrutadores y se almacena en una tabla de almacenamiento IP, y los paquetes se reenvían consultando esta tabla. Uno que implemente MPLS, posteriormente utiliza la tabla de ruteo para establecer e intercambiar etiquetas y almacena esa información en la tabla *Label Forwarding*. Los paquetes que entren y salgan del enrutador, se etiquetarán entonces según la información de esta tabla.

Finalmente, una red MPLS va a estar compuesta por dos tipos de nodos. Estos nodos son denominados LER (Label Edge Routers) y LSR (Label Switching Routers)[2].

1.1.1.2 Ventajas y desventajas de MPLS.

a) Mediante MPLS, los proveedores de servicio de Internet pueden soportar servicios diferenciados. Ante el aumento de la demanda de nuevas aplicaciones, que suponen nuevos requerimientos de ancho de banda y tolerancia a retardos, MPLS ofrece una gran flexibilidad en cuanto a los diferentes servicios ofertados, lo que permite responder a esta demanda de forma óptima.

b) MPLS ofrece un mecanismo sencillo para crear VPNs, ya que permite la creación de circuitos o túneles virtuales dentro de la red IP, y esto a su vez, garantiza poder aislar el tráfico y el acceso al mismo.

c) Permite ahorrar costes entre un 10%-25% frente a otros servicios de datos, en función de la combinación específica de aplicaciones y de la configuración de red de la empresa. En los

últimos años, se han efectuado diversas pruebas que incluso han alcanzado el 40 % de ahorro de costes respecto a ATM o Frame Relay.

d) Mejora del rendimiento, ya que al ser su naturaleza "muchos-a-muchos", los diseñadores de red pueden reducir el número de saltos entre puntos, permitiendo a su vez mejorar los tiempos de respuesta y rendimiento de las aplicaciones.

e) Recuperación ante desastres: Los servicios basados en MPLS permiten la recuperación de diferentes maneras. En primer lugar, permiten conectar los emplazamientos clave a la nube MPLS, y a través de ella, a otros sitios de la red. Además, es posible, reconectar los sitios remotos a localizaciones que actúen como copia de seguridad en caso de desastre. Todo ello lo hace una de las principales razones por las cuales las empresas están migrando a esta tecnología.

Ahora bien, MPLS no es perfecto, y también cuenta con algunas desventajas. En primer lugar, su aparente flexibilidad no es completa del todo, ya que ciertas características o su forma de implementación en el protocolo no han sido estandarizadas, dejándose al arbitrio de cada fabricante de red. El hecho de que sea un protocolo joven también hace que se vea infrautilizado en algunos casos, dado que, al estar en continua evolución, aún se siguen especificando estándares y borradores para algunas características. Finalmente, la desventaja principal es que MPLS no posee ningún mecanismo "per se" para proteger la seguridad en las comunicaciones, teniendo que poner el proveedor de servicio sus propios medios para obtenerla[3].

1.1.2 MPLS-TP

La IETF y la UIT se unieron con la intención de estandarizar un nuevo perfil de transporte para la tecnología MPLS, con fines de proporcionar la base para la próxima generación de redes de transporte de paquetes. La idea fundamental de esta actividad es extender MPLS donde sea necesario con herramientas de Operación, Administración y Mantenimiento (OAM), que actualmente son aplicadas en tecnologías de redes de transporte existentes, tales como, SONET/SDH u OTN. El objetivo de esta nueva estandarización es desarrollar extensiones de MPLS con fines de satisfacer los requerimientos de la red de transporte.

Según los requerimientos establecidos en la RFC-5654 [4], el plano de datos MPLS-TP constituye un subconjunto del plano de datos MPLS definido por la IETF, y selecciona solo la parte necesaria y suficiente para que sea aplicable a las redes de transporte; en su diseño se reutilizan hasta donde es posible, los estándares existentes de MPLS; los mecanismos y capacidades son capaces de inter-operar con las existentes arquitecturas MPLS y supuestas conexiones de extremo a extremo (PWE3) establecidas por la IETF en la RFC-3031 [5] y RFC-3985 [6] respectivamente; además de que es operado y configurado sin ninguna capacidad de reenvío IP. Todas estas exigencias se encuentran estandarizadas y normalizadas por los diferentes organismos.

1.1.2.1 Características principales de MPLS-TP.

- Es estrictamente orientado a la conexión.
- Es cliente agnóstico (puede llevar servicios en las capas 1, 2 y 3).
- Es agnóstico en la capa física (puede correr sobre IEEE Ethernet, SONET/SDH y OTN, usando, WDM, etc.).
- Proporciona funciones de operaciones robustas, administración y mantenimiento (OAM), las cuales funcionan de forma similar a las redes de transporte ópticas disponibles (SONET/SDH, OTN); estas funciones de OAM son parte esencial del Plano de Datos de MPLS-TP y son independientes del Plano de Control.
- Permite la administración de red centralizada.
- Proporciona diferentes esquemas de protección similar a aquellos disponibles en redes de transporte ópticas tradicionales.
- El plano de control GMPLS es aplicable a las capas cliente o servidor MPLS y permiten al usuario usar un método común para la administración y control de redes de transporte multi-capas [7].

1.1.2.2 Adaptación de servicios nativos de MPLS-TP.

Un servicio nativo es el servicio de red de la capa cliente que es transportado por la red MPLS-TP, en otras palabras, es el tráfico perteneciente al cliente de dicha red [6]; se utiliza para su adaptación dos tipos de mecanismo de emulación de conexiones punto a punto:

Supuestas conexiones de extremo a extremo (PWE3): En general, los mecanismos de emulación de conexiones punto a punto, denominados supuestos alambres, en MPLS-TP trabajan de igual forma que en redes IP/MPLS. MPLS-TP utiliza estos mecanismos de emulación de conexiones punto a punto, definidos por la IETF, para emular servicios particulares como Ethernet, Frame Relay o PPP/HDLC. Además, se utilizan para proporcionar Servicio de Cable Privado Virtual (VPWS), Servicio de LAN Privada Virtual (VPLS), Servicio de Multidifusión Privado Virtual (VPMS) y Servicio de LAN IP (IPLS).

Caminos de etiquetas conmutados (LSP): Un trayecto LSP de MPLS-TP es un LSP que reutiliza un subconjunto de las capacidades de un LSP MPLS con el propósito de que sea apropiado con las características de una red de transporte MPLS. El LSP es contenido en un túnel, puede estar protegido o no, y cada uno posee OAM.

1.1.3 VPN/MPLS

Una Red Privada Virtual es una red de información privada que utiliza una infraestructura de Telecomunicaciones pública y conecta a usuarios de forma remota hacia una red principal y su objetivo es brindar aplicaciones integrando soluciones multimedia.

Las VPNs tradicionales ya sean basadas en PVC (Circuitos Virtuales Permanentes) o túneles IP han sido de gran beneficio, pero tienen ciertos inconvenientes que pueden ser resueltos con la utilización de MPLS.

Las VPNs basadas en PVC utilizan la infraestructura de las redes ATM o Frame Relay y los PVCs se establecen entre los nodos de extremo a extremo con la configuración manual de cada uno, lo que implica complejidad en la gestión de la red del proveedor ya que se trata de una topología lógica mallada sobrepuesta a la red física y al agregar un nuevo miembro a la VPN es necesario restablecer todos los PVCs [8].

1.1.3.1 Ventajas y desventajas de las VPNs.

Los inconvenientes más comunes que tienen las VPN tradicionales son las siguientes:

- Se basan en conexiones punto a punto (PVC o túneles).

- La configuración de cada nodo de la VPN es manual y cada vez que se integra uno supone la reconfiguración de todos los anteriores.
- La Calidad de Servicio se ofrece hasta cierta parte, mas no durante el transporte.
- El modelo topológico sobrepuesto a la red existente implica poca flexibilidad en la provisión y gestión del servicio.

Utilizando MPLS para implementar VPNs se eliminan los inconvenientes de las tecnologías anteriores. En primera instancia el modelo topológico que se crea no se sobrepone sino se acopla a la red del proveedor, esto elimina las conexiones extremo a extremo (túneles IP convencionales o circuitos virtuales) y los túneles se van creando con el intercambio de las etiquetas formándose así los LSP que vendrían a ser los "túneles MPLS".

Las ventajas que se tiene al usar VPN con MPLS son:

- Se elimina la complejidad de los túneles y los PVCs.
- Para la implementación no es necesario realizar cambios en todos los puntos involucrados como ocurre con las VPNs tradicionales, por lo contrario, solo se configura a nivel del proveedor evitando tareas complejas y riesgosas.
- Las garantías de Calidad de Servicio se mantienen de extremo a extremo separando los flujos de tráfico por clases.
- Para aumentar la seguridad se pueden utilizar los protocolos de encriptación manejados también por las VPNs tradicionales como IPSec (Internet Protocol Security).
- Con la Ingeniería de Tráfico que ofrece MPLS se garantiza que en el servicio VPN no influyan parámetros que afecten la calidad de extremo a extremo [8].

1.1.3.2 Generalidades de la Arquitectura de las VPN/MPLS.

Una VPN/MPLS básica está formada de tres elementos físicos que son: P (Provider) o router interno del proveedor, PE (Provider Edge) o enrutador de la frontera del proveedor y CE (Customer Edge) denominado así al enrutador frontera del cliente. Además, existen dos aspectos internos de la arquitectura de las VPN soportadas en MPLS que son: el Router Distinguisher y el Router Target, mecanismos que permiten distinguir los requerimientos del cliente suscrito a una VPN.

1.1.4 L2VPN.

Dentro de las categorías de VPN, Las VPNs de capa 2 (L2VPN) se clasifican como "Provider-Provisioned". Esto significa que la responsabilidad de crear y administrar los túneles para el tráfico privado entre los sitios recae en el proveedor. El proveedor utiliza MPLS como medio de transporte para crear túneles entre los sitios privados.

Utilizando L2VPNs se logra conectividad en la capa 2 entre los sitios, tunelizando las diferentes tecnologías en caminos LSP. De esta forma, se logra transportar una trama L2 entre dos sitios remotos. Desde el punto de vista del cliente, la red del proveedor simula ser una conexión directa (cable) entre los sitios. Las L2VPN son de tipo punto a punto. Los equipos frontera del cliente (Router Customer Edge, CE) mapean el tráfico a un circuito específico (Ethernet, ATM, Frame Relay, etc.) y lo envían al proveedor (Router Provider Edge, PE). El proveedor encapsula dicho tráfico en un LSP, y lo envía hacia el enrutador PE remoto asociado a dicha conexión. Para obtener conectividad entre varios sitios de una L2VPN, se debe configurar un esquema full-mesh entre los enrutadores PE.

Las tramas del cliente se transmiten utilizando un stack de dos etiquetas MPLS. La etiqueta externa identifica al LSP entre los enrutadores PE, y la interna identifica a la VPN (Circuito L2) que se está interconectando. Este esquema permite que múltiples VPNs utilicen el mismo LSP de transporte. Debido a que la conexión a través del proveedor se realiza en capa 2, el esquema de ruteo del cliente se implementa en los equipos CE y no involucra al proveedor.

Existen dos variantes de VPNs de capa 2. La diferencia entre las mismas radica en el protocolo de señalización y control que utilizan. Dicho protocolo se utiliza para establecer las sesiones entre enrutadores PE, y para negociar la etiqueta VPN a utilizar. Los esquemas son BGP L2VPN (Utiliza el protocolo BGP) y LDP L2VPN o LDP L2 Circuit (Utiliza el protocolo LDP). Al utilizar el protocolo BGP se logra mayor escalabilidad y prestaciones como auto-descubrimiento de vecinos, pero el esquema se hace más complejo. Al utilizar el protocolo LDP, se logra un ambiente más sencillo, pero se debe configurar explícitamente cada vecino y como consecuencia se pierde escalabilidad [9].

1.1.5 L3VPN.

En L3VPN, los enrutadores del proveedor participan en el esquema de ruteo del cliente. En el mismo se incluyen a los equipos de frontera del proveedor (PE), en los cuales se generan tablas de ruteo especiales para separar las rutas privadas de los clientes de las rutas del proveedor. El proveedor asume la responsabilidad de manejar tablas de ruteo específicas para cada VPN, y distribuir esas rutas a los sitios remotos de la VPN. El enrutador PE del proveedor mantiene una tabla separada para cada VPN que tenga configurada, y estas tablas se completan con la información de prefijos que reciben desde los Routers Customer Edge (CE) conectados. Los enrutadores PE anuncian estas rutas específicas utilizando sesiones Multiprotocol BGP (MP-BGP) a otros PE en donde la VPN tenga presencia. MP-BGP se utiliza para distribuir información de las VPNs, distribuir las rutas específicas de cada VPN, y negociar una etiqueta para la VPN. El PE recibe estos anuncios y coloca las rutas en la tabla especifica de la VPN correspondiente, identificándola utilizando los atributos de comunidades extendidas BGP de cada anuncio. En lo que respecta al forwarding, se utilizan LSPs MPLS para enviar el tráfico de la VPN, que pueden ser señalizados con protocolos tales como LDP o RSVP. El protocolo negociará etiquetas, que se conocen como etiquetas externas o de transporte. En el plano de control para identificar inequívocamente la VPN correspondiente, la sesión MP-BGP negocia una etiqueta asociada a la VPN (La misma se agrega antes de la etiqueta de transporte y se conoce como Etiqueta Interna o Etiqueta de la VPN). Es importante remarcar que solo se utiliza una sesión MP-BGP para señalización y control de todas las VPNs entre dos enrutadores PE, y solo se utiliza un LSP de transporte para todo el tráfico entre enrutadores PE lo cual hace que este esquema sea altamente escalable [10].

1.2 Herramientas de simulación.

1.2.1 OPNET Modeler.

Permite diseñar y estudiar redes, dispositivos, protocolos y aplicaciones; brinda escalabilidad y flexibilidad, cualidades que le permiten a los usuarios trabajar en procesos de investigación y desarrollo [11].

Está basado en la teoría de colas e incorpora librerías que facilitan el modelado de redes, con un extenso grupo de aplicaciones y protocolos como: TCP, IP, OSPF, BGP, RIP, RSVP, Frame Relay, FDDI, ATM, WIFI, MPLS, PNNI, DOCSIS, UMTS, IP Multicast, Movil IP, etc.

El desarrollo de los modelos se realiza jerárquicamente, mediante la interconexión de nodos de múltiples tecnologías, utilizando diferentes tipos de enlaces. En OPNET Modeler, se implementan tres tipos de modelos [12]: modelo de red, modelo de nodos y modelo de procesos.

1.2.2 COMNET III.

COMNET III es una herramienta comercial orientada al diseño, configuración y estudio de las redes de comunicaciones. Fue desarrollada por CACI Product Inc. con el uso del lenguaje de programación MODSIM II. Por medio de este programa es posible crear tecnologías de redes complejas, configurar varias tecnologías, protocolos y dispositivos de red para hacer un análisis detallado del funcionamiento y del rendimiento de redes tipo LAN, MAN y WAN, utilizando una interfaz gráfica en un ambiente de ventanas [13].

Este software está basado en una interfaz gráfica de usuario. Permite analizar y predecir el funcionamiento de redes, desde topologías básicas de interconexión hasta esquemas mucho más complejos de simulación con múltiples redes interconectadas con diversos protocolos y tecnologías como: Ethernet, ATM, satelitales, Frame Relay, etc. Dentro del área de trabajo del programa, se hace la descripción gráfica del modelo de red, se asocian las fuentes generadoras de tráfico, se configuran los parámetros y las características de los dispositivos de acuerdo a la aplicación que se desea implementar; luego se pone en marcha la simulación y finalmente se analizan los reportes estadísticos sobre el desempeño de la red, los cuales son generados automáticamente al finalizar la simulación. Los informes pueden contener información acerca de la ocupación de los enlaces o nodos, la cantidad de mensajes generados, el número de colisiones, entre otros [14].

1.2.3 OMNET++.

OMNET++ es un simulador de redes de eventos discretos por medio de módulos orientados a objetos.

Un modelo en OMNET++, se construye con módulos jerárquicos que intercambian mensajes, los cuales pueden contener estructuras complejas de datos, con parámetros propios que permiten personalizar el envío de paquetes a los destinos a través de rutas, compuertas y conexiones. Los módulos de más bajo nivel son llamados simples módulos y son programados en C++ utilizando una librería de simulación.

Las simulaciones en OMNET++ pueden utilizar varias interfaces de usuario, dependiendo del propósito. Una de las características más importantes de OMNET++ es la posibilidad de ejecutar simulaciones distribuidas y paralelas, gracias a la programación por módulos; además se debe resaltar que se puede acceder a los archivos fuente del programa por medio de compiladores de C++, lo que permite que el simulador, las interfaces y las herramientas de desarrollo OMNET++, puedan ser ejecutadas sin inconvenientes sobre diferentes sistemas operativos como Windows, Linux [15].

1.2.4 NCTUNS.

NCTUns (National Chiao Tung University, Network Simulator) es un simulador y emulador de redes y sistemas de telecomunicaciones avanzado. NCTUns es software libre y se ejecuta sobre Linux. Debido a sus características, es considerado como el más avanzado de simulación para redes de telecomunicaciones [16].

Las simulaciones ejecutadas con esta herramienta, cuentan con características muy especiales, ya que NCTUns simula en tiempo real y con una interfaz similar a la de los sistemas reales, lo cual permite familiarizar más el usuario con el diseño, configuración e implementación de aplicaciones en redes de comunicaciones.

Permite la simulación de arquitecturas de redes sencillas. Sin embargo, su mayor potencial está en la simulación de redes tan complejas como las redes GPRS, satélites y ópticas. Puede ser utilizado como emulador.

Permite definir obstáculos, trayectorias de movimiento y el desplazamiento de los terminales móviles (celulares GPRS y computadoras portátiles), al tiempo en que se hacen las mediciones de atenuación, interferencia y de ancho de banda.

En NCTUns, la configuración de una red simulada, es exactamente igual a la configuración de una red IP del mundo real [16].

Simula protocolos de redes como: IEEE 802.3, IEEE 802.11, IP, IP Mobile, Diffserv, RIP, OSPF, UDP, TCP, RTP/RTCP, SDP, FTP, entre otros.

1.2.5 PACKET TRACER.

Es un simulador gráfico de redes desarrollado y utilizado por Cisco como herramienta de entrenamiento para obtener la certificación CCNA. Packet Tracer es un simulador de entorno de redes de comunicaciones de fidelidad media, que permite crear topologías de red mediante la selección de los dispositivos y su respectiva ubicación en un área de trabajo, utilizando una interfaz gráfica.

Packet Tracer es un simulador que permite realizar el diseño de topologías, la configuración de dispositivos de red, así como la detección y corrección de errores en sistemas de comunicaciones. Ofrece como ventaja adicional el análisis de cada proceso que se ejecuta en el programa de acuerdo a la capa de modelo OSI que interviene en dicho proceso; razón por la cuál es una herramienta de gran ayuda en el estudio y aprendizaje del funcionamiento y configuración de redes de comunicaciones y aplicaciones telemáticas.

Ofrece una interfaz basada en ventanas, que le brinda al usuario facilidades para el modelado, la descripción, la configuración y la simulación de redes. Packet Tracer tiene tres modos de operación: el primero de estos es el modo topology (topología), que aparece en la ventana de inicio cuando se abre el programa, el otro es el modo simulation (simulación), al cual se accede cuando se ha creado el modelo de la red; finalmente aparece el modo real time (tiempo real), en donde se pueden programar mensajes SNMP para detectar los dispositivos que están activos en la red y si existen algún problema de direccionamiento o tamaño de tramas entre las conexiones [17].

1.2.6 Network Simulator.

El Network Simulator, es una plataforma orientada a simular eventos discretos. Se desarrolló con base en dos lenguajes de programación: uno de ellos es el C++ y el otro es una extensión de TCL, orientada a objetos. Este programa ha sido diseñado especialmente para el área de la investigación de redes telemáticas.

Network Simulator es una herramienta con un amplio rango de uso y que continuamente sirve como base para el desarrollo de otros programas de simulación. Además, soporta una gran cantidad de protocolos de las capas de aplicación y transporte, además de otros utilizados para el enrutamiento de los datos, entre los cuales están: HTTP, FTP CBR, TCP, UDP, RTP y SRM. Puede representar redes cableadas, inalámbricas locales o vía satélite. Es aplicable a grandes redes con topologías complejas y con un gran número de generadores de tráfico. Para visualizar los resultados se puede instalar el Network Animador (NAM), el cual es una herramienta de interfaz gráfica muy sencilla de utilizar. Network Simulator depende de algunos componentes externos como Tcl/TK, Otcl, TclCL y xgraph.

Network Simulator es un intérprete de scripts orientados a objetos, el cual tiene un planificador de eventos de simulación, librerías de objetos de componentes de red y librerías de módulos de instalación de red. Esto quiere decir que la simulación se debe programar en el lenguaje de scripts OTCL.

Dentro del desarrollo de este simulador han surgido nuevos simuladores a partir de su creación como es el Network Simulator -2 y el Network Simulator -3, los cuales de por sí se diferencian y cada uno constituye un nuevo simulador y no la continuación del anterior. A partir de lo anterior surge entonces el simulador GNS3, que avanza grandemente al incorporar el ambiente gráfico al Network Simulator -3 como sistema de simulación de redes orientado a Internet [18].

1.2.7 GNS3

GNS3 es un simulador gráfico de redes que permite diseñar fácilmente topologías de red y luego ejecutar simulaciones. Soporta IOS de enrutadores ATM, Frame Relay, Switchs Ethernet[19]. Utiliza Dynamips, un emulador de IOS de Cisco; QEMU, un emulador de

máquina virtual de código abierto y en parte Dynagen, un front-end basado en texto para Dynamips desarrollado en Python a través de PyQt la interfaz gráfica [20], confeccionada con la poderosa librería Qt, famosa por su uso en el proyecto KDE, también utiliza la tecnología SVG (Scalable Vector Graphics) para proveer símbolos de alta calidad para el diseño de las topologías de red [21].

GNS3 es utilizado por cientos de miles de ingenieros de redes a nivel mundial para emular, configurar, probar y solucionar problemas de redes virtuales y reales. GNS3 permite desde ejecutar una pequeña topología que consta de solo unos pocos dispositivos en una computadora portátil, hasta aquellos que tienen muchos dispositivos alojados en múltiples servidores o incluso alojados en la nube. GNS3 es un software libre, de código abierto que se puede descargar desde https://www.gns3.com/software/download.

Este software está activamente desarrollado y respaldado, y cuenta con una comunidad en crecimiento de más de 800,000 miembros. Cuando se une a la comunidad GNS3 se está uniendo a otros estudiantes, ingenieros de redes, arquitectos y profesionales que han descargado GNS3 más de 10 millones de veces hasta la fecha. GNS3 se utiliza en empresas de todo el mundo, incluidas las compañías Fortune 500, es una excelente herramienta complementaria a los laboratorios reales para los ingenieros de redes, administradores y personas que quieran estudiar para las certificaciones como Cisco CCNA, CCNP, CCIP y CCIE, así como JNCIA Juniper, JNCIS y JNCIE. También se puede utilizar para características experimentales de Cisco IOS, JunOS Juniper o para comprobar configuraciones que necesiten ser desplegadas posteriormente en enrutadores reales [18].

Gracias a su integración con VirtualBox y VMware los ingenieros de sistemas y los administradores pueden realizar simulaciones con máquinas reales virtuales lo que permite crear redes integradas a los servicios que se puedan ofrecer en dichas máquinas virtuales como por ejemplo correo, proxy, internet etc.

GNS3 ha permitido a los ingenieros de red virtualizar dispositivos de hardware reales durante más de 10 años. Originalmente solo emulaba dispositivos Cisco que usaban software Dynamips, ahora ha evolucionado y admite muchos dispositivos de múltiples proveedores de

red, incluidos conmutadores virtuales Cisco, Cisco ASA, Brocade vRouters, conmutadores Cumulus Linux, instancias Docker, HPE VSR, múltiples dispositivos Linux y muchos otros. En el siguiente link puede ver una lista de dispositivos que soporta GNS3: https://gns3.com/marketplace/appliances. GNS3 ahora puede probar la interoperabilidad entre muchos proveedores e incluso probar configuraciones esotéricas usando tecnologías de red con SDN, NFV, Linux y Docker. Por otra parte, tiene integración con Wireshark desde donde se pueden obtener capturas de paquetes y observar el correcto funcionamiento de las topologías creadas.

1.2.7.1 Empleo de GNS3 en las universidades del mundo.

El campo de la red informática cambia constantemente debido al rápido desarrollo de nuevas tecnologías. La necesidad de trabajo práctico es alta cuando se trata de entender cómo funcionan las redes de computadoras. Muchas universidades ofrecen a los estudiantes trabajar en equipos de redes en vivo. Desafortunadamente, esto no es muy eficiente para la enseñanza de laboratorios de redes y aunque es preferible tener laboratorios con equipo físico, esto no siempre es posible debido a las limitaciones de recursos y para superar los problemas existentes de hardware limitado y accesibilidad en los laboratorios físicos es necesario crear un laboratorio de redes virtuales. El laboratorio les brinda a los estudiantes la capacidad de implementar instancias virtuales de dispositivos de red reales. Este laboratorio se ejecutará dentro de una única computadora física, por lo que la principal ventaja de usar un laboratorio virtual es el costo, ya que los dispositivos virtuales cuestan solo una fracción en comparación con sus contrapartes físicas. A continuación, se enumeran algunas de las universidades del mundo que emplean la herramienta GNS3 con fines educativos e investigativos:

- En la Universidad Distrital Francisco José de Caldas, Bogotá. Profesor Patrocinador: Ing. Luis Felipe Wanumen Silva. Facultad de Ingeniería de Sistemas. Tema investigativo: Sistema para configurar una red EIGRP de enrutador GNS3 virtualizados, desde una aplicación Android [22].
- En la Universidad Nacional Autónoma de México. Profesor patrocinador: Ing. Azael Fernández Alcántara. Facultad de Ingeniería, División de Ingeniería Eléctrica. Tema

investigativo: Simulador de redes GNS3: estudio, pruebas con prácticas y propuesta de uso [23].

- En la Universidad Complutense de Madrid existe un Proyecto de Innovación Software libre para ciencias e ingenierías donde se encuentra GNS3 y este es utilizado en las asignaturas de Grado en Ingeniería Electrónica de Comunicaciones y en Redes y Servicios I, donde realizan trabajos de laboratorios con el mismo, además cuentan con sus métodos de instalación y manuales [24].
- En la Universidad de Alicante en la XIII Jornadas de Redes de Investigación en Docencia Universitaria se crearon nuevas estrategias organizativas y metodológicas en la formación universitaria para responder a la necesidad de adaptación y cambio. Autores: G. J. García; P. Gil; F. A. Candelas; M. J. Blanes; M. A. Baquero; B. Alacid; A. Torre. Departamento de Física, Ingeniería de Sistemas y Teoría de la Señal. Tema investigativo: Virtualización de Redes de Computadores con GNS3: Evaluación de soluciones para el aprendizaje a distancia [25].
- En la Universidad de Alicante también las nuevas topologías de redes de computadoras virtuales han sido evaluadas en temas de comunicación de redes. Los profesores propusieron una práctica sesión sobre el laboratorio real que se puede desarrollar ya con el entorno virtual usando GNS3[26].

1.3 Conclusiones del capítulo

Esta primera parte del trabajo resume las características y el funcionamiento que tienen las tecnologías actuales de redes de transporte de banda ancha como son MPLS, MPLS-TP, VPN/MPLS, L2VPN, L3VPN; las cuales son de gran importancia en el desarrollo de las redes actuales, además de ser una solución muy efectiva para redes de proveedores de servicio y grandes empresas. Se caracterizaron algunas herramientas de emulación y simulación y debido a las ventajas que nos ofrece GNS3 se llegó a la conclusión que es la más adecuada a emplear en el desarrollo del proyecto.

CAPITULO 2: “LABORATORIOS PARA LA ENSEÑANZA DE REDES DE TRANSPORTE DE BANDA ANCHA”

Se elaboraron un total de cuatro laboratorios diseñados en la herramienta GNS3 para la enseñanza de redes de transporte de banda ancha, cada uno de ellos poseen distintos escenarios, con el objetivo de dar cumplimiento a las habilidades trazadas en el programa analítico de la asignatura Redes III.

Habilidades:

- Crear nuevos laboratorios y configurar físicamente cada uno de los dispositivos de red en el espacio de trabajo de GNS3.
- Seleccionar los dispositivos de interconexión para las tecnologías MPLS.
- Configurar Enrutadores/Conmutadores de Capa 3.
- Configurar y describir las características y funciones del protocolo IPv4 en los casos prácticos.
- Configurar protocolos de enrutamiento como OSPF acorde a las características de la red modelada.
- Crear y configurar redes privadas virtuales con las potencialidades que ofrece GNS3 a partir de la interfaz de línea de comandos de Cisco (CLI).
- Configurar rutas estáticas entre enrutadores.
- Utilizar y configurar el protocolo de enrutamiento BGP para redistribuir el tráfico en la red.
- Determinar el desempeño de Redes IP/MPLS.

CAPITULO 2: "LABORATORIOS PARA LA ENSEÑANZA DE REDES DE TRANSPORTE DE BANDA ANCHA"

2.1 Laboratorio #1: "Red básica MPLS"

Objetivo:

Configurar una red básica utilizando el multiprotocolo de conmutación de etiquetas (MPLS) haciendo uso del protocolo de enrutamiento OSPF, para garantizar la correcta distribución de etiquetas en toda la red y que el enrutamiento se realice por la ruta más corta.

Objetivos Específicos:

1. Crear y configurar la topología de red física en GNS3 utilizando las imágenes de Cisco que soportan el protocolo MPLS.
2. Configurar manualmente el direccionamiento IPv4 a través de la CLI.
3. Crear y configurar las interfaces de loopback en los enrutadores.
4. Configurar enrutamiento OSPF entre los enrutadores.
5. Habilitar MPLS IP en los enrutadores de la red emulada.

Preparación Previa:

Para el desarrollo de este laboratorio de red, se debe estar familiarizado con los protocolos y tecnologías que se utilizan en esta práctica, tales como: MPLS, IPv4 y OSPF.

Tarea a Desarrollar:

Configuración de una red MPLS con direccionamiento IP y enrutamiento OSPF que está referido en la RFC 5340[27], donde los enrutadores se interconectan a través de interfaces seriales.

Técnica Operatoria:

Mediante la herramienta GNS3 se realiza la simulación de una red MPLS básica con el editor de proyectos que posee la misma.

Pasos a Seguir:

a) Definición de un nuevo proyecto

En el Menú File del software GNS3 se selecciona "New Blank Project" para comenzar un nuevo proyecto, luego se le asigna nombre y localización para los archivos de trabajo de este escenario. La tabla 2.1 muestra los valores para conformar este laboratorio.

Nombre	**Localización**
Red básica MPLS	C:\Users\Username\GNS3\projects\Red básica MPLS

Tabla 2.1 Valores de inicio del laboratorio #1

b)Desarrollo de la Topología

En el desarrollo de este material, se utiliza en todos los enrutadores la imagen c3640-jk9s-mz.124-16.bin, la cual permite configuraciones básicas y avanzadas para las tecnologías de banda ancha: IPv4/IPv6, VPN, VoIP, MPLS y MPLS-VPN. En el Anexo 1.1 se muestra la topología de red de este laboratorio.

Para elaborar la topología de red de este laboratorio se insertan en el espacio de trabajo seis enrutadores de la serie c3600 de Cisco. Una vez insertados se configuran, físicamente, con al menos una interfaz serial. Para ello, se da clic derecho en el enrutador, se selecciona la herramienta "Configure", se navega hasta la pestaña "Slots" y se selecciona el tipo de interfaz "NM-4T" en el primer slot físico. Se debe realizar el mismo procedimiento para los otros cinco enrutadores.

Para utilizar estas interfaces seriales en este laboratorio, se selecciona la herramienta "Add Link" del panel de la izquierda, se da clic en un enrutador y luego en otro para cerrar el enlace. Es necesario seleccionar el mismo número de interfaces (s0/0 o s0/1) que posee la figura de topología de red de este laboratorio, debido a que todas las configuraciones que se realizan en los enrutadores se basan en la numeración de estas interfaces.

Una vez insertados los enrutadores c3600 y asignado las interfaces seriales, se da clic derecho en cada uno de ellos y se selecciona la herramienta "Start", para iniciar el sistema en cada uno de ellos.

c) Direccionamiento IP

Para que los enrutadores puedan comunicarse entre sí, es necesario establecer un direccionamiento de red en las interfaces físicas de cada uno de ellos, con el objetivo de garantizar, tanto el funcionamiento de OSPF, como el protocolo de distribución de etiquetas con MPLS. Por tanto, la tabla 2.2 muestra el direccionamiento de red para cada una de las interfaces de los seis enrutadores [28].

Enrutador	Interfaz	IP Subred	Máscara de Red
R1	s0/0	10.1.1.14	255.255.255.252
R2	s0/0	10.1.1.22	255.255.255.252
R3	s0/0	10.1.1.13	255.255.255.252
R3	s0/1	10.1.1.5	255.255.255.252
R3	s0/2	10.1.1.1	255.255.255.252
R3	s0/3	10.1.1.17	255.255.255.252
R4	s0/0	10.1.1.21	255.255.255.252
R4	s0/1	10.1.1.6	255.255.255.252
R4	s0/2	10.1.1.9	255.255.255.252
R5	s0/0	10.1.1.2	255.255.255.252
R5	s0/1	10.1.1.10	255.255.255.252
R6	s0/0	10.1.1.18	255.255.255.252

Tabla 2.2 Direccionamiento de red para cada una de las interfaces Seriales

En el anexo A1.2 se muestran los pasos a seguir, mediante línea de comandos, para asignar direcciones IPv4 y máscara de red en interfaces seriales. Se toma como ejemplo el enrutador "R4" el cual posee tres interfaces de red (s0/0, s0/1 y s0/2). Se deben hacer las configuraciones para el resto de los enrutadores según la tabla 2.2, para ello es posible guiarse con la sección de comandos del anexo A1.2.

d) Creación y configuración de interfaces de loopback en los enrutadores.

MPLS IP es comúnmente llamado MPLS clásico/tradicional, es uno de los servicios más utilizados por los Proveedores de Servicio de Internet (ISP). Para que MPLS IP estándar pueda establecer las bases de reenvío es necesario configurar el protocolo de enrutamiento OSPF y los prefijos de Loopback de los enrutadores. Por simplificación en este laboratorio, las

interfaces virtuales Loopback se han introducido para representar la red LAN 10.10.10.0/24. Por tanto, cada enrutador va a distribuir los prefijos punto a punto, con el objetivo de establecer las rutas entre las redes externas y las redes internas.

En esta sección del laboratorio se crean las interfaces de Loopback con una dirección IP de 32 bits con máscara de 32 bits con el objetivo de ser accesibles a través de la tabla de ruta del enrutador. La tabla 2.3 muestra el direccionamiento de red para cada una de las interfaces de Loopback en los seis enrutadores [28].

Enrutador	Interfaz	IP Subred	Máscara de Red
R1	loopback	10.10.10.4	255.255.255.255
R2	loopback	10.10.10.6	255.255.255.255
R3	loopback	10.10.10.1	255.255.255.255
R4	loopback	10.10.10.3	255.255.255.255
R5	loopback	10.10.10.2	255.255.255.255
R6	loopback	10.10.10.5	255.255.255.255

Tabla 2.3 Direccionamiento de red para cada una de las interfaces Loopback

En el caso de este laboratorio, al crear una interfaz de loopback, de manera predeterminada, la ruta hacia ese bucle se anuncia como la ruta más específica: prefijo /32 y se ignora cualquier prefijo configurado. Por ejemplo, para el caso del enrutador R1: interfaz Loopback0 dirección IP 10.10.10.4 255.255.255.255, la dirección de red de bucle invertido es 10.10.10.0/24. Por defecto, OSPF anunciará esta ruta a loopback0 como 10.10.10.4/32 (la ruta más específica para ese loopback). Para anular esto, se tiene que cambiar el tipo de red a punto a punto. Después de este OSPF anunciará la dirección a loopback como 10.10.10.4/24.

En el anexo A1.3 se muestran los pasos a seguir, mediante línea de comandos, para asignar direcciones IPv4 con máscara de red en interfaces Loopback y la configuración del protocolo de enrutamiento OSPF. Se toma como ejemplo el enrutador "R4". Se deben hacer las configuraciones para el resto de los enrutadores según la tabla 2.3.

e) Configuración MPLS

Para habilitar MPLS en los routers, se indica qué interfaces del router van a participar en este protocolo. Para ello se va configurando en dichas interfaces del router el comando "mpls ip" de forma que se indica al router que conmute en entrada y salida las tramas MPLS que reciba o envíe, así como que detecte vecindades de routers MPLS con el protocolo de distribución de etiquetas. En el anexo A1.4 se muestran las configuraciones finales del laboratorio #1 "Red Básica MPLS" correspondientes a MPLS, se toma como ejemplo el enrutador R4. Se deben hacer las configuraciones para el resto de los enrutadores según el anexo correspondiente. En el capítulo 3 se evalúan los resultados correspondientes a este laboratorio [28].

2.2 Laboratorio #2: "Filtrado de etiquetas MPLS en GNS3"

Objetivo:

Configurar una red MPLS con listas de control de acceso (ACL) asegurando que todos los prefijos se publiquen con una etiqueta haciendo uso de listas de control de acceso, para evitar que las etiquetas MPLS sean divulgadas hacia redes innecesarias y de este modo garantizar la seguridad de la red.

Objetivos Específicos:

1. Crear y configurar la topología de red física en GNS3 utilizando las imágenes de Cisco que soportan el protocolo MPLS.
2. Configurar manualmente el direccionamiento IPv4 a través de la CLI.
3. Configurar enrutamiento OSPF entre los enrutadores.
4. Habilitar MPLS IP en los enrutadores de la red emulada.
5. Crear las Listas de control de acceso (ACL) para filtrar el tráfico de MPLS.

Preparación Previa:

Para el desarrollo de este laboratorio de red, se debe estar familiarizado con los protocolos y tecnologías que se utilizan en esta práctica, tales como: MPLS, ACL, IPv4 y OSPF.

Tarea a Desarrollar:

Configuración de una red MPLS con enrutamiento OSPF, donde los enrutadores se interconectan a través de interfaces FastEthernet y realizan filtrado de etiquetas.

Técnica Operatoria:

Mediante la herramienta GNS3 se va a crear y simular una red MPLS con ACL en el editor de proyectos que posee la misma. Este laboratorio se enfoca en la configuración de MPLS en los enrutadores Cisco y la realización de filtrado de etiquetas.

Pasos a Seguir:

a) Definición de un nuevo proyecto

En el Menú File del software GNS3 se selecciona "New Blank Project" para comenzar un nuevo proyecto, luego se le asigna nombre y localización para los archivos de trabajo de este escenario. La tabla 2.4 muestra los valores para conformar este laboratorio.

Nombre	**Localización**
Filtrado de Etiquetas MPLS	C:\Users\Username\GNS3\projects\Filtrado de Etiquetas MPLS

Tabla 2.4 Valores de inicio del laboratorio #2

b) Desarrollo de la Topología

En el desarrollo de este laboratorio, se utiliza en todos los enrutadores la imagen c3640-jk9s-mz.124-16.bin, la cual permite configuraciones básicas y avanzadas para las tecnologías de banda ancha: IPv4/IPv6, VPN, VOip, MPLS y MPLS-VPN. En el Anexo 2.1 se muestra la topología de red de este laboratorio.

Para elaborar la topología de red de este laboratorio se insertan en el espacio de trabajo tres enrutadores de la serie c3600 de Cisco. Una vez insertados se configuran, físicamente, con al menos dos interfaces FastEthernet. Para ello, se da clic derecho en el enrutador, se selecciona

la herramienta "Configure", se navega hasta la pestaña "Slots" y se selecciona el tipo de interfaz "NM-1FE-TX" en los dos primeros slots físicos. Se debe realizar el mismo procedimiento para los otros dos enrutadores.

Para utilizar estas interfaces FastEthernet en este laboratorio, se selecciona la herramienta "Add Link" del panel de la izquierda, se da clic en un enrutador y luego en otro para cerrar el enlace. Es necesario seleccionar el mismo número de interfaces (f0/0 o f0/1) que posee la figura de topología de red de este laboratorio, debido a que todas las configuraciones que se realizan en los enrutadores se basan en la numeración de estas interfaces.

Una vez insertados los enrutadores c3600 y asignado las interfaces FastEthernet, se da clic derecho y se selecciona la herramienta "Start", para iniciar el sistema en cada uno de ellos.

c) Direccionamiento IP

Para que los enrutadores puedan comunicarse entre sí, es necesario establecer un direccionamiento de red en las interfaces físicas de cada uno de ellos, con el objetivo de garantizar, tanto el funcionamiento de OSPF, como el protocolo de distribución de etiquetas con MPLS. Por tanto, la tabla 2.5 muestra el direccionamiento de red para cada una de las interfaces de los tres enrutadores [29].

Enlace (Interfaz)	**IP Subred**	**Máscara de Red**	**Dirección IP – Nodo 1 y Nodo 2**
R1(f0/0)-R2(f0/0)	192.168.12.0	255.255.255.0	R1 (0/0) - 192.168.12.1 R2 (0/0) - 192.168.12.2
R2(f1/0)-R3(f0/0)	192.168.23.0	255.255.255.0	R2 (1/0) - 192.168.23.2 R3 (0/0) - 192.168.23.3

Tabla 2.5 Direccionamiento de red para cada una de las interfaces FastEthernet

En el anexo A2.2 se muestran los pasos a seguir, mediante líneas de comandos, para asignar direcciones IPv4 y máscara de red en interfaces FastEthernet. Se toma como ejemplo el enrutador "R2" el cual posee dos interfaces de red (f0/0 y f0/1). Se deben hacer las configuraciones para R1 y R3 según la tabla 2.2, para ello es posible guiarse con la sección de comandos del anexo A2.2.

d)Creación y configuración de interfaces de loopback en los enrutadores.

MPLS con filtrado de etiquetas es definido por la adición de funciones extras con el MPLS clásico/tradicional y da más escalabilidad, seguridad, simplicidad y manejabilidad para entregar los servicios MPLS punto a punto. Para realizar el filtrado de etiquetas, se trasladan o distribuyen los prefijos entre las áreas divididas en segmentos, para este caso se utilizan prefijos del protocolo de enrutamiento OSPF y los prefijos de Loopback de los enrutadores. Por simplificación en este laboratorio, las interfaces virtuales Loopback se han introducido para representar las redes LAN 1.1.1.0/24, 2.2.2.0/24 y 3.3.3.0/24. Por tanto, cada enrutador va a distribuir los prefijos punto a punto, con el objetivo de establecer las rutas entre las redes externas y las redes internas.

En esta sección del laboratorio se crean las interfaces de Loopback con una dirección IP de 32 bits con máscara de 24 bits con el objetivo de ser accesibles a través de la tabla de ruta del enrutador. La tabla 2.6 muestra el direccionamiento de red para cada una de las interfaces de Loopback en los tres enrutadores [29].

Enrutador	Nombre Interfaz	Dirección IP	Máscara de Red
R1	loopback0	1.1.1.1	255.255.255.0
R2	loopback0	2.2.2.2	255.255.255.0
R3	loopback0	3.3.3.3	255.255.255.0

Tabla 2.6 Direccionamiento de red para cada una de las interfaces Loopback

En el caso de este laboratorio, al crear una interfaz de loopback, de manera predeterminada, la ruta hacia ese bucle se anuncia como la ruta más específica: prefijo /32 y se ignora cualquier prefijo configurado. Por ejemplo: interfaz Loopback0 dirección IP 2.2.2.2 255.255.255.0 Aquí, la dirección de red de bucle invertido es 2.2.2.0/24. Por defecto, OSPF anunciará esta ruta a loopback0 como 2.2.2.2/32 (la ruta más específica para ese loopback). Para anular esto, se tiene que cambiar el tipo de red a punto a punto. Después de este OSPF anunciará la dirección a loopback como 2.2.2.0/24.

En el anexo A2.3 se muestran los pasos a seguir, mediante línea de comandos, para asignar direcciones IPv4 con máscara de red en interfaces Loopback y la configuración del protocolo de enrutamiento OSPF. Se toma como ejemplo el enrutador "R2". Se deben hacer las configuraciones para R1 y R3 según la tabla 2.6.

e) Enrutamiento OSPF.

El protocolo Open Shortest Path First (OSPF) es un protocolo en enrutamiento abierto — no propietario — del tipo Link State. Este fue desarrollado por la organización IETF como un Interior Gateway Protocol (IGP) con el objetivo de reemplazar al protocolo RIP. OSPF utiliza el algoritmo Dijstra para encontrar la mejor ruta hacia la red de destino. La red de este laboratorio implementa OSPF, tanto en las interfaces de loopback como en las de FastEthernet. El anexo A2.4 muestra las configuraciones de OSPF en las interfaces de red en el enrutador R2, así como la explicación de los comandos en sí. Este proceso se debe realizar para los enrutadores R1 y R3.

f) Configuración de MPLS y ACL

Para aumentar la seguridad en una red MPLS es tarea del proveedor de servicios realizar un filtrado de etiquetas MPLS mediante las ACL, con el objetivo de evitar que se publiquen las etiquetas MPLS hacia redes innecesarias. Una ACL filtra el tráfico de una red según las configuraciones que se definan en la sintaxis de las ACL. Pueden referirse al filtrado por IP o por puertos según el tipo de servicio, ejemplo http puerto 80. También se utilizan para definir el tráfico para traducción de dirección de red (NAT) o cifrado, o bien filtrar protocolos que no sean IP, como AppleTalk o IPX. En el caso de este laboratorio se filtrarán los prefijos de las etiquetas MPLS en las interfaces de loopback para que no se publiquen en redes adyacentes. En el Anexo A2.5 se muestra el concepto y la configuración básica de una ACL estándar para el caso del enrutador "R2". Esta misma configuración se debe realizar para el resto de los enrutadores.

Una vez configuradas las ACL estándar, típicamente, se asignan a una interfaz de red; en este caso se asigna al protocolo MPLS para evitar que se publiquen las etiquetas. Cuando se trata

de filtrado de etiquetas en MPLS, no se deben advertir las etiquetas por todas las interfaces de red configuradas, solo por las que pertenecen al núcleo MPLS. También las interfaces de red físicas configuradas deben soportar el servicio MPLS o MPLS-IP. En el Anexo A2.6 se muestran las configuraciones por línea de comandos para el filtrado de etiquetas y el servicio MPLS para el caso de R2. Esta misma configuración se debe realizar para el resto de los enrutadores teniendo en cuenta el nombre de cada interfaz de red.

2.3 Laboratorio #3: "MPLS con Protocolo de distribución de etiquetas (LDP)"

Objetivo:

Configurar una red MPLS con protocolo de distribución de etiquetas LDP que sea altamente escalable con el objetivo de añadir nuevos servicios para los clientes que puedan ir adicionándose al núcleo MPLS.

Objetivos Específicos:

1. Crear y configurar la topología de red física en GNS3 utilizando las imágenes de Cisco que soportan el protocolo MPLS.
2. Configurar manualmente el direccionamiento IPv4 a través de la CLI.
3. Configurar enrutamiento OSPF entre los enrutadores.
4. Configurar los enrutadores R1, R2, R3 y R4 para activar MPLS.
5. Configurar todos los enrutadores que solo utilicen un rango de etiquetas entre 20-200.
6. Configurar todos los enrutadores para enviar paquetes "Hola MPLS" cada 2 segundos, con tiempo de espera de 10 segundos.
7. Configurar todos los enrutadores para usar la autenticación MPLS MD5, con contraseña: "UCLV".

Preparación Previa:

Para el desarrollo de este laboratorio de red, se debe estar familiarizado con los protocolos y tecnologías que se utilizan en esta práctica, tales como: MPLS-LDP, IPv4 y OSPF.

Tarea a Desarrollar:

Configurar una red MPLS LDP con enrutamiento OSPF, donde los enrutadores se interconectan a través de interfaces FastEthernet con manejo de etiquetas que se encuentren en un rango entre 20-200.

Técnica Operatoria:

Mediante la herramienta GNS3 se va a crear y simular una red MPLS LDP en el editor de proyectos que posee la misma. Este laboratorio se enfoca en el manejo de etiquetas que se encuentren en un rango específico y en la autenticación de los enrutadores con MPLS MD5.

Pasos a Seguir:

a) Definición de un nuevo proyecto

En el Menú File del software GNS3 se selecciona "New Blank Project" para comenzar un nuevo proyecto, luego se le asigna nombre y localización para los archivos de trabajo de este escenario. La tabla 2.7 muestra los valores para conformar este laboratorio.

Nombre	**Localización**
MPLS LDP	C:\Users\Username\GNS3\projects\MPLS LDP

Tabla 2.7 Valores de inicio del laboratorio #3

b)Desarrollo de la Topología

En el desarrollo de este material, se utiliza en todos los enrutadores la imagen c3640-jk9s-mz.124-16.bin, la cual permite configuraciones básicas y avanzadas tal como se comentó en el laboratorio anterior. En el Anexo 3.1 se muestra la topología de red de este laboratorio.

Para elaborar la topología de red de este laboratorio se insertan en el espacio de trabajo cuatro enrutadores de la serie c3600 de Cisco. Una vez insertados se configuran, físicamente, con al menos dos interfaces FastEthernet. Para ello, se da clic derecho en el enrutador, se selecciona la herramienta "Configure", se navega hasta la pestaña "Slots" y se selecciona el tipo de

interfaz "NM-1FE-TX" en los dos primeros slots físicos. Se debe realizar el mismo procedimiento para los otros tres enrutadores.

Para utilizar las interfaces FastEthernet en este laboratorio, se selecciona la herramienta "Add Link" del panel de la izquierda, se da clic en un enrutador y luego en otro para cerrar el enlace. Es necesario seleccionar el mismo número de interfaces (f0/0 o f0/1) que posee la figura de topología de red de este laboratorio, debido a que todas las configuraciones que se realizan en los enrutadores se basan en la numeración de estas interfaces.

Una vez insertados los enrutadores c3600 y asignado las interfaces FastEthernet, se da clic derecho en cada uno de ellos y se selecciona la herramienta "Start", para iniciar el sistema.

c) Direccionamiento IP

Para que los enrutadores puedan comunicarse entre sí, es necesario establecer un direccionamiento de red en las interfaces físicas de cada uno de ellos, con el objetivo de garantizar, tanto el funcionamiento de OSPF, como el protocolo de distribución de etiquetas con MPLS. Por tanto, la tabla 2.8 muestra el direccionamiento de red para cada una de las interfaces de los cuatro enrutadores [30].

Enlace (Interface)	IP Subred	Máscara de Red	Dirección IP – Nodo 1 y Nodo2
R1(f0/0)-R2(f0/0)	192.168.12.0	255.255.255.0	R1 (0/0) - 192.168.12.1 R2 (0/0) - 192.168.12.2
R2(f1/0)-R4(f0/0)	192.168.24.0	255.255.255.0	R2 (1/0) - 192.168.24.2 R4 (0/0) - 192.168.24.4
R4(f1/0)-R3(f1/0)	192.168.34.0	255.255.255.0	R4 (1/0) - 192.168.34.4 R3 (1/0) - 192.168.34.3
R3(f0/0)-R1(f1/0)	192.168.13.0	255.255.255.0	R3 (0/0) - 192.168.13.3 R1 (1/0) - 192.168.13.1

Tabla 2.8 Direccionamiento de red para cada una de las interfaces FastEthernet

En el anexo A3.2 se muestran los pasos a seguir, mediante línea de comandos, para asignar direcciones IPv4 y máscara de red en interfaces FastEthernet. Se toma como ejemplo el enrutador "R1" el cual posee dos interfaces de red (f0/0 con la red 192.168.12.0/24 y f0/1 con

la red 192.168.13.0/24). Se deben hacer las configuraciones para el resto de los enrutadores según la tabla 2.8, para ello es posible guiarse con la sección de comandos del anexo A3.2.

d)Interfaces de loopback y enrutamiento OSPF

Una vez configurado el direccionamiento IP es necesario, para proseguir con la configuración de MPLS, establecer el enrutamiento OSPF y el direccionamiento en interfaces de loopback. En esta sección del laboratorio se crean las interfaces de Loopback con una dirección IP de 32 bits con máscara de 32 bits con el objetivo de ser incluidas en la tabla de rutas de OSPF. La tabla 2.9 muestra el direccionamiento de red para cada una de las interfaces de Loopback en los cuatro enrutadores [30].

Enrutador	Nombre Interfaz	Dirección IP	Máscara de Red
R1	loopback0	1.1.1.1	255.255.255.255
R2	loopback0	2.2.2.2	255.255.255.255
R3	loopback0	3.3.3.3	255.255.255.255
R4	loopback0	4.4.4.4	255.255.255.255

Tabla 2.9 Direccionamiento de red para cada una de las interfaces Loopback

En el anexo A3.3 se muestran los pasos a seguir, mediante línea de comandos, para asignar direcciones IPv4 con máscara de red en interfaces Loopback y la configuración del protocolo de enrutamiento OSPF. Se toma como ejemplo el enrutador "R1". Se deben hacer las configuraciones para R2, R3 y R4 según la tabla 2.9.

Para que OSPF abarque tanto el direccionamiento asignado a las interfaces FastEthernet como de loopback, se utilizan todos los bits disponibles de la wildcard para que enrute y aprenda todas las direcciones de red y rutas posibles. Para propósitos generales se utiliza solo un área OSPF (área 0) El anexo A3.3 muestran las configuraciones de OSPF en las interfaces de red en el enrutador R1. Este proceso se debe realizar para los enrutadores R2, R3 y R4 según la tabla 2.9.

e) Configuraciones para MPLS LDP

MPLS LDP proporciona los bloques de construcción para aplicaciones habilitadas para MPLS, tales como redes privadas virtuales (VPN) de MPLS. LDP proporciona una metodología estándar para la distribución hop-by-hop, o dynamic label, en una red MPLS mediante la asignación de etiquetas a las rutas que han sido elegidas por los protocolos de enrutamiento subyacentes del Protocolo de puerta de enlace interior (IGP). Las rutas etiquetadas resultantes, denominadas rutas de conmutación de etiquetas (LSP), reenvían el tráfico de etiquetas a través de una red troncal MPLS a destinos particulares. Estas capacidades permiten a los proveedores de servicios implementar VPN IP basados en MPLS y servicios IP + ATM en redes MPLS de múltiples proveedores.

En esta sección del laboratorio se configura MPLS LDP, para ello, se realizan los siguientes pasos:

- Se configura un rango de etiquetas de 20 (mínimo) a 200 (máximo) para usar las características de etiquetas estáticas que brinda MPLS.
- Se habilita la distribución de etiquetas asociadas con la ruta predeterminada de IP que existen en las tablas de rutas.

Se mejora el tiempo de convergencia de etiquetas para los enrutadores R1, R2, R3 y R4, debido a que están conectados directamente. Esto se realiza anunciando los vecinos de cada enrutador más una palabra clave (UCLV) como contraseña por seguridad para que el enrutador genere un resumen MD5 de cada segmento enviado en la conexión TCP y verifique el resumen MD5 de cada segmento recibido de la conexión TCP.

Se limita el número de saltos permitidos en una ruta de etiqueta conmutada (LSP) establecida por el método de distribución de etiquetas. En este laboratorio se utiliza un máximo de saltos permitidos de 10.

Se habilita el reenvío de paquetes IPv4 a lo largo de las rutas MPLS que soportan LDP.

Cada uno de estos pasos conlleva a una o varias líneas de comandos las cuales permiten configurar MPLS LDP en los cuatro enrutadores de este laboratorio. El anexo A3.4 muestra

estos comandos, así como la representación gráfica de ellos en el momento en que fueron introducidos en los enrutadores [30].

2.4 Laboratorio #4: "Redes Privadas Virtuales (VPN) sobre MPLS"

Objetivo:

Configurar una red MPLS sobre VPN utilizando tablas VRF con direcciones de familia IPv4 y protocolos de enrutamiento OSPF, EIGRP y BGP con direcciones de familia vpnv4 (VPN para IPv4), para permitir que varios clientes se interconecten de modo transparente a través de una red de proveedor de servicio e impedir que la información se envíe fuera de la VPN y de esta manera se pueda usar la misma subred en varias VPN sin causar problemas de dirección IP duplicada.

Objetivos Específicos:

1. Crear y configurar la topología de red física en GNS3 utilizando las imágenes de Cisco que soportan el protocolo MPLS.
2. Configurar manualmente el direccionamiento IPv4 a través de la CLI.
3. Configurar enrutamiento BGP, EIGRP y OSPF entre los enrutadores seleccionados.
4. Configurar MPLS para que utilice las interfaces de loopback como el identificador de los enrutadores.
5. Configurar VRF "CUSTOMER" en R2 y R3.
6. Configurar EIGRP AS 100 en los enrutadores R4 y R5.
7. Configurar BGP AS 1 entre los enrutadores R2 y R3.
8. Configurar las familias de direcciones BGP.
9. Redistribuir EIGRP en BGP.
10. Redistribuir nuevamente la información de BGP a EIGRP.

Preparación Previa:

Para el desarrollo de este laboratorio de red, se debe estar familiarizado con los protocolos y tecnologías que se utilizan en esta práctica, tales como: MPLS- VPN, IPv4, VRF, BGP y EIGRP.

Tarea a Desarrollar:

Configurar una red MPLS sobre VPN, con enrutamiento BGP y EIGRP para los clientes finales, donde los enrutadores se interconectan a través de interfaces FastEthernet.

Técnica Operatoria:

Mediante la herramienta GNS3 se va a crear y simular una red MPLS sobre VPN en el editor de proyectos que posee la misma. Este laboratorio se enfoca la configuración de redes privadas virtuales con enrutadores Cisco y se realiza un enrutamiento con BGP y EIGRP.

Pasos a Seguir:

a) Definición de un nuevo proyecto

En el Menú File del software GNS3 se selecciona "New Blank Project" para comenzar un nuevo proyecto, luego se le asigna nombre y localización para los archivos de trabajo de este escenario. La tabla 2.10 muestra los valores para conformar este laboratorio.

Nombre	**Localización**
MPLS VPN	C:\Users\Username\GNS3\projects\MPLS VPN

Tabla 2.10 Valores de inicio del laboratorio #4

b) Desarrollo de la Topología

En el desarrollo de este material, se utiliza en todos los enrutadores la imagen c3640-jk9s-mz.124-16.bin, la cual permite configuraciones básicas y avanzadas tal como se comentó en el laboratorio #2. En el Anexo 4.1 se muestra la topología de red de este laboratorio.

Para elaborar la topología de red de este laboratorio se insertan en el espacio de trabajo cinco enrutadores de la serie c3600 de Cisco. Una vez insertados se configuran, físicamente, con al menos dos interfaces FastEthernet. Para ello, se da clic derecho en el enrutador, se selecciona la herramienta “Configure”, se navega hasta la pestaña “Slots” y se selecciona el tipo de interfaz “NM-1FE-TX” en los dos primeros slots físicos. Se debe realizar el mismo procedimiento para los otros cuatro enrutadores.

Para utilizar estas interfaces FastEthernet en este laboratorio, se selecciona la herramienta “Add Link” del panel de la izquierda, se da clic en un enrutador y luego en otro para cerrar el enlace. Es necesario seleccionar el mismo número de interfaces (f0/0 o f0/1) que posee la figura de topología de red de este laboratorio, debido a que todas las configuraciones que se realizan en los enrutadores se basan en la numeración de estas interfaces.

Una vez insertados los enrutadores c3600 y asignado las interfaces FastEthernet, se da clic derecho en cada uno de ellos y se selecciona la herramienta “Start”, para iniciar el sistema.

c) Direccionamiento IP

Para que los enrutadores puedan comunicarse entre sí, es necesario establecer un direccionamiento de red en las interfaces físicas de cada uno de ellos, con el objetivo de garantizar, tanto el funcionamiento de OSPF, como el protocolo de distribución de etiquetas con MPLS. Por tanto, la tabla 2.11 muestra el direccionamiento de red para cada una de las interfaces de los cinco enrutadores [31].

Enrutador	Interfaz	IP Subred	Máscara de Red
R1	f0/0	192.168.23.3	255.255.255.0
R1	f1/0	192.168.34.3	255.255.255.0
R2	f0/0	192.168.23.2	255.255.255.0
R2	f1/0	192.168.12.2	255.255.255.0
R3	f0/0	192.168.45.4	255.255.255.0
R3	f1/0	192.168.34.4	255.255.255.0
R4	f0/0	192.168.12.1	255.255.255.0
R5	f0/0	192.168.45.5	255.255.255.0

Tabla 2.11 Direccionamiento de red para cada una de las interfaces FastEthernet

En el anexo A4.2 se muestran los pasos a seguir, mediante línea de comandos, para asignar direcciones IPv4 y máscara de red en interfaces FastEthernet. Se toma como ejemplo el enrutador "R1" el cual posee dos interfaces de red (f0/0 con la red 192.168.23.0/24 y f1/0 con la red 192.168.34.0/24). Se deben hacer las configuraciones para el resto de los enrutadores según la tabla 2.11, para ello ver la sección de comandos del anexo A4.2.

d)Interfaces de loopback en todos los enrutadores y enrutamiento OSPF en R1, R2 y R3

Una vez configurado el direccionamiento IP es necesario, para proseguir con la configuración de MPLS sobre VPN, establecer el enrutamiento OSPF y el direccionamiento en interfaces de loopback. En esta sección del laboratorio se crean las interfaces de Loopback con una dirección IP de 32 bits con máscara de 24 bits con el objetivo de ser incluidas en la tabla de rutas de OSPF. La tabla 2.12 muestra el direccionamiento de red para cada una de las interfaces de Loopback en los cinco enrutadores [31].

Enrutador	Nombre Interfaz	Dirección IP	Máscara de Red
R1	loopback0	3.3.3.3	255.255.255.0
R2	loopback0	2.2.2.2	255.255.255.0
R3	loopback0	4.4.4.4	255.255.255.0
R4	loopback0	1.1.1.1	255.255.255.0
R5	loopback0	5.5.5.5	255.255.255.0

Tabla 2.12 Direccionamiento de red para cada una de las interfaces Loopback

En el anexo A4.3 se muestran los pasos a seguir, mediante línea de comandos, para asignar direcciones IPv4 con máscara de red en interfaces Loopback y la configuración del protocolo de enrutamiento OSPF. Se toma como ejemplo el enrutador "R1". Se deben hacer las configuraciones para el resto de los enrutadores según la tabla 2.12.

Para que OSPF abarque tanto el direccionamiento asignado a las interfaces FastEthernet como de loopback, se utilizan los primeros tres octetos disponibles de la wildcard para que enrute y aprenda todas las direcciones de red y rutas posibles. Para propósitos generales se utiliza solo un área OSPF (área 0). El anexo A4.3 muestra las configuraciones de OSPF en las interfaces de red de loopback en el enrutador R1. Este proceso se debe realizar para el resto de los enrutadores según la tabla 2.12.

e) VPN / Enrutamiento y Reenvío Virtual (VPN / Virtual Routing and Forwarding)

Cuando se utiliza con MPLS, la función VPN permite que varios sitios se interconecten de modo transparente a través de una red de proveedor de servicio. Una red proveedora de servicios puede ofrecer soporte a varias VPN IP diferentes. Cada una de estas les aparece a sus usuarios como una red privada, separada de todas las otras redes. Dentro de una VPN, cada sitio puede enviar paquetes IP a cualquier otro sitio dentro de la misma VPN. Cada VPN está asociada con uno o más casos de reenvío o ruteo VPN (VRF). Un VRF consiste de una tabla de IP Routing, una tabla Cisco Express Forwarding (CEF) derivada y un conjunto de interfaces que usen estas tablas de reenvío. El enrutador mantiene un ruteo separado y una tabla CEF para cada VRF. Esto impide que la información se envíe fuera de la VPN y permite que pueda usarse la misma subred en varias VPN sin causar problemas de dirección IP duplicada.

En este laboratorio se crea una VRF llamada CUSTOMER, la cual va a poseer dos discriminadores de rutas, uno para importar y otro para exportar. El Anexo A4.4 muestra los comandos para crear las VRF en "R2", de la misma forma se debe hacer para R3 utilizando los mismos comandos [31].

f) Configuración de BGP e EIGRP

Con el objetivo de que el enrutador que utilice BGP *(R2 y R3)* y multiprotocolo (MP-BGP) distribuya la información de ruteo VPN utilizando las comunidades ampliadas MP-BGP, es necesario hacer una serie de configuraciones para el protocolo de enrutamiento BGP en los enrutadores R2 y R3:

- Adicionar los sistemas autónomos remotos o vecinos con valor de 1.
- Actualizar la fuente del vecino como la interfaz Loopback.
- No sumariar las rutas.
- Crear una dirección de familia vpnv4. Activarla para los vecinos definidos y enviar la comunidad a los vecinos en modo both.
- Crear una dirección de familia ipv4 vrf llamada CUSTOMER. En la misma, redistribuir eigrp con id 100 y no sincronizar.

También es necesario hacer una serie de configuraciones para el protocolo de enrutamiento EIGRP en R2 y R3:

- Sumariar las rutas
- Crear una dirección de familia IPv4 vrf Customer, redistribuir BGP con métricas específicas, no sumariar en la dirección de familia y definirla como un sistema autónomo con id 100

Al terminar con R2 y R3, es necesario definir EIGRP con ID 100 en las redes de R4 y R5, para establecer una comunicación final con la VPN a través de las VRF.

Luego de configurar ambos protocolos, es necesario habilitar MPLS LDP en la interfaz de loopback.

En el Anexo A4.5 se muestra la configuración para los enrutadores R2 y R3 de EIGRP y BGP, y solo EIGRP para los enrutadores R4 y R5 [31].

2.5 Conclusiones del capítulo.

En este capítulo se crean las guías de los cuatros laboratorio propuestos:

1. "Red básica MPLS"
2. "Filtrado de etiquetas MPLS en GNS3"
3. "MPLS con Protocolo de distribución de etiquetas (LDP)"
4. "Redes Privadas Virtuales (VPN) sobre MPLS"

CAPITULO 2: “LABORATORIOS PARA LA ENSEÑANZA DE REDES DE TRANSPORTE DE BANDA ANCHA”

Se describen sus objetivos, esquemas topológicos, los pasos a seguir para su elaboración y se cumple con el objetivo de desarrollar las habilidades trazadas en el programa analítico de la asignatura Redes III.

CAPÍTULO 3: EVALUACIÓN DE LOS RESULTADOS OBTENIDOS DE LOS LABORATORIOS.

En este capítulo se realiza una evaluación de los resultados alcanzados en los laboratorios desarrollados en el campo de las redes de transporte de banda ancha para la asignatura de Redes III.

3.1 Análisis de los resultados.

A continuación, se analizan los resultados alcanzados en cada uno de los cuatro laboratorios desarrollados para la asignatura de Redes III.

3.1.1 Laboratorio #1 “Red básica MPLS”

Este laboratorio representa una red básica utilizando el multiprotocolo de conmutación de etiquetas (MPLS), haciendo uso de enrutamiento con OSPF. A medida que se vaya avanzando en el análisis de los resultados de este laboratorio se van a ir mostrando imágenes que representan comandos de verificación en la interfaz de línea de comandos de GNS3.

De la topología de red de este escenario se toma como referencia el enrutador R4. La figura 3.1 muestra la ruta IP hacia el destino 10.10.10.4. El resultado de este comando de verificación se utiliza para mostrar la ruta IP para el destino 10.10.10.4, en la tabla de enrutamiento de R4; este caso indica que se debe usar la interfaz Serial0/1 para establecer la comunicación.

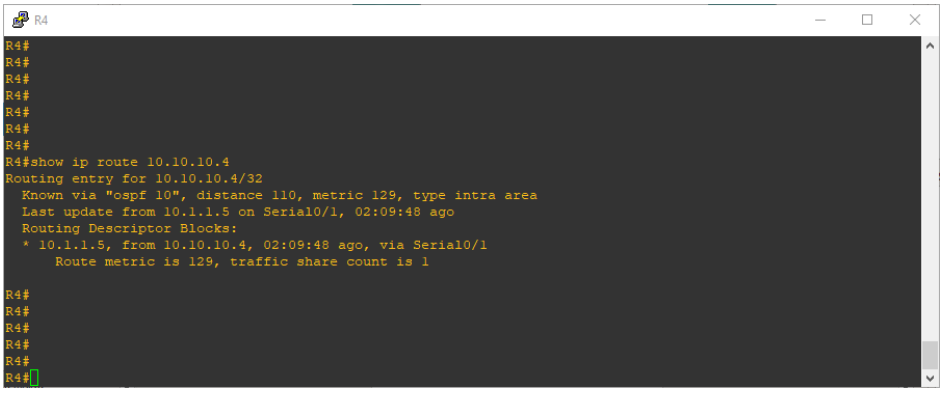


Figura 3.1 Comando “show ip route 10.10.10.4” en R4. Fuente: “GNS3”

Mostrar la tabla de reenvío de MPLS es una manera de saber información específica de este protocolo. La figura 3.2 muestra un comando que realiza esta acción.

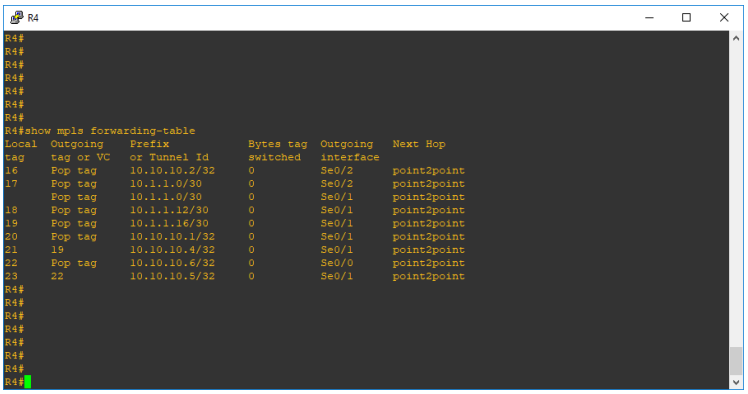


Figura 3.2 Comando "show mpls forwarding-table" en R4. Fuente: "GNS3"

El comando anterior se utiliza para marcar la tabla de reenvío MPLS, que es la equivalente de Label Switching de la tabla de IP Routing para el Routing IP estándar. Contiene las escrituras de las etiquetas entrantes y salientes y las descripciones de los paquetes.

Para ver en detalles la tabla de reenvíos de MPLS se utiliza el comando *show mpls forwarding-table 10.10.10.4 32 detail*. La representación de este comando se muestra en la figura 3.3. Este solicita, de la tabla de reenvío MPLS, los detalles para la dirección IP 10.10.10.4.

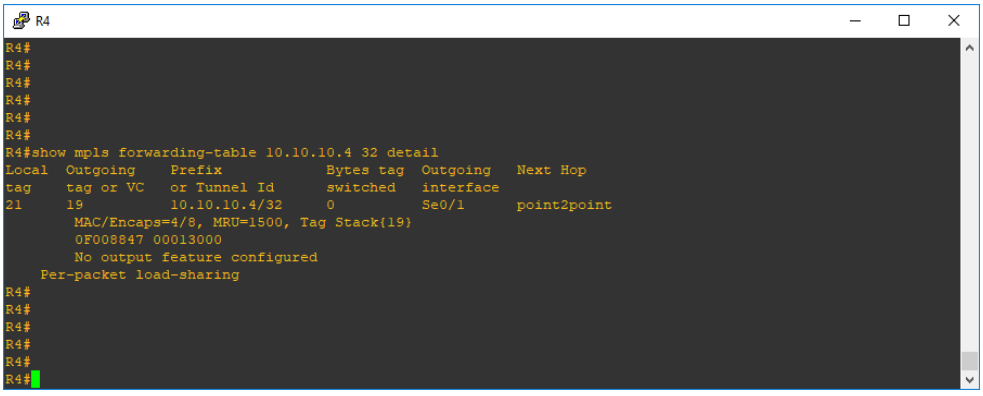


Figura 3.3 Comando "show mpls forwarding-table 10.10.10.4 32 detail" en R4. Fuente: "GNS3"

Para mostrar las etiquetas de conmutación locales o remotas en un enrutador con LDP en MPLS se utiliza el comando *show tag-switching tdp binding* de la figura 3.4. Se observa que las escrituras de la etiqueta para cada clase de reenvío están establecidas en cada LSR, incluso si no están en la trayectoria (más corta) preferida. En este caso, un paquete destinado a 10.10.10.4/32 puede ir por 10.10.10.1 (con la escritura de la etiqueta 20) o por 10.10.10.2 (con la escritura de la etiqueta 22). El LSR elige la primera solución porque es la más corta. Esta decisión se toma con la tabla de IP Routing estándar, que, en este caso, se construye con OSPF.

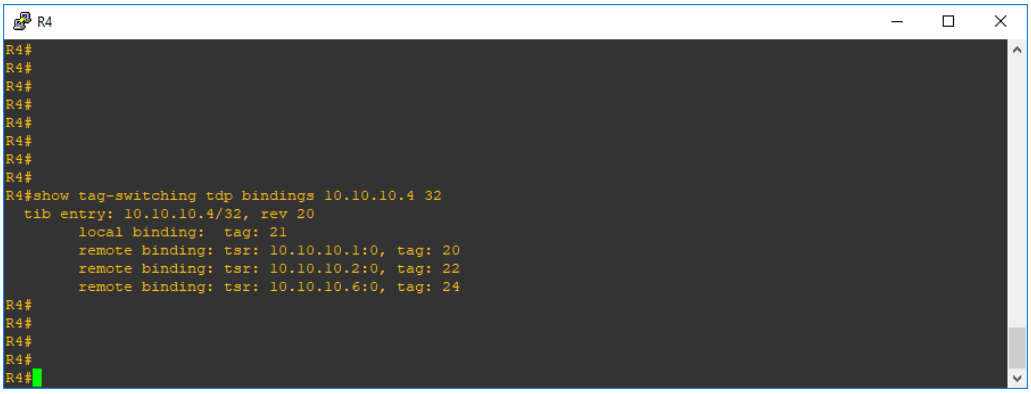


Figura 3.4 Comando "show tag-switching tdp binding 10.10.10.4 32" en R4. Fuente: "GNS3"

El comando de la figura 3.5 muestra el uso detallado de CEF para el IP 10.10.10.4. Se utiliza para marcar que el Cisco Express Forwarding trabaja correctamente y que las etiquetas están intercambiadas correctamente. El Cisco Express Forwarding (CEF) es avanzado y utiliza la tecnología de conmutación IP de capa 3. CEF optimiza el rendimiento y la escalabilidad de la red para redes con patrones de tráfico grandes y dinámicos, como Internet, en redes caracterizadas por aplicaciones intensivas basadas en la Web o sesiones interactivas.

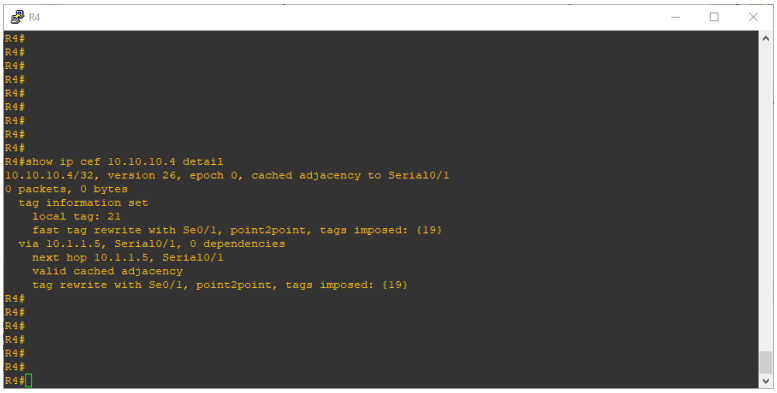


Figura 3.5 Comando "show ip cef 10.10.10.4 detail" en R4. Fuente: "GNS3"

3.1.2 Laboratorio #2 "Filtrado de etiquetas MPLS"

En este laboratorio se configura una red MPLS con LDP asegurando que todos los prefijos se publiquen con una etiqueta, haciendo uso de listas de control de acceso (ACL) para de este modo realizar el filtrado de etiquetas. A medida que se vaya avanzando en el análisis de los resultados de este laboratorio se van a ir mostrando imágenes que representan comandos de verificación en la interfaz de línea de comandos de GNS3.

El comando *show ip route* es una gran herramienta para usar en este laboratorio, la figura 3.6 muestra este comando. Se puede ver directamente la tabla de enrutamiento para determinar si existe una entrada para el host.

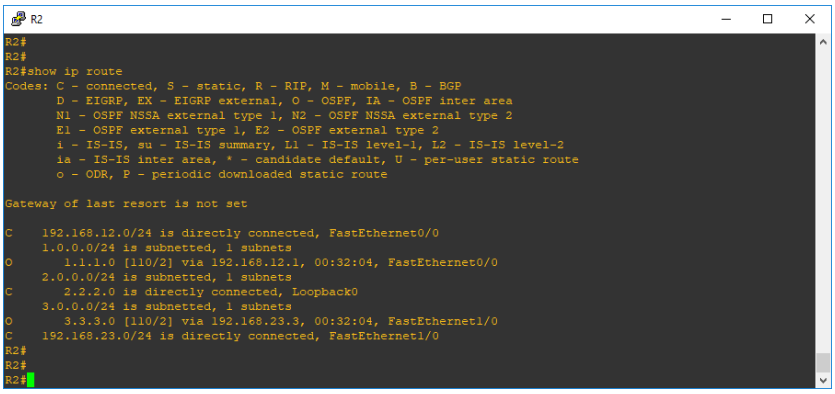


Figura 3.6 Comando "show ip route" en R2. Fuente: "GNS3"

El resultado de *show ip route* muestra las entradas en la tabla de enrutamiento, así como los medios por los que se determinaron, la red directamente conectada, la ruta estática o cuál fue el protocolo de enrutamiento utilizado para seleccionar la ruta. También muestra la puerta de enlace del último recurso y las direcciones de loopback correspondientes.

Se configuró una ruta estática por el usuario que enruta la dirección IP 0.0.0.0. (todos los destinos) a través de un único host (la puerta de enlace). El resultado de establecer una puerta de enlace es que, si no existe una entrada de tabla de enrutamiento para una dirección de destino, los paquetes destinados que lleguen a esa dirección se reenviarán al enrutador de puerta de enlace.

Para mostrar información de todas las interfaces que están configuradas para la conmutación de etiquetas, se usa el comando de la figura 3.7 en el modo EXEC privilegiado.

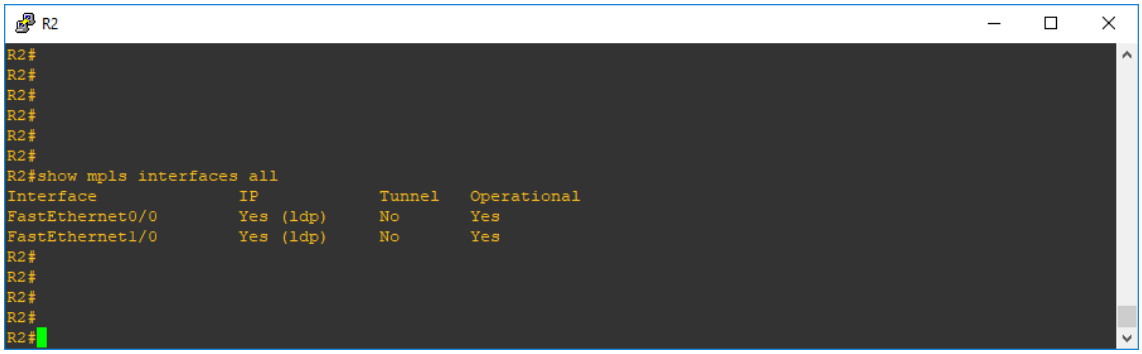


Figura 3.7 Comando "show mpls interfaces all" en R2. Fuente: "GNS3"

Cuando la palabra clave *all* se detalla en la figura anterior, sola en este comando, la información sobre las interfaces configuradas para la conmutación de etiquetas se muestra para todas las VPN, incluidas las VPN en el dominio de enrutamiento predeterminado.

Lo mismo sucede para el caso de la figura 3.8. Donde el comando muestra la información mpls específica de cambio de etiqueta de la interfaz FastEthernet0/0 en detalles.

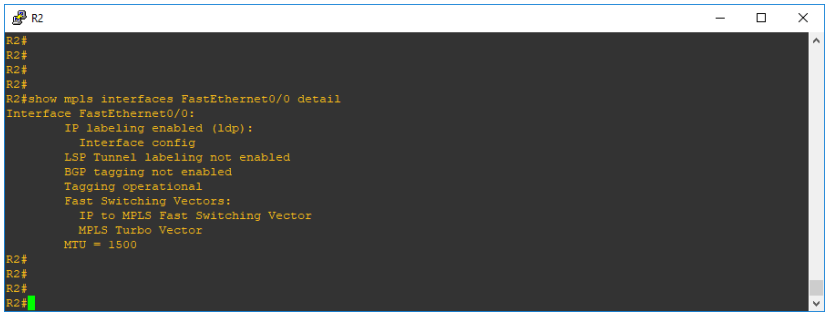


Figura 3.8 Comando "show mpls interfaces FastEthernet0/0 detail" en R2. Fuente: "GNS3"

Mediante el commando *show mpls ldp neighbor* se muestra el estado del protocolo de distribución de etiquetas LDP, así como cada uno de sus vecinos y sus identificaciones loopback, tal como se muestra en la figura 3.9.

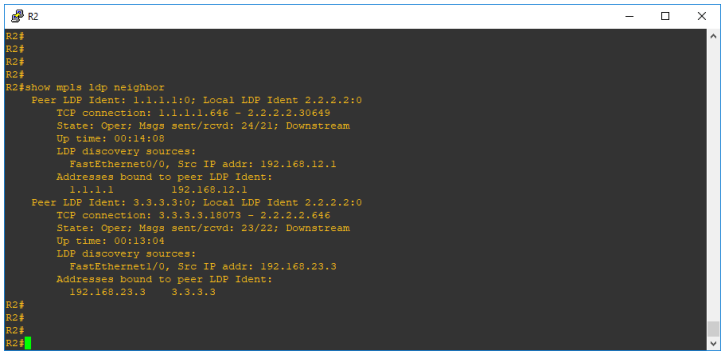


Figura 3.9 Comando "show mpls ldp neighbor" en R2. Fuente: "GNS3"

Para mostrar los parámetros actuales del protocolo de distribución de etiquetas (LDP), se utiliza el comando *show mpls ldp parameters* en el modo EXEC privilegiado, tal como se muestra en la figura 3.10.

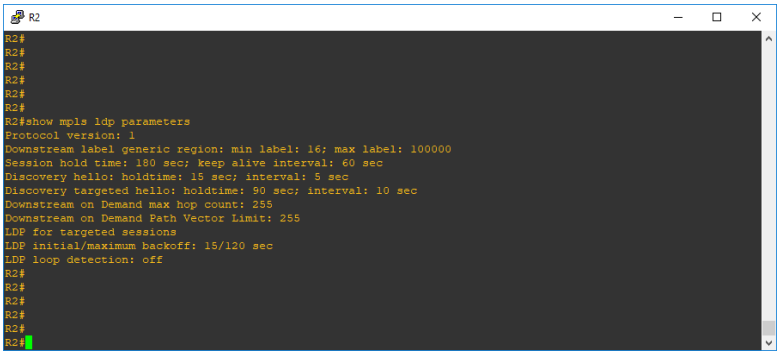


Figura 3.10 Comando "show mpls ldp parameters" en R2. Fuente: "GNS3"

Entre los parámetros de relevancia que se muestran están:

- La versión de protocolo que indica la versión de LDP que se ejecuta en la plataforma.
- Los parámetros Discovery Hello que indican el tiempo necesario para recordar que una plataforma vecina desea una sesión LDP sin recibir un mensaje de saludo LDP del vecino (tiempo de retención), y el intervalo de tiempo entre la transmisión de mensajes Hello LDP consecutivos a los vecinos (intervalo).

Para revelar el estado del proceso de descubrimiento del protocolo de distribución de etiquetas (LDP), se utiliza el comando *show mpls ldp discovery* en el modo EXEC privilegiado. Este comando muestra la lista de interfaces sobre las cuales se ejecuta el proceso de descubrimiento de LDP y el identificador del mismo. Tal como se muestra en la figura 3.11.

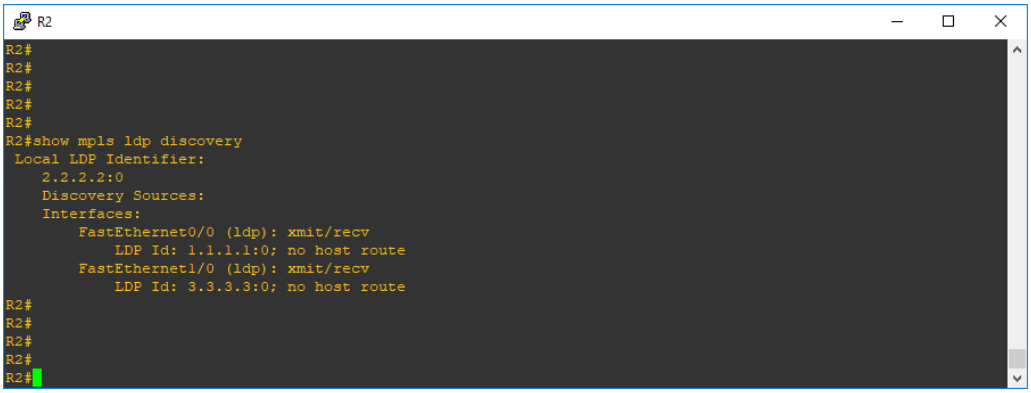


Figura 3.11 Comando "show mpls ldp discovery" en R2. Fuente: "GNS3"

En este laboratorio se propuso incrementar la seguridad en una red MPLS a través del filtrado de etiquetas MPLS mediante ACL con el objetivo de evitar que se publiquen las etiquetas MPLS hacia redes innecesarias para garantizar la seguridad de las misma en todo momento.

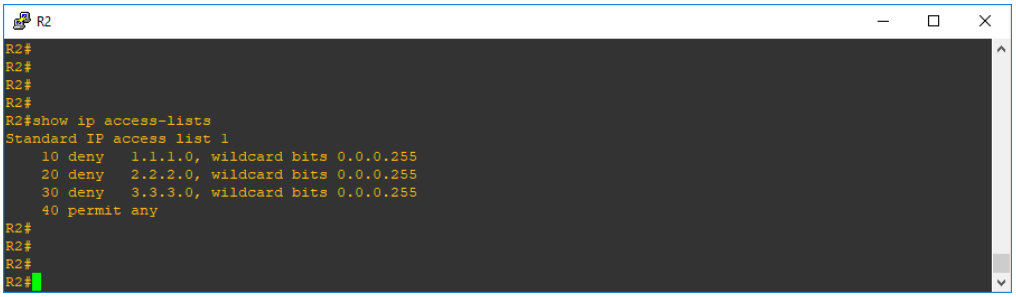


Figura 3.12 Comando "show ip access-lists" en R2. Fuente: "GNS3"

El comando que se utiliza para visualizar las ACL que filtrarán los prefijos de las etiquetas MPLS en las interfaces de loopback para que no se publiquen en redes adyacentes, se muestra en la figura 3.12

3.1.3 Laboratorio #3 "MPLS con Protocolo de distribución de etiquetas (LDP)"

En este laboratorio se configura una red MPLS con LDP altamente escalable que permite añadir nuevos servicios para los clientes e ir adicionándose al núcleo MPLS. A medida que se vaya avanzando en el análisis de los resultados de este laboratorio se van a ir mostrando imágenes que representan comandos de verificación en la interfaz de línea de comandos de GNS3.

El comando *show ip route* es una poderosa herramienta para usar en este laboratorio, la figura 3.13 muestra este comando. Se puede examinar directamente la tabla de enrutamiento para determinar si existe una entrada para el host.

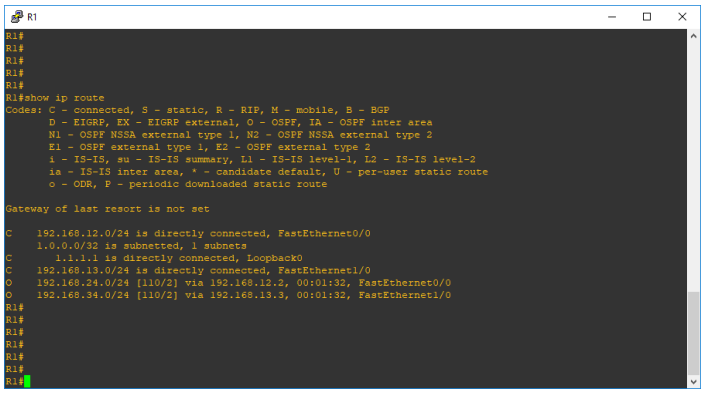


Figura 3.13 Comando "show ip route" en R1. Fuente: "GNS3"

El resultado de *show ip route* muestra las entradas en la tabla de enrutamiento, así como los medios por los que se determinaron (red directamente conectada, ruta estática o qué protocolo de enrutamiento se utilizó para seleccionar la ruta). También muestra la puerta de enlace de último recurso, a veces llamada puerta de enlace predeterminada, si existe una que esté configurada.

Esta es una ruta estática configurada por el usuario que enruta la dirección IP 0.0.0.0. (todos los destinos) a través de un único host (la puerta de enlace). El efecto de establecer una puerta de enlace es que, si no existe una entrada de tabla de enrutamiento para una dirección de destino, los paquetes destinados a esa dirección se reenviarán al enrutador de puerta de enlace.

Para mostrar información sobre las interfaces que estén configuradas para la conmutación de etiquetas, se debe usar el comando de la figura 3.15 en el modo EXEC privilegiado.

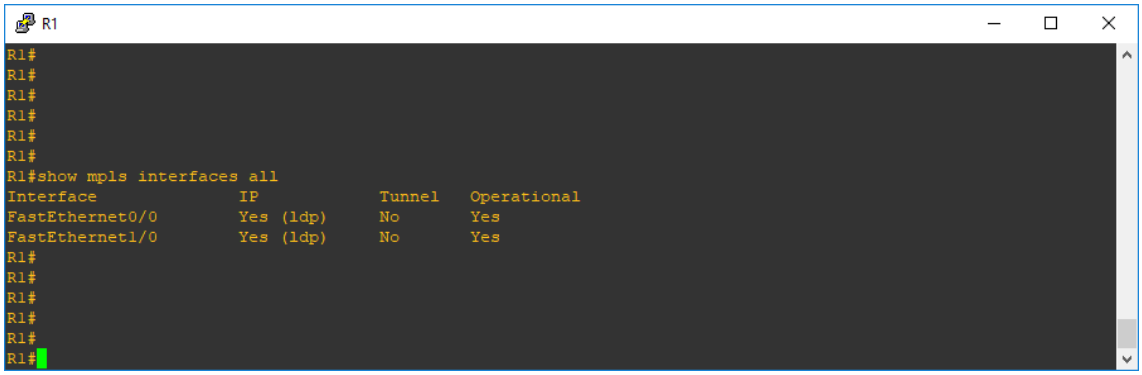


Figura 3.14 Comando "show mpls interfaces all" en R1. Fuente: "GNS3"

Cuando la palabra clave *all* se específica en la figura anterior, sola en este comando, la información sobre las interfaces configuradas para la conmutación de etiquetas se muestra para todas las VPN, incluidas las VPN en el dominio de enrutamiento predeterminado.

Lo mismo sucede para el caso de la figura 3.15. Donde el comando muestra la información mpls específica de cambio de etiqueta de la interfaz FastEthernet 0/0 en detalles.

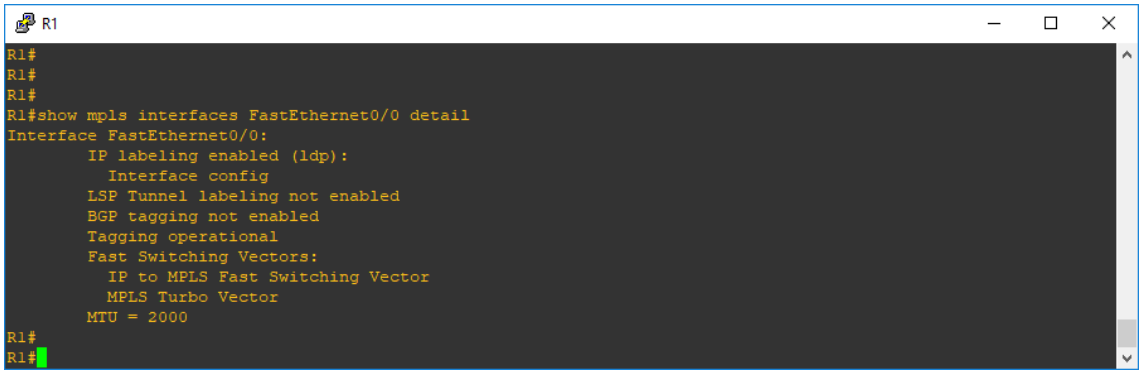


Figura 3.15 Comando "show mpls interfaces FastEthernet0/0 detail" en R1. Fuente: "GNS3"

Para mostrar el estado de las sesiones del protocolo de distribución de etiquetas (LDP), se emite el comando *show mpls ldp neighbor* en el usuario EXEC o en el modo EXEC privilegiado, tal como se muestra en la figura 3.16.

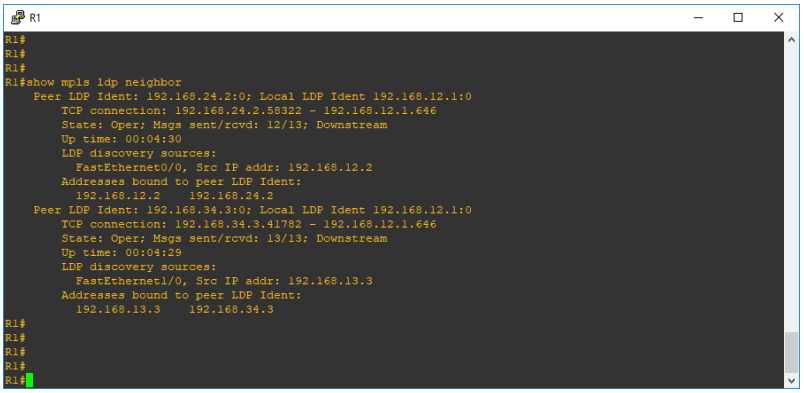


Figura 3.16 Comando "show mpls ldp neighbor" en R1. Fuente: "GNS3"

Para mostrar los parámetros actuales del protocolo de distribución de etiquetas (LDP), se utiliza el comando *show mpls ldp parameters* en el modo EXEC privilegiado, tal como se muestra en la figura 3.17.

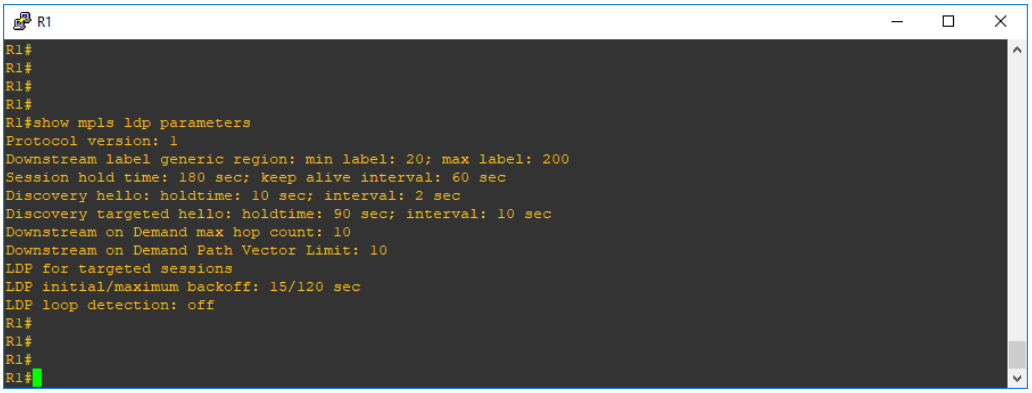


Figura 3.17 Comando "show mpls ldp parameters" en R1. Fuente: "GNS3"

Entre los parámetros de relevancia que se muestran están:

- La versión de protocolo que indica la versión de LDP que se ejecuta en la plataforma.
- Los Discovery Hello que indican la cantidad de tiempo para recordar que una plataforma vecina desea una sesión LDP sin recibir un mensaje de saludo LDP del vecino (tiempo de retención), y el intervalo de tiempo entre la transmisión de mensajes Hello LDP consecutivos a los vecinos (intervalo).

Para mostrar el estado del proceso de descubrimiento del protocolo de distribución de etiquetas (LDP), se utiliza el comando *show mpls ldp discovery* en el modo EXEC privilegiado. Este comando genera una lista de interfaces sobre las cuales se ejecuta el proceso de descubrimiento de LDP. Tal como se muestra en la figura 3.18.

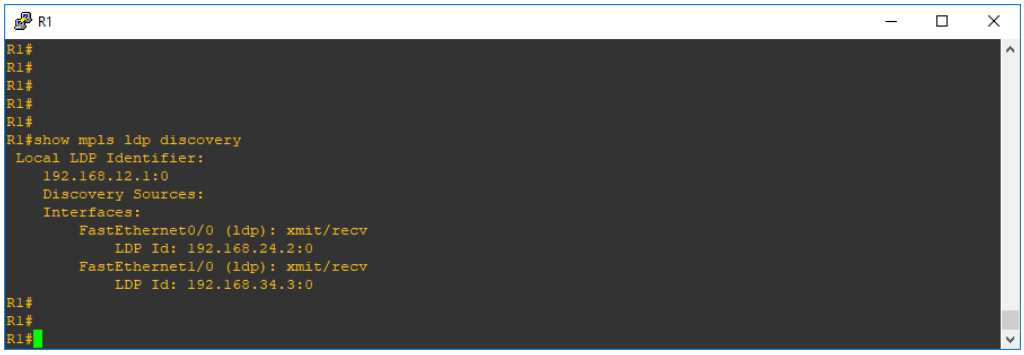


Figura 3.18 Comando "show mpls ldp discovery" en R1. Fuente: "GNS3"

Entre los parámetros de relevancia que se muestran está:

- Identificador local de LDP: El identificador LDP para el enrutador local. Un identificador LDP es una construcción de 6 bytes que se muestra en la forma "Dirección IP: número". Por convención, los primeros cuatro bytes del identificador LDP constituyen la identificación del enrutador; los enteros, comenzando con 0, constituyen los dos bytes finales de la dirección IP: construcción numérica.

Para visualizar los contenidos de la base de información de etiquetas (LIB), use el comando *show mpls ldp bindings* en modo EXEC privilegiado: como la figura 3.19.

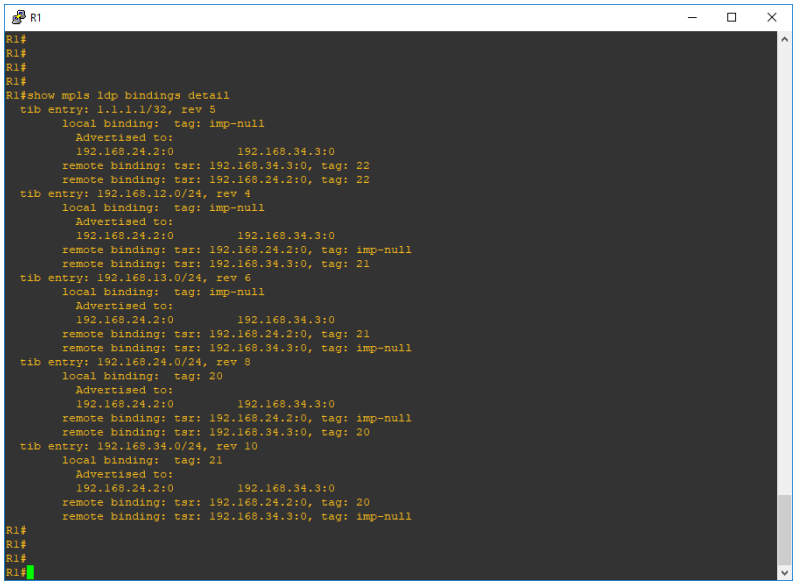


Figura 3.19 Comando "show mpls ldp bindings details" en R1. Fuente: "GNS3"

El comando *show mpls ldp bindings*, también, muestra los enlaces de etiquetas aprendidos por el protocolo de distribución de etiquetas (LDP) o el Tag Distribution Protocol (TDP). Una solicitud puede especificar que se muestre toda la base de datos o que la visualización se limite a un subconjunto de entradas de acuerdo con lo siguiente:

- Prefijo
- Rangos o valores de etiquetas de entrada o salida
- Vecino anunciando la etiqueta

3.1.4 Laboratorio #4 “MPLS VPN”

En este laboratorio se configura una red MPLS sobre VPN utilizando tablas VRF con direcciones de familia IPv4 y protocolos de enrutamiento OSPF, EIGRP y BGP con direcciones de familia vpnv4 (VPN para IPv4), para evaluar el desempeño de la red utilizando la interfaz de línea de comandos de GNS3.

La figura 3.20 muestra el conjunto de VRF definido, en este caso es CUSTOMER, asignado con el ID 100:1 a la interfaz ethernet Fa1/0. Este mismo VRF se define en los enrutadores restantes.

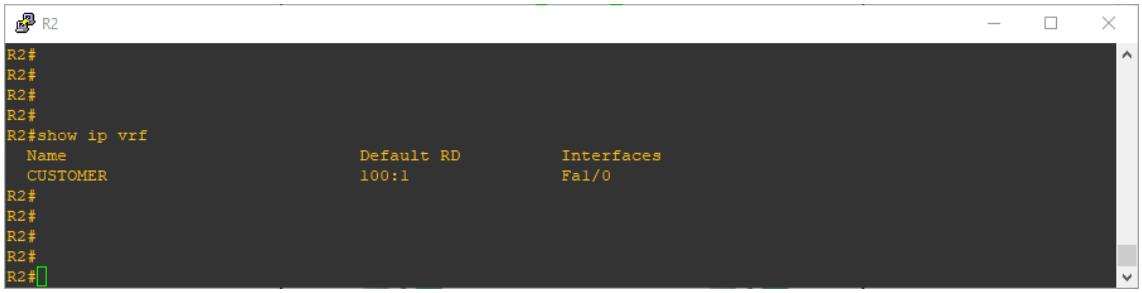


Figura 3.20 Comando “show ip vrf” en R1. Fuente: “GNS3”

Algo similar sucede con la expresión del comando *show ip vrf interfaces*. La figura 3.21 muestra este resultado. El enfoque es diferente, pero, básicamente, existe el mismo resultado, aunque un poco más detallado. La interfaz Fa1/0 posee la dirección 192.168.12.2, la cual tiene asignado la VRF CUSTOMER y el estado del protocolo en sí, está activo.

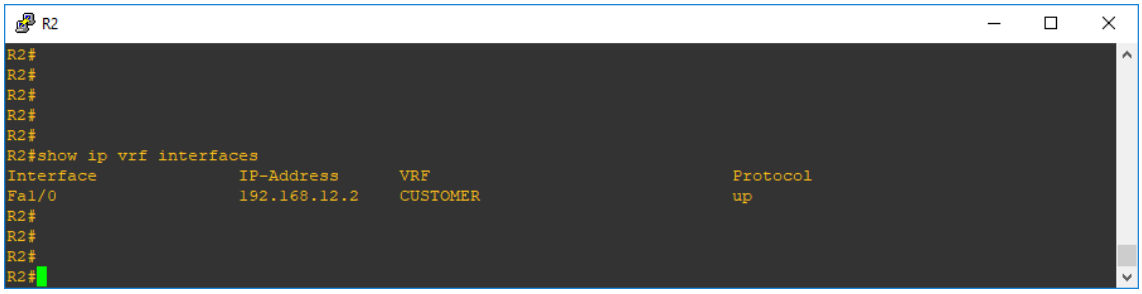


Figura 3.21 Comando “show ip vrf” en R2. Fuente: “GNS3”

El comando *show ip route vrf* muestran el mismo prefijo 200.0.6.0/24 en ambas las salidas. Esto es porque el enrutador PE tiene la misma red para los clientes, CUSTOMER, que se permite en una solución típica del MPLS VPN. La demostración de este comando se muestra en la figura 3.22 y 3.23.

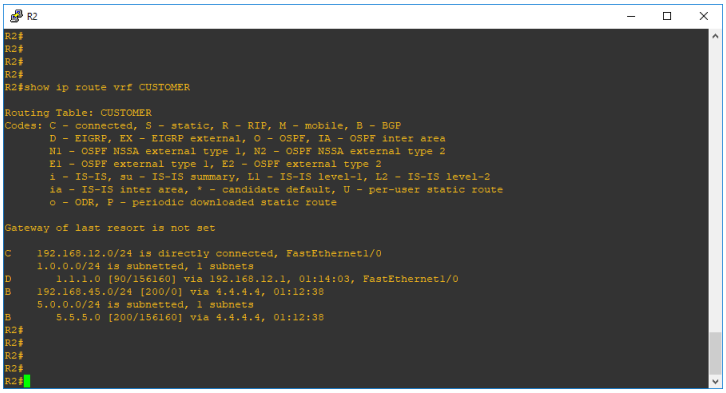


Figura 3.22 Comando "show ip route vrf CUSTOMER" en R2. Fuente: "GNS3"

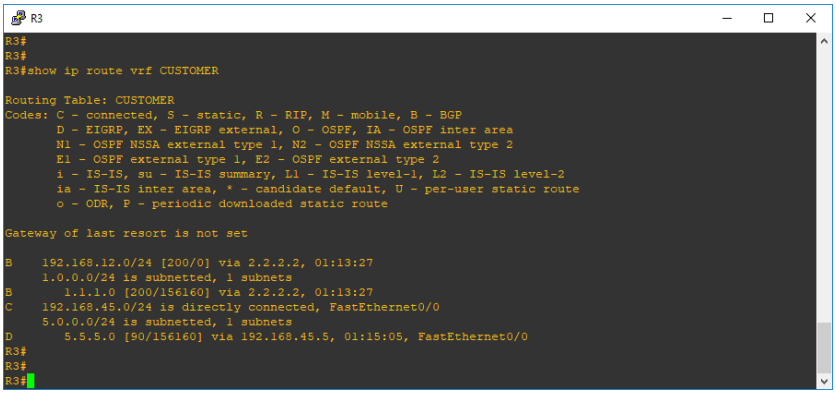


Figura 3.23 Comando "show ip route vrf CUSTOMER" en R3. Fuente: "GNS3"

Si se ejecuta un *traceroute* entre dos sitios del CUSTOMER, es posible ver la pila de etiquetas usada por la red MPLS (si es configurada por el mpls IP usando el TTL). La pila de etiquetas para este sitio se muestra en la figura 3.24.

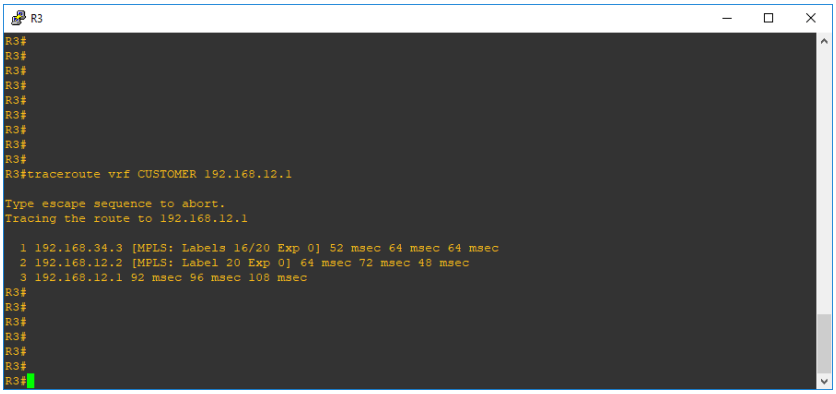


Figura 3.24 Comando "traceroute vrf CUSTOMER 192.168.12.1" en R3. Fuente: "GNS3"

1.3 Conclusiones del capítulo

En este capítulo se llegó a la conclusión de que existía un correcto funcionamiento y desempeño de los cuatro laboratorios desarrollados mediante el uso de comandos que así lo demostraron.

CONCLUSIONES

Con la realización de este trabajo de investigación se obtuvieron los siguientes resultados:

- Se ha realizado un profundo análisis de las tecnologías de transporte de banda ancha para poder comprenderlas e implementarlas en los laboratorios. El estudio ha sido muy revelador sobre las fortalezas y debilidades de dichas tecnologías.
- Se ha estudiado los diferentes tipos de simuladores existentes con el objetivo de tener una visión lo suficientemente amplia para decidir correctamente cuál se utilizará, y se escoge GNS3 por ser una excelente herramienta que ofrece resultados muy precisos, confiables y de gran utilidad para el campo de la docencia y la planificación de redes.

Los resultados obtenidos para los laboratorios desarrollados fueron:

Laboratorio #1:

Se distribuyen correctamente las etiquetas en toda la red utilizando el multiprotocolo de conmutación de etiquetas (MPLS) y el enrutamiento se desarrolla por la ruta más corta al emplearse como protocolo enrutamiento OSPF, concluyendo de esta manera el adecuado funcionamiento de la topología realizada.

Laboratorio #2:

Se confirmó al hacer uso de las listas de control de acceso (ACL) que todos los prefijos se publicaran con la etiqueta deseada para evitar que las etiquetas MPLS fueran divulgadas y de este modo garantizar la seguridad de la red.

Laboratorio #3:

En esta topología se demostró que se pueden añadir nuevos servicios para los clientes que puedan ir adicionándose al núcleo MPLS al configurar la red utilizando MPLS con LDP que es altamente escalable.

Laboratorio #4:

Se hizo posible la configuración para lograr la interconexión de varios clientes de modo transparente a través de una red de proveedor de servicio y se logró impedir que el envío de la información quedara fuera de la VPN para de esta forma usar la misma subred en varias VPN sin causar problemas de direcciones IP duplicadas, utilizando protocolos OSPF, EIGRP y BGP, tablas VRF, direcciones de familia IPv4 y vpnv4 en una red MPLS sobre VPN.

RECOMENDACIONES

Estos laboratorios pueden ser empleados como actividades complementarias extra clase para los estudiantes de la carrera y en general para cualquier interesado en los temas expuestos pues constituyen un valioso material de consulta.

1. Continuar desarrollando otros laboratorios sobre temas relacionados que puedan ser puestos a disposición de los estudiantes contribuyendo a mejorar sus habilidades en las asignaturas.
2. Mantener actualizada toda la información disponible para cada contenido, con el objetivo de estimular al estudiante al trabajo con estos laboratorios, los cuales facilitan el desarrollo de su formación.
3. Incluir estos laboratorios en el plan de estudio de la asignatura de redes, con el objetivo de lograr que los estudiantes puedan familiarizarse con estas topologías y así poner en práctica los conocimientos adquiridos de las conferencias de redes.

REFERENCIAS BIBLIOGRÁFICAS

[1] M. Luisa and H. Belmont, “Regulación de la Banda Ancha : Experiencia Internacional y aplicación al caso peruano,” 2010.

[2] M. Rouse, “Multiprotocol Label Switching (MPLS),” 2014.

[3] M. O. TAPASCO, “MPLS, EL PRESENTE DE LAS REDES IP,” *PROGRAMA INGERIERIA Sist. Y Comput. PEREIRA*, 2008.

[4] M. NIVEN-JENKINS, B., BRUNGARD, D. & BETTS, “E. ROSEN, A., VISWANATHAN & CALLON, R. Jan 2001. Multiprotocol Label Switching Architecture. Internet Engineering Task Force, RFC 3031.,” 2009.

[5] R. E. ROSEN, A., VISWANATHAN & CALLON, “Multiprotocol Label Switching Architecture. Internet Engineering Task Force, RFC 3031.,” 2001.

[6] P. BRYANT, S. & PATE, “Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture. Internet Engineering Task Force, RFC 3985.,” 2005.

[7] R. BELLER, D. & SPERBER, “MPLS-TP – The New Technology for Packet Transport Networks. Alcatel-Lucent, Deutschland AG,” 2012.

[8] S. K. Pupiales, “Backbone MPLS,” 2012.

[9] C. Systems, “‘Implementing Cisco Service Provider Next-Generation Edge Network Services’ Student Guide v1.2,” 2014.

[10] L. De Ghein, “‘MPLS Fundamentals,’” *Cisco Press*, 2007.

[11] A. Kim, “OPNET Tutorial,” 2005. .

[12] O. Modeler, “Tutorial Opnet Modeler,” 2012. .

[13] J. SULLIVAN, “COMNET III Getting Started Guide, Relase 2.0. CACI Products,” 2012.

[14] J. SULLIVAN, “COMNET III Tutorial. A Detailed Guide for Modeling Networks, Relase 2.1. CACI Products,” 2012.

[15] R. W. QUONG, “OMNET++ User’s Manual,” 2012.

[16] S.-Y. WANG, “The Gui User Manual for the NCTUns 2.0 Network Simulator and

Emulator,” 2012.

[17] I. CISCO SYSTEMS, “Tutorial Packet Tracer 5.3.1,” 2010. .

[18] G. TEAM, “Graphical Network Simulator - GNS3,” 2012.

[19] G. A. P. PIEDRA, “Estudio de Red ATM y Simulador GNS3. Universidad Tecnológica América.,” 2010.

[20] G. J. PACE, “Modelos y Simulación, UNNE FCNA.,” 2003.

[21] G. TEAM, “Foro de consultas de Dynamips, Dynagen,” 2012.

[22] G. Aranzalez, J. Eliecer, J. D. Grisales Garzón, and others, “Sistema para Configurar una Red EIGRP de Routers GNS3 Virtualizados, desde una Aplicación Android,” 2016.

[23] I. A. F. Alcántara, “Simulador de redes GNS3: estudio, pruebas con prácticas y propuesta de uso,” *Univ. Nac. Autónoma México.*, 2015.

[24] U. C. de Madrid, “Proyecto de Innovación Software libre para ciencias e ingenierías,” 2014.

[25] J. D. P. B. Tortosa Ybáñez, María Teresa Álvarez Teruel, “XIII Jornadas de Redes de Investigación en Docencia Universitaria. Nuevas estrategias organizativas y metodológicas en la formación universitaria para responder a la necesidad de adaptación y cambio,” 2015.

[26] U. de Alicante, “Topologías de redes de computadoras virtuales,” 2015.

[27] R. Coltun, D. Ferguson, J. Moy, and A. Lindem, “RFC 5340, OSPF for IPv6,” *IETF. July*, vol. 24, 2008.

[28] CISCO SYSTEMS, “Configuración básica de MPLS usando OSPF,” 2005.

[29] CISCO SYSTEMS, “1 - MPLS Label Filtering,” 2008.

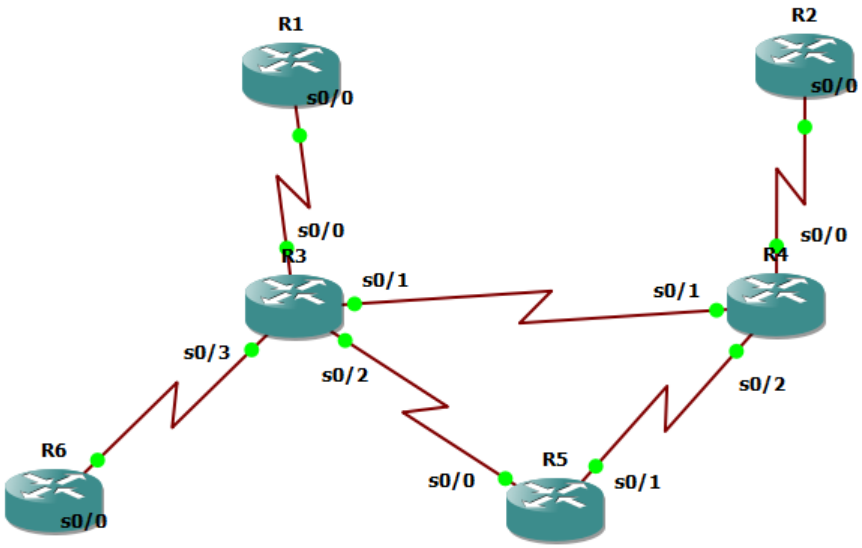
[30] CISCO SYSTEMS, “MPLS LDP Configuration Guide, Cisco IOS Release,” 2011.

[31] CISCO SYSTEMS, “Configuración de una VPN MPLS básica,” 2007.

ANEXOS

Anexo 1: Parámetros y configuraciones del laboratorio #1

A2.1 Topología de Red del laboratorio 1.



A2.2 Comandos para el direccionamiento IP en interfaces seriales de los enrutadores

R4#

R4#configure terminal

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

R4(config)#interface Serial0/0

R4(config-if)#ip address 10.1.1.21 255.255.255.252

R4(config-if)#no shutdown

R4(config-if)#exit

R4(config)#interface Serial0/1

R4(config-if)#ip address 10.1.1.6 255.255.255.252

R4(config-if)#no shutdown

R4(config-if)#exit

R4(config)#interface Serial0/2

R4(config-if)#ip address 10.1.1.9 255.255.255.252

R4(config-if)#no shutdown

R4(config-if)#end

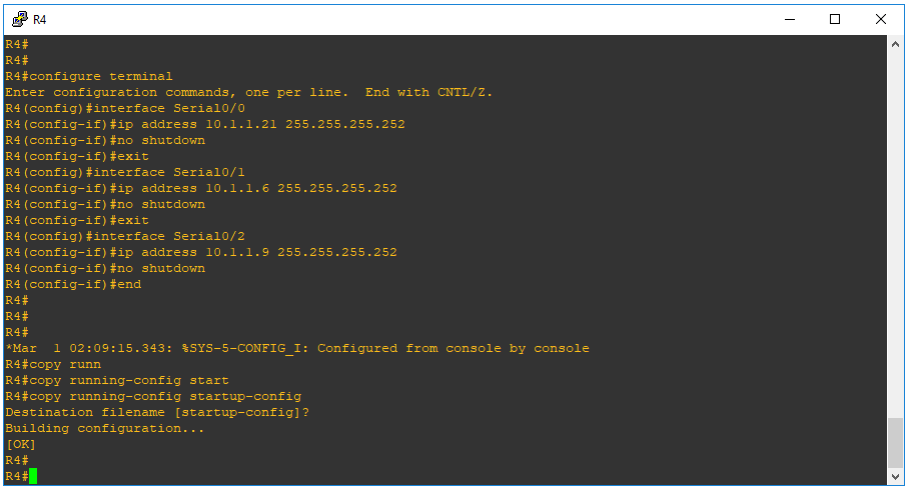
R4#

R4#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]



A2.3 Comandos para el direccionamiento IP en interfaces loopback y enrutamiento OSPF

R4#

R4#configure terminal

R4(config)#interface Loopback0

R4(config-if)#ip address 10.10.10.3 255.255.255.255

R4(config-if)#exit

R4(config)#router ospf 10

R4(config-router)#log-adjacency-changes

R4(config-router)#network 10.0.0.0 0.255.255.255 area 9

R4(config-router)#end

R4#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

A2.4 Comandos para la configuración de MPLS IP en R4

R4#configure terminal

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

R4(config)#interface Serial0/0

R4(config-if)#mpls ip

R4(config-if)#interface Serial0/1

R4(config-if)#mpls ip

R4(config-if)#interface Serial0/2

R4(config-if)#mpls ip

R4(config-if)#end

R4#cop

*Mar 1 02:49:46.707: %SYS-5-CONFIG_I: Configured from console by console

R4#copy runn

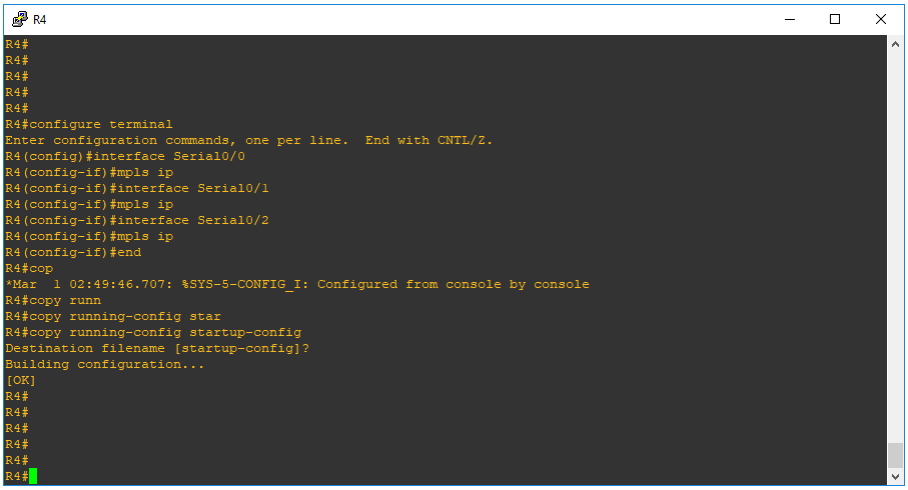
R4#copy running-config star

R4#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

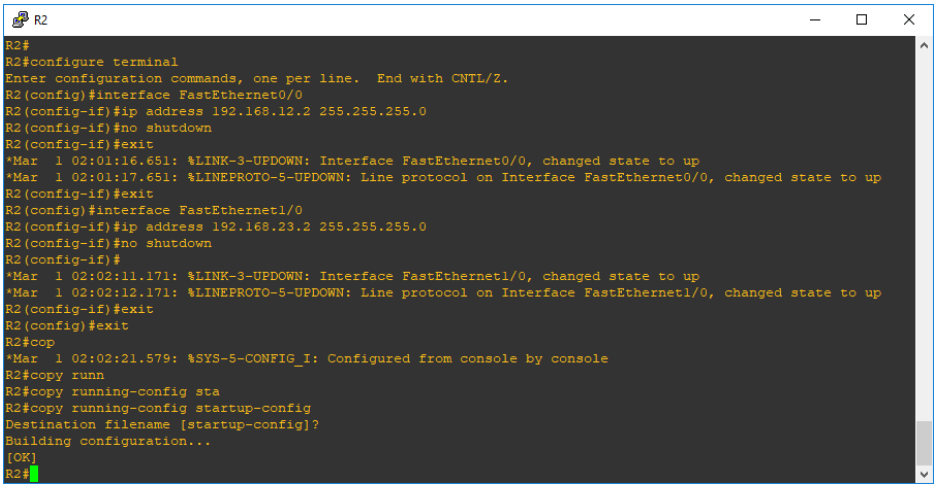
[OK]


R4
R4#
R4#
R4#
R4#
R4#
R4#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#interface Serial0/0
R4(config-if)#mpls ip
R4(config-if)#interface Serial0/1
R4(config-if)#mpls ip
R4(config-if)#interface Serial0/2
R4(config-if)#mpls ip
R4(config-if)#end
R4#cop
*Mar 1 02:49:46.707: %SYS-5-CONFIG_I: Configured from console by console
R4#copy runn
R4#copy running-config star
R4#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R4#
R4#
R4#
R4#
R4#
R4#

Anexo 2: Parámetros y configuraciones del laboratorio #2

A2.1 Topología de Red del laboratorio 2.

A2.2 Comandos para el direccionamiento IP en interfaces Fast Ethernet de los tres enrutadores.



Comandos utilizados para el direccionamiento en interfaces de red Fast Ethernet:

R2#configure terminal

R2(config)#interface FastEthernet0/0

R2(config-if)#ip address 192.168.12.2 255.255.255.0

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#interface FastEthernet1/0

R2(config-if)#ip address 192.168.23.2 255.255.255.0

R2(config-if)#no shutdown

R2(config-if)#end

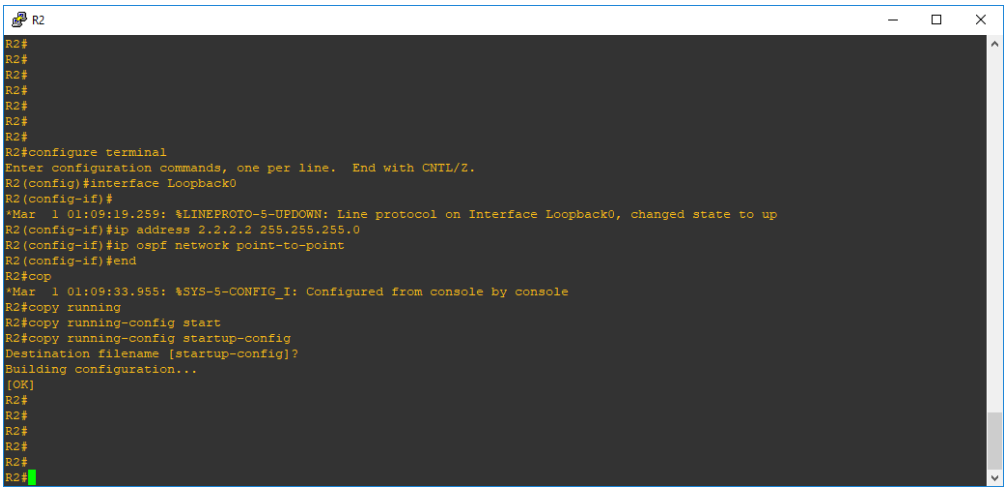
R2#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

A2.3 Comandos para el direccionamiento IP en interfaces Loopback de los tres enrutadores



Comandos utilizados para el direccionamiento en interfaces de red Loopback:

R2#configure terminal

R2(config)#interface Loopback0

R2(config-if)#ip address 2.2.2.2 255.255.255.0

R2(config-if)#ip ospf network point-to-point

R2(config-if)#end

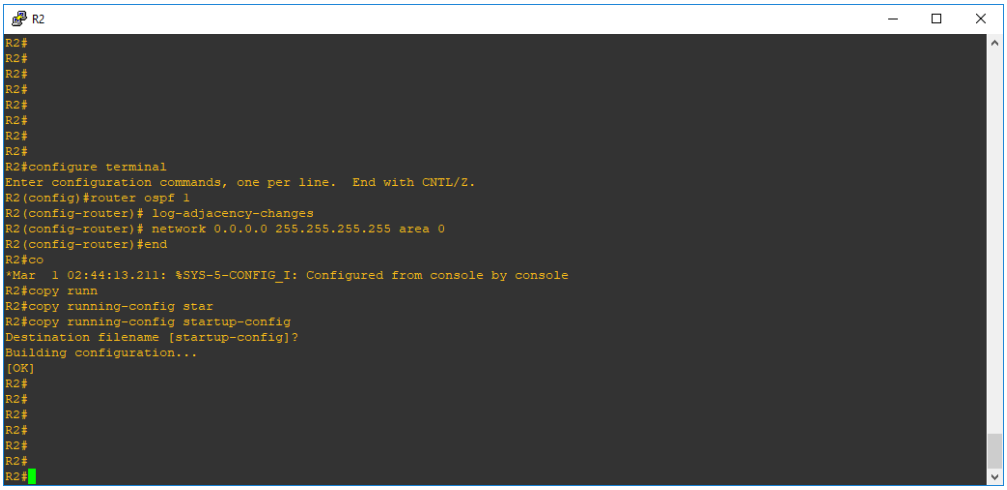
R2#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

A2.4 Enrutamiento OSPF



Comandos:

 # router ospf 1

Activa el protocolo OSPF en el Cisco Router. El "1" significa "Process ID". Por favor NO confundir con Sistema Autónomo (AS). Esta variable NO tiene que ser idéntica en todos los routers de la red. Esta variable simplemente identifica el proceso en ejecución dentro del Cisco IOS.

 # network 0.0.0.0 255.255.255.255 area 0

El comando Network activa el protocolo OSPF en todas las interfaces del router que su dirección IP estén dentro del rango de la red 0.0.0.0 (Todas para este caso). La parte de "255.255.255.255" NO es una máscara de red, sino más bien un Wildcard. Un Wilcard es lo contrario de una máscara de red. Los bits que están en cero son los bits de la dirección de red que se van a tomar en cuanta. Los bits puestos en uno (255) NO se toman en cuenta. El argumento "área 0" indica el área a la que van pertenecer las interfaces del router.

A2.5 Listas de Control de Accesos

Las ACL estándar son el tipo más antiguo de ACL. Datan ya del Cisco IOS Software, versión 8.3. Las ACL estándar controlan el tráfico por la comparación de la dirección de origen de los paquetes IP con las direcciones configuradas en la ACL. Este es el formato de sintaxis del comando de una ACL estándar configurada en R2.

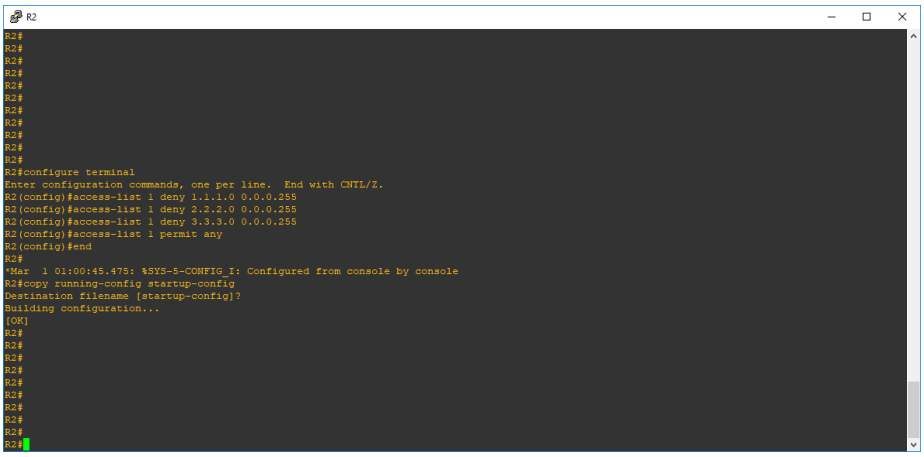
access-list access-list-number {permit|deny} {host|source source-wildcard|any}

access-list 1 deny   1.1.1.0 0.0.0.255

access-list 1 deny   2.2.2.0 0.0.0.255

access-list 1 deny   3.3.3.0 0.0.0.255

access-list 1 permit any



A2.6 Filtrado de etiquetas MPLS y servicio mpls ip

configure terminal

no mpls ldp advertise-labels

mpls ldp advertise-labels for 1

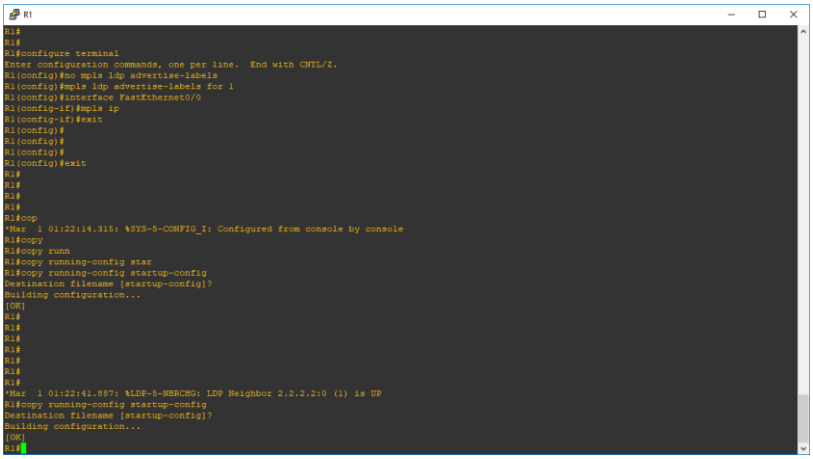
interface FastEthernet0/0

mpls ip

exit

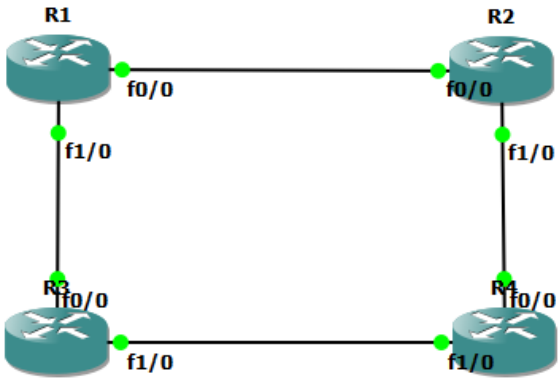
interface FastEthernet1/0

mpls ip

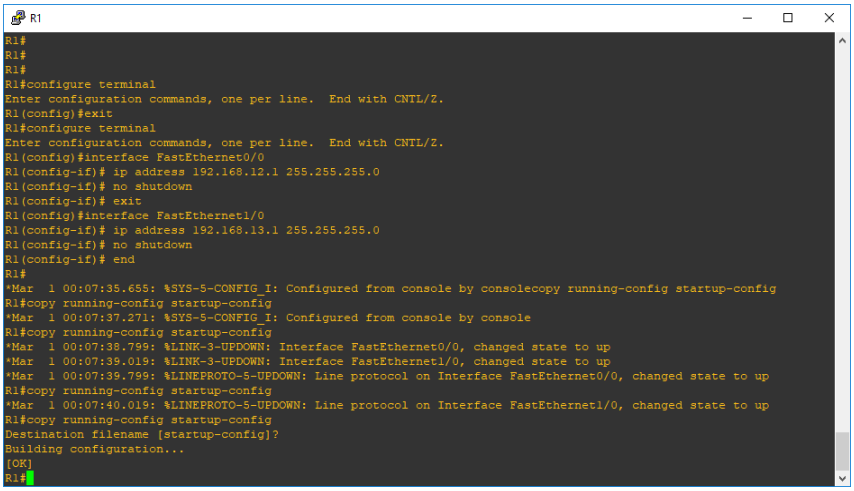


Anexo 3: Parámetros y configuraciones del laboratorio #3

A3.1 Topología de Red del laboratorio 3.



A3.2 Comandos para el direccionamiento IP en interfaces Fast Ethernet en los enrutadores R1 R2 R3 y R4.



Comandos utilizados para el direccionamiento en interfaces de red Fast Ethernet:

R1#configure terminal

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

R1(config)#exit

R1#configure terminal

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

R1(config)#interface FastEthernet0/0

R1(config-if)# ip address 192.168.12.1 255.255.255.0

R1(config-if)# no shutdown

R1(config-if)# exit

R1(config)#interface FastEthernet1/0

R1(config-if)# ip address 192.168.13.1 255.255.255.0

R1(config-if)# no shutdown

R1(config-if)# end

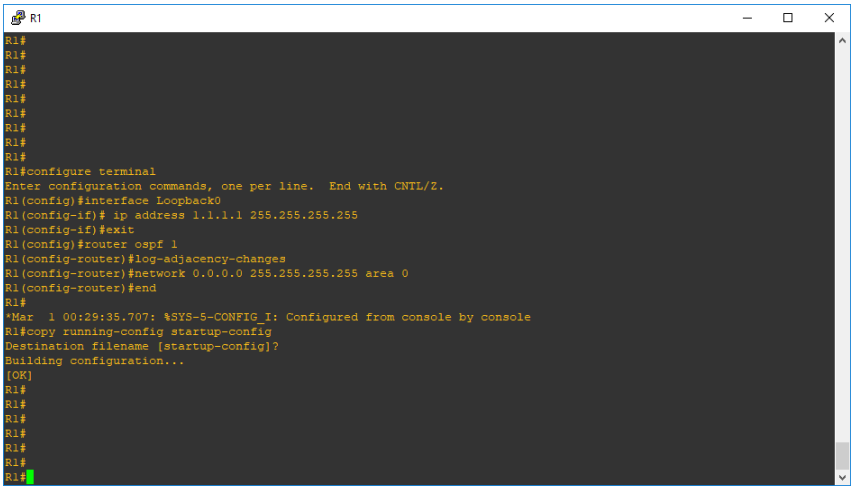
R1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

A3.3 Comandos para el direccionamiento IP en interfaces loopback y enrutamiento OSPF en los enrutadores R1 R2 R3 y R4.



Comandos utilizados para el direccionamiento en interfaces de loopback y enrutamiento OSPF:

R1#configure terminal

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

R1(config)#interface Loopback0

R1(config-if)# ip address 1.1.1.1 255.255.255.255

R1(config-if)#exit

R1(config)#router ospf 1

R1(config-router)#log-adjacency-changes

R1(config-router)#network 0.0.0.0 255.255.255.255 area 0

R1(config-router)#end

*Mar 1 00:29:35.707: %SYS-5-CONFIG_I: Configured from console by console

R1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

A3.4 Comandos para las configuraciones de MPLS LDP

Comandos para R1

R1#configure terminal

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

R1(config)#mpls label range 20 200

R1(config)#mpls ip default-route

R1(config)#mpls ldp neighbor 3.3.3.3 password UCLV

R1(config)#mpls ldp neighbor 2.2.2.2 password UCLV

R1(config)#mpls ldp discovery hello interval 2

R1(config)#mpls ldp discovery hello holdtime 10

R1(config)#mpls ldp maxhops 10

R1(config)#interface FastEthernet0/0

R1(config-if)# mpls ip

R1(config-if)# mpls mtu 2000

R1(config-if)# exit

R1(config)#interface FastEthernet1/0

R1(config-if)# mpls ip

R1(config-if)# mpls mtu 2000

R1(config-if)# exit

R1(config)#mpls ldp router-id FastEthernet0/0 force

R1(config)#end

R1#copy running-config startup-config

*Mar 1 00:13:32.491: %SYS-5-CONFIG_I: Configured from console by console

R1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Comando para R2

R2#configure terminal

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

R2(config)#mpls label range 20 200

R2(config)#mpls ip default-route

R2(config)#mpls ldp neighbor 4.4.4.4 password UCLV

R2(config)#mpls ldp neighbor 1.1.1.1 password UCLV

R2(config)#mpls ldp discovery hello interval 2

R2(config)#mpls ldp discovery hello holdtime 10

R2(config)#mpls ldp maxhops 10

R2(config)#interface FastEthernet0/0

R2(config-if)# mpls ip

R2(config-if)# exit

R2(config)#interface FastEthernet1/0

R2(config-if)# mpls ip

R2(config-if)# exit

R2(config)#end

R2#copy running-config startup-config

*Mar 1 00:14:45.871: %SYS-5-CONFIG_I: Configured from console by console

R2#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Comandos para R3

R3#configure terminal

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

R3(config)#mpls label range 20 200

R3(config)#mpls ip default-route

R3(config)#mpls ldp neighbor 4.4.4.4 password UCLV

R3(config)#mpls ldp neighbor 1.1.1.1 password UCLV

R3(config)#mpls ldp discovery hello interval 2

R3(config)#mpls ldp discovery hello holdtime 10

R3(config)#mpls ldp maxhops 10

R3(config)#interface FastEthernet0/0

R3(config-if)# mpls ip

R3(config-if)# exit

R3(config)#interface FastEthernet1/0

R3(config-if)# mpls ldp discovery transport-address interface

R3(config-if)# mpls ip

R3(config-if)# exit

R3(config)#end

R3#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

*Mar 1 00:15:23.995: %SYS-5-CONFIG_I: Configured from console by console

Comandos para R4

R4#configure terminal

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

R4(config)#mpls label range 20 200

R4(config)#mpls ip default-route

R4(config)#mpls ldp neighbor 2.2.2.2 password UCLV

R4(config)#mpls ldp neighbor 3.3.3.3 password UCLV

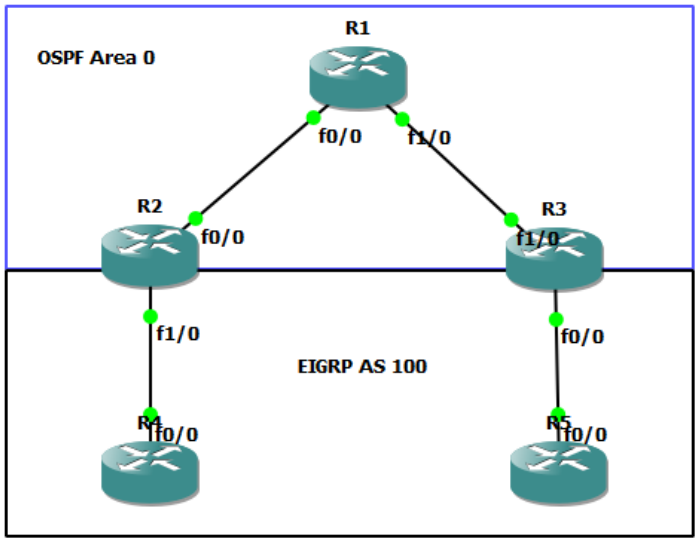
R4(config)#mpls ldp discovery hello interval 2

R4(config)#mpls ldp discovery hello holdtime 10

```
R4(config)#mpls ldp maxhops 10
R4(config)#interface FastEthernet0/0
R4(config-if)# mpls ip
R4(config-if)# exit
R4(config)#interface FastEthernet1/0
R4(config-if)# mpls ldp discovery transport-address interface
R4(config-if)# mpls ip
R4(config-if)# exit
R4(config)#end
R4#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Anexo 4: Parámetros y configuraciones del laboratorio #4

A4.1 Topología de Red del laboratorio 4.



A4.2 Comandos para el direccionamiento IP en interfaces Fast Ethernet en el enrutador R1

R1#configure terminal

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

R1(config)#interface FastEthernet0/0

R1(config-if)#ip address 192.168.23.3 255.255.255.0

R1(config-if)#no shutdown

R1(config-if)#interface FastEthernet1/0

R1(config-if)#ip address 192.168.34.3 255.255.255.0

R1(config-if)#no shutdown

R1(config-if)#exit

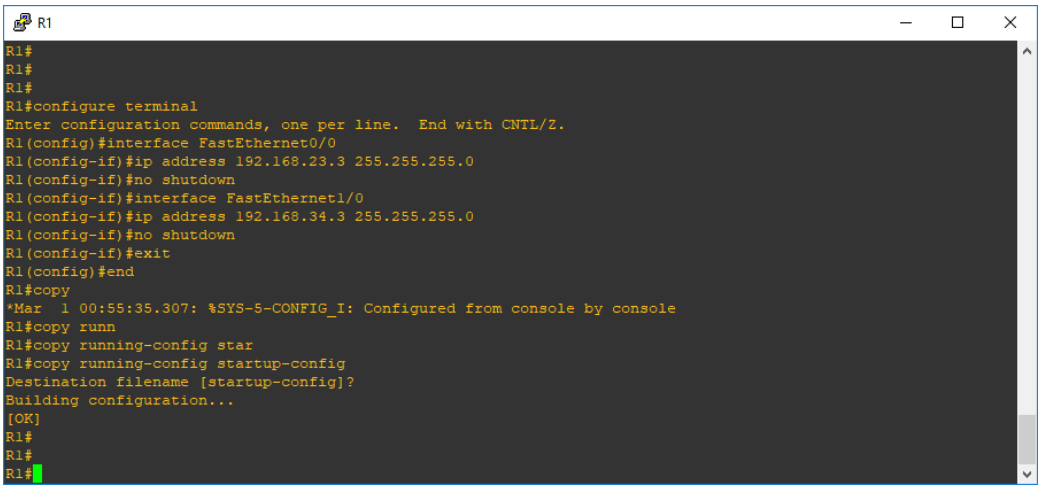
R1(config)#end

R1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]



A4.3 Direccionamiento para interfaces loopback en todos los enrutadores y enrutamiento OSPF en el enrutador R1 como ejemplo.

R1#configure terminal

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

R1(config)#interface Loopback0

R1(config-if)#ip address 3.3.3.3 255.255.255.0

R1(config-if)#ip ospf network point-to-point

R1(config-if)#exit

R1(config)#router ospf 1

R1(config-router)#log-adjacency-changes

R1(config-router)#network 3.3.3.0 0.0.0.255 area 0

R1(config-router)#network 192.168.23.0 0.0.0.255 area 0

R1(config-router)#network 192.168.34.0 0.0.0.255 area 0

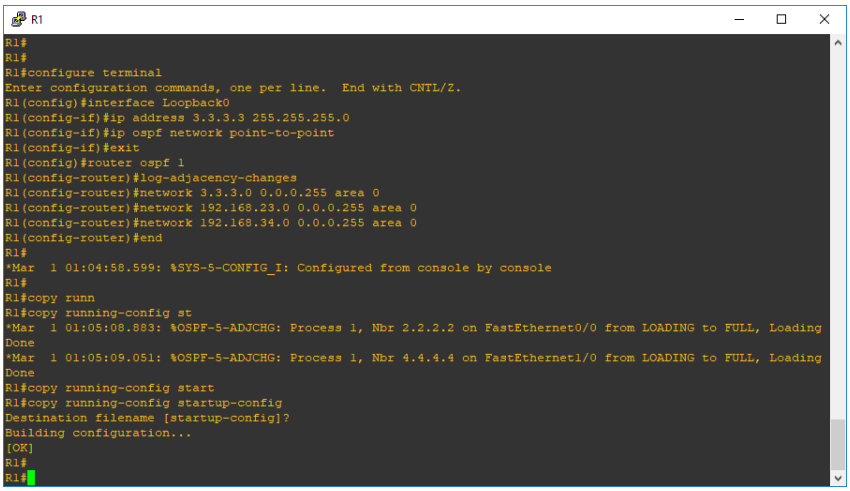
R1(config-router)#end

R1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]



A4.4 VPN / Enrutamiento y Reenvío Virtual (VPN / Virtual Routing and Forwarding)

R2#configure terminal

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

R2(config)#ip vrf CUSTOMER

R2(config-vrf)#rd 100:1

R2(config-vrf)#route-target export 1:100

R2(config-vrf)#route-target import 1:100

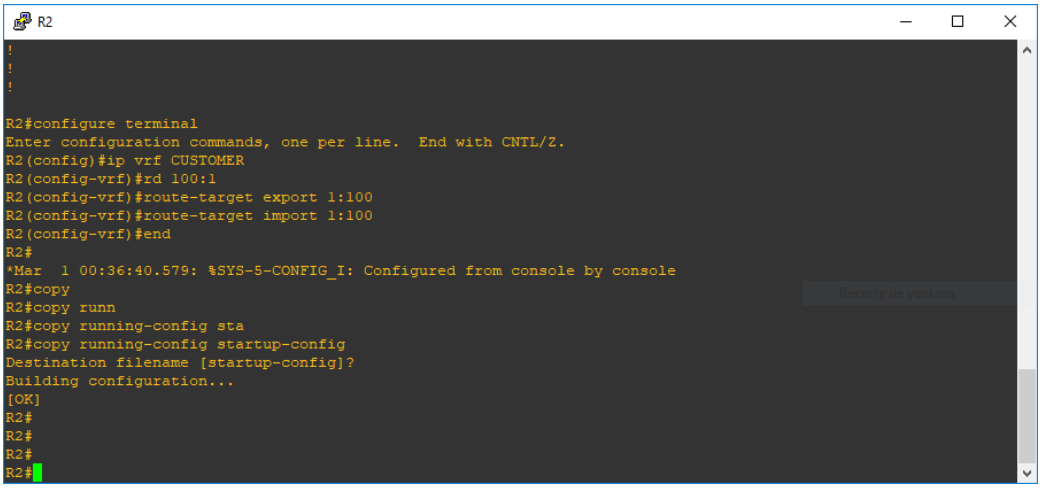
R2(config-vrf)#end

R2#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]



A4.5 BGP y EIGRP

EIGRP - R2

router eigrp 1

auto-summary

address-family ipv4 vrf CUSTOMER

redistribute bgp 1 metric 1500 4000 200 10 1500

network 192.168.12.0

no auto-summary

autonomous-system 100

exit-address-family

EIGRP – R3

router eigrp 1

auto-summary

address-family ipv4 vrf CUSTOMER

redistribute bgp 1 metric 1500 400 20 20 1500

network 192.168.45.0

no auto-summary

autonomous-system 100

exit-address-family

EIGRP – R4

router eigrp 100

network 1.0.0.0

network 192.168.12.0

no auto-summary

EIGRP – R5

router eigrp 100

network 5.0.0.0

network 192.168.45.0

no auto-summary

BGP – R2

router bgp 1

no synchronization

bgp log-neighbor-changes

neighbor 4.4.4.4 remote-as 1

neighbor 4.4.4.4 update-source Loopback0

no auto-summary

address-family vpnv4

neighbor 4.4.4.4 activate

neighbor 4.4.4.4 send-community both

exit-address-family

address-family ipv4 vrf CUSTOMER

redistribute eigrp 100

no synchronization

exit-address-family

mpls ldp router-id Loopback0

BGP – R3

router bgp 1

no synchronization

bgp log-neighbor-changes

neighbor 2.2.2.2 remote-as 1

neighbor 2.2.2.2 update-source Loopback0

no auto-summary

address-family vpnv4

neighbor 2.2.2.2 activate

neighbor 2.2.2.2 send-community extended

exit-address-family

address-family ipv4 vrf CUSTOMER

redistribute eigrp 100

no synchronization

exit-address-family

mpls ldp router-id Loopback0

GLOSARIO

***ATM**: Asyncronous Transfer Mode. Modo de transferencia asincrónico.*

***AS:** Sistema autónomo*

***ACL:** Listas de Control de Acceso*

***BGP:** Border Gateway Protocol. Protocolo de puerta de enlace de frontera.*

***CBR:** Constant Bit Rate. Tasa de Bits constante.*

***CCIE:** Cisco Certified Internetwork Expert.*

***CCNA:** Cisco Certified Network Associate.*

***CCNP:** Cisco Certified Network Professional.*

***CE:** Customer Edge. Borde del cliente.*

***CLI:** interfaz de línea de comandos.*

***CoS:** Class of service. Clases de servicio.*

***CR-LDP:** Constraint-based Routing LDP. Direccionamiento basado en restricción*

***DOCSIS:** Data Over Cable Service Interface Specification. Especificación de interfaz de servicio de datos por cable.*

***FDDI**: Data interfaces sent by fiber. Interfaces de datos enviados por fibra.*

***FEC**: Forwarding Equivalent Class. envió equivalente Clase.*

***FIE:** Faculty of Electrical Engineering. Facultad de ingeniería eléctrica.*

***FTP:** file transfer protocol. Protocolo se transferencia de ficheros.*

***GMPLS:** General Multiprotocol Label Switching. Conmutación General multi-protocolo mediante etiquetas.*

***GNS3:** Graphic network simulator. Simulador Gráfico de redes.*

***HTTP:** Hypertext transfer protocol. Protocolo de transferencia de hipertexto.*

***ICMP:** Internet Control Message Protocol. Protocolo de mensaje de control de internet.*

***IEEE**: Institute of Electrical and Electronic Engineering. Instituto de ingeniería eléctrica y electrónica.*

IETF: *Internet Engineering Task Force. Grupo de Trabajo de Ingeniería de Internet.*

IGP: *Interior Gateway Protocol. Protocolo de vía de acceso de interior.*

IP: *Internet Protocol. Protocolo de internet.*

IPSec: *Internet Protocol Security. Seguridad del Protocolo de Internet.*

IPv4: *Internet protocol version 4. Protocolo de internet versión 4.*

IPv6*: Internet protocol version 6. Protocolo de internet versión 6.*

ISO*: International Organization for Standardization. Organización internacional para la normalización.*

ITU-T: *International Telecommunication Union -Telecommunication. Unión internacional de telecomunicadores-Telecomunicadores.*

L2VPN: *Layer 2 Virtual private network. Red privada virtual de Capa 2.*

L3VPN*: Layer 3 Virtual private network. Red privada virtual de Capa 3.*

LAN*: Local area network. Red de área local.*

LDP: *Label Distribution Protocol. Protocolo de distribución de etiquetas.*

LER*: Label Edge Router. Enrutador de nivel de borde.*

LSP*: Label:Switched Path. Ruta de conmutación de etiquetas.*

LSR*: Label Switched Routers. Rótulos con conmutador de etiquetas.*

MAC*: Media access control. Control de acceso al medio.*

MAN: *Network of metropolitan área. Red de área metropolitana.*

MP-BGP: *Multi Protocol-Border Gateway Protocol.Multi Protocolo de puerta de enlace de frontera.*

MPLS*: Multiprotocol Label Switching. Conmutación multi-protocolo mediante etiquetas.*

MPLS-TP: *Multiprotocol Label Switching - Transport Profile. Conmutación de etiquetas multiprotocolo -Perfil de transporte.*

OAM*: Operations, Administration and Maintenance. Operación, administración y mantenimiento.*

OSI*: Interconnection of open systems. Interconexión de sistemas abiertos.*

OSPF*: Open Shortest Path First. Protocolo de Primera Ruta Abierta más Corta.*

OTN*: Optical Transport Network. Red de transporte óptica.*

P: *Provider. Proveedor.*

PE*: Provider Edge. Borde de proveedor.*

PNNI: *Private Network:to:Network Interface. Interfaz de red privada a red.*

PPP*: Point to point protocol. Protocolo punto a punto.*

PWE3: *Pseudo Wire Emulation Edge to Edge. Pseudowire de emulación de borde a borde.*

QoS*: Quality of Service. Calidad de Servicio.*

RDSI: *digital Network of integrated services. Red digital de servicios integrados.*

RFC*: Request for Comments. Pedido para los comentarios.*

RIP*: Routing Information Protocol. Protocolo de información de encaminamiento.*

RSVP*: Resource Reservation Protocol. Protocolo de reservación de recurso.*

RSVP-TE: *Reservation Protocol - Traffic Engineering Protocolo de reserva - Ingeniería de tráfico.*

RTP: *Real-Time Transport Protocol. Protocolo de transporte de tiempo real.*

SDH*: Synchronous Digital Hierarchy. Jerarquía Digital simultánea.*

SDP: *protocol of direct socket. protocol de socket directo.*

SNMP: *Simple Network Management protocol. Protocolo simple de administración de red.*

SONET*: Synchronous optical network. Red óptica sincrónica.*

SRMS: *Shuttle Remote Manipulator System. Servicio Remoto del Sistema manipulador.*

SVG: *Scalable Vector Graphics. Vector gráfico escalable.*

Tcl/TK: *tool command language tool kit. Lenguaje de herramientas de comando/juego de herramientas.*

TCP: *Transmission Control Protocol. Protocolo de Control de Transmisión.*

UCLV*: Central University of the Villas. Universidad Central de las Villas.*

UDP: *user datagram protocol. protocolo de datagrama de Usuario.*

UMTS*: Universal mobile telecommunications system. Sistema universal de telecomunicaciones móviles.*

***VLAN**: Virtual local area network. Red de área local virtual.*

***VoIP:** Voice over Internet Protocol. Voz sobre protocolo de internet.*

***VPLS:** LAN Privada Virtual Virtual Private LAN Service. Servicio de LAN privada virtual.*

***VPMS:** Private Multicast Service. Servicio de Multidifusión Privado Virtual. Virtual.*

***VPN**: Virtual private network. Red privada virtual.*

***VPWS:** Virtual Leased Line. Línea virtual arrendada.*

***VRF:** Virtual routing and forwarding. Enrutamiento Virtual y Reenvío.*

***WAN:** Wide Area Network. Red de área amplia.*

***WDM**: Wavelength Division Multiplexing. Multiplexación por división de longitud de onda.*

***WIFI:** Wireless Fidelity. Fidelidad inalámbrica.*

***Wildcard:** Máscara de bits que indica qué partes de una dirección de IP son relevantes para la ejecución de una determinada acción.*