UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE CUENCA

CARRERA DE TELECOMUNICACIONES

DESARROLLO DE UN MANUAL DE PRÁCTICAS EN IPV6 PARA EL LABORATORIO DE REDES DE COMPUTADORAS DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, SEDE CUENCA

Trabajo de titulación previo a la obtención del título de Ingeniero en Telecomunicaciones

AUTORES: CARLOS ENRIQUE CORREA QUISHPE
ANGEL ERNESTO JIMBO TINIZHAÑAY
TUTOR: ING. JUAN DIEGO JARA SALTOS, MgT.

Cuenca – Ecuador
2024

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Nosotros, Carlos Enrique Correa Quishpe con documento de identificación N° 0105811426 y Angel Ernesto Jimbo Tinizhañay con documento de identificación N° 0106721186; manifestamos que:

Somos los autores y responsables del presente trabajo; y, autorizamos a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Cuenca, 16 de febrero del 2024

Atentamente,

Carlos Enrique Correa Quishpe
0105811426

Angel Ernesto Jimbo Tinizhañay
0106721186

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Nosotros, Carlos Enrique Correa Quishpe con documento de identificación N° 0105811426 y Angel Ernesto Jimbo Tinizhañay con documento de identificación N° 0106721186, expresamos nuestra voluntad y por medio del presente documento cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del Proyecto técnico: "Desarrollo de un manual de prácticas en IPv6 para el laboratorio de redes de computadoras de la Universidad Politécnica Salesiana, Sede Cuenca", el cual ha sido desarrollado para optar por el título de: Ingeniero en Telecomunicaciones, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Cuenca, 16 de febrero del 2024

Atentamente,

Carlos Enrique Correa Quishpe
0105811426

Angel Ernesto Jimbo Tinizhañay
0106721186

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Juan Diego Jara Saltos con documento de identificación N°0103543658, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: DESARROLLO DE UN MANUAL DE PRÁCTICAS EN IPv6 PARA EL LABORATORIO DE REDES DE COMPUTADORAS DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, SEDE CUENCA, realizado por Carlos Enrique Correa Quishpe con documento de identificación N° 0105811426 y por Angel Ernesto Jimbo Tinizhañay con documento de identificación N° 0106721186, obteniendo como resultado final el trabajo de titulación bajo la opción Proyecto técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Cuenca, 16 de febrero del 2024

Atentamente,

Ing. Juan Diego Jara Saltos, Mgt.
0103543658

AGRADECIMIENTOS

Agradecimiento de Carlos Enrique Correa Quishpe

Quisiera expresar mi agradecimiento a Dios por permitirme alcanzar este momento crucial en mi vida. Agradezco profundamente a mis padres por su amor incondicional y respaldo moral, siendo su fe en mí el pilar fundamental de este logro, incluso en los momentos más desafiantes. También, deseo expresar mi reconocimiento a mis hermanos por su apoyo incondicional, así como a mis abuelitos y tíos, quienes estuvieron presentes cuando más los necesitaba. Sin su contribución, este logro no habría sido posible; su amor y sacrificio han iluminado mi camino a lo largo de este trayecto académico y el cumplimiento de mis metas. Extendiendo mi gratitud a mi tutor, Juan Diego Jara, por sus valiosas aportaciones y comentarios que enriquecieron el desarrollo de este Trabajo de Titulación. Quiero manifestar mi profundo agradecimiento a todas las personas que desempeñaron un papel crucial en la realización de esta tesis. También, agradezco a mis amigos por compartir conocimientos, intercambiar ideas y brindar apoyo durante los momentos tensos. Un reconocimiento especial va dirigido a mi compañero de tesis, Ernesto Jimbo, quien ha sido mi colega desde la secundaria y ha estado presente, alentándome y motivándome para alcanzar nuestro objetivo. Quisiera destacar especialmente el apoyo de Antonella Quizhpe, quien estuvo presente en los últimos años, brindándome apoyo y dándome fuerzas en los momentos de debilidad que atravesé. Sin duda, sus palabras y su singular forma de expresarse me permitieron seguir adelante y lograr esta meta. Además, quiero expresar mi gratitud a todas las personas que, a lo largo de mi formación académica, me respaldaron y apoyaron para seguir adelante. Este logro no habría sido posible sin la ayuda y el amor de todos ustedes. Gracias por ser parte fundamental de este capítulo significativo en mi vida académica. Atentamente, Carlos Enrique Correa Quishpe

AGRADECIMIENTOS

Agradecimiento de Angel Ernesto Jimbo Tinizhañay

Estoy profundamente agradecido con Dios por brindarme la dicha de tener a mis padres, quienes han sido mi motor principal, mi impulso, mi compañía, siempre me han ayudado a salir adelante a pesar de las adversidades con su sabiduría y consejos. Gracias a su amor incondicional y su fe que han sido mi guía durante este viaje de mi etapa de vida. A mi tutor de tesis, expreso mi más profundo agradecimiento al Ing. Juan Diego Jara por su invaluable contribución y orientación durante el desarrollo de este trabajo de titulación. Su dedicación y apoyo han sido fundamentales para el éxito de este trabajo académico. Un sincero agradecimiento a Carlos Correa, mi amigo y compañero de tesis, con quien hemos compartido la misma ilusión de cumplir este sueño a lo largo de muchos años. A pesar de las dificultades, su tenacidad, apoyo y confianza han sido muy valiosos. A todos mis amigos y compañeros que compartieron momentos únicos de alegría, estrés, tristeza y frustración durante esta etapa universitaria, quiero expresarles mi más sincero agradecimiento. Su apoyo, confianza y amistad han sido invaluables. Cada uno de ustedes ha contribuido a mi ánimo de una manera u otra. Gracias por ser mi apoyo, mi equipo de trabajo y, lo más importante, la familia que hemos formado y que he elegido.

Atentamente, Angel Ernesto Jimbo Tinizhañay

DEDICATORIA

Dedicatoria de Carlos Enrique Correa Quishpe

A lo largo de esta significativa etapa de mi vida, he tenido el privilegio de encontrarme con personas excepcionales que han desempeñado un papel crucial en mi trayectoria hacia la realización de esta tesis. Quiero expresar mi sincero agradecimiento y afecto a mi familia, quienes han sido un pilar fundamental en este viaje. A mis padres, Enrique y María, les dedico esta meta cumplida. Ellos desde una edad temprana, aspiraron a alcanzar metas académicas similares. A pesar de enfrentar momentos de aprendizaje diferentes, su dedicación y sacrificio se reflejan hoy en el logro de mis objetivos de vida. A mi hermano, quien, con sus constantes ideas de negocios, brindó un apoyo crucial en momentos claves de mi mejora personal y profesional. A mi hermana, cuya alegría única me impulsa a ser su modelo a seguir y la persona en la que puede confiar. A mis abuelitos, Carlos y Rosa, cuya sabiduría proporcionó un respaldo constante para alcanzar este propósito. A mi tío John, quien no solo es un tío sino también un padre y amigo. A mis amigos y compañeros, quienes han compartido risas y lágrimas, su compañía inquebrantable ha hecho que este viaje sea inolvidable. Guardaré en mi corazón sus palabras de aliento y su disposición para compartir tanto mis triunfos como mis desafíos. Cada uno de ustedes ha sido una pieza fundamental en la construcción de este logro. Sus bondades y dedicación quedarán grabadas en mi memoria de manera única. Con un profundo sentimiento de gratitud y cariño, agradezco a todos quienes han contribuido a esta importante meta de mi vida.

Con gratitud, Carlos Correa.

DEDICATORIA

Dedicatoria de Angel Ernesto Jimbo Tinizhañay

Agradezco a Dios por tener unos padres maravillosos que me han enseñado el sacrificio y la perseverancia en la vida. Por ello, este logro no es sólo mío sino también de ellos, y dedico esta trabajo de titulación a mis padres, Ángel y Blanca. Les expreso mi más sincero agradecimiento por su inmenso amor, que ha sido fuente de inspiración, y por sus consejos que me han guiado a lo largo de mi vida, permitiéndome alcanzar esta meta que no es sino el fruto de nuestro sacrificio. A mi querida familia, que ha demostrado constantemente un apoyo y una ayuda inquebrantables durante mi trayectoria académica, le expreso mi más sincera gratitud. Su inquebrantable aliento y su firme apoyo han sido decisivos para mi éxito. Agradezco profundamente su ayuda inquebrantable y su amor perdurable. "No hay amor más grande que dar la vida por sus amigos". A mis queridos amigos Carlos, Jorqui, Marlon y Andrés, que se han convertido en como una familia para mí, que siempre han estado ahí ante cualquier adversidad, en las buenas y en las malas. Estoy profundamente agradecida por el tiempo, los consejos, los sacrificios, las alegrías y las penas que hemos compartido juntos en este viaje llamado vida. A mi querida amiga Estefanny, con la que tuve la gran oportunidad de vivir momentos de alegría y tristeza, cómo no agradecerle su inestimable apoyo incondicional, sus consejos y sus ánimos durante el momento más crucial de mi vida, que fueron una contribución fundamental para poder decir: "¡Lo conseguí!". Gracias a todos mis amigos y a las personas que han formado parte de mi vida. Que Dios os bendiga a todos.

Con gratitud, Ernesto Jimbo

Índice General

Índice de Figuras

Índice de Tablas

Resumen

En este trabajo, se ha desarrollado un material didáctico con un enfoque práctico de competencias en el ámbito de redes de datos IP versión seis. El manual de prácticas se ha estructurado para facilitar el entendimiento en cuanto, a los procedimientos de configuración mediante el uso de software de simulación como GNS3, Máquinas virtuales y análisis de tráfico con Wireshark. Siendo específicamente diseñado para su ejecución en el Laboratorio de redes de computadoras de la Universidad Politécnica Salesiana, sede Cuenca. Abordando niveles que van desde lo básico hasta lo avanzado de manera progresiva. El formato adoptado sigue las pautas establecidas por la Universidad Politécnica Salesiana, respaldando un enfoque pedagógico que se alinea con los modelos de aprendizaje avalados por las prestigiosas escuelas Cisco y MikroTik.

A través de la aplicación de este método educativo, los estudiantes adquieren conocimientos teóricos y la oportunidad de poner en práctica sus habilidades en proyectos concretos. Esto les permite no solo diseñar y construir, sino también probar y resolver problemas reales que se encuentran en el amplio espectro de las redes de datos IP versión seis.

Cada práctica ha sido diseñada, teniendo en cuenta los protocolos más relevantes y fundamentales en el ámbito de redes de computadoras. Este enfoque se alinea perfectamente con el silabo de las materias de redes de computadoras 1 y 2, asegurando una integración coherente y progresiva del contenido curricular.

Palabras clave: IPv4; IPv6; DHCP; RIPng; OSPFv3; EIGRP; BGP; IS-IS; MPLS; LDP; ACL.

Abstract

In this work, a didactic material has been developed with a practical approach of competences in the field of IP data networks version six. The practice manual has been structured to facilitate the understanding of the configuration procedures through the use of simulation software such as GNS3, Virtual Machines and traffic analysis with Wireshark. Being specifically designed for its execution in the Laboratory of computer networks of the Salesian Polytechnic University, Cuenca. Addressing levels ranging from basic to advanced in a progressive manner. The format adopted follows the guidelines established by the Salesian Polytechnic University, supporting a pedagogical approach that is aligned with the learning models endorsed by the prestigious Cisco and MikroTik schools.

Through the application of this educational method, students acquire theoretical knowledge and the opportunity to put their skills into practice in concrete projects. This allows them not only to design and build, but also to test and solve real problems encountered in the broad spectrum of IP version six data networks.

Each practicum has been designed, taking into account the most relevant and fundamental protocols in the field of computer networking. This approach aligns perfectly with the syllabus of computer networking subjects 1 and 2, ensuring a coherent and progressive integration of the curricular content.

Keywords: IPv4; IPv6; DHCP; RIPng; OSPFv3; EIGRP; BGP; IS-IS; MPLS; LDP; ACL.

Introducción

El protocolo de red de datos IP versión seis ejerce un rol fundamental en el desarrollo de conexiones en la era digital, al incrementar la capacidad de direcciones IP disponibles en comparación con IP versión cuatro. En la actualidad, el agotamiento de direcciones IP versión cuatro es una realidad, y la adopción de IP versión seis se vuelve imprescindible para asegurar la continuidad de las comunicaciones y facilitar el crecimiento en un entorno digital en constante evolución [15].

Este trabajo tiene como objetivo ofrecer a los docentes y estudiantes de redes de computadoras una herramienta de referencia confiable que facilite una transición efectiva hacia IP versión seis.

El documento se describe como un manual práctico y accesible, diseñado para proporcionar orientación detallada paso a paso en todas las etapas del despliegue de los protocolos en IP versión seis. Se presenta una estructura clara y exhaustiva que abarca desde la asimilación de los principios de IP versión seis, su configuración y la solución de problemas, hasta la integración de conocimientos teóricos con enfoques prácticos.

Se garantiza que las prácticas propuestas cumplen con el nivel de aprendizaje, al tiempo que estimulan el desarrollo de sus habilidades técnicas.

ANTECEDENTES DEL PROBLEMA DE ESTUDIO

El Protocolo de red de datos Internet versión 6, (de sus siglas en ingles *Internet Protocol Versión 6, IPv6*), representa una versión avanzada que aborda las limitaciones y desafíos de su predecesor. Con el aumento considerable de dispositivos conectados a Internet, las direcciones del protocolo de Internet versión cuatro (de sus siglas en ingles *Internet Protocol Versión cuatro, IPv4*), no son suficientes para cumplir con la demanda actual de direccionamiento, generando la necesidad de su implementación. Sin embargo, muchas instituciones aún no han actualizado sus programas educativos y tecnologías para incluir este protocolo, lo que ha resultado en una falta de conocimiento y experiencia en estudiantes y profesionales. Esta falta de preparación ha dificultado la transición a IP versión seis en la sociedad. Un estudio realizado entre los exalumnos de la Universidad Politécnica Salesiana, sede Cuenca, mostró que el 31 % de los encuestados sugiere la necesidad de cursos en redes de datos basado en IP versión seis. Esto demuestra la carencia de formación en el ámbito de las redes de datos, lo cual podría tener un impacto adverso en la capacidad de las empresas y organizaciones para adecuarse a las nuevas tecnologías y exigencias de conectividad.

JUSTIFICACIÓN

La adopción del Internet de las Cosas (de sus siglas en inglés *Internet Of Things, IoT*), ha generado la necesidad de emplear IP versión seis para asignar direcciones únicas del Protocolo de Internet (de sus siglas en inglés *Internet Protocol, IP*), debido a la cantidad de dispositivos conectados a internet. El conocimiento avanzado en la configuración de equipos utilizando IP versión seis garantiza la correcta conectividad de los dispositivos de IoT y asegura su adecuado funcionamiento. Sin embargo, el conocimiento y la experiencia son esenciales en el ámbito tecnológico actual debido a que cada vez es más común el uso de dispositivos que se encuentran conectados al internet y la necesidad de direcciones IP, sumado a que las empresas están migrando al uso de IP versión seis. Es recomendable entonces que, las instituciones educativas incluyan cursos específicos sobre IPv6 en su programa de formación para que los estudiantes estén listos para hacer frente a las demandas del mercado laboral. La Universidad Politécnica Salesiana, sede Cuenca, se encuentra equipada con laboratorios especializados en Redes de Computadoras para formar a sus estudiantes en esta área. Sin embargo, existe un problema en cuanto a la falta de un manual de prácticas estructuradas de laboratorio en IPv6 que se ajuste a las necesidades profesionales actuales con el fin de proporcionar a los alumnos un aprendizaje completo y prepararlos en el ámbito de las Redes de Computadoras. Además, es importante desarrollar un manual que garantice un proceso de aprendizaje eficaz, tanto para estudiantes como para profesionales mejorando el perfil en el ámbito de las telecomunicaciones.

OBJETIVOS

Objetivo General

- Desarrollar un manual de prácticas en IPV6 para el laboratorio de redes de computadoras de la Universidad Politécnica Salesiana, sede Cuenca.

Objetivos específicos:

- Analizar el estado del arte del protocolo IPv6 y su aplicación en la actualidad para las prácticas en el laboratorio de redes de computadoras.
- Identificar las técnicas de enrutamiento y conmutación más relevantes para implementar en los laboratorios de redes de computadoras Cisco y Telecomunicaciones utilizando los equipos disponibles de Cisco y Mikrotik, así como en máquinas virtuales integradas con el software GNS3.
- Ejecutar las prácticas de laboratorio mediante pruebas de funcionamiento con equipos de enrutamiento y conmutación de los fabricantes Cisco y MikroTik, en función del componente práctico de las asignaturas de Redes de Computadoras 1 y 2.
- Documentar el manual de prácticas tanto para el docente como para los estudiantes siguiendo un modelo de aprendizaje verificado y teniendo en cuenta los formatos establecidos por la Universidad.

Capítulo 1

Fundamentación Teórica o estado del arte.

Este capítulo se centra principalmente en la teoría necesaria para comprender el Protocolo de Internet versión seis (IPv6) y también se analizan sus características principales. Durante el desarrollo de este capítulo, se profundizará en los aspectos fundamentales, brindando un sólido conocimiento teórico que permitirá comprender y apreciar plenamente el funcionamiento de este protocolo de próxima generación.

1.1. TCP/IP

El conjunto de normas conocido como Protocolo de control de transmisión/Protocolo de Internet (de sus siglas en inglés *Transmission Control Protocol/Internet Protocol, TCP/IP*), representa una piedra angular en las comunicaciones contemporáneas y constituye la base esencial de la infraestructura de Internet. Los dispositivos críticos en una red, como enrutadores, conmutadores y puertas de enlace, en su mayoría, se apoyan en los protocolos TCP/IP [32]. Este protocolo sigue un modelo similar al Modelo de Interconexión de Sistemas Abiertos (de sus siglas en inglés *Open Systems Interconnection, OSI*), se compone de cuatro capas: Aplicación, Transporte, Internet y Acceso a la Red, tal como se ilustra en la Figura 1.1. Cada capa incorpora protocolos específicos que desempeñan

funciones distintas durante la comunicación. Esta estructura modular simplifica la transmisión de datos y fomenta la interoperabilidad entre sistemas y redes.

El protocolo TCP/IP se compone de módulos independientes con funciones específicas. Los protocolos en cada capa son independientes y se eligen según las necesidades del sistema. En TCP/IP, cada capa superior es compatible con los protocolos de la capa inferior, lo que crea una estructura similar a un reloj de arena. Esto permite seleccionar y combinar protocolos de manera flexible para satisfacer los requisitos de comunicación de diversos sistemas y redes [23] , [31].

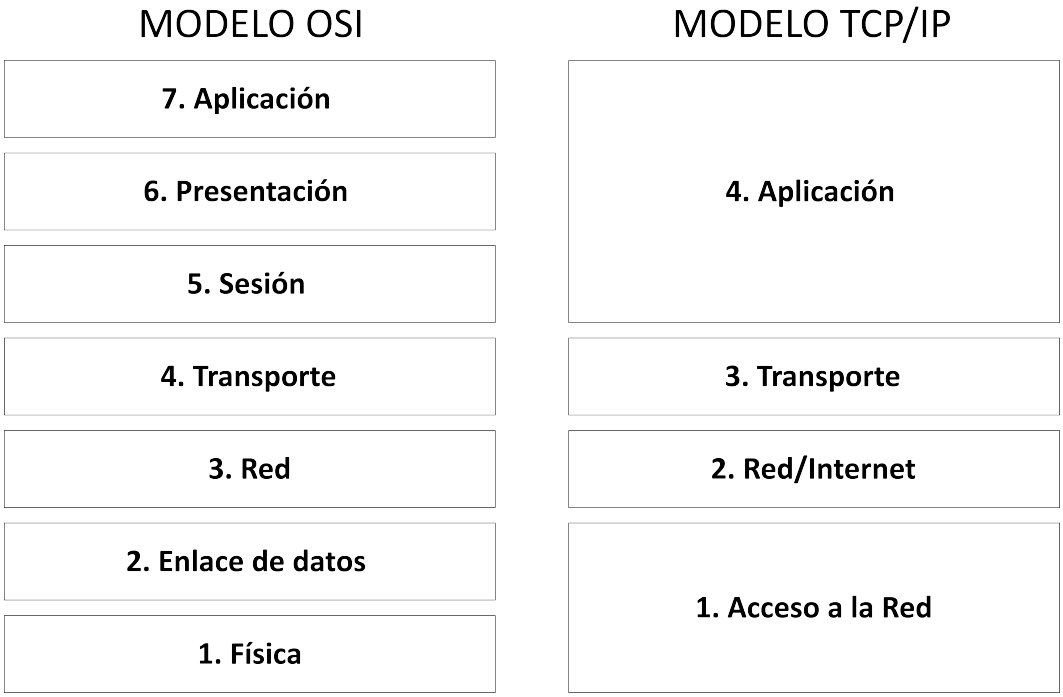


Figura 1.1: Modelo OSI y TCP/IP [Fuente: Autores.]

1. La estrategia de gestión del nivel de Acceso a la Red se centra en la administración de componentes hardware, como las tarjetas de red, y de los medios físicos, tales como cables de conexión.

2. El nivel de Red/Internet opera mediante el empleo del Protocolo de Internet (IP) para la transmisión de paquetes, también conocidos como datagramas, a través de un proceso de conmutación de paquetes.

3. El nivel de Transporte utiliza el Protocolo de Datagrama de Usuario (de sus siglas en inglés *User Datagram Protocol, UDP*), y Protocolo de Control de Transmisión

(de sus siglas en inglés*Transmission Control Protocol, TCP*), para establecer conexiones y garantizar una transmisión precisa de los datos.

4. El nivel de Aplicación se centra en proporcionar servicios de red a las aplicaciones de usuariodesempeñando el papel de interfaz para facilitar la comunicación entre aplicaciones a través de una red informática.

1.1.1. Protocolo de Control de Transmisión (TCP)

El Protocolo de Control de Transmisión (de sus siglas en inglés *Transmission Control Protocol, TCP*), es un componente esencial del conjunto de protocolos de Internet conocido como TCP/IP. Su principal propósito consiste en asegurar la transmisión ordenada y fiable de datos entre sistemas informáticos. TCP se emplea en aplicaciones críticas como el correo electrónico, la transferencia de archivos y World Wide Web.

Además de TCP, existen otros protocolos complementarios como SMTP, FTP y SSH, los cuales posibilitan el envío de correo electrónico, la transferencia de archivos y el acceso seguro a sistemas remotos, respectivamente. Aunque existen otras suites de protocolos como OSI, TCP/IP ha sido el líder indiscutible en las comunicaciones e intercambio de datos en Internet, superando las expectativas en comparación con el modelo OSI [32].

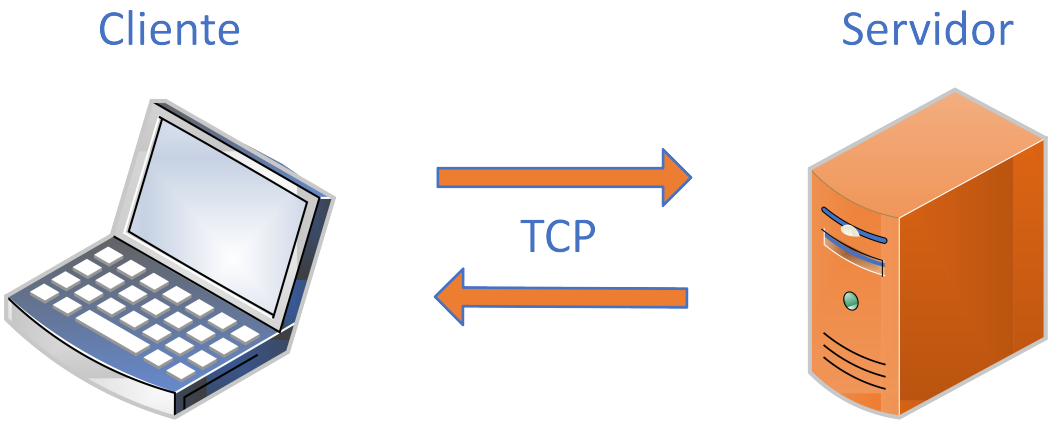


Figura 1.2: Protocolo TCP [Fuente: Los Autores.]

1.1.2. Protocolo de Datagramas de Usuario (UDP)

Este protocolo de comunicación es utilizado en el Internet debido a que intercambia datagramas entre aplicaciones sin la necesidad de establecer canales especiales. En el modelo OSI este protocolo se encuentra ubicado en el nivel de transporte y se caracteriza por su interfaz sencilla entre el nivel de red y el nivel de aplicación. A diferencia de TCP, UDP no ofrece garantías de confiabilidad, orden o integridad de los datos transmitidos. Sin embargo, proporciona una transmisión rápida y en tiempo real, lo que cual permite una gran comodidad en aplicaciones como juegos en línea, transmisión de medios y servicios de nombres de dominio. UDP tiene un encabezado de datagrama pequeño, lo que reduce la sobrecarga de administración de red. Aunque UDP no ofrece mecanismos de corrección de errores, admite la difusión y multidifusión de paquetes. Además esto permite a todos los dispositivos enviar paquetes en una red local o a un grupo específico de suscriptores [4] , [32].

Figura 1.3: Protocolo TCP,UDP [Fuente: Autores.]

1.1.3. Protocolo de Internet (IP)

Es esencial en la exitosa transmisión de datos. Está diseñado para manejar la parte de dirección de un paquete para que llegue al destino correcto. Su implementación tiene lugar en la capa de Internet, donde despliega funciones de enrutamiento a lo largo de diversas redes, implementado no solo en los sistemas finales, sino también en los enrutadores [32].

1.2. Protocolo de Internet versión 4 (IPv4)

La versión cuatro del Protocolo de Internet emplea direcciones representadas en notación decimal con puntos, como ejemplificado por 192.149.252.76. Estas direcciones se dividen en dos componentes: una destinada a la red y otra al host, siendo esta división determinada por la clase de dirección (A, B, C, D o E), que a su vez se define por los primeros bits. El rango total de direcciones IPv4 asciende a 4,294,967,296 [16].

A diferencia de las asignadas por DHCP, las direcciones IP no poseen un tiempo de vida intrínseco, a menos que sean asignadas dinámicamente por este protocolo. Las direcciones privadas, utilizadas internamente en las organizaciones, no son enrutables a través de la red. Las direcciones IP se asignan a los terminales mediante DHCP o configuración estática [7].

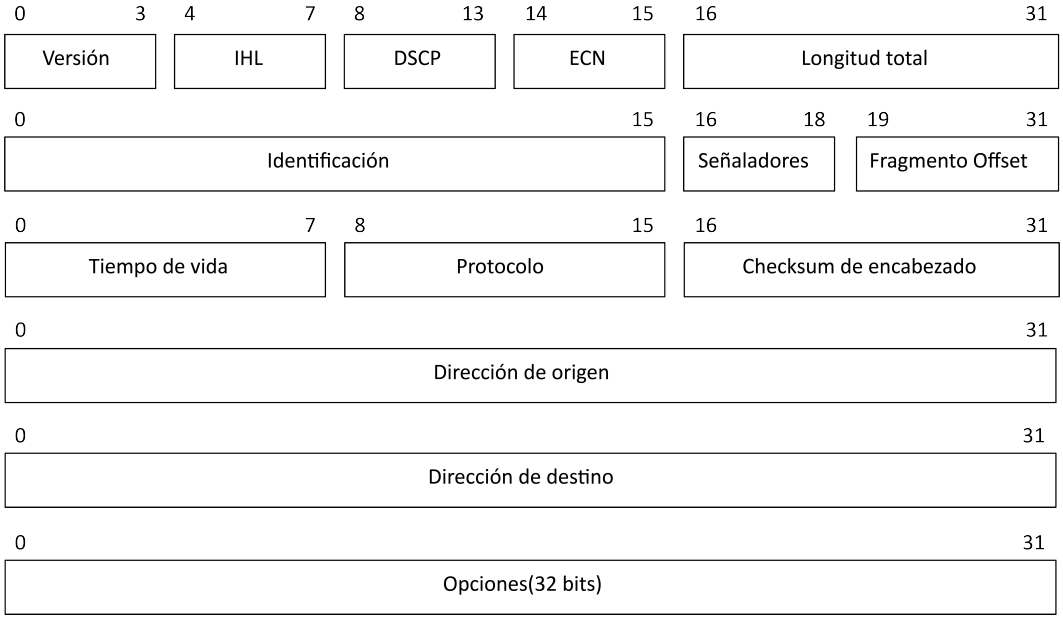


Figura 1.4: Encabezado Ip versión 4[Fuente: Autores.]

1.3. Protocolo de Internet versión 6 (IPv6)

Una dirección IPv6 es distinta de una dirección IPv4 debido a que la primera posee 8 grupos de dígitos hexadecimales que están divididos por dos puntos. Estas direcciones están compuestas por un prefijo de 64 bits y un identificador de

interfaz de 64 bits, que suman en total 128 bits. Una muestra de dirección IPv6 es 2024:00c8:aece:0000:0000:1242:0290:2904, que además es posible representarse como 2024:c8:aece::1242:0290:2904[13].

Las direcciones IP versión seis se clasifican de la siguiente manera:

Unicast: Se refiere a una dirección única asignada a un solo host en una red.

Multicast: Envía un paquete a muchos o a un grupo de interfaces. Todos los hosts en el grupo de multicast recibirán el paquete. No admite mensajes de difusión, por lo que se utilizará la dirección multicast en su lugar.

Anycast: Se refiere a un grupo de interfaces en diferentes ubicaciones. Anycast es similar a multicast con la excepción de que los paquetes solo serán recibidos por el host más cercano en ese grupo anycast, a diferencia de un grupo multicast.

1.4. Protocolos de Switching IPv6

1.4.1. Redes de Área Local Virtuales (VLANs)

El estándar IEEE 802.1Q especifica la metodología para la implementación del trunking de VLAN en una infraestructura de red Ethernet [5]. Las VLANs, o Redes de Área Local Virtuales (de sus siglas en inglés *Virtual Local Area Network*), son definidas de manera concisa como la partición de una red informática en segmentos que abarcan la computadora de destino dentro de un subconjunto específico de la misma LAN. En este escenario, la comunicación se limita al ámbito de una única VLAN, lo que permite la interacción exclusiva entre los dispositivos que pertenecen a esa VLAN [29], [1].

1.4.2. Protocolo Enrutamiento entre VLAN (Inter-VLAN Routing)

El procedimiento de direccionar el tráfico de red desde una VLAN hacia otra VLAN, mediante la aplicación del principio de enrutamiento, independientemente del dispositivo utilizado, se denomina enrutamiento entre VLAN (del inglés, *Inter-VLAN Routing*) [1].

1.4.3. Protocolo de Troncales de VLAN (VTP)

El Protocolo de Troncales de VLAN (de sus siglas en inglés *VLAN Trunking Protocol, VTP*), se utiliza para sincronizar las configuraciones de nomenclatura y para excluir selectivamente VLAN de los enlaces de troncales destinados a dispositivos de Capa 2 que carecen de puertos activos dentro de la VLAN correspondiente. Los usuarios tienen la opción de designar un nombre de dominio VTP para una identificación fácil. Esto implica la activación de troncales, a través de las cuales el nombre de dominio VTP se propaga, incluso a interruptores donde el nombre de dominio no está configurado. Las instancias de VTP con nombres de dominio distintos se abstienen de intercambiar información [28].

1.4.4. Protocolo de Árbol de Expansión (STP)

El Protocolo de Árbol de Expansión (de sus siglas en inglés *Spanning Tree Protocol, STP*), constituye un protocolo destinado a prevenir la formación de bucles de conmutación en el nivel 2 del modelo OSI. Se activa al identificar la presencia de conexiones innecesarias en la infraestructura de red. Durante el proceso de elección, una candidatura STP se somete a un procedimiento electoral basado en la prioridad del puente, siendo el conmutador con la mínima prioridad designado como el puente raíz. La totalidad de la información es dirigida hacia el puente raíz y posteriormente retransmitida. Sin embargo, cabe cuestionarse cuál criterio se emplea para la selección del puente raíz y en caso de no ser el puente raíz, cómo se lleva a cabo su designación, así como el modo/estado que deben asumir sus puertos en los conmutadores [14].

1.4.5. Árbol de expansión por VLAN (PVST)

El protocolo exclusivo de Cisco conocido árbol de expansión común (de sus siglas en inglés *Common Spanning Tree, CST*), emplea una única instancia del Protocolo STP, para toda la infraestructura de conmutadores, lo que resulta en retrasos en la emisión de Unidades de datos de protocolo de puente (de sus siglas en inglés *Bridge Protocol Data Units, BPDUs*). Para abordar esta limitación, se introdujo

el Árbol de expansión por VLAN (de sus siglas en inglés *Per-VLAN Spanning Tree, PVST*), también de propiedad exclusiva de Cisco, el cual implementa una situación independiente de STP en cada VLAN en la red. El CST puede experimentar demoras en la recepción de BPDUs, lo cual puede impactar negativamente en la velocidad de convergencia de la red. PVST soluciona estos inconvenientes al posibilitar la configuración independiente de cada VLAN, mejorando el rendimiento mediante la implementación de una instancia de STP separada para cada una de ellas. Es crucial destacar que el uso de PVST requiere la utilización de Inter-Switch Link (ISL) [22].

1.5. Protocolos de Enrutamiento IPv6

1.5.1. Protocolos de Enrutamiento Estático y Dinámico

El enrutamiento estático en IPv6 se caracteriza por ser un método en el cual los administradores configuran manualmente las rutas de red, en los dispositivos de enrutamiento. Este procedimiento se lleva a cabo mediante la configuración de rutas estáticas en los dispositivos correspondientes. Cada entrada en la tabla de enrutamiento incluye la dirección de destino y la interfaz de salida correspondiente. Cuando un dispositivo recibe un paquete, examina su tabla de enrutamiento estática para calcular la ruta adecuada y enviar dicho paquete. Si encuentra una coincidencia entre la dirección de destino del paquete el dispositivo reenvía el paquete a través de la interfaz de salida especificada. De esta manera, este protocolo implica la configuración manual de rutas y no se ajusta automáticamente a variaciones en la configuración de la red [17].

Por otro lado, el enrutamiento dinámico en IPv6 se refiere a un conjunto de protocolos y algoritmos que posibilitan a los dispositivos de red intercambiar información de enrutamiento de manera automática para determinar las mejores rutas en una red IPv6. Este protocolo se ajusta de forma automática a cambios en las estructuras de la red. En el contexto de IPv6, existen diversos protocolos de enrutamiento dinámico diseñados para facilitar el intercambio de información entre routers. Entre los más comunes se encuentran OSPFv3, RIPng y BGP. Estos

protocolos permiten a los routers descubrir automáticamente nuevas redes y adaptarse a los cambios en la topología de la red [17].

1.5.2. Protocolo de Enrutamiento de Próxima Generación (RIPng)

RIPng (de sus siglas en inglés *Routing Information Protocol next generation, RIPng*), este protocolo de enrutamiento dinámico es diseñado específicamente para IP versión seis, por lo tanto, dicho protocolo es una versión actualizada y mejorada del protocolo de enrutamiento RIP utilizado en IP versión cuatro. RIPng intercambia la información de enrutamiento entre routers en una red y emplea el enfoque de vector de distancia. Cada router que ejecuta RIPng anuncia sus rutas a los routers vecinos, incluyendo la métrica o costo asociado a cada ruta. Los routers vecinos actualizan las tablas de enrutamiento en función de esta información y propagan las actualizaciones a otros routers en la red. Una de sus principales ventajas es su sencillez de configuración y uso. Es un protocolo fácil de implementar y no requiere una configuración compleja, sin embargo, debido a su enfoque vector distancia RIPng se recomienda principalmente para redes más pequeñas o menos complejas [24]

1.5.3. Protocolo de Enrutamiento de Estado de Enlace de Área Abierta versión 3 (OSPFv3)

Es un protocolo de enrutamiento Estado-Enlace, comparte los mismos fundamentos que OSPv2 como el algoritmo Camino más Corto Primero (de sus siglas en inglés *Shortest Path First, SPF*), las inundaciones, la elección de Router designado, las áreas, las métricas y los temporizadores. En el Protocolo de Estado de Enlace de Área Abierta versión 3 (de sus siglas en inglés *Open Shortest Path First version 3, OSPFv3*), el protocolo puede intercambiar paquetes entre dos vecinos en el mismo enlace, incluso si pertenecen a subredes diferentes. Los LSA del tipo Router LSA (LSA tipo1) y Network LSA ya no contienen direcciones IP, en su lugar se crea un nuevo tipo de LSA. Sin embargo, se mantiene el identificador del router (de sus siglas en inglés *ID router, RID*), expresado como un valor de 32 bits. En OSPFv2 los

vecinos en redes de difusión se identificaban mediante la dirección IP de la interfaz, mientras que en enlaces punto a punto se utilizaban el RID. Estas inconsistencias se eliminan en OSPFv3, donde todos los routers se identifican mediante su RID [20].

1.5.4. Protocolo de Enrutamiento Interior de Puerta de Enlace (EIGRP)

EIGRP (de sus siglas en inglés *Enrutamiento Interior Gateway Protoco, EIGRP*), es una versión actualizada y mejorada del EIGRP utilizado en IP versión cuatro. Este protocolo de enrutamiento fue desarrollado por Cisco con la finalidad de compartir la información de enrutamiento entre routers en una red de manera más eficiente. EIGRP en IPv6 utiliza la combinación de dos propiedades, estado de enlace y vector distancia, lo cual implica que aprovecha las propiedades de ambos métodos. Estos brindan beneficios como una rápida convergencia, estabilidad de carga y ademas de adaptarse a cambios en la topología en una red. El protocolo EIGRP está basado en el concepto de vecindades, estableciendo relaciones de cercanía entre routers adyacentes. Los routers EIGRP intercambian información de estado de enlace, que contiene detalles sobre las rutas disponibles y sus métricas. Esta información permite construirlas tablas de enrutamiento. [3].

1.5.5. Protocolo de Enrutamiento de Puerta de Enlace Fronteriza (BGP)

BGP (de sus siglas en inglés *Border Gateway Protocol, BGP*), se utiliza para la transmisión de datos de dirección de internet entre distintos sistemas autonomous (de sus siglas en inglés *autonomous systems, AS*). El protocolo BGP se utiliza para establecer y mantener la conectividad y las rutas entre los routers de diferentes sistemas autónomos en una red IPv6. El funcionamiento de este protocolo implica el intercambio de anuncios de rutas entre los routers de los sistemas autónomos. Cada anuncio de ruta lleva los datos de las redes alcanzables y las rutas elegidas. Estos anuncios son intercambiados entre los routers BGP, quienes toman decisiones sobre las rutas más óptimas a utilizar [21].

1.5.6. Protocolo de Enrutamiento Sistema Intermedio a Sistema Intermedio (IS-IS)

IS-IS(de sus siglas en inglés *Intermediate System to Intermediate System, IS-IS*), en IP versión seis es un protocolo de enlace utilizado para determinar las rutas mas óptimas en un sistema autónomo. Este protocolo utiliza información sobre el estado de los enlaces, como la capacidad y las métricas asociadas, para encontrar las rutas optimas . Los routers IS-IS intercambian información de enrutamiento a través de enlaces vecinos, utilizando mensajes de actualización y divulgación de enrutamiento para mantener al tanto de la topología de la red. IS-IS es reconocido por manejar redes extensas comúnmente utilizado por los proveedores que brinda servicio de internet. [3].

1.6. Listas de Control de Acceso (ACL)

Las Listas de Control de Acceso (de sus siglas en inglés *Access Control List,ACL*), facilitan el control del tráfico en una red [30]. Se pueden realizar diversas configuraciones en la entrada o salida de una red, especificando el protocolo, el puerto o servicio que se desea permitir o denegar [18]. Las ACL se dividen en dos categorías: listas de acceso estándar y listas de acceso extendido. Las listas de acceso estándar filtra los paquetes de datos según el origen de la dirección que fue enviado el paquete. Por otro lado, las listas de acceso extendido considera tanto el origen (remitente) como el destino (destinatario) del paquete de datos, además del protocolo y el tipo utilizado. En el caso de IP versión seis, la lista de acceso extendido es más específica en el filtrado de paquetes de datos y se implementa en redes con IPv6 [30]. La evaluación de la acción en una ACL se basa únicamente en dos valores: "Permit", que otorga acceso a la red, y en caso contrario, "Deny", que deniega la entrada [18].

1.7. Transición IPv4 a Ipv6

1.7.1. Dual Stack

El enfoque Pila Dual (en inglés, *Dual Stack*), implica la capacidad de utilizar tanto IP versión cuatro como IP versión seis simultáneamente. Esto se logra asignando direcciones de ambas versiones al dispositivo, permitiéndole comunicarse con otros nodos. Este enfoque se conoce como IP versión cuatro e IP versión seis nativo. En el escenario de un terminal con doble direccionamiento, el dispositivo emitirá solicitudes DNS inicialmente en una versión y, en caso de no recibir respuesta, procederá a validar la solicitud utilizando la otra versión disponible. La elección de la versión que se utiliza primero, ya sea IP versión seis o IP versión cuatro, dependerá de la tecnología y del fabricante. En el contexto de un router configurado en modo Dual Stack, es imperativo que todas las interfaces conectadas posean asignaciones de direcciones IP versión seis, y que el enrutamiento se lleve a cabo empleando el mismo protocolo. Normalmente, la topología y el diseño de la red en un entorno Dual Stack guardarán una similitud notable con las configuraciones ya establecidas para IP versión cuatro [27].

1.7.2. Tunneling

Con túneles (en inglés, *Tunneling*), los routers que ejecutan simultáneamente IP versión seis e IP versión cuatro encapsularán el tráfico IP versión seis dentro de paquetes IP versión cuatro. En este procedimiento, los paquetes IP versión cuatro se originan en el router local y se dirigen al router ubicado en el extremo del túnel. Al recibir el paquete IP versión cuatro, el router de destino procede a desencapsularlo, reenviando así el tráfico encapsulado en la versión seis del protocolo IP [6]. Los túneles punto a punto son diseñados para conectar únicamente dos nodos, estableciendo un enlace virtual entre ellos; estos se configuran estáticamente en ambos extremos. En contraste, los túneles punto a multipunto posibilitan que un nodo inicial se comunique a través del túnel con varios destinos remotos, siempre y cuando estos también permitan el establecimiento del mencionado túnel [27].

1.8. Definición de Conmutación de Etiquetas Multiprotocolo (MPLS)

Protocolo de Etiquetas Multiprotocolo (de sus siglas en inglés *Multiprotocol Label Switching ,MPLS*), es un protocolo de capa 2.5, lo que implica su operación entre el nivel de enlace de datos y el nivel de red, mejorando la confiabilidad del reenvío de paquetes. Para llevar a cabo esta función, MPLS añade un encabezado adicional que indica las etiquetas asociadas a cada paquete [19].

A través del principio de conmutación de etiquetas, MPLS optimiza la manipulación de paquetes IP, simplificando significativamente el proceso en comparación con una red IP convencional. Mientras en una red IP convencional cada enrutador examina el encabezado IP para identificar el destino y consulta la base de datos de rutas (de sus siglas en inglés *Routing Information Base, RIB*), para determinar la ruta del siguiente salto o la interfaz de salida, MPLS introduce métodos de enrutamiento más avanzados. Entre ellos, se destaca la Base de Información de Reenvío (de sus siglas en inglés *Forwarding Information Base, FIB*), que organiza las resoluciones realizadas por la RIB, y una tabla adicional para almacenar detalles pertinentes al encapsulado vinculado a el nivel de enlace de datos. Un ejemplo representativo de tales innovaciones es la Conmutación de Etiquetas de Entrada (de sus siglas en inglés *Cisco Express Forwarding, CEF*).

MPLS simplifica la gestión del direccionamiento de paquetes mediante rutas predefinidas conocidas como Rutas de Conmutación de Etiquetas (de sus siglas en inglés *Label Switched Path, LSP*). Los enrutadores intermedios, denominados Routers de Conmutación de Etiquetas (de sus siglas en inglés *Label Switching Routers, LSR*), procesan de manera eficiente la información primaria de las etiquetas, dado que el LSP se establece previamente. La asignación de etiquetas a lo largo de la ruta es responsabilidad del Protocolo de Distribución de Etiquetas (de sus siglas en inglés *Label Distribution Protocol, LDP*), mientras que el protocolo RSVP se encarga de determinar la ruta [2].

En el tráfico del protocolo MPLS, se utiliza LDP cuando una red no emplea BGP para la distribución de etiquetas. Este método opera en situaciones donde BGP

no está activo o no se ejecuta, anunciando etiquetas a través de otros protocolos. Sin embargo, presenta la limitación de no ser compatible con el protocolo nativo, como OSPF, EIGRP, entre otros [19].

Capítulo 2

Descripción de Equipos del Laboratorio de Redes de Computadoras

Este capítulo aborda de manera detallada las características, el funcionamiento y las especificaciones técnicas de los dispositivos utilizados en el Laboratorio de redes de computadoras para llevar a cabo las prácticas.

En la Tabla 2.1 se muestran los dispositivos disponibles en el Laboratorio de redes de computadoras que se usarán para la creación del manual de prácticas.

Tabla 2.1: Equipos disponibles en el laboratorio 8 de redes.

Total	Dispositivo	Etiqueta	Estándar
11	Router	Cisco	Cisco 4321 ISR
11	Router	Cisco	C1111-4PW
11	Switch	Cisco	C1000-24P-4G-L
11	Router	MikroTik	CR1009-7G-1C-1S+

2.1. Router de servicios integrados Cisco 4321 ISR

El router Cisco 4321, parte de la Serie 4000 de Routers, diseñado específicamente para satisfacer los requisitos de conectividad de pequeñas y medianas empresas, así como sucursales. Destaca por su capacidad para ofrecer un

rendimiento superior, una seguridad robusta y funciones avanzadas, convirtiéndolo en una opción versátil para abordar diversas necesidades de red. Instalado en nuestro Laboratorio de redes de computadoras, el router Cisco 4321 ISR posibilita la implementación de soluciones eficientes para optimizar la conectividad y el rendimiento de la red en entornos empresariales.

Las características y especificaciones más relevantes del router Cisco 4321 ISR se encuentran destalladas en la Tabla 2.2:

Tabla 2.2: Propiedades y Detalles Técnicos Cisco 4321 ISR [10].

Propiedades	Detalles Técnicos
Rendimiento	Enrutamiento con una tasa máxima de transferencia de hasta 50 Mbps.
Conectividad WAN	Dos puertos Gigabit Ethernet integrados para facilitar la conectividad WAN.
Conectividad LAN	Dos puertos Gigabit Ethernet incorporados para la conectividad LAN.
Ranuras modulares	Ranuras para módulo de interfaz de red (NIM) y módulo de servicio mejorado (SM-X).
Seguridad	Cortafuegos, VPN (red privada virtual) y opciones de conectividad segura.
Gestión	Software IOS XE de Cisco para la administración, configuración y gestión mediante CLI o interfaz web, local o remota.

La Figura 2.1 muestra el equipo Router Cisco 4321 ISR.

Figura 2.1: Router 4321 [Fuente: Cisco.]

2.1.1. Descripción puertos router Cisco 4321 ISR

La Figura 2.2 muestra los puertos del panel posterior en el modelo Cisco 4321.

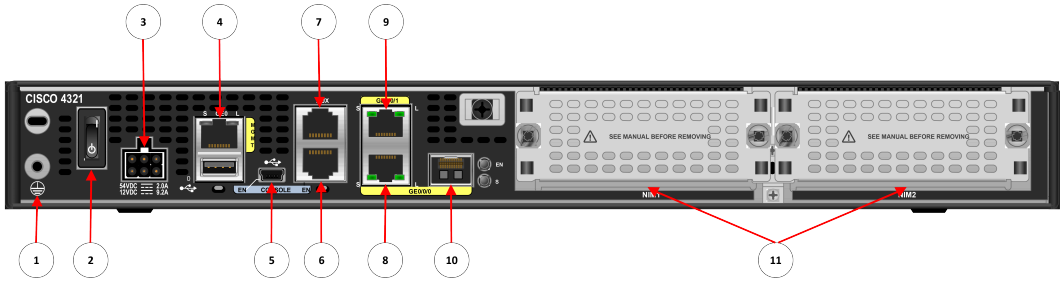


Figura 2.2: Router 4321 [Fuente: Autores]

En la Tabla 2.3 siguiente, se detalla la descripción de los puertos traseros del Router Cisco 4321.

1	Conexión a tierra	2	Interruptor de energía
3	Entrada de suministro eléctrico	4	Puerto GE "MGMT "(con puerto USB debajo)
5	Mini puerto USB tipo B	6	Puerto de consola
7	Puerto auxiliar	8	GE 0/0/0 (puerto de cable de cobre)
9	GE 0/0/1 RJ-45 (puerto de cable de cobre)	10	GE 0/0/0 SFP (puerto de fibra óptica)
11	Ranuras NIM		

Tabla 2.3: Puertos del panel posterior en Cisco 4321 ISR

A continuación, en la Tabla 2.3, se expone la explicación de la vista frontal.

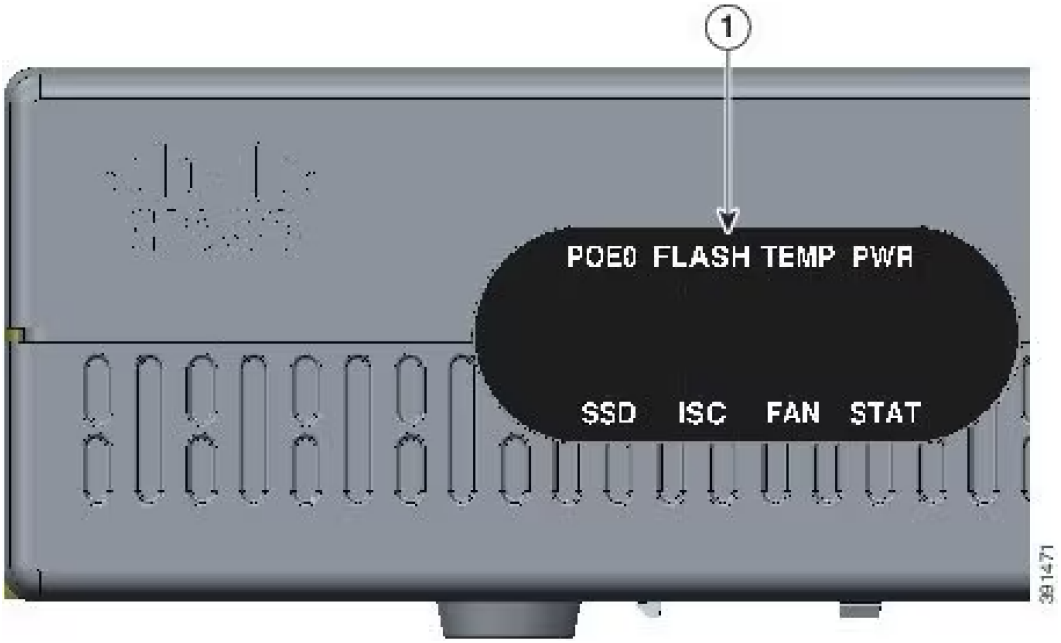


Figura 2.3: LEDs en Cisco 4321 ISR [Fuente: Cisco.]

En la siguiente Tabla 2.4, se muestra la descripción de la vista frontal.

1	Leds

Tabla 2.4: Leds de Cisco 4321

2.1.2. Módulo de interfaz de red Gigabit EtherSwitch de 4 puertos de capa 2 de Cisco

El módulo NIM-ES2-4 está equipado con cuatro puertos Ethernet Gigabit capaces de admitir velocidades de hasta 1 Gigabit por segundo, según se ilustra en la Figura 2.4, Además, cumple con varios estándares Ethernet, incluidos IEEE 802.3, 802.3u y 802.3ab, lo que permite su conexión a diversos dispositivos de red como computadoras, servidores, switches y otros enrutadores mediante el uso de cables Ethernet estándar [9].

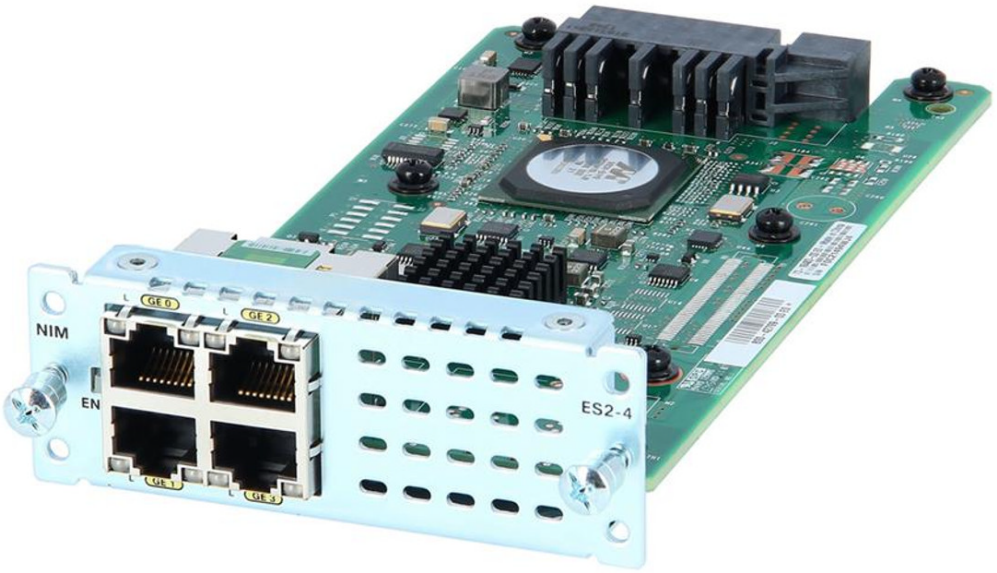


Figura 2.4: Módulo Cisco NIM-ES2-4 [Fuente:Servers4less.]

La Figura 2.5 muestra la descripción del módulo Cisco NIM-ES2-4.

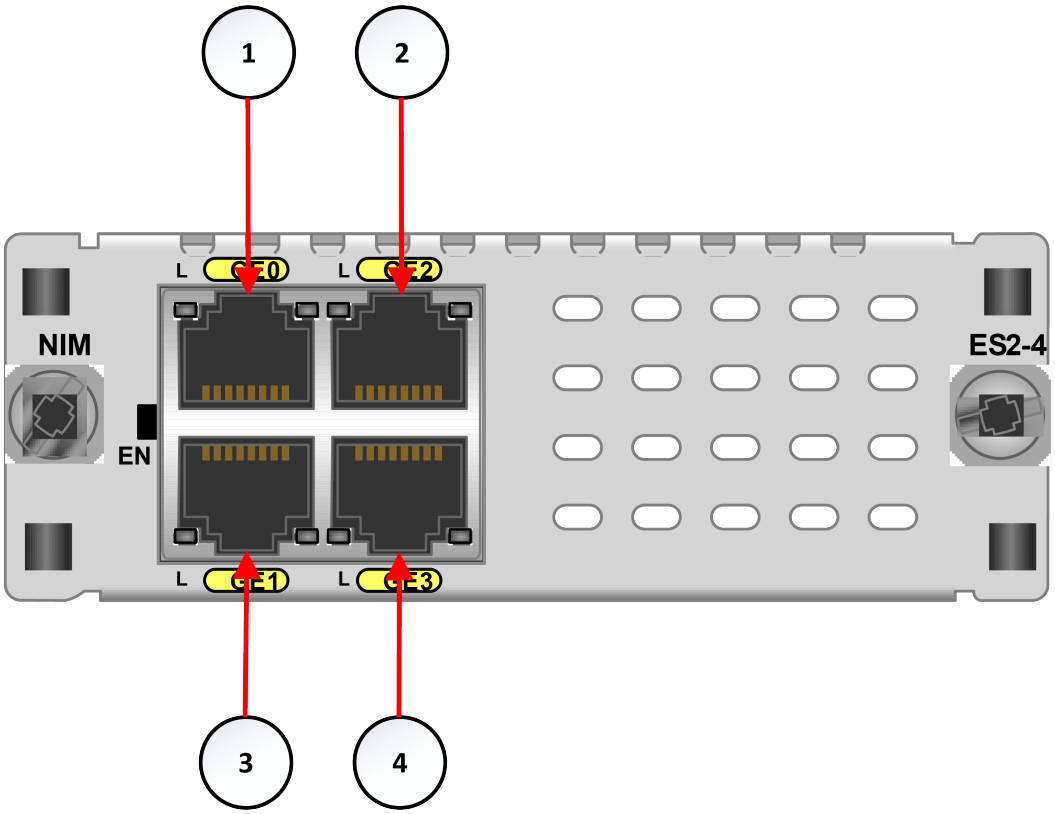


Figura 2.5: Módulo Cisco NIM-ES2-4 [Fuente: Autores.]

Se puede observar la descripción de los puertos en la Tabla 2.5.

1	Gigabit Ethernet 0	2	Gigabit Ethernet 2
3	Gigabit Ethernet 1	4	Gigabit Ethernet 3

Tabla 2.5: Puertos NIM Gigabit EtherSwitch de 4 puertos de capa 2 de Cisco

2.2. Router de servicios integrados Cisco C1111-4PW

El router Cisco C1111-4PW, parte de la serie 1000 de enrutadores de servicios integrados (ISR) de Cisco, instalado en el Laboratorio de redes de computadoras, para satisfacer las demandas de conectividad segura y confiable, diseñado para entornos empresariales Compañías de pequeña y mediana envergadura, así como en sucursales. Este dispositivo, identificado como "4PW.[en] su nombre, destaca por la presencia de cuatro puertos LAN, lo que amplía significativamente las opciones de conectividad. Además, su capacidad de suministrar energía a través de Ethernet (PoE) añade un nivel adicional de versatilidad y eficiencia a nuestras operaciones.

Las características y especificaciones más relevantes del router Cisco C1111-4PW se encuentran destalladas en la Tabla 2.6:

Tabla 2.6: Propiedades y Detalles Técnicos Cisco C1111-4PW [8].

Propiedades	Detalles Técnicos
Rendimiento	Rendimiento WAN de hasta 300 Mbps.
Conectividad LAN	Cuatro puertos LAN Gigabit Ethernet.
Alimentación a través de Ethernet	Admite Power over Ethernet (PoE) en los cuatro puertos LAN.
Conectividad inalámbrica	Equipado con capacidades integradas de Wi-Fi 802.11ac Wave 2.
Conectividad WAN	Gigabit Ethernet, VDSL2, ADSL2/2+ y LTE (Long-Term Evolution).
Seguridad	Ofrece sólidos mecanismos de seguridad para salvaguardar la infraestructura de red y los datos.
Gestión	Gestionable mediante el IOS de Cisco, admite protocolos de gestión como SNMP y CLI.

La Figura 2.6 muestra el modelo Router Cisco C1111-4PW.

Figura 2.6: Router C1111-4PW [Fuente: router-switch.]

2.2.1. Descripción puertos router Cisco C1111-4PW

Puertos del panel posterior en el modelo Cisco C1111-4PW, tal como se muestras en la Figura 2.7, son los siguientes:

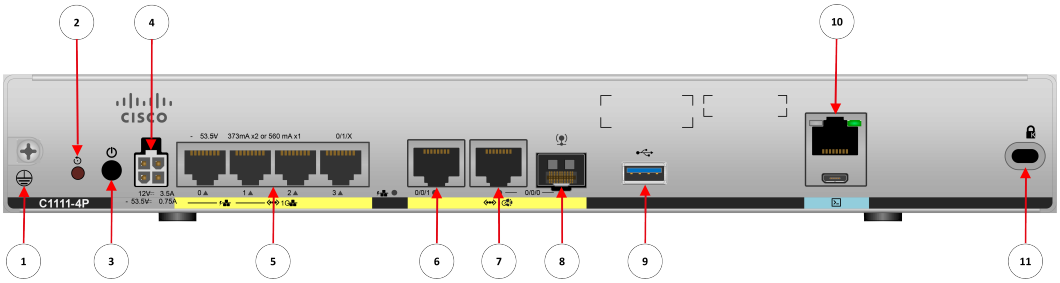


Figura 2.7: Router C1111-4PW [Fuente: Autores.]

En la siguiente Tabla 2.7, se muestra la descripción de los puertos posteriores del router Cisco C1111-4PW.

1	Puesta a tierra	2	Botón de restablecimiento
3	Conmutador eléctrico	4	Enchufe eléctrico de 4 pines
5	Switch Ethernet	6	GE 0/0/1
7	GE 0/0/0: RJ45	8	GE 0/0/0: SFP
9	USB3.0	10	RJ45/consola de Micro USB
11	Ranura para candado Kensington		

Tabla 2.7: Descripción puertos modelo router Cisco C1111-4PW

2.3. Switch Cisco Catalyst serie C1000-24P-4G-L

El Conmutador Cisco Catalyst C1000-24P-4G-L forma parte de la serie de switches Cisco Catalyst 1000, instalado en el Laboratorio de redes de computadoras, diseñado para atender las necesidades de redes en pequeñas y medianas empresas.

Las características y especificaciones más relevantes del switch Cisco Catalyst C1000-24P-4G-L se encuentran destalladas en la Tabla 2.8:

Tabla 2.8: Propiedades y Detalles Técnicos Catalyst C1000-24P-4G-L [11].

Propiedades	Detalles Técnicos
Conectividad LAN	24 puertos Ethernet con velocidades de 10/100/1000 GbE.
Conectividad de Enlace Ascendente	Cuatro puertos de enlace ascendente de 1 GbE.
Alimentación por Ethernet	Soporta Power over Ethernet (PoE) y PoE+
Conmutación de Nivel 2	Operación en el nivel 2 del modelo OSI, con funciones como VLANs,Protocolo de Árbol de Expansión (STP) y consolidación de enlaces.
Seguridad	Engloba listas de control de acceso (ACL), vigilancia DHCP y salvaguarda de origen IP.
Servicio (QoS)	Ofrece características de QoS para priorizar el tráfico según aplicaciones o servicios.
Gestión	Gestión mediante interfaz web o línea de comandos (CLI) de Cisco. Compatible con SNMP para la supervisión y gestión de la red.

La Figura 2.8 exhibe el modelo Switch Cisco Catalyst.

Figura 2.8: Cisco Catalyst serie C1000-24P-4G-L [Fuente: Cisco.]

2.3.1. Descripción puertos Switch Cisco Catalyst serie C1000-24P-4G-L

Puertos del panel posterior en el modelo Cisco Catalyst serie C1000-24P-4G-L, tal como se muestras en la Figura 2.9, son los siguientes:

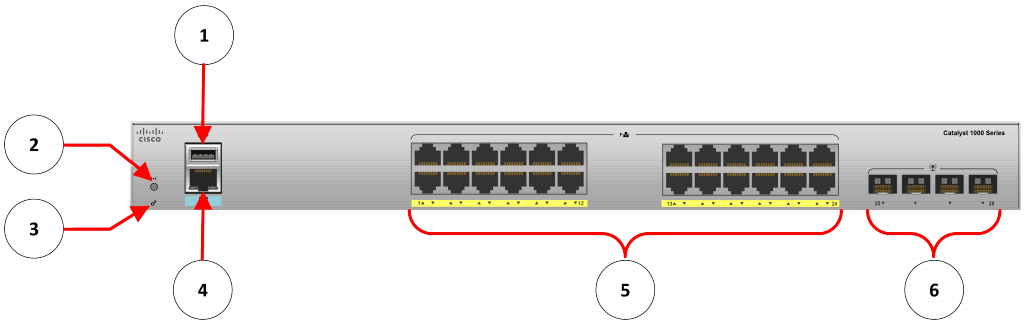


Figura 2.9: Cisco Catalyst serie C1000-24P-4G-L [Fuente: Autores.]

En la siguiente Tabla 2.9, se muestra la descripción de los puertos.

1	Puerto USB tipo A	4	Puerto de consola RJ-45
2	Botón de reinicio	5	24 puertos 10/100/1000 PoE+
3	LED del sistema	6	Ranuras para módulos SFP

Tabla 2.9: Descripción puertos modelo Cisco Catalyst serie C1000-24P-4G-L

2.4. Router MikroTik CCR1009-7G-1C-1S+

El enrutador CCR1009-7G-1C-1S+ es un dispositivo fabricado por MikroTik, especializado en redes avanzadas y de alto rendimiento. Disponible en el Laboratorio de redes de computadoras, facilita conexiones de alta velocidad, tanto cableadas como mediante enlaces de fibra óptica.

Las características y especificaciones más relevantes del enrutador MikroTik CCR1009-7G-1C-1S+ se destalladan en la Tabla 2.10:

Tabla 2.10: Características y Especificaciones MikroTik CCR1009-7G-1C-1S+ [25].

Característica	Descripción
Tipo de dispositivo	Cloud Core Router (CCR)
Procesador	Tilera Tile-Gx9
Puertos Ethernet	7 puertos Gigabit Ethernet (7G)
Puertos SFP	1 puerto SFP+ (1S+)
Conectividad	Alta velocidad, cableada y fibra óptica
Seguridad	Soporte para cifrado de hardware
Memoria Flash NAND	Almacenamiento a bordo, capacidad variable según modelos
Sistema Operativo	RouterOS de MikroTik
Rendimiento	Destacado en situaciones de enrutamiento de alto rendimiento
Aplicaciones	Centros de datos, redes empresariales

La Figura 2.10 muestra el modelo MikroTik CCR1009-7G-1C-1S+.

Figura 2.10: MikroTik CCR1009-7G-1C-1S+ [Fuente:MikroTik CCR1009-7G-1C-1S+ User Guide.]

2.4.1. Descripción puertos MikroTik serie C1000-24P-4G-L

Puertos del panel posterior en el modelo MikroTik serie C1000-24P-4G-L, tal como se muestras en la Figura 2.11, son los siguientes:

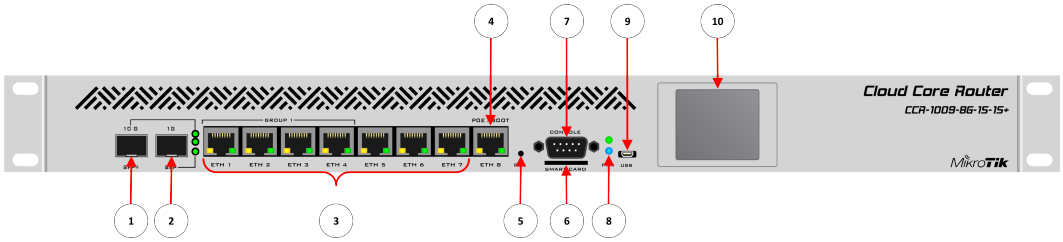


Figura 2.11: Descripción modelo MikroTik serie C1000-24P-4G-L [Fuente: Autores.]

En la Tabla 2.11, se indica la descripción de los puertos.

1	Ranura para módulos SFP+1 cage	4	Puerto PoE/Boot
2	Ranura para módulos SFP	5	Botón de reinicio
3	Puertos Ethernet	6	Ranura para tarjeta SD
7	Puerto consola	8	LED del sistema
9	Micro USB	10	Pantalla LCD

Tabla 2.11: Descripción modelo MikroTik serie C1000-24P-4G-L

Capítulo 3

Desarrollo de Practicas

Este capítulo se dedica a la descripción de las prácticas realizadas mediante el uso de equipos Cisco y Mikrotik, el diseño del manual practico se ideó con la finalidad de facilitar la configuración de los equipos en el Laboratorio de redes de computadoras, abarcando niveles que van desde lo básico hasta lo avanzado de manera progresiva. Con base en un sistema donde el docente presenta la materia que integra los fundamentos teóricos-prácticos. Este enfoque sigue un modelo de aprendizaje validado por las directrices de las escuelas Cisco y Mikrotik [12] , [26]. La estructuración de las practicas busca proporcionar una comprensión clara acerca del protocolo IPv6 y sus respectivas funciones y configuración de los dispositivos utilizados dentro de una red de datos.

3.1. Conexión de terminales en un entorno IPv6

En el desarrollo de cualquier práctica, la preparación de todas las herramientas necesarias es esencial para garantizar su correcto funcionamiento. En este caso específico, se emplean los equipos Cisco y Mikrotik junto con los programas Putty y Winbox, los cuales posibilitan el acceso a estos dispositivos, se procede como primera instancia a la conexión inicial de los terminales en un entorno IPv6.

Es necesario verificar que las configuraciones de seguridad o antivirus estén desactivadas, lo que incluye tanto el Firewall de Windows como cualquier

software antivirus. No obstante, en entornos de laboratorio o pruebas aisladas, se sugiere desactivar temporalmente el firewall o el software antivirus para eliminar posibles obstáculos en la comunicación entre dispositivos, cuyos procedimientos se encuentran detallados en el Anexo: Prácticas de Laboratorio.

3.2. Descripción Física del laboratorio

El Laboratorio de redes de computadoras de la Universidad Politécnica Salesiana, sede Cuenca, está equipado de equipos Cisco y MikroTik. Este laboratorio incluye un rack central con conexión a internet y dos racks destinados a pruebas: uno central y otro individual en la mesa de trabajo. Se puede observar en la Figura 3.1 los elementos y su disposición, la cual representa el diseño del laboratorio.

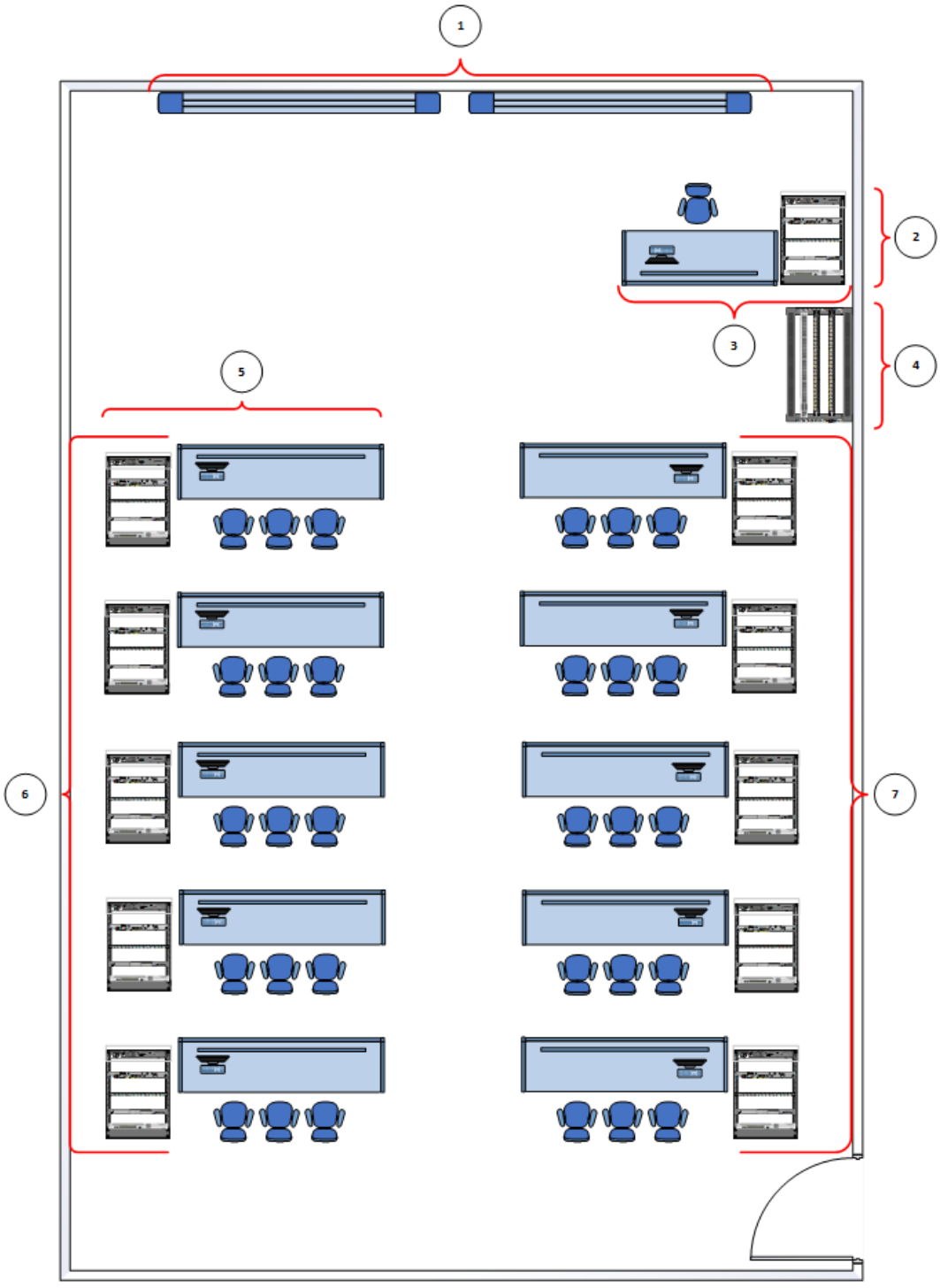


Figura 3.1: Laboratorio de Computo 8, [Fuente: Autores.]

En la siguiente Tabla 3.1, se muestra los detalles específicos del laboratorio.

1	Panel táctil	2	Rack de equipos para el docente
3	Estación de trabajo para el docente	4	Rack de conexiones principal
5	Estación de trabajo para los estudiantes	6	Rack de equipos en el lado izquierdo
7	Rack de equipos en el lado derecho		

Tabla 3.1: Estructura del Laboratorio de Cómputo 8

Es necesario Identificar el rack de conexiones principal, que actúa como el punto de interconexión primario para todos los demás racks en el entorno del Laboratorio. Es fundamental comprender la disposición de la conexión tanto en la estación de trabajo para los estudiantes como en el rack de conexiones principal del laboratorio. En la siguiente Figura 3.2,se describe el rack central del laboratorio.

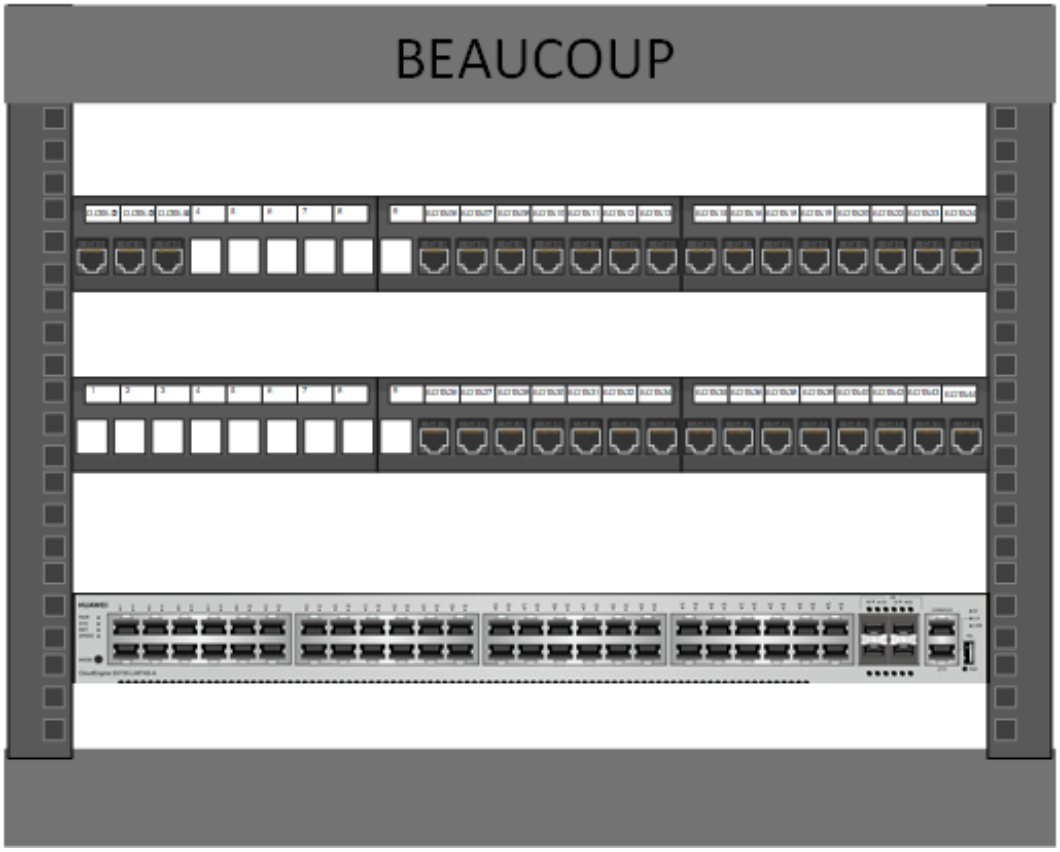


Figura 3.2: Rack central del Laboratorio, [Fuente: Autores.]

Para identificar los elementos y su disposición en cuanto a los equipos, se puede observar en la Figura 3.3, el rack destinado a pruebas ubicado en la estación de trabajo para los estudiantes.

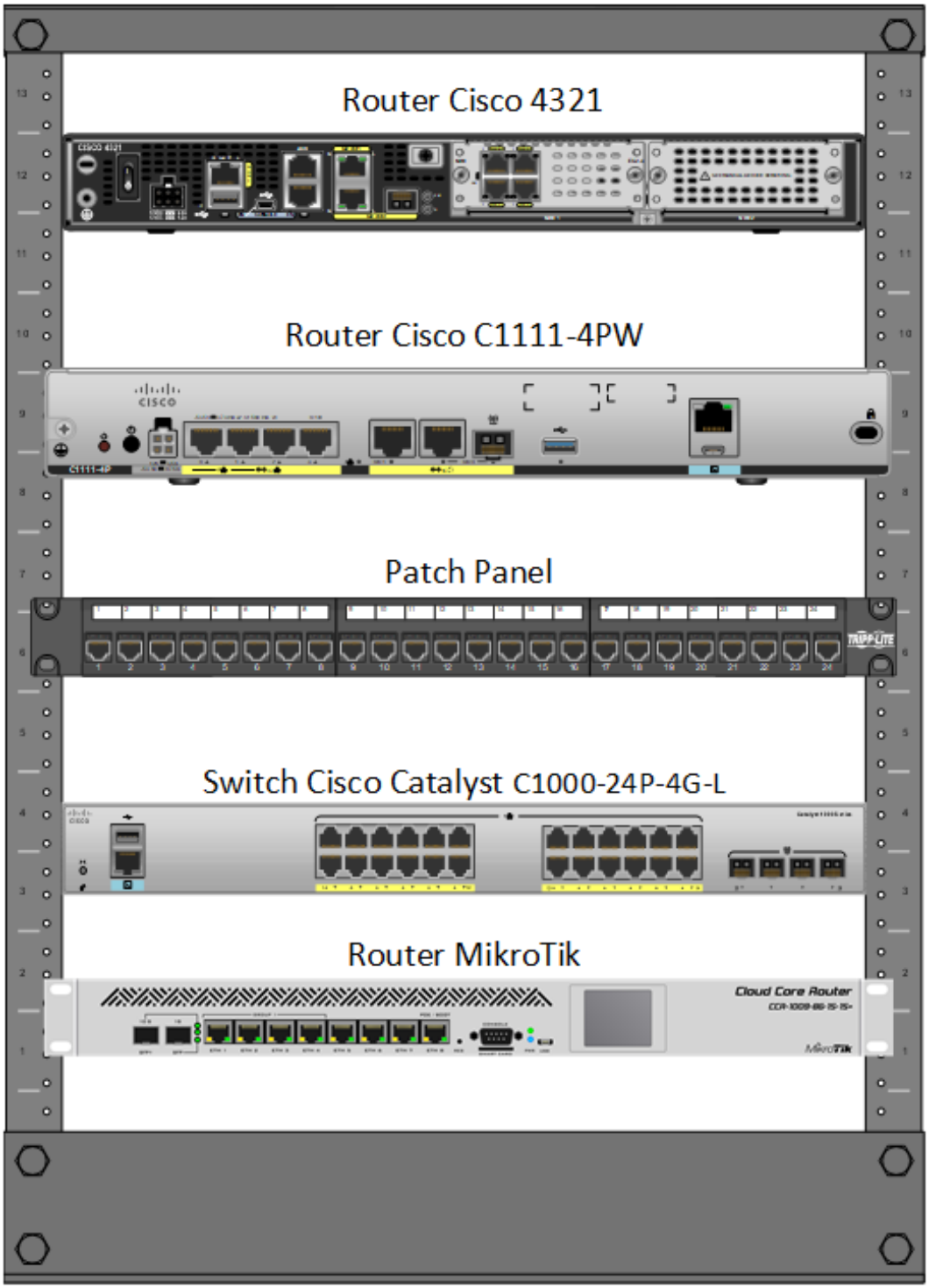
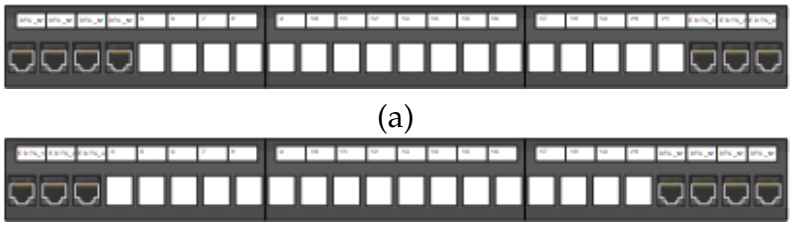


Figura 3.3: Diseño rack estación de trabajo para los estudiantes, [Fuente: Autores.]

3.2.1. Distribución de los paneles de conexión entre equipos del Laboratorio de redes de computadoras

Se dispone de estaciones de trabajo para los estudiantes los cuales han sido diseñados en función de su disposición. Se sugiere analizar el panel de conexión del rack asociado con cada estación de trabajo.



(a)

(b)

Figura 3.4: Paneles de conexión estación de trabajo estudiantes; (a) Panel de Conexión lado Izquierdo, (b) Panel de Conexión lado derecho, [Fuente: Los Autores.]

Las Figuras 3.4 ilustra los paneles de conexión del lado izquierdo y derecho, respectivamente, cuyos procedimientos se encuentran detallados en el Anexo: Prácticas de Laboratorio.

3.3. Estándar RFC 3315

El estándar RFC 3315 (DHCPv6) automatiza el proceso de asignación de direcciones IPv6 el cual resulta especialmente beneficiosa en entornos de redes extensas, donde la asignación manual de direcciones sería impracticable debido al tiempo y los recursos que implicaría. Gestiona de manera automática la asignación de direcciones IPv6, reduciendo así el riesgo de conflictos de direcciones que podrían surgir cuando varios dispositivos intentan utilizar la misma dirección, lo que podría afectar la conectividad.

Además, ofrece una gestión centralizada de la configuración de red, permitiendo a los administradores controlar y ajustar eficientemente la configuración desde un servidor DHCPv6 central. Esto asegura la consistencia en toda la red, facilitando la administración y la implementación de cambios en la configuración de manera uniforme. Figura 3.5 ilustra el esquema de funcionamiento

del estándar RFC 3315.

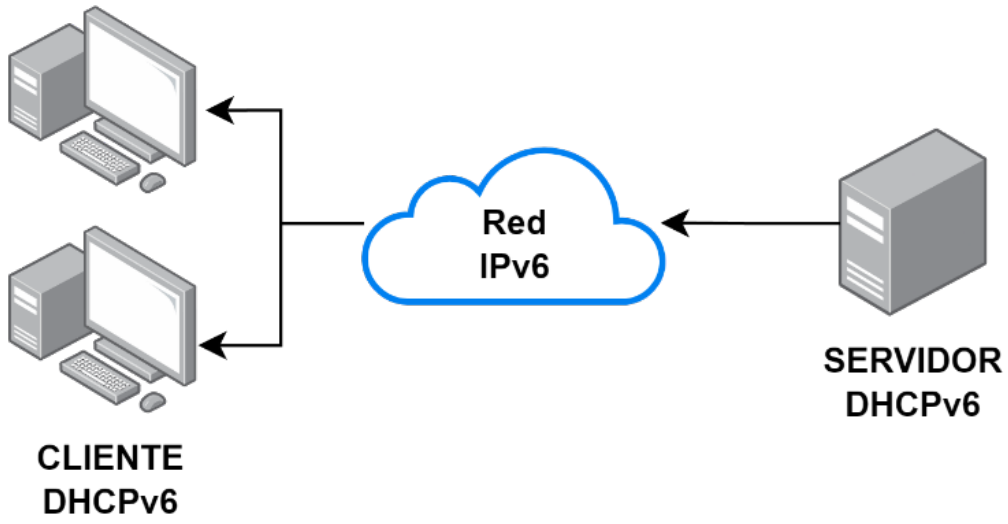


Figura 3.5: Estándar RFC 3315, [Fuente: Autores.]

3.4. Prácticas de Conmutación

En el ámbito profesional, resulta esencial adquirir competencias para la identificación y solución de problemas en el ámbito de redes. La partición de la red mediante el uso de VLANs emerge como una estrategia crucial para fortalecer la seguridad, al restringir la comunicación entre determinados conjuntos de dispositivos, disminuyendo la superficie de ataque y mitigando accesos no autorizados. El Protocolo de Árbol Expansivo (STP) y sus derivados, como PVSTP, ejercen una labor fundamental en la prevención de bucles en topologías de red redundantes. Estos protocolos aseguran la existencia de una única ruta funcional entre dos dispositivos, evitando así las tormentas de broadcast y los bucles de red. Asimismo, el Protocolo de Troncales VLAN (VTP) facilita la gestión centralizada de las VLANs en una red, posibilitando la configuración de VLANs en un único switch y la propagación automática de dichos cambios a otros switches en la red, simplificando de este modo la administración.

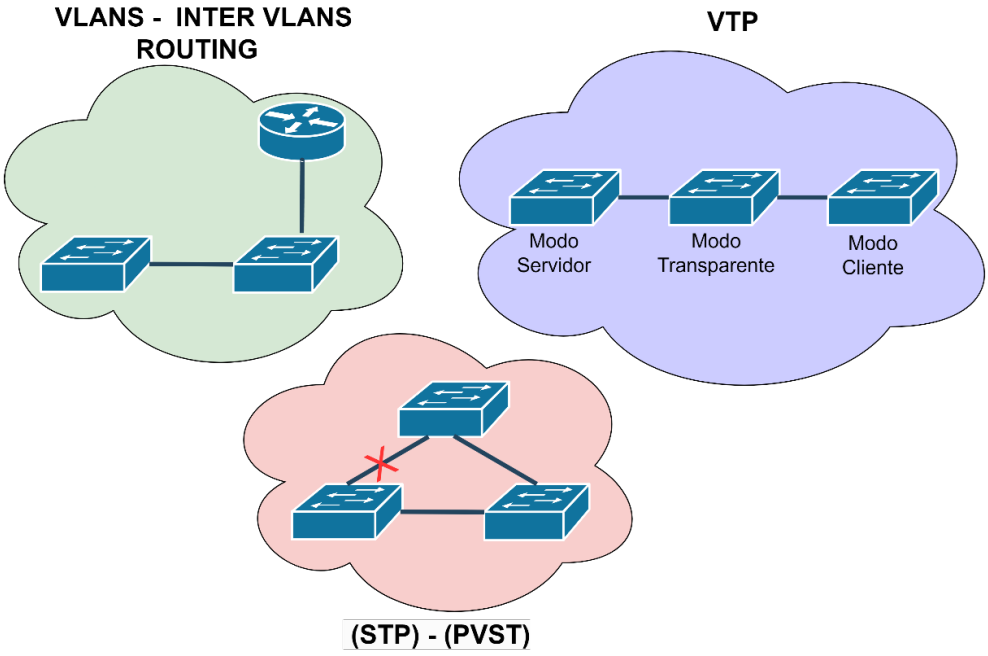


Figura 3.6: Protocolos de conmutación, [Fuente: Autores.]

La Figura 3.6 muestra los protocolos de conmutación realizados en estas prácticas, se lleva a cabo la implementación de conmutación con el objetivo de proporcionar a los estudiantes la posibilidad de cultivar habilidades prácticas, incrementar su comprensión y prepararlos para enfrentar futuros desafíos en sus trayectorias profesionales, mediante la utilización del dispositivo Switch Cisco Catalyst serie C1000-24P-4G-L. Este enfoque permitirá la integración de estos componentes en la infraestructura de red preexistente en el entorno de laboratorio. La información requerida para llevar a cabo las mencionadas prácticas se detalla en el Anexo: Prácticas de Laboratorio.

3.5. Prácticas de Enrutamiento

El papel fundamental del enrutamiento se manifiesta en el ámbito de las redes de computadoras, donde la definición de prácticas se sustenta en los principios tanto del enrutamiento estático como de los protocolos esenciales para el enrutamiento dinámico, tales como OSPF, BGP, EIGRP, etc. Adquirir un conocimiento más profundo de estos protocolos y las tecnologías conexas resulta

fundamental para el diseño y mantenimiento efectivo de redes. La obtención de experiencia práctica en enrutamiento permite a los profesionales optimizar la eficiencia operativa al reducir el tiempo de inactividad, mejorar la gestión del tráfico y facilitar la escalabilidad de la red.

3.5.1. Enrutamiento Estático

La configuración de rutas estáticas proporciona a los administradores de red un nivel más elevado de control sobre la selección de rutas, siendo muy útil en circunstancias específicas que demandan personalización en el flujo de datos dentro de la red. Este enfoque contribuye a prevenir posibles ataques de enrutamiento malintencionados, asegurando que el tráfico circule exclusivamente por las rutas autorizadas. Esta característica resulta beneficiosa en entornos donde la conservación de recursos es prioritaria. En determinados escenarios, el enrutamiento estático puede exhibir una mayor escalabilidad y estabilidad en comparación con sus contrapartes dinámicas.

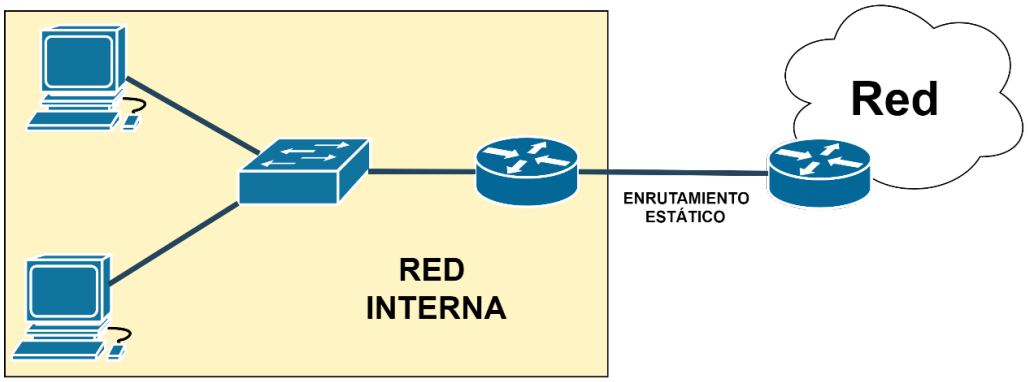


Figura 3.7: Protocolo de enrutamiento Estático, [Fuente: Autores.]

En la Figura 3.7, se presenta un esquema de enrutamiento estático elemental orientado a configuraciones fundamentales. La información necesaria para realizar dichas prácticas se detalla en el Anexo 1: Prácticas de Laboratorio.

3.5.2. Enrutamiento Dinámico

El enrutamiento dinámico permite la configuración automática de rutas alternativas ante un fallo en la ruta principal, mejorando así la resiliencia de la red y asegurando que el tráfico pueda encontrar rutas de respaldo en situaciones problemáticas de la red. Al expandirse la red o integrar nuevas ubicaciones, el enrutamiento dinámico simplifica la incorporación de estos cambios sin necesidad de realizar ajustes manuales en todos los routers afectados. Esta tecnología proporciona una solución más flexible, eficiente y escalable para la gestión de redes, especialmente en entornos extensos y dinámicos. Su habilidad para ajustarse de manera automática a modificaciones en la topología y proporcionar resiliencia y redundancia la posiciona como una herramienta esencial en la gestión de redes.

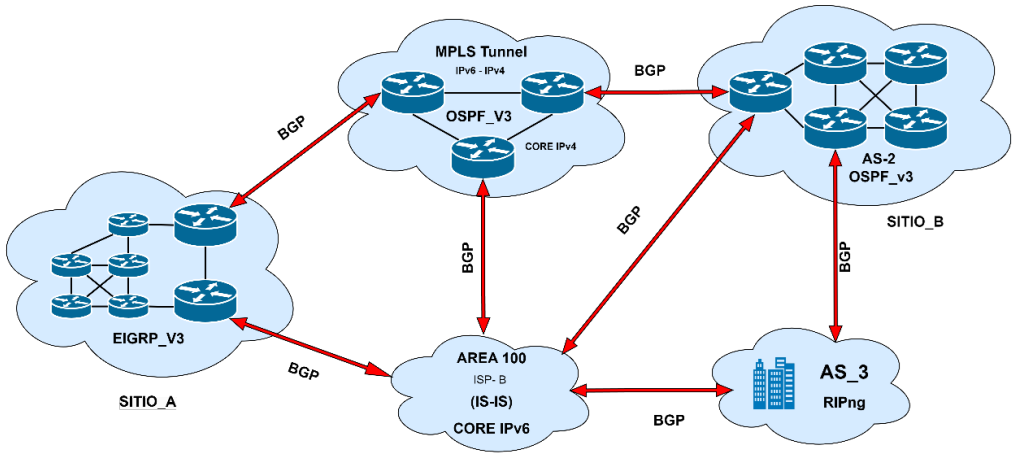


Figura 3.8: Protocolos de enrutamiento dinámico, [Fuente: Autores.]

La Figura 3.8 presenta un esquema correspondiente a los protocolos de enrutamiento creados. Es crucial destacar que la propuesta de conexión se desarrolló para satisfacer las necesidades de conexión. Con esta configuración, se busca optimizar tanto la disponibilidad como la calidad de la conexión en el laboratorio, proporcionando a los estudiantes habilidades prácticas fundamentales. Esto les permitirá comprender los principios esenciales del enrutamiento y los preparará para abordar los desafíos inherentes al diseño y mantenimiento de redes de computadoras. La información necesaria para estas prácticas se detalla en el Anexo: Prácticas de Laboratorio.

3.6. Listas de Control de Acceso

El despliegue de listas de control de acceso (ACLs) puede inicialmente resultar imponente, pero es imperativo desmitificar este proceso. Estas listas proporcionan un método efectivo para gestionar y supervisar el tráfico, salvaguardando la infraestructura contra potenciales amenazas y asegurando un entorno de red seguro y eficaz. Las ACLs ofrecen la capacidad de gestionar y filtrar el flujo de datos dentro de una red que utiliza el protocolo IPv6, permitiendo especificar qué tipos de tráfico son admitidos o bloqueados. La elaboración de normativas dentro de ACLs contribuye significativamente a fortalecer la seguridad de las redes IPv6, previniendo accesos no autorizados y ataques maliciosos. Este enfoque asegura que solo se permita el tráfico legítimo de acuerdo con las políticas de seguridad establecidas. Adicionalmente, se pueden utilizar de manera efectiva para mitigar el impacto de ataques de denegación de servicio distribuido al bloquear o filtrar el tráfico no deseado, contrarrestando así los intentos de sobrecargar los recursos de la red.

La representación esquemática en la Figura 3.9 ilustra el funcionamiento de las Listas de Control de Acceso (ACLs).

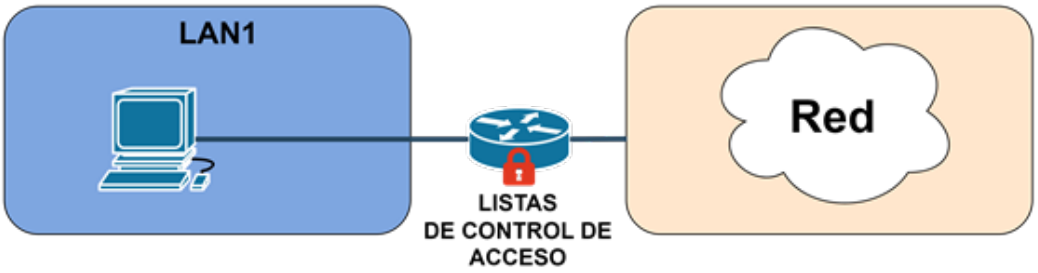


Figura 3.9: Funcionamiento de ACLs, [Fuente: Autores.]

Dentro del contexto del desarrollo de la práctica, se centró en la configuración ACLs para IPv6. Para llevar a cabo este procedimiento, fue necesario comprender en detalle la sintaxis y estructura específicas para IPv6, así como la implementación efectiva de estas reglas para administrar el tráfico dentro de la red. La práctica proporciona una perspectiva aplicada sobre cómo emplear las ACLs con el propósito de controlar de manera selectiva el flujo de paquetes, una función esencial

para potenciar la seguridad y la eficacia en entornos de redes basadas en IPv6. La información necesaria para esta práctica se detalla en el Anexo: Prácticas de Laboratorio.

Capítulo 4

Conclusiones y Trabajos Futuros

El protocolo IP versión seis cumple una función crucial en la transformación de las conexiones en la transformación digital actual, proporcionando un aumento significativo en la disponibilidad de direcciones IP en comparación con IP versión cuatro. La conmutación en redes de computadoras se posiciona como un elemento esencial en el intercambio de datos, para asegurar la eficacia, la seguridad y la confiabilidad en las comunicaciones entre dispositivos. De esta manera, la transición hacia IP versión seis no solo representa un avance tecnológico, sino también un proceso que demanda una base sólida en las bases de las redes de datos para garantizar una implementación efectiva y eficiente.

Con estos antecedentes el manual de prácticas resulta fiable para el aprendizaje de la asignatura de redes de computadoras, se logra un aporte valioso en el ámbito educativo orientado al aprendizaje de interconexión de redes con protocolo IP versión seis, siguiendo un modelo el cual integra la combinación de la teoría con un enfoque práctico, diseñado específicamente para su ejecución en el Laboratorio de Redes de Computadoras. Durante el análisis del desarrollo de practicas se a visto necesario que los estudiantes posean conocimientos previos en enrutamiento utilizando IP versión cuatro. En consecuencia, se recomienda llevar a cabo la implementación de este material de manera continua, permitiendo así que los estudiantes y los docentes interactúen progresivamente para lograr una asimilación perdurable de los contenidos.

De los resultados alcanzados, la metodología adoptada en este proceso

de aprendizaje practico de laboratorio integra de manera objetiva la teoría con los resultados de aprendizaje de la asignatura, permitiendo a los estudiantes desarrollar un conocimiento practico-empresarial en el manejo de equipos, de los fabricantes Cisco y MikroTik. Así también la ejecución de escenarios simulados avanzados mediante el uso de máquinas virtuales y el software GNS3, constituye un desafío a los estudiantes al aplicar sus conocimientos en situaciones más complejas y preparándolos así para los desafíos reales en el ámbito de las redes de telecomunicaciones

Considerando los aspectos anteriores, el manual de practicas fue validado durante algunas sesiones de laboratorio cuyos principales actores fueron los estudiantes de las carreras de Telecomunicaciones y Electrónica. Con estas actividades los involucrados logran alcanzar sus objetivos de aprendizaje en cuanto a conmutación, DHCP, enrutamiento, ACLs y MPLS. Las encuestas realizadas mediante formularios corroboran este trabajo de titulación de manera positiva, demostrando la efectividad y calidad del manual en el desarrollo educativo.

En resumen, este trabajo de titulación ofrece una valiosa contribución al proceso educativo en la materia de redes de computadoras, mediante un recurso documental completo y estructurado que facilita la comprensión y aplicación efectiva de IP versión seis para practicas de laboratorio.

En el ámbito de los futuros trabajos de titulación, se sugiere considerar la elaboración de una tesis centrada en el desarrollo de Multiprotocol Label Switching (MPLS) debido a que, actualmente, los equipos de laboratorio no admiten configuraciones para IP versión seis. Este enfoque exploraría la optimización y eficiencia de las redes mediante la implementación de la versión más reciente del Protocolo de Internet, abordando las complejidades y desafíos que surgen al integrar MPLS en un entorno IPv6. El trabajo podría incluir la creación de metodologías, pruebas y análisis exhaustivos para analizar la factibilidad y el desempeño de integración de MPLS con IP versión seis, así como la exploración de protocolos en desarrollo, aportando una contribución valiosa al avance de las redes modernas.

Adicionalmente, otra perspectiva interesante para futuros trabajos podría consistir en una tesis que se enfoque en técnicas efectivas de migración de IP versión

cuatro a IP versión seis, con el propósito de abordar un marco de referencia sólido para la certificación. Este desarrollo generaria estrategias prácticas, consideraciones de seguridad y desafíos comunes asociados con la transición de infraestructuras de red de IP versión cuatro a IP versión seis. La tesis no solo sería beneficiosa para profesionales en Telecomunicaciones y redes de computadoras, sino que también proporcionaría una guía valiosa para la industria en la adaptación progresiva hacia la adopción generalizada de IP versión seis, promoviendo la eficiencia y la seguridad en las comunicaciones en red.

Glosario

ACL Lista de Control de Acceso – Access Control List.

BGP Protocolo de Puerta de Enlace – Border Gateway Protocol.

DHCP Protocolo de Configuración dinámica de Host – Dynamic Host Configuration Protocol.

EIGRPv3 Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado versión 3 – Enhanced Interior Gateway Routing Protocol version 3.

IPv4 Protocolo de Internet versión 4 – Internet Protocol version 4.

Ipv6 Protocolo de Internet versión 6 – Internet Protocol versión 6.

IS-IS Sistema Intermedio a Sistema Intermedio – Intermediate System to intermediate System.

LDP Protocolo de Distribución de Etiquetas – Label Distribution Protocol.

MPLS Mecanismo de Transporte de Datos – Multiprotocol Label Switching.

OSPFv3 Abrir el Camino Más Corto Primero versión 3 – Open Shortest Path First version 3.

RIPng Protocolo de Información de enrutamiento de última generación – Routing Information Protocol next generation.

Bibliografía

[1] Iqbal Ahmad. Design and implementation of network security using inter-vlan-routing and dhcp. *Asian Journal of Applied Science and Technology*, 4:37–44, 2020.

[2] Ayoub Bahnasse, Fatima Ezzahraa Louhab, Hafsa Ait Oulahyane, Mohamed Talea, and Assia Bakali. Novel sdn architecture for smart mpls traffic engineering-diffserv aware management. *Future Generation Computer Systems*, 87:115–126, 2018.

[3] Ganesh Babu C, Banupriya N, and Nagarajan N. Performance breakdown and redistribution amidst ospf, eigrp is-is dynamic routing protocols in ipv6 network, 12 2022.

[4] Manuel Andrés Vélez-Guerrero Aura Ximena González Cely Mauro Callejas-Cuervo. *Control digital de orientación, posición y velocidad basado en movimientos de la cabeza para un prototipo de simulación de silla de ruedas*. Editorial UPTC, 1.ª ed. edition, 2022.

[5] Juan Carlos Yungán Cazar and Carina Valeria Narváez Contero. Evaluacion del protocolo 802.1 q en la implementación de vlans en entornos wireless mediante la aplicación de software libre. *Dominio de las Ciencias*, 8(3):44, 2022.

[6] Jhamir Jesus Quispe Chavez et al. Aplicación de un sistema de seguridad en la red (internet) utilizando el tunel gre de cisco sobre ipv6 en la institución financiera"prendamas".

[7] Simone Cirani, Gianluigi Ferrari, Marco Picone, and Luca Veltri. *Internet of Things: Architectures, Protocols and Standards*. 7 2018.

[8] Cisco. Cisco 1000 series integrated services routers data sheet - cisco.

[9] Cisco. Cisco 4-port, 8-port, and 8-port with poe/poe+ gigabit ethernet lan switch network interface modules data sheet - cisco.

[10] Cisco. Cisco 4321 integrated services router - cisco.

[11] Cisco. Ficha técnica de los switches cisco catalyst de la serie 1000 - cisco.

[12] Cisco. Aprendizaje y habilidades digitales, 2024. 05/02/2024.

[13] Ramon de la Rosa Falguera. Fundamentos teorico-practicos del protocolo ipv6. 2016.

[14] Lazaro Laz Diaz. *CCNA Routing and Switching 200-125 Certification Guide: The ultimate solution for passing the CCNA certification and boosting your networking career*. Packt Publishing Ltd, 2018.

[15] Khalid El Khadiri, Najib El Kamoun, Samir El Ouaham, Ouidad Labouidya, Kawtar Smahi, and Rachid Hilal. Performance and scalability of ipv4/ipv6 transition mechanisms for real-time applications. *Journal of Theoretical and Applied Information Technology*, 101(23):7826 – 7836, 2023. Cited by: 0.

[16] Anthony Freda. ¿qué diferencia hay entre ipv4 e ipv6?, 3 2021. Accessed: 2023-7-13.

[17] Novi Trisman Hadi. Comparison of ipv6 dynamic routing protocols on routing hole handling, 11 2022.

[18] Talhia HERNANDEZ, Pedro SALAZAR, and Saul SOTO. Sistema inteligente para validar una lista de control de acceso (acl) en una red de comunicaciones. *Revista de Simulación*, 1:24–31, 2017.

[19] Mohd. Imran, Mohd Amir Khan, and Mohammed Abdul Qadeer. Design and simulation of traffic engineering using mpls in gns3 environment. pages 1026–1030, 2018.

[20] Neha Jain and Ashish Payal. Comparison between ipv4 and ipv6 using ospf and ospfv3 on riverbed modeler, 12 2019.

[21] Siyuan Jia, Matthew Luckie, Bradley Huffaker, Ahmed Elmokashfi, Emile Aben, Kimberly Claffy, and Amogh Dhamdhere. Tracking the deployment of ipv6: Topology, routing and performance. *Computer Networks*, 165:106947, 2019.

[22] Sivalasya Kasu, Larry Hash, John Marsh, Ronny Bull, et al. Spanning tree protocol. 2015.

[23] Wilson Kevin. *Exploring Computer Systems : The Illustrated Guide to Understanding Computer Systems, Hardware Networks.*, volume 2019 edition. Elluminet Press, 2019.

[24] Siti Ummi Masruroh, Mohammed Fajarullah Furtami, Andrew Fiade, Asep Taufik Muharram, Hendra Bayu Suseno, and Saepul Aripiyanto. Performance evaluation of routing protocol ripng and ospfv3 on ipv6 using fhrp protocol, 9 2022.

[25] MikroTik. Mikrotik routers and wireless - products: Ccr1009-7g-1c-1s+.

[26] Mikrotik. Capacitación, 2023. 08/03/2023.

[27] Milagros Maribel Chinguel Rodriguez. Mecanismos de transición para la migración de ipv4–ipv6. 2020.

[28] Glen D Singh, Michael Vinod, and Vijay Anandh. *CCNA Security 210-260 Certification Guide: Build your knowledge of network security and pass your CCNA Security exam (210-260)*. Packt Publishing Ltd, 2018.

[29] Sasalak Tongkaw and Aumnat Tongkaw. Multi-vlan design over ipsec vpn for campus network. *2018 IEEE Conference on Wireless Sensors (ICWiSe)*, pages 66–71, 11 2018.

[30] Mochamad Wahyudi et al. Network performance optimization using dynamic enhanced interior routing protocols gateway routing protocol for ipv6 (eigrpv6) and ipv6 access control list. volume 1830, page 12017, 2021.

[31] Goralski Walter. *The Illustrated Network : How TCP/IP Works in a Modern Network.*, volume Second edition. Morgan Kaufmann, 2017.

[32] Shuangbao Paul Wang. *Communication, TCP/IP, and Internet*. Springer Singapore, 2021.

ANEXOS: PRÁCTICAS DE LABORATORIO

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN**
REALIZADO POR:		
CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**1**	**TÍTULO PRÁCTICA:** Configuración y Verificación de Conectividad IPv6.

OBJETIVO:

- Familiarizarse con la estructura y configuración de direcciones IPv6.
- Implementar y comprobar la conectividad entre dispositivos utilizando IPv6.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

1. (1) Switch Cisco Catalyst.
2. (3) Computadoras con soporte para IPv6.
3. (3) Cables de red Ethernet.
4. (1) Cable serial.

NOTA: Es necesario contar con 3 computadoras equipadas con interfaces Ethernet para llevar a cabo la práctica. Se brinda la opción de utilizar su propia computadora junto con la que se encuentra en la mesa de trabajo. En caso de no contar con dicha interfaz, se deberá disponer de adaptadores Ethernet, ya que la práctica se ha diseñado para ser ejecutada en cada estación de trabajo en el laboratorio de cómputo 8.

DESCRIPCIÓN GENERAL:

En esta práctica de laboratorio, los terminales se conectan por primera vez en un entorno IPv6 y se comprueba la conectividad entre ellos.

INSTRUCCIONES:

1. Descripción de equipos.

Revise la **Figura 1**, para identificar el dispositivo Switch Cisco Catalyst serie C1000-24P-4G-L que será empleado para el desarrollo de la práctica.

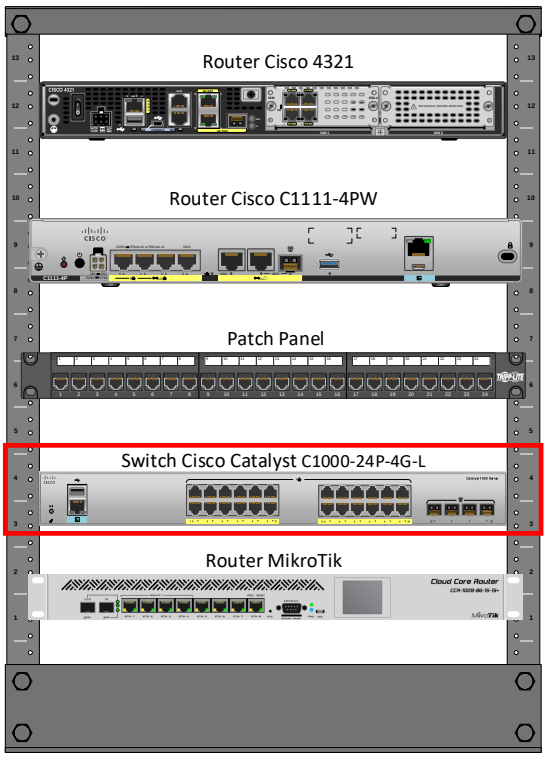


Figura 1. Diseño Rack Laboratorio de Cómputo 8.

En la **Figura 2** se muestra el equipo y cada una de sus partes, los cuales se detallan en la **Tabla 1**.

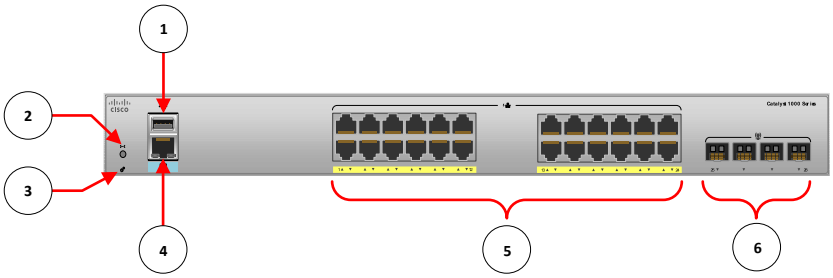


Figura 2. Switch Cisco Catalyst serie C1000-24P-4G-L.

Especificaciones del equipo

Catalyst 1000 Series C1000-24P-4G-L.			
1	Puerto USB tipo A	2	Botón de reinicio
3	LED del sistema	4	Puerto de consola RJ-45
5	24 puertos 10/100/1000 PoE+	6	Ranuras para módulos SFP

Tabla 1. Especificaciones Switch Cisco

En la **Figura 3** se muestra la secuencia de numeración de los puertos los cuales siguen una disposición de izquierda a derecha y de arriba a abajo, comenzando desde el número 1 y continuando en orden ascendente.

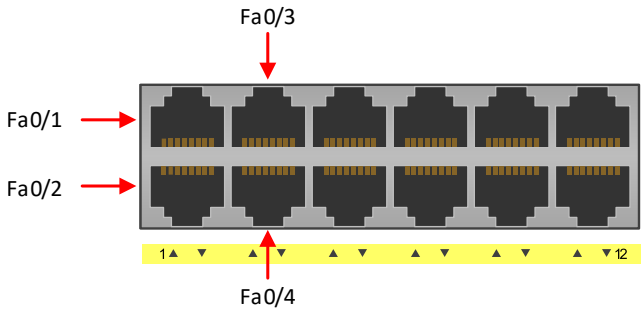


Figura 3. 24 puertos 10/100/1000 PoE+.

2. Esquema de la práctica a desarrollar.

En esta práctica usted deberá conectar los equipos del laboratorio de redes como se muestra a continuación:

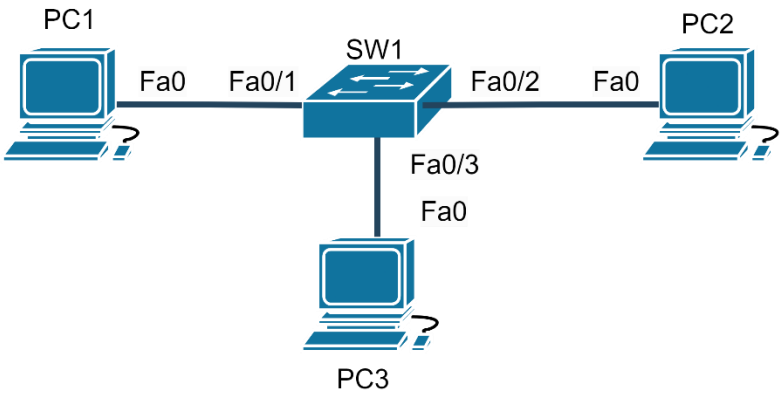


Figura 4. Topología de la red.

Conecte los cables Ethernet a los puertos Fast Ethernet del switch, tal como se muestra en la **Figura 4**, teniendo en cuenta las especificaciones de los equipos. Verifique la activación de un indicador luminoso de tonalidad verde en la interfaz física del switch; en caso de no observarse esta señal, reubique los cables a diferentes puertos del switch y continúe con la práctica.

3. Configuración de direccionamiento IPv6 en los terminales.

A continuación, se describen los pasos que deben seguirse para configurar una dirección IPv6 en el sistema operativo Windows 10 utilizado en el entorno del laboratorio de cómputo 8.

Haga clic en Inicio > Panel de Control > Red e Internet > Centro de redes y recursos compartidos.

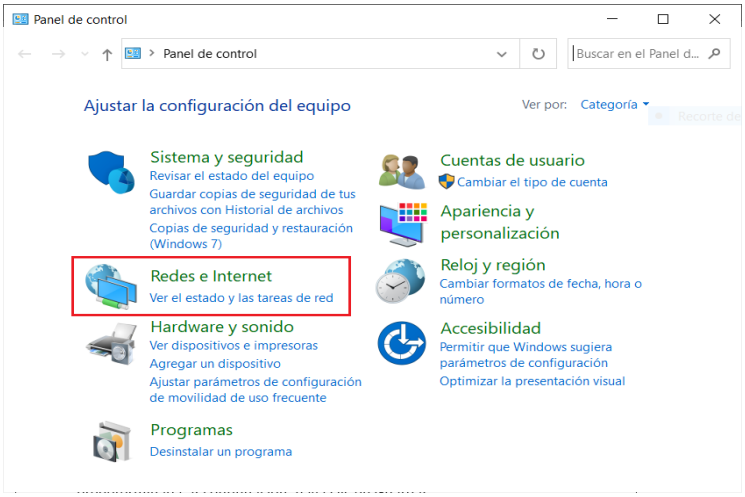


Figura 5. Panel de Control.

En su conexión de área local, haga clic en Cambiar configuración del adaptador.

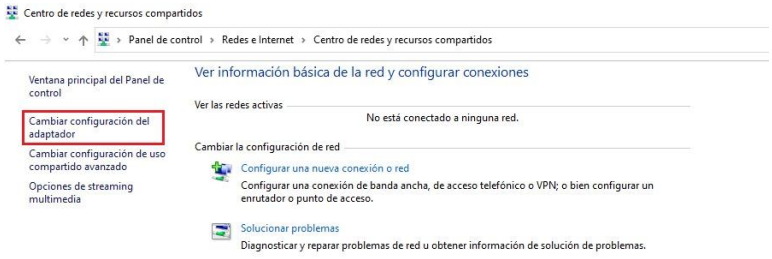


Figura 6. Centro de redes y recursos compartidos.

Seleccione la tarjeta de interfaz de red Ethernet, haga clic en propiedades.

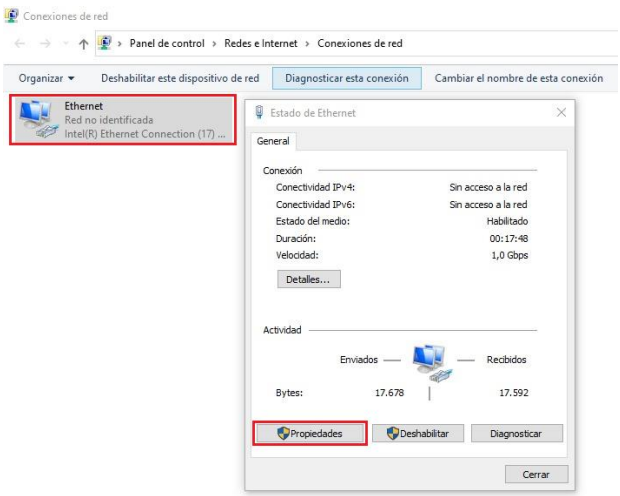


Figura 7. Configuraciones del Adaptador

Dentro de propiedades de Ethernet, seleccione protocolo de internet versión 6 (TCP/IPv6), asegúrese de que la casilla está marcada.

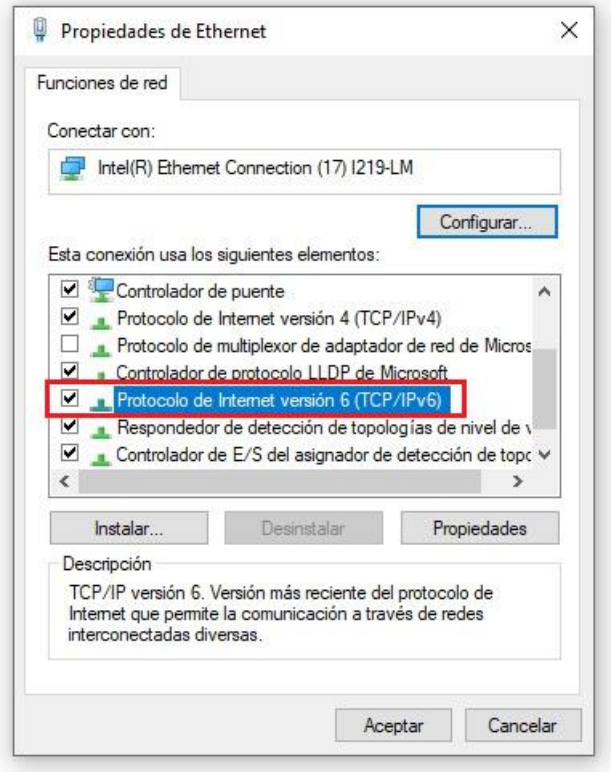


Figura 8. Propiedades de Ethernet

Por defecto, estará marcada la opción Obtener dirección IP automáticamente, cambiamos a usar la siguiente dirección IPv6.

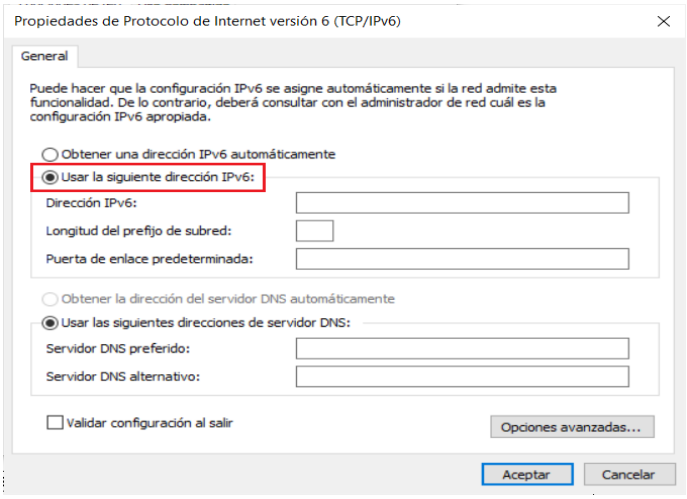


Figura 9. Propiedades de Protocolo de Internet versión 6 (TCP/IP).

Introduzca la Dirección IPv6, el prefijo de subred y la puerta de enlace predeterminada. A continuación, haga clic en Aceptar.

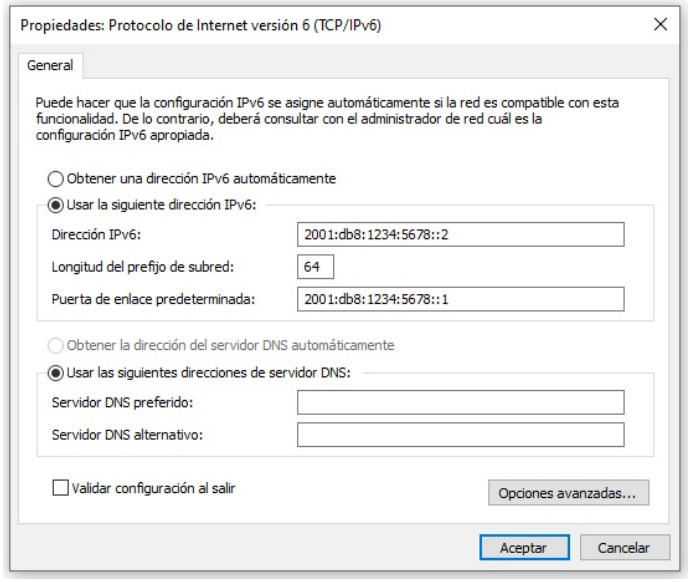


Figura 10. Configuración de IPv6.

Asigne direcciones IPv6 a cada **terminal,** como se muestra en la **Tabla 2**.

Equipos	Interfaz	Dirección	Mask
PC1	NIC	2001:0db8:1234:5678::2	/64
PC2	NIC	2001:0db8:1234:5678::3	/64
PC3	NIC	2001:0db8:1234:5678::4	/64
Puerta de enlace Predeterminada		2001:0db8:1234:5678::1	

Tabla 2. Asignación de direcciones IPv6

NOTA: El prefijo "NIC" se utiliza para denotar la tarjeta de interfaz de red de cada computadora.

RECOMENDACIÓN: Es necesario verificar que las configuraciones de seguridad o antivirus estén desactivadas en el terminal o PC, lo que incluye tanto el Firewall de Windows como cualquier software antivirus, ya que podrían surgir problemas durante la ejecución de pruebas de conectividad.

A continuación, se describen los pasos que deben seguirse para desactivar el Firewall de Windows.

Haga clic en Inicio > Panel de Control > Sistema y Seguridad.

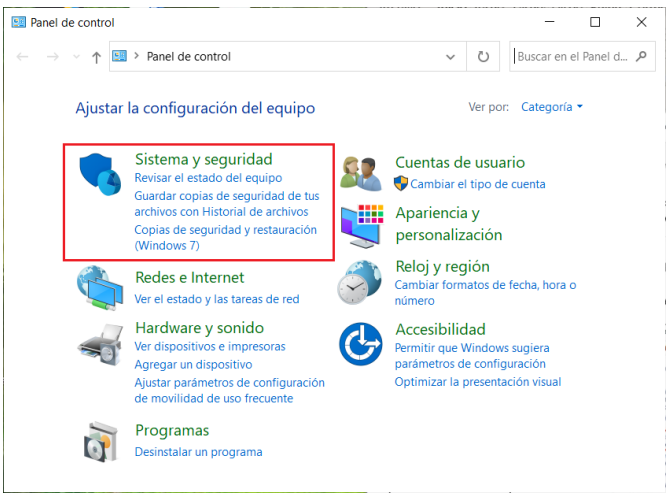


Figura 11. Panel de Control.

Dentro de la sección denominada “Sistema y Seguridad”, procedemos a seleccionar la opción Firewall Windows Defender.

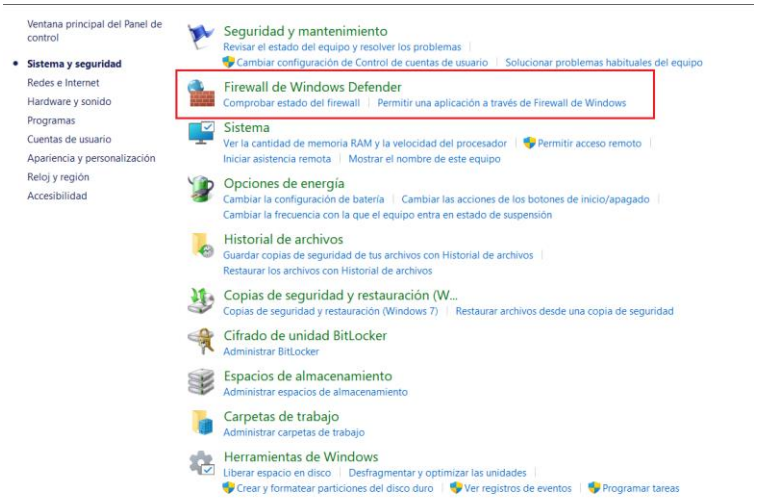


Figura 12. Sistema y Seguridad.

En la configuración del Firewall de Windows Defender, seleccionar la opción Activar o desactivar Firewall de Windows Defender.

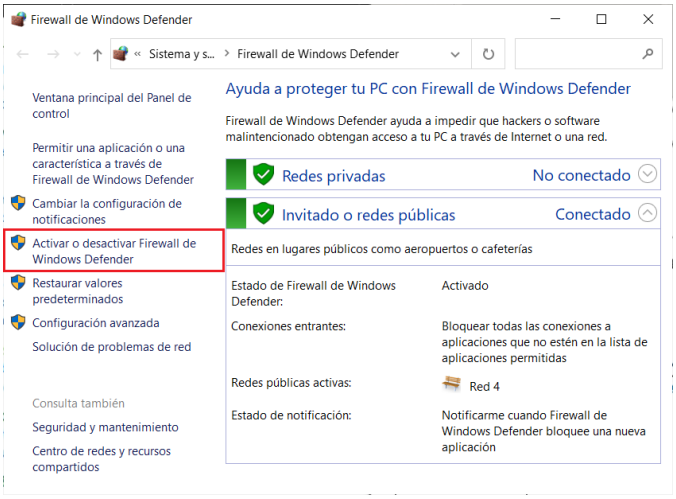


Figura 13. Activar o desactivar Firewall de Windows Defender.

Haga clic en Desactivar Firewall de Windows Defender.

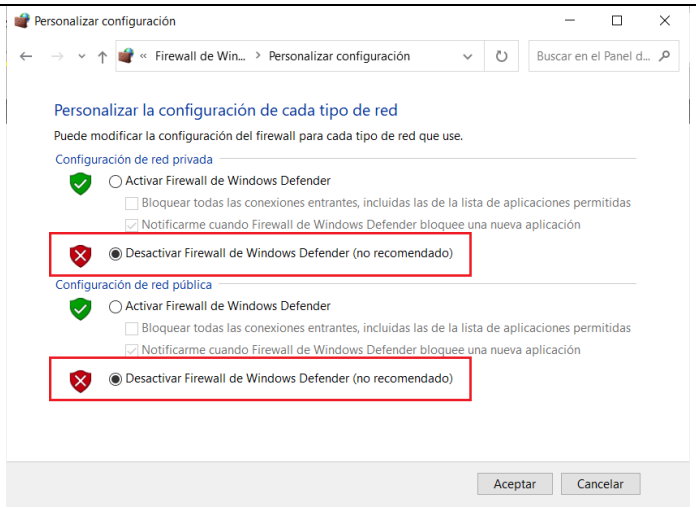


Figura 14. Desactivar Firewall de Windows Defender.

Nota: Algunos Terminales (Computadoras) al deshabilitar las configuraciones de seguridad y el Antivirus aún pueden seguir bloqueando el tráfico al momento de realizar pruebas de conectividad. Si se presenta esta situación se recomienda probar con otro Terminal.

4. Verificación de conectividad en IPv6.

Al igual que en IPv4, se utiliza el comando “ping” seguido de la dirección IPv6 para realizar la verificación, acceda a la interfaz de línea de comandos de Windows mediante los siguientes pasos:

1. Acceda a la interfaz de línea de comandos de Windows:
   - Haga clic en "Inicio" o presione la tecla con el logo de Windows.
   - Escriba “Símbolo del sistema” o “cmd” en la barra de búsqueda y presione “Enter”.
2. Dentro de la ventana de comandos, use el comando “ping” seguido de la dirección IPv6 del destino:

Ejemplo:

```
ping 2001:0db8:1234:5678::4
```

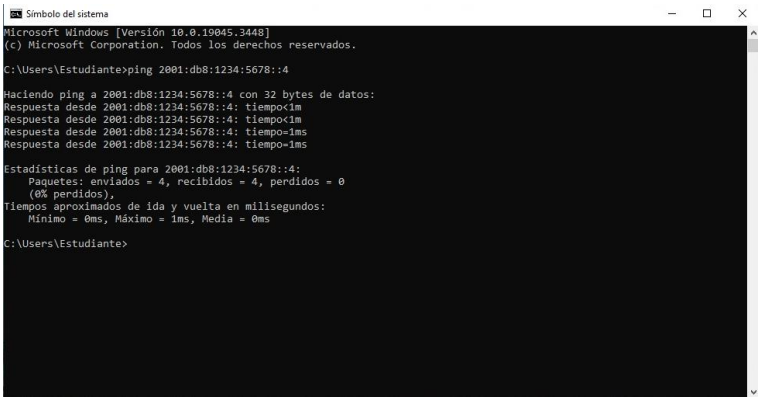


Figura 15. Prueba de Conectividad.

3. Para realizar un "ping" continuo, use la opción "-t":

Ejemplo:

```
ping 2001:0db8:1234:5678::4 -t
```

- Para detener el ping continuo, presione Ctrl + C.

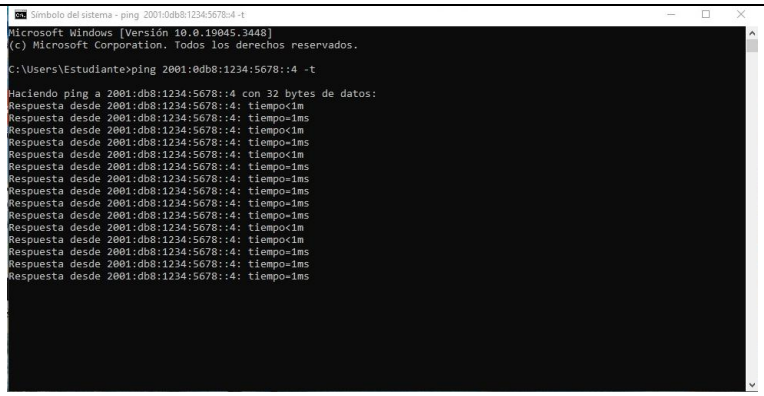


Figura 16. Prueba de Conectividad, ping cargado.

4. Después de realizar las pruebas, analice los resultados y adjunte evidencia de los mismos al final de la práctica.

RECOMENDACIÓN: Si experimenta dificultades al ejecutar el comando “ping”, se recomienda verificar los indicadores LED del switch. En caso de que el LED no muestre actividad, considere la opción de redirigir el tráfico a otros puertos del switch, espere unos segundos para que se encienda el LED correspondiente y continue con las pruebas correspondientes.

5. Formato de direcciones IPv6.

En la **Tabla 3**, se requiere completar las direcciones IPv6 correspondientes, aplicando las reglas para la reducción y expansión de direcciones IPv6.

COMPLETO	ABREVIADO
2001:0db8:0000:0000:0000:0000:0000:0001	
	2001:db8:1234:5678:abcd::abcd
2001:0db8:0a0b:0c0d:0e0f:0e0f:0e0f:0e0f	
	2001:db8:1111:2222:3333:4444:5555:6666
2001:0db8:aaaa:bbbb:cccc:dddd:eeee:ffff	
2600:0000:0000:0000:1234:5678:abcd:ef01	
	2001:db8:8765:4321:fedc:ba98:7654:3210

Tabla 3. Formato de direcciones IPv6

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. **¿Qué es IPv6 y cuál es su importancia en comparación con IPv4?**
2. **¿Cuáles son las limitaciones de IPv4 que motivaron la necesidad de desarrollar IPv6?**
3. **¿Cuál es la estructura de una dirección IPv6 y cuál es la diferencia principal en comparación con una dirección IPv4?**
4. **¿En qué formatos es posible expresar una abreviatura de una dirección IPv6?**
5. **¿Cuáles son los tipos de direcciones IPv6 y para qué se utilizan?**
   ¿Cuál es el estado actual de la adopción de IPv6 a nivel mundial?

ACTIVIDADES DESARROLLADAS

(Anotar las actividades que siguió para el desarrollo de la práctica)

El estudiante deberá redactar los pasos a cumplir en las instrucciones.

Verificación de Conectividad

Incluya los resultados adquiridos en las pruebas de conectividad, acompañados de un análisis.

Prueba de Conectividad desde PC1 hacia PC3

Aquí usted deberá adjuntar la evidencia de la prueba de conectividad entre los terminales.

Prueba de Conectividad desde PC1 hacia PC2

Aquí usted deberá adjuntar la evidencia de la prueba de conectividad entre los terminales.

En el recuadro el estudiante deberá redactar su análisis de la práctica en lo que respecta a las pruebas de conectividad.

Análisis:

Aquí usted deberá adjuntar la evidencia de la prueba de conectividad entre los terminales.

Formato de Direcciones IPv6

Aquí usted deberá completar la tabla con las direcciones IPv6 correspondientes, aplicando las reglas para la reducción y expansión de direcciones IPv6.

COMPLETO	ABREVIADO
2001:0db8:0000:0000:0000:0000:0000:0001	
	2001:db8:1234:5678:abcd::abcd
2001:0db8:0a0b:0c0d:0e0f:0e0f:0e0f:0e0f	
	2001:db8:1111:2222:3333:4444:5555:6666
2001:0db8:aaaa:bbbb:cccc:dddd:eeee:ffff	
2600:0000:0000:0000:1234:5678:abcd:ef01	
2001:db8:8765:4321:fedc:ba98:7654:33210	2001:db8:8765:4321:fedc:ba98:7654:3210

CONCLUSIONES:

BIBLIOGRAFIA:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN**
REALIZADO POR:		
CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**2**	**TÍTULO PRÁCTICA:** Configuración básica IPv6 Router Cisco.

OBJETIVO:

- Realizar configuraciones básicas en un enrutador.
- Configurar y habilitar las interfaces Ethernet con direcciones IPv6.
- Realizar pruebas y verificar las configuraciones realizadas.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

1. (1) Router Cisco.
2. (1) Switch Cisco Catalyst.
3. (2) Dispositivos con capacidad para soportar IPv6 (p. ej. computadoras).
4. (3) Cables de red Ethernet.
5. (1) Cable serial.

NOTA: Es necesario contar con 2 computadoras equipadas con interfaces Ethernet para llevar a cabo la práctica. Se brinda la opción de utilizar su propia computadora junto con la que se encuentra en la mesa de trabajo. En caso de no contar con dicha interfaz, se deberá disponer de adaptadores Ethernet, ya que la práctica se ha diseñado para ser ejecutada en cada estación de trabajo en el laboratorio de cómputo 8.

DESCRIPCIÓN GENERAL:

En esta práctica de laboratorio, los terminales y los enrutadores se conectan por primera vez en un entorno IPv6.

INSTRUCCIONES:

1. Descripción de equipos

Revise la **Figura 1**, para identificar los dispositivos Router Cisco 4321 y Switch Cisco Catalyst serie C1000-24P-4G-L que serán empleados para el desarrollo de la práctica.

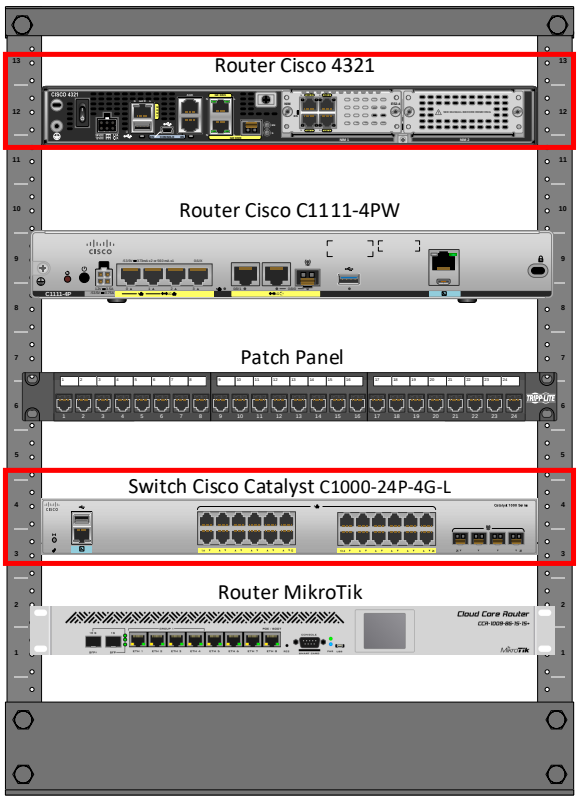


Figura 1. Diseño Rack Laboratorio de Cómputo 8.

En la **Figura 2 y 3** se muestran los equipos y cada una de sus partes, los cuales se detallan en las siguientes **Tablas 1 y 2**.

Router Cisco 4321.

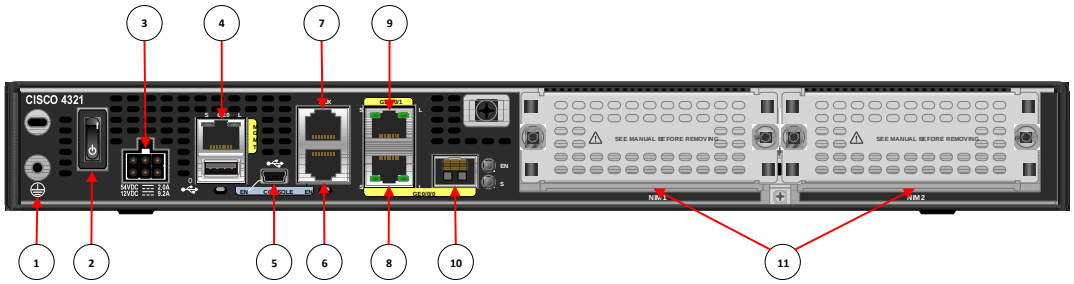


Figura 2. Router Cisco 4321.

Especificaciones del equipo

CISCO 4321			
1	Puesta a tierra	2	Interruptor de alimentación
3	Conector de entrada de alimentación	4	Puerto GE "MGMT" (con puerto USB debajo)
5	Minipuerto USB tipo B	6	Puerto de consola
7	Puerto auxiliar	8	GE 0/0/0 RJ-45 (puerto de cable)
9	GE 0/0/1 RJ-45 (puerto de cable)	10	GE 0/0/0 SFP (puerto de fibra óptica)
11	Ranuras NIM		

Tabla 1. Especificaciones Router Cisco 4321 ISR.

Switch Cisco Catalyst serie C1000-24P-4G-L.

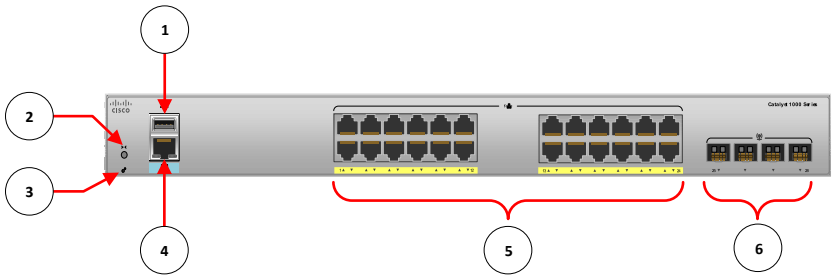


Figura 3. Switch Cisco Catalyst serie C1000-24P-4G-L.

Especificaciones del equipo

Catalyst 1000 Series C1000-24P-4G-L.			
1	Puerto USB tipo A	2	Botón de reinicio
3	LED del sistema	4	Puerto de consola RJ-45
5	24 puertos 10/100/1000 PoE+	6	Ranuras para módulos SFP

Tabla 2. Especificaciones Switch Cisco.

2. Esquema de la práctica a desarrollar.

En esta práctica usted deberá conectar los equipos del laboratorio de red como se muestra a continuación:

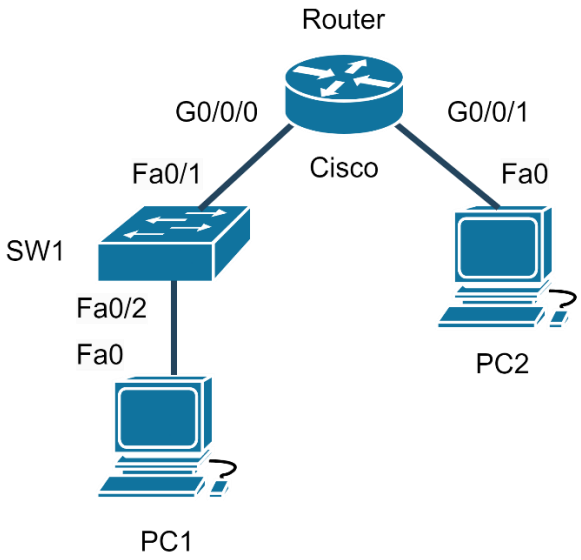


Figura 4. Topología de la red.

Conecte los cables Ethernet a los puertos Gigabit Ethernet 0/0/0, 0/0/1 del router y switch Fa0/1, Fa0/2 tal como se muestra en la **Figura 4**, teniendo en cuenta las especificaciones de los equipos. Es importante recordar que para configurar los routers Cisco, se debe establecer una conexión a través del puerto de consola.

3. Configuración del router Cisco a través del Puerto Consola.

Para establecer una conexión entre un router CISCO y un sistema operativo Windows, se requiere la utilización de un cable Cisco DB9/RS232 a RJ45, el cual debe estar acompañado de un adaptador USB, que comúnmente se conoce como “Cable Serial”, tal como se muestra en la **Figura 5**.

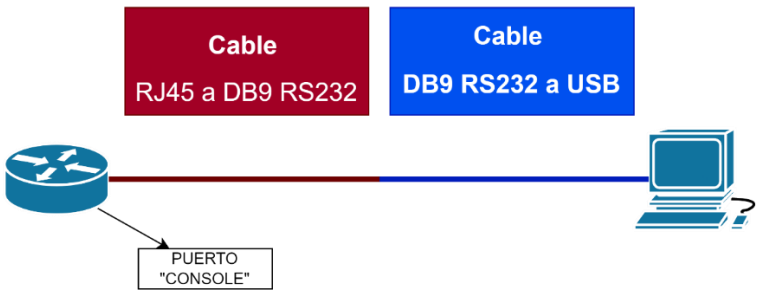


Figura 5. Esquema de conexión por consola cable serial.

A continuación, se detallan las instrucciones necesarias para llevar a cabo este procedimiento. Una vez encendido el enrutador y conectado el cable serial al puerto de consola (representado en la **Figura 5**), es necesario determinar el puerto serial, también conocido como COM (en Windows).

Para identificar el puerto al que está conectado nuestro enrutador, realizaremos un clic derecho en el menú de inicio y seleccionaremos "Administrador de dispositivos".

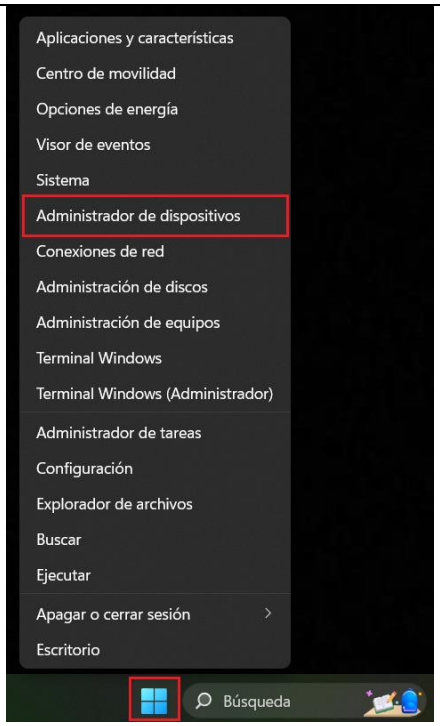


Figura 6. Menú inicio.

En la nueva ventana, accederemos a la sección "Puertos (COM y LPT)" y localizaremos el dispositivo USB-Serial, prestando especial atención al puerto COM que se muestra entre paréntesis. En este caso, identificamos el puerto COM3.

Nota: En caso de que el cable serial no sea reconocido, será necesario descargar el controlador correspondiente para el dispositivo USB to UART RS232 Serial de la marca Prolific. Para llevar a cabo esta acción, se debe realizar una búsqueda con el término “Prolific USB-to-Serial Comm Port Driver”.

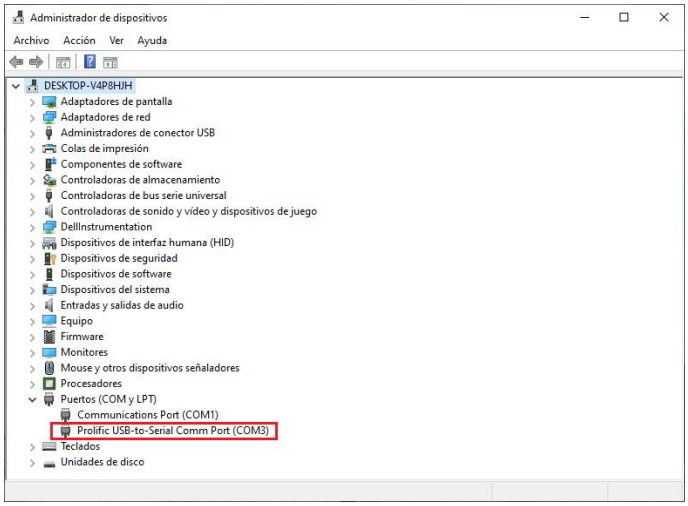


Figura 7. Ventana Administrador de dispositivos, Puerto ‘COM’ del convertidor usb-serie.

Una vez identificado el nombre del puerto serial detectado, se debe abrir el emulador de terminal PuTTY y seleccionar la opción de conexión serial.

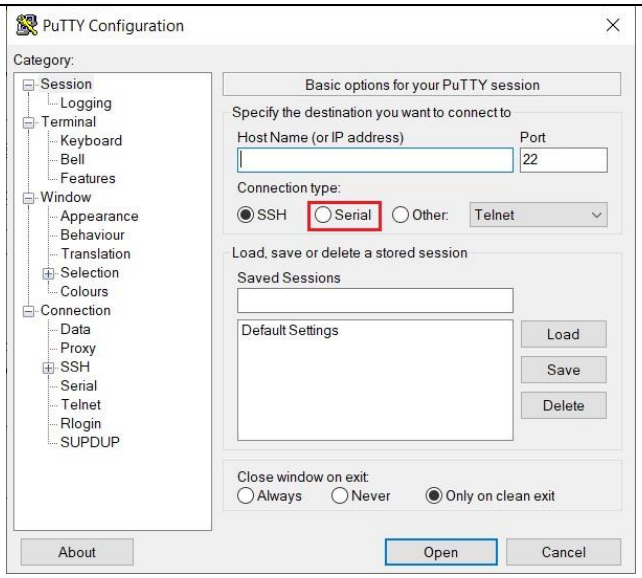


Figura 8. Ventana de Configuración PuTTY.

Nos pedirá que especifiquemos el nombre del puerto "COM" que identificamos en el equipo y la velocidad de transmisión, por defecto se elige 9600.

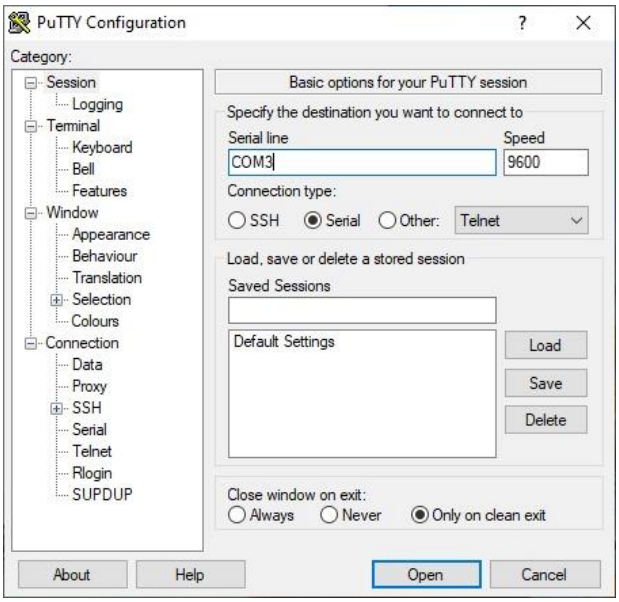


Figura 9. Configuración de puerto y velocidad de transmisión.

4. Configuración de direcciones IPv6.

Las interfaces se configurarán utilizando las direcciones presentadas en la **Tabla 3** de direccionamiento de este laboratorio.

Equipos	Interfaz	Direccion	Mask	Gateway
Router	G0/0/0	2001:db8:7777:1::1	/64	NA
	G0/0/1	2001:db8:8888:2::1	/64	NA

Tabla 3. Tabla de direcciones IPv6.

En esta práctica se utilizan dos interfaces GigabitEthernet (1000Mbps), para ello usted debe realizar las siguientes instrucciones:

1. Entre al modo EXEC privilegiado escribiendo **"enable"**.

```
Router>enable
```

2. En el modo EXEC privilegiado, ingrese el comando **"configure terminal"** para acceder al Modo de configuración global.

```
Router#configure terminal
```

3. Asegúrese de que está en el Modo de configuración global, donde puede ingresar comandos de configuración. Debería ver el siguiente mensaje de confirmación:

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

4. En el Modo de configuración global, asigne un nombre al router ingresando el siguiente comando **"hostname",** seguido del nombre que desee para el enrutador, en este ejercicio práctico se utilizara "R1" como nombre para identificar el router.

```
Router(config)#hostname R1
```

5. En el Modo de configuración global, habilite el enrutamiento IPv6 en el router ingresando el siguiente comando **"*ipv6 unicast-routing*"**.

```
Router(config)#ipv6 unicast-routing
```

Este comando permite habilitar el protocolo IPv6 a nivel global en el router.
6. Ahora, configure la dirección IPv6 en la interfaz Gigabit Ethernet. Para hacerlo, primero ingrese al modo de configuración de interfaz utilizando el siguiente comando ***"interface gigabitEthernet [interfaz]"***

Donde:

- **"[interfaz]"** es el nombre de la interfaz que se va a configurar.

```
Router(config)#interface gigabitEthernet 0/0/0
```

(Reemplace **GigabitEthernet0/0/0** con el nombre de la interfaz que desee configurar).

7. Una vez dentro del modo de configuración de interfaz, configure la dirección IPv6 en la interfaz usando el siguiente comando ***"ipv6 address [dirección IPv6] / [prefijo de red]"*** (sustituya la dirección IPv6 y la máscara de subred deseada):

```
Router(config-if)#ipv6 address 2001:db8:7777:1::1/64
```

Donde:

- **"[dirección IPv6]"** es la dirección IPv6 de la red de destino a la que deseas enrutar el tráfico. No debes usar corchetes alrededor de la dirección IPv6.
- **"[prefijo de red]"** es la máscara de subred expresada en notación de prefijo (por ejemplo, "/64" para una red típica).

8. Asegúrese de que la interfaz esté habilitada usando el comando **"no shutdown"**.

```
Router(config-if)#no shutdown
```

9. Asegúrese de que la interfaz este habilitado. Debería ver el siguiente mensaje de confirmación:

```
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/0, changed state to up
```

10. Salga del modo de configuración de interfaz escribiendo **“exit”**.

```
Router(config-if)#exit
```

11. Repita los pasos 6 a 10 para cada interfaz Gigabit Ethernet que desee configurar con una dirección IPv6.

Estos pasos te permitirán configurar las interfaces Gigabit Ethernet con direcciones IPv6 en el router. Asegúrese de adaptar los nombres de las interfaces y las direcciones IPv6 según los requisitos de esta práctica.

Nota: Si experimenta problemas durante la configuración, elimine las configuraciones anteriores de todos los enrutadores y realice un reinicio. De lo contrario, omita este paso y continúe con las directrices correspondientes. Para ejecutar adecuadamente este procedimiento, siga las indicaciones que se presentan a continuación.

Eliminar Configuración el Enrutador.

El siguiente comando permite al usuario cambiar de modo de usuario (modo de usuario privilegiado). En el modo de usuario privilegiado, puedes acceder a comandos avanzados y de configuración.

```
Router>enable
```

El siguiente comando elimina la configuración guardada en la memoria NVRAM (startup-config), que contiene la configuración guardada de forma persistente.

```
Router#erase startup-config
```

Instrucción:

- Asegúrate de estar en el modo privilegiado (Router#). Escribe el comando **erase startup-config** y presiona Enter.
- Te aparecerá una advertencia sobre la eliminación de la configuración. Debes confirmar escribiendo **confirm** y presionar Enter. Después de confirmar, verás el mensaje **[OK]** indicando que la eliminación fue exitosa.
- Una vez que hayas confirmado la eliminación de la configuración, recibirás este mensaje que confirma que la memoria NVRAM ha sido borrada con éxito.

```
Erase of nvram: complete
```

Reiniciar el enrutador.

El siguiente comando reinicia el dispositivo. Después de borrar la configuración, es posible que desees reiniciar el dispositivo para aplicar los cambios y comenzar con una configuración limpia.

```
Router#reload
```

Instrucción:

- Una vez que hayas borrado la configuración, en el modo privilegiado (Router#). Escribe “**reload”** y presiona “Enter”.
- Te aparecerá un mensaje en donde te pedirá que confirmes si deseas guardar la configuración actual antes de reiniciar. En este caso, para continuar con el reinicio sin guardar ninguna configuración, escriba **no** y presione “Enter”.
- Luego, cuando se te pregunte si deseas continuar con el reinicio, escribe “**confirm”** y presiona “Enter”.
- Aguarde a que se reinicie el dispositivo antes de proseguir con su configuración.

5. Configuración de direcciones IPv6 en los terminales.

Configurar en cada terminal la dirección IPv6 y la puerta de enlace correspondiente.

Equipos	Interfaz	Direccion	Mask	Gateway
PC1	NIC	2001:db8:7777:1::2	/64	2001:db8:7777:1::1
PC2	NIC	2001:db8:8888:2::2	/64	2001:db8:8888:2::1

Tabla 4. Asignación de direcciones IPv6 en los hosts.

NOTA: Ejecutar los procedimientos de la práctica previa en caso de que surjan complicaciones.

RECOMENDACIÓN: Es necesario verificar que las configuraciones de seguridad o antivirus estén desactivadas en el terminal o PC, lo que incluye tanto el Firewall de Windows como cualquier software antivirus, ya que podrían surgir problemas durante la ejecución de pruebas de conectividad.

6. Verificación de conectividad en IPv6.

Al igual que en IPv4, existen una serie de comandos tipo show que permiten verificar el comportamiento de las interfaces conectadas.

El siguiente comando permite verificar el estado del puerto, determinar si está encendido o apagado, comprobar la activación del protocolo IPv6, revisar la dirección asignada, y examinar otros parámetros relacionados. (Reemplace **gigabitEthernet0/0/0** con el nombre de la interfaz que desee configurar).

```
Router>enable
Router# show ipv6 interface gigabitEthernet 0/0/0
```

Una vez ingresado el comando. **¿La dirección Ipv6 de la interfaz coincide con la configuración previamente realizada?**

El siguiente comando es parecido al previo, con la diferencia de que no requiere especificar una interfaz particular, ya que proporciona un resumen del estado de todas las interfaces disponibles.

```
Router>enable
Router# show ipv6 interface brief
```

Debe existir conectividad exitosa entre el dispositivo final y el enrutador. Para esta práctica, puede comprobarse la conectividad entre el enrutador y cada uno de los hosts PC1 y PC2, y entre ellos. **Usted deberá realizar un análisis de la práctica en lo que respecta a las pruebas de conectividad y adjuntar evidencia de los resultados obtenidos en la parte final de la misma.**

NOTA: Ejecutar los procedimientos de la práctica previa en caso de que surjan complicaciones.

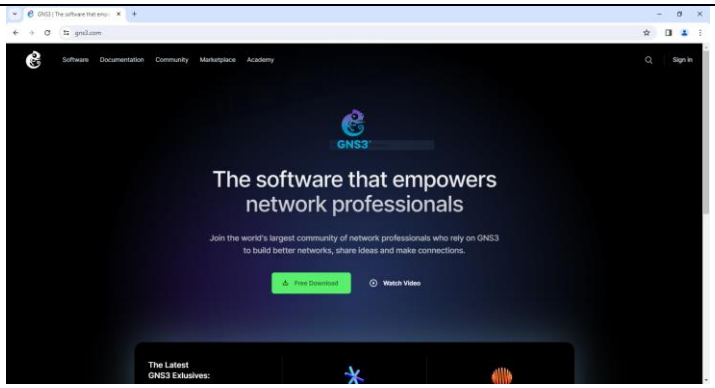
7. Actividad para el Hogar

A continuación, se indica el procedimiento para instalar el software GNS3 y el router Cisco, los cuales serán utilizados en el transcurso de las prácticas.

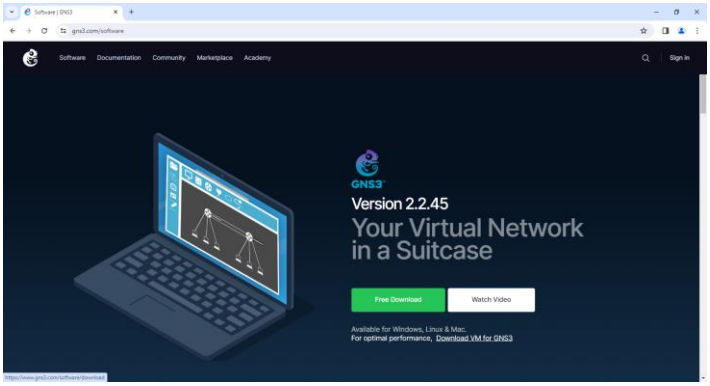
Instalación de GNS3

Previamente a la instalación de GNS3 se recomienda instalar VMware Workstation Pro.

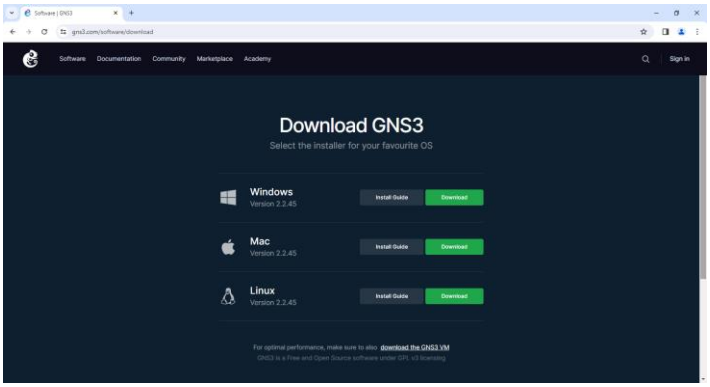
1. Ingresar a la pagina oficial de GNS3 “www.gns3.com” .



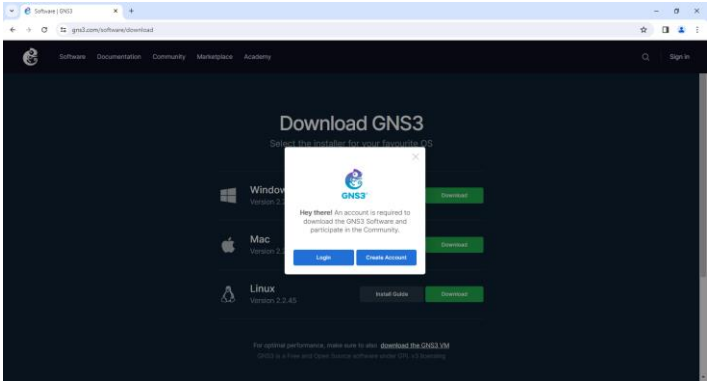
2. Dar clic en la pestaña Software y seleccionar “Free Download”.



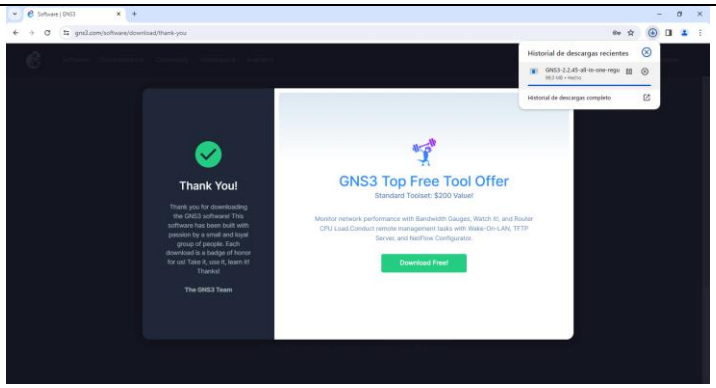
3. Seleccionar la opcion “Download” para Windows.



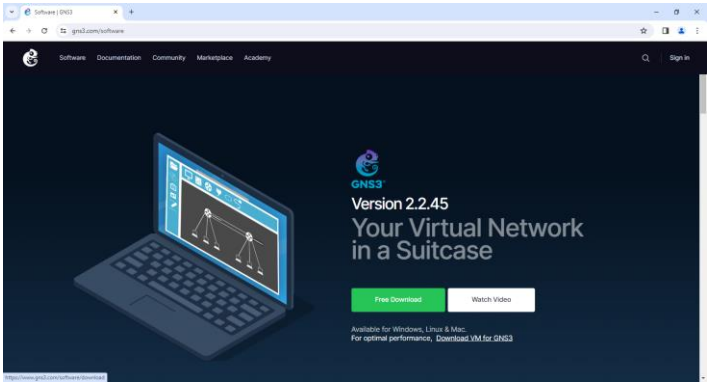
4. Crear un usuario para continuar con la descarga de GNS3.



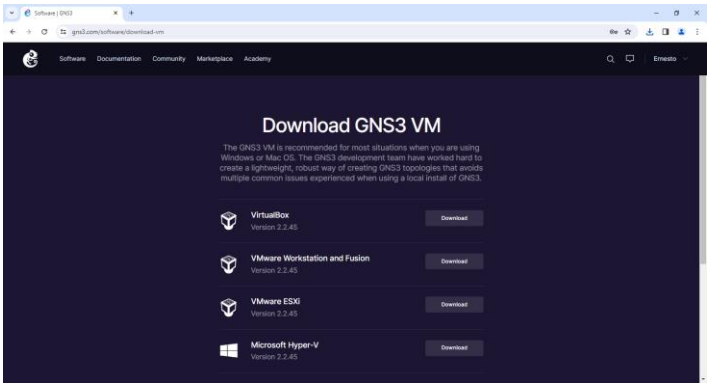
5. A crear el usuario se habilita la opcion de descargar GNS3.



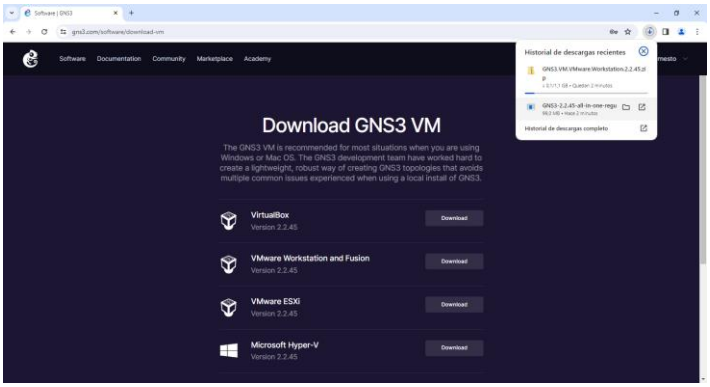
6. Regresar a la pestaña de “Software” y elegir la opción “Download VM for GNS3”.



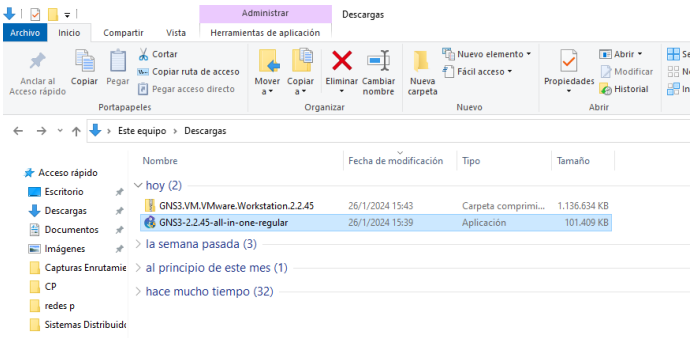
7. Elegir la opción “VMware Workstation and Fusion”.



8. Automáticamente la descarga iniciara.

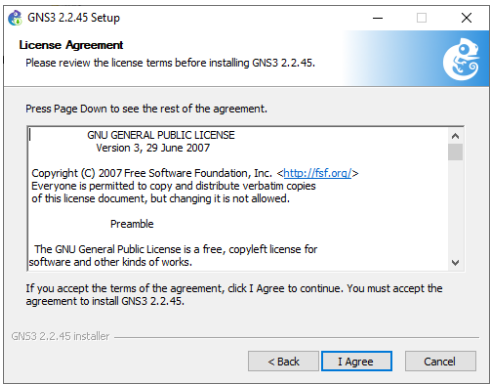


9. Ejecutar el archivo “GNS3-2.2.45 all in one regular” y permitir los permisos de administrador.

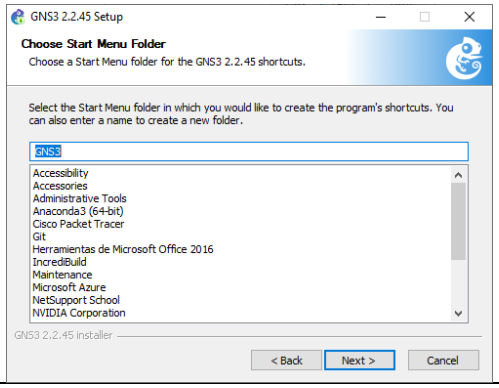


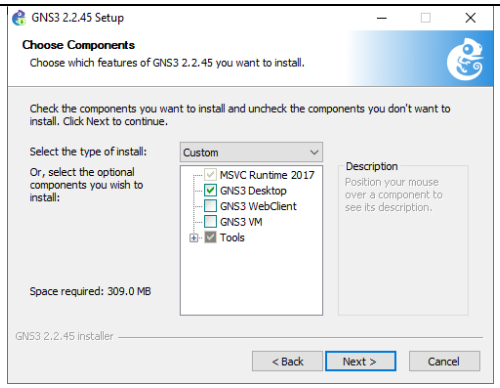
10. Seleccionar “Next”.

11. Aceptar la licencia de contrato.

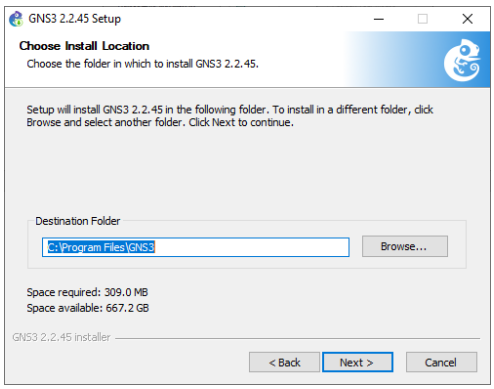


12. En las siguientes 2 ventanas, seleccionar “Next”.

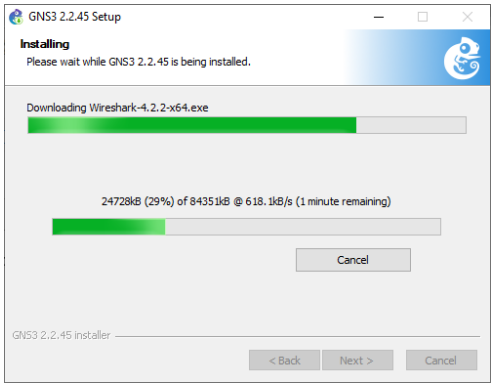




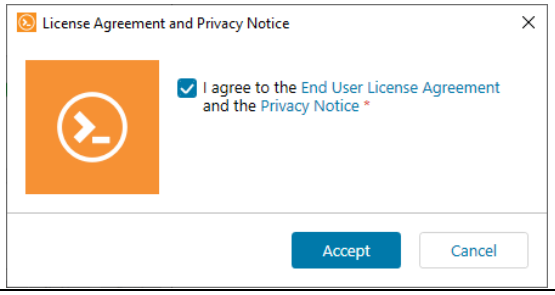
13. Dejar por defecto la ubicación de instalación de GNS3 y seleccionar “Next”.

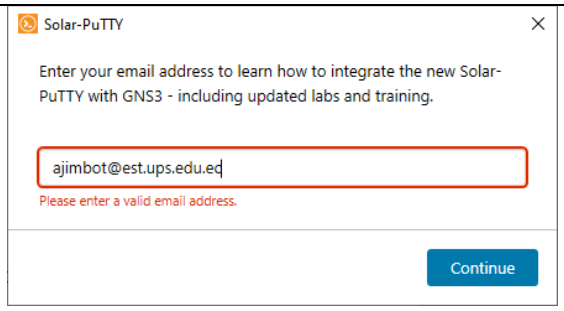


14. Durante la instalación, aceptar los términos de “WinPcap”.

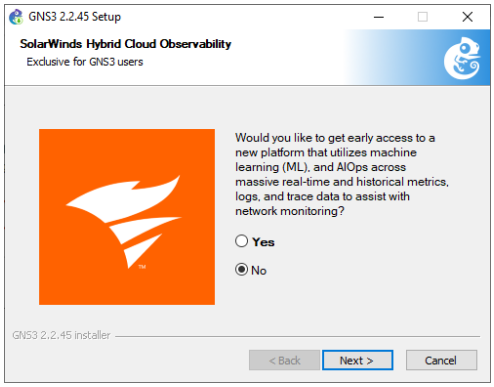


15. Para finalizar, seleccionamos la siguiente licencia e ingresamos el correo electrónico creado anteriormente:

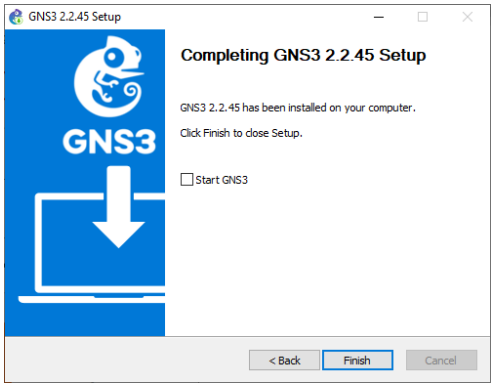




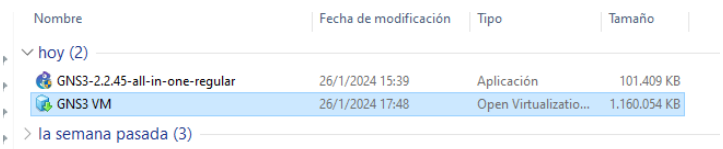
16. Seleccionar “No” y “Next”.



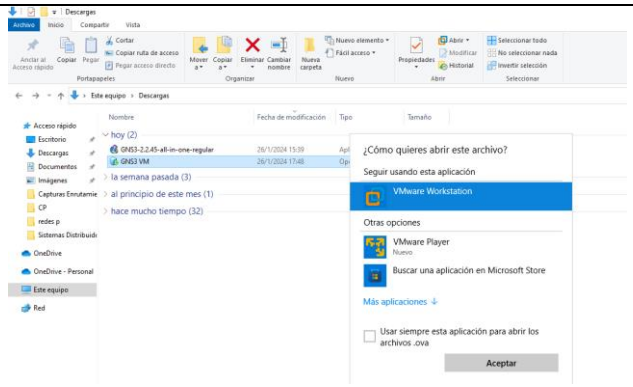
17. Desmarcar la opción “Start GNS3” y seleccionar “Finish”.



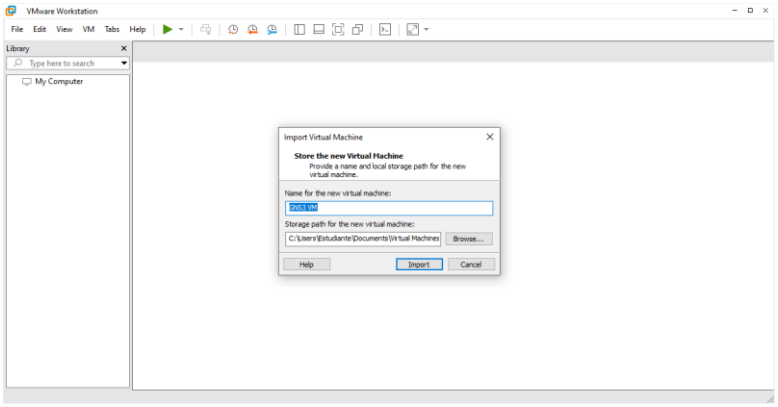
18. Extraer el archivo “GNS3 VMWare” y dar doble clic para ejecutar la instalación.



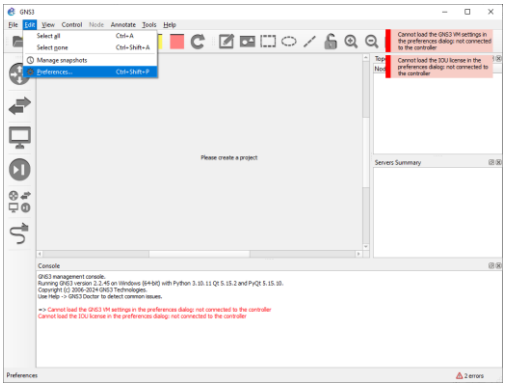
19. Seleccionamos “VMWare Workstation” y clic en “Aceptar”.



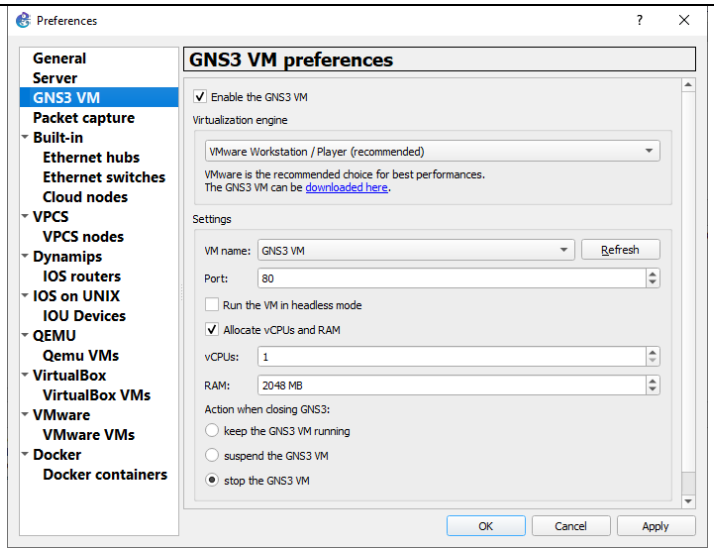
20. Ingresar el nombre “GNS3 VM” y clic en “Import”.



21. Abrir GNS3, damos clic en Edit>Preferences.

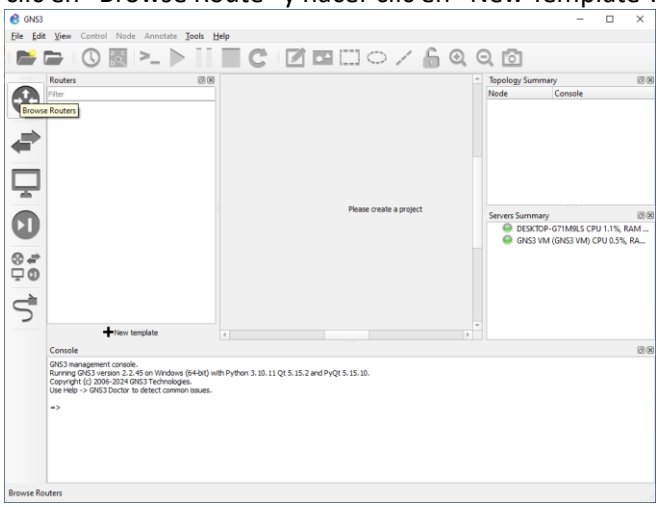


22. Seleccionar la opción “GNS3 VM” y realizar las configuraciones tal como se muestra en la Figura. 2, luego dar clic en “Apply” y en “OK”.

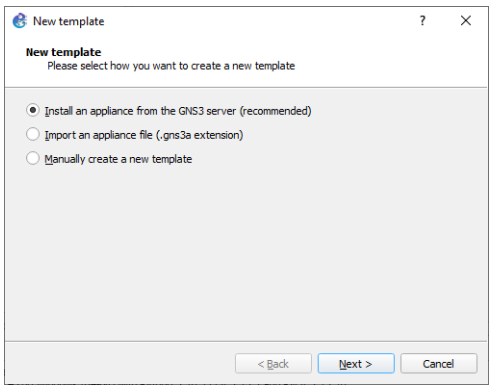


Instalación IOS Router Cisco

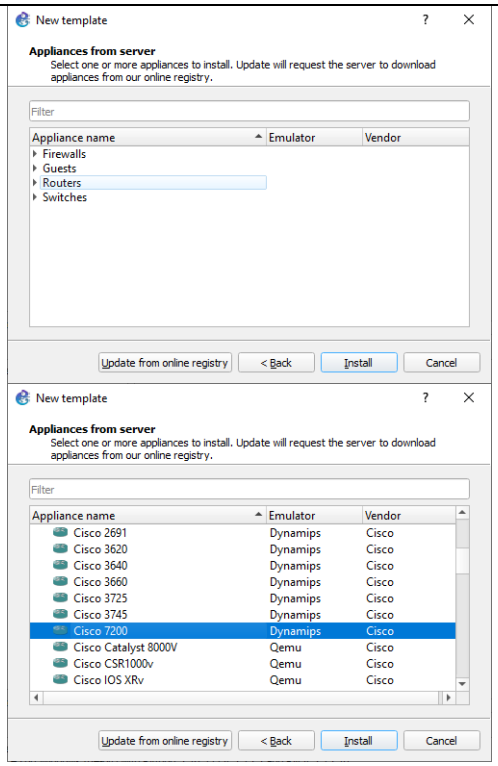
1. En GNS3 hacer clic en “Browse Route” y hacer clic en “New Template”.



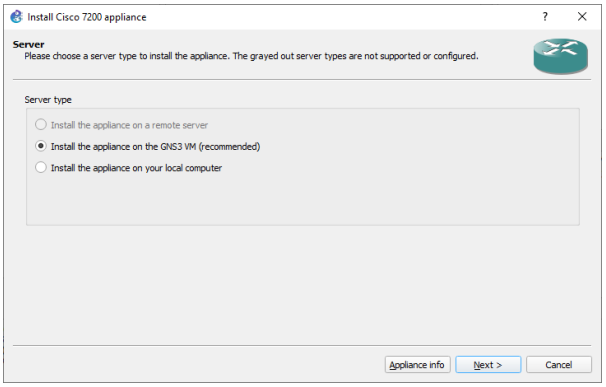
2. Seleccionar la opción “Install an appliance from GNS3 server” y clic en “Next”.



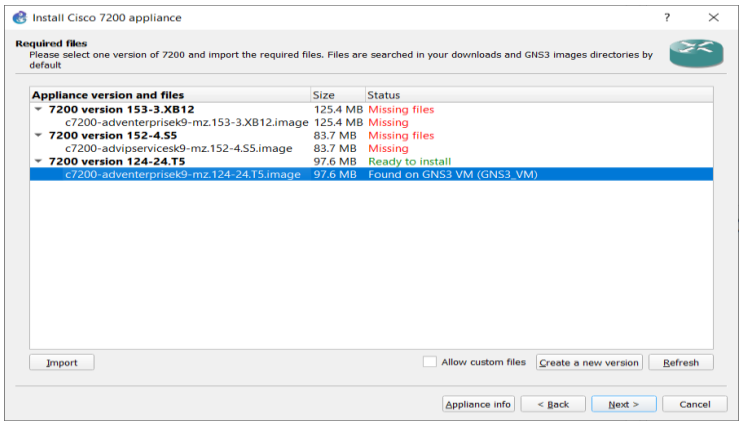
3. Hacer clic en “Update from online registry”, luego seleccionar “Routers”, buscar el Router “Cisco 7200” y clic en “Install”.



4. Seleccionar la opción “Install the appliance on the GNS3” y clic en “Next”.



5. Seleccionar la versión 124-24.TS y clic en “Next”. En caso de no habilitarse esta opción se debe descargar manualmente la imagen del Router para luego importar y continuar con la instalación.



Una vez finalizada la instalación, estaremos listos para comenzar a crear las topologías con el router Cisco. Es importante recordar siempre ejecutar la máquina virtual y asegurarse de que los routers

	se estén ejecutando a través de la máquina virtual de GNS3 para evitar consumir todos los recursos de la computadora física.

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. **¿Cuáles son los pasos fundamentales para realizar configuraciones básicas en un enrutador?**
2. **¿Cuál es el proceso para configurar y habilitar las interfaces Ethernet en un enrutador con direcciones IPv6?**
3. **¿Cuáles son las herramientas o comandos comunes que se utilizan para verificar las configuraciones realizadas en un enrutador?**

ACTIVIDADES DESARROLLADAS

(Anotar las actividades que siguió para el desarrollo de la práctica)

El estudiante deberá redactar los pasos a cumplir en las instrucciones.

Verificación de la conectividad

Para responder la pregunta planteada: **¿La dirección Ipv6 de la interfaz coincide con la configuración previamente realizada?** El comando "show ipv6 interface brief" es la mejor opción para verificar las 2 interfaces.

En R1

Aquí usted deberá adjuntar los resultados obtenidos del comando de verificación y realizar su respectivo análisis de lo que se muestra en pantalla.

Equipos	Interfaz	Direccion	Mask	Gateway
R1	G0/0/0		/64	NA
	G0/0/1		/64	NA

Análisis. - *Aquí usted deberá adjuntar las direcciones proporcionadas en esta práctica y llevar a cabo una comparación con el resultado generado por el comando correspondiente, seguido de un análisis correspondiente.*

Incluya los resultados adquiridos en las pruebas de conectividad, acompañados de un análisis.

Prueba de Conectividad, entre el R1 y PC2:

Aquí usted deberá adjuntar la evidencia de la prueba de conectividad.

Prueba de Conectividad, entre la PC1 y PC2:

Aquí usted deberá adjuntar la evidencia de la prueba de conectividad entre los terminales.

Análisis:

Aquí usted deberá adjuntar un análisis de las pruebas de conectividad.

CONCLUSIONES:

BIBLIOGRAFIA:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN**
REALIZADO POR:		
CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**3**	**TÍTULO PRÁCTICA:** Configuración básica IPv6 equipo MikroTik.

OBJETIVO:

- Realizar configuraciones básicas en un enrutador.
- Configurar y habilitar las interfaces Ethernet con direcciones IPv6.
- Realizar pruebas y verificar las configuraciones realizadas.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

1. (1) Router Mikrotik
2. (1) Switches Cisco
3. (2) Dispositivos con capacidad para soportar IPv6 (p. ej. computadoras)
4. (3) Cables de red Ethernet

NOTA: Es necesario contar con 2 computadoras equipadas con interfaces Ethernet para llevar a cabo la práctica. Se brinda la opción de utilizar su propia computadora junto con la que se encuentra en la mesa de trabajo. En caso de no contar con dicha interfaz, se deberá disponer de adaptadores Ethernet, ya que la práctica se ha diseñado para ser ejecutada en cada estación de trabajo en el laboratorio de cómputo 8.

DESCRIPCIÓN GENERAL:

En esta práctica de laboratorio, los hosts y los enrutadores se conectan por primera vez en un entorno IPv6 utilizando un Router Mikrotik.

INSTRUCCIONES:

1. Descripción de equipos

Revise la **Figura 1**, para identificar los dispositivos Router Mikrotik y Switch Cisco Catalyst serie C1000-24P-4G-L que serán empleados para el desarrollo de la práctica.

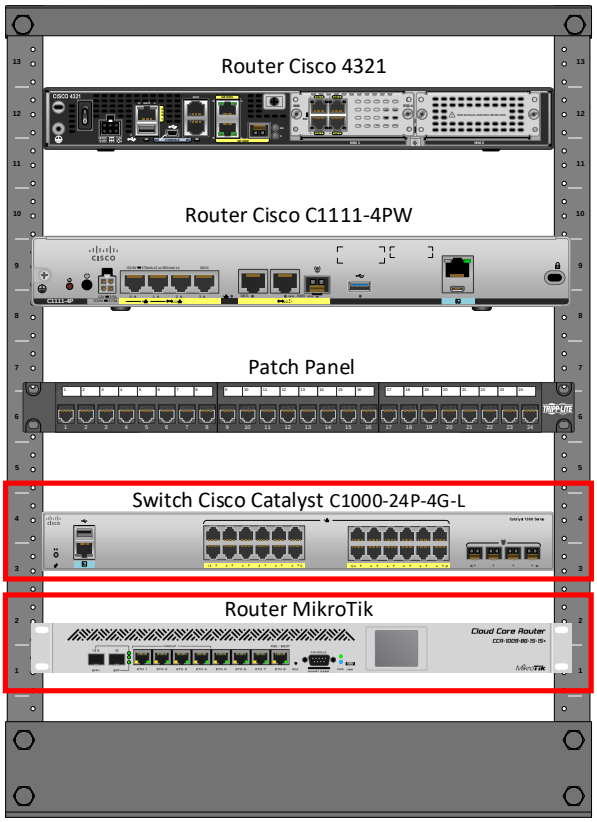


Figura 1. Diseño Rack Laboratorio de Cómputo 8.

En la **Figura 2 y 3** se muestran los equipos y cada una de sus partes, los cuales se detallan en las siguientes **Tablas 1 y 2**.

Router Mikrotik.

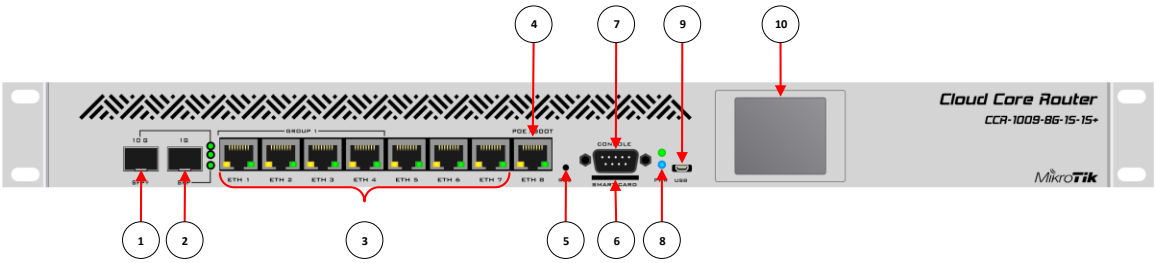


Figura 2. Router Mikrotik serie C1000-24P-4G-L.

Especificaciones del equipo

1	Ranura para módulos SFP+1 cage	2	Puerto PoE/Boot
3	Puertos Ethernet	4	Ranura para módulos SFP 5
5	Botón de reinicio	6	Ranura para tarjeta SD
7	Puerto consola	8	LED del sistema
9	Micro USB 10	10	Pantalla LCD

Tabla 1. Especificaciones MikroTik serie C1000-24P-4G-L.

Switch Cisco Catalyst serie C1000-24P-4G-L.

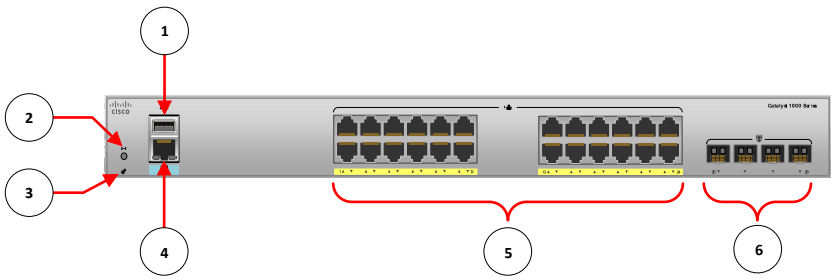


Figura 3. Switch Cisco Catalyst serie C1000-24P-4G-L.

Especificaciones del equipo

Catalyst 1000 Series C1000-24P-4G-L.			
1	Puerto USB tipo A	2	Botón de reinicio
3	LED del sistema	4	Puerto de consola RJ-45
5	24 puertos 10/100/1000 PoE+	6	Ranuras para módulos SFP

Tabla 2. Especificaciones Switch Cisco.

Conecte los cables Ethernet a los puertos correspondientes de cada equipo, siguiendo la representación visual proporcionada en la Figura 1. Asegúrese de realizar una verificación del cableado y de encender los dispositivos previamente al inicio del proceso.

2. Esquema de la práctica a desarrollar.

En esta práctica usted deberá conectar los equipos del laboratorio de red como se muestra a continuación:

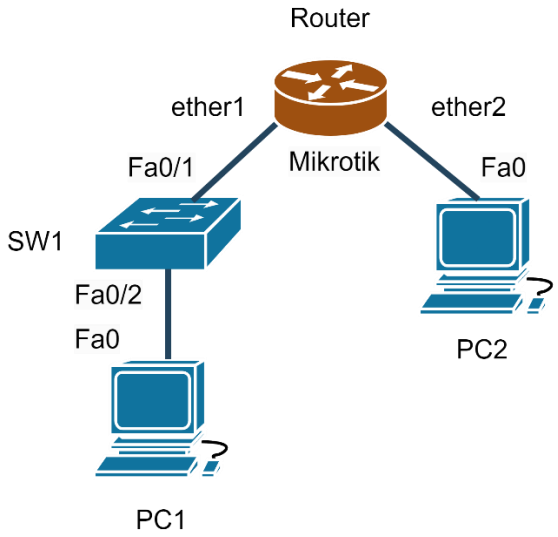


Figura 4. Topología de la red.

Conecte los cables Ethernet a los puertos ether1, ether2 del Router y switch Fa0/1, Fa0/2 tal como se muestra en la **Figura 4**, teniendo en cuenta las especificaciones de los equipos. Es importante recordar que para configurar los Routers MikroTik, se debe establecer una conexión a través de cualquier interfaz ether con un cable de red Ethernet. Se recomienda usar la interfaz ether 7 para fines prácticos.

3. Configuración del Router MikroTik a través de WinBox.

Para acceder a un dispositivo MikroTik por primera vez, es necesario proceder con la descarga de la aplicación Winbox desde el sitio web oficial de MikroTik (www.mikrotik.com).

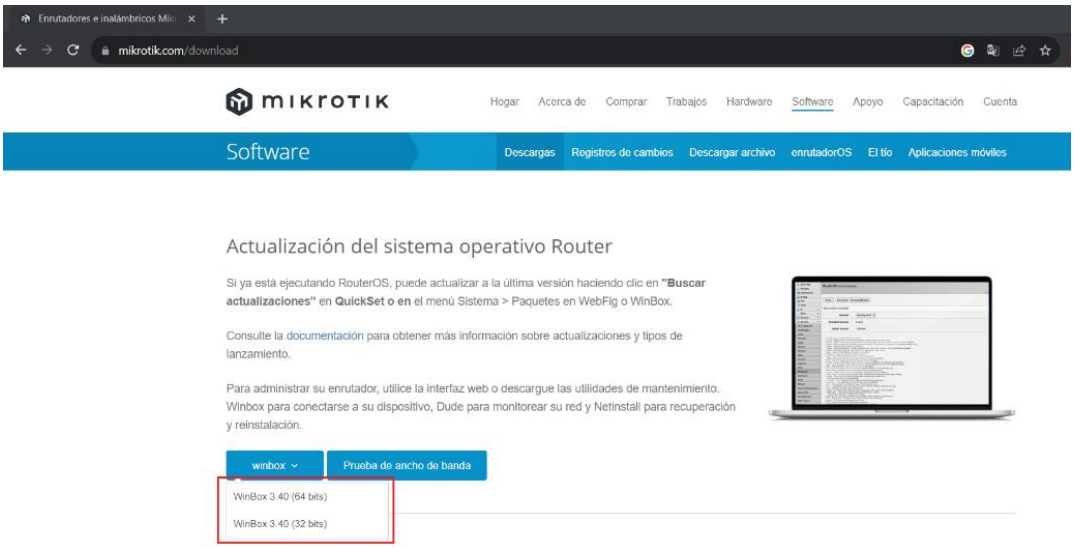


Figura 5. Descarga de Winbox.

NOTA: Antes de iniciar el proceso de descarga, resulta esencial realizar una comprobación de la arquitectura del sistema operativo presente en la computadora, con el propósito de determinar si es una arquitectura de 32 bits o de 64 bits. Para llevar a cabo esta verificación, se debe acceder a

la sección de “Información del Sistema” y, específicamente, observar la categoría denominada “Tipo de Sistema”.

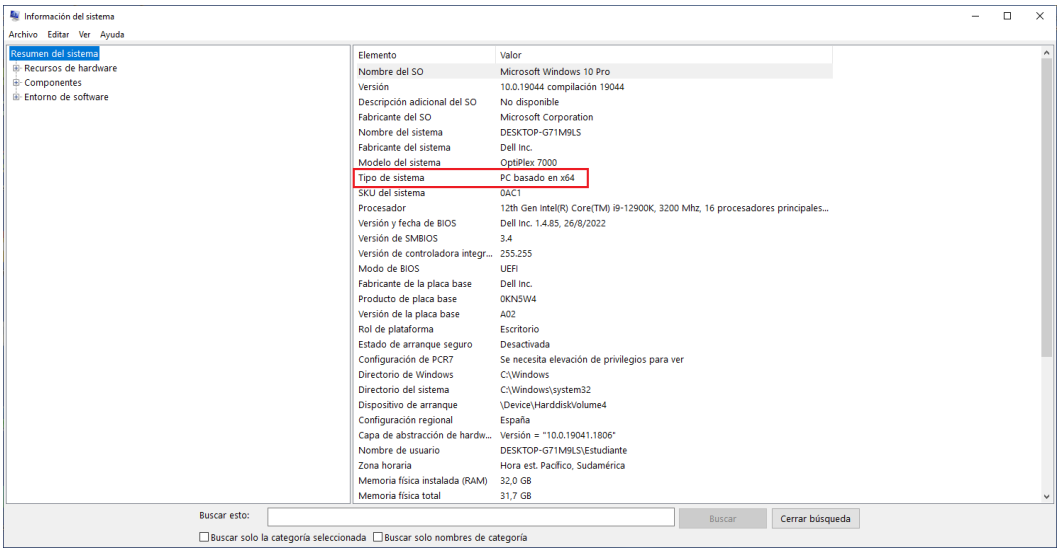


Figura 6. Información del Sistema.

Una vez que la aplicación ha sido descargada e instalada, se procederá a la interfaz de configuración.

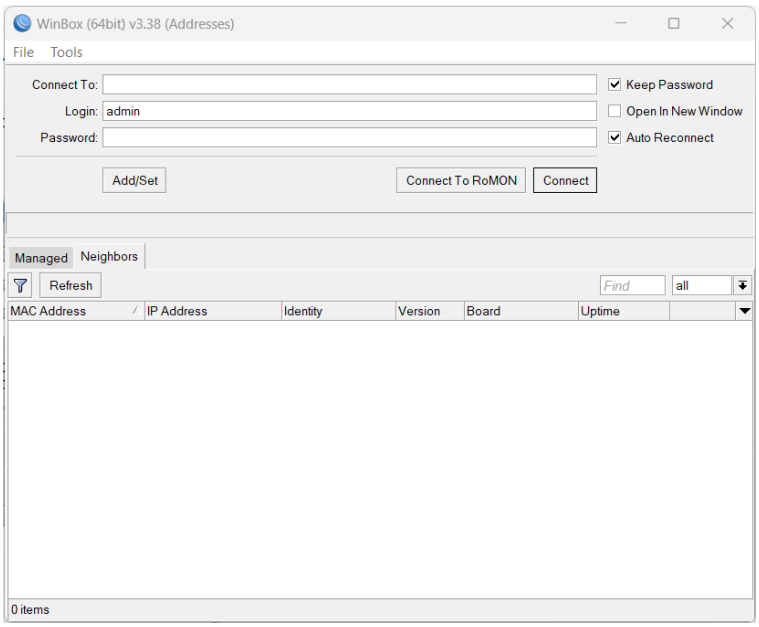


Figura 7. Interfaz de configuración.

Cuando se conecta una computadora a un enrutador MikroTik a través de un cable Ethernet, generalmente al puerto ether7, la aplicación Winbox detectará el router en la Capa 2 de la red. Para visualizar los dispositivos disponibles en la red, se debe cambiar a la pestaña “Neighbors”.

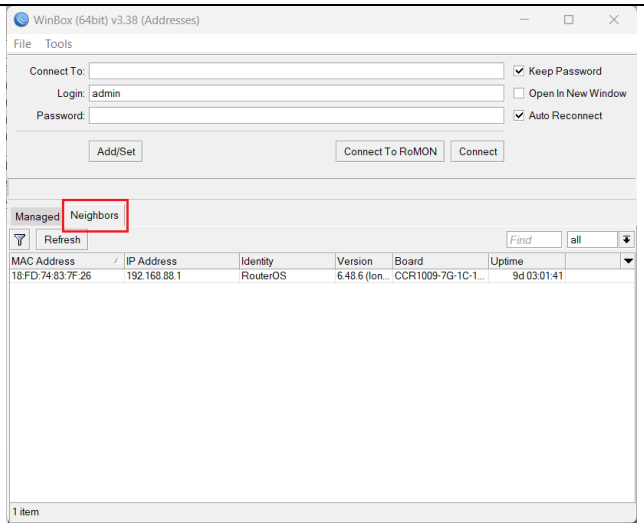


Figura 8. Pestaña "Neighbors".

En el caso de que el Router MikroTik esté configurado con una dirección IP, y la computadora esté en el mismo segmento de red, se podrá acceder al Router haciendo clic en la dirección IP correspondiente y luego presionando el botón “Connect”.

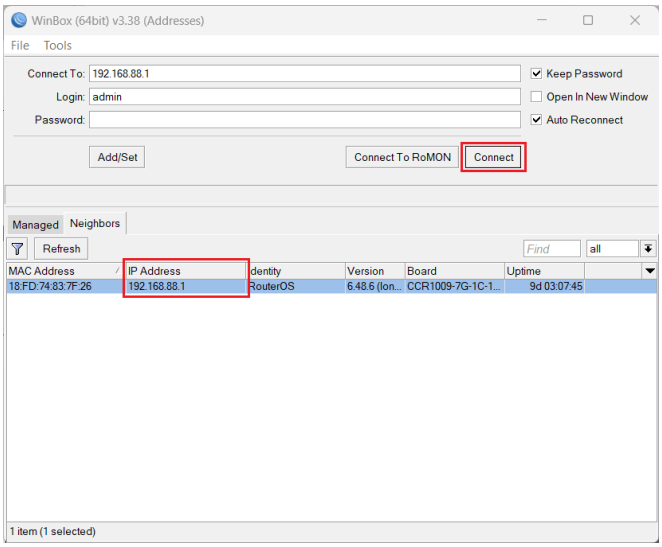


Figura 9. Dirección IP.

Si el Router no está configurado con una dirección IP o no es accesible mediante una dirección IP, se debe acceder a través de la dirección MAC en la Capa 2. Para hacerlo, se debe hacer clic en la dirección MAC y luego presionar el botón “Connect”.

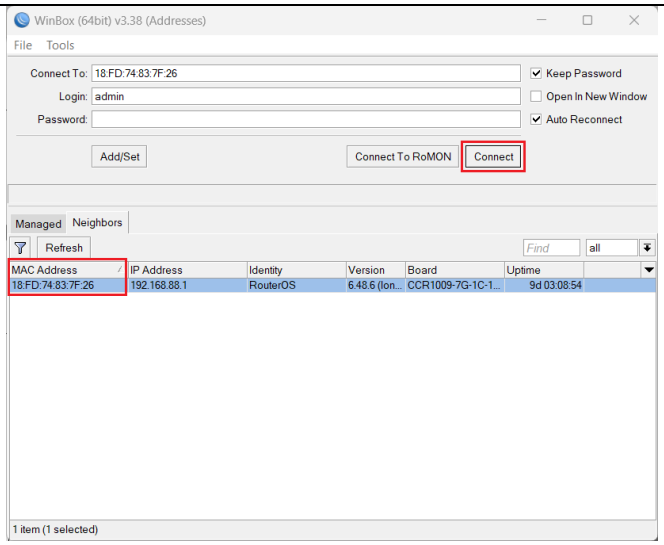


Figura 10. Dirección MAC.

Una vez que haya accedido al Router y se encuentre en la interfaz correspondiente, proceda a seleccionar la opción “System” con el fin de verificar que IPv6 este activado en el router.

Figura 11. System.

A continuación, en el menú “System”, optamos por la opción “Packages”.

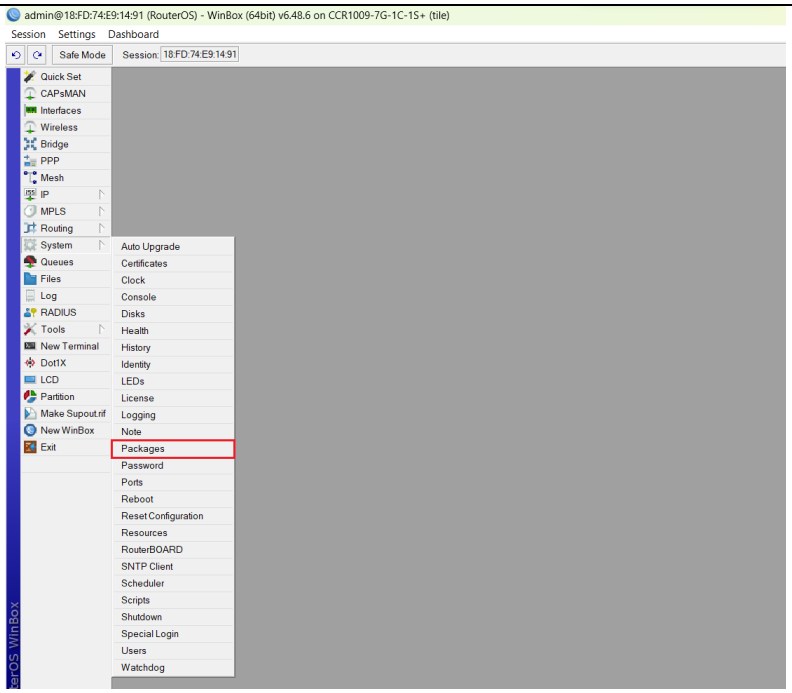


Figura 12. Packages.

Comprobar que este habilitado el protocolo IPv6; en caso de no estar activado, procederemos con los pasos siguientes.

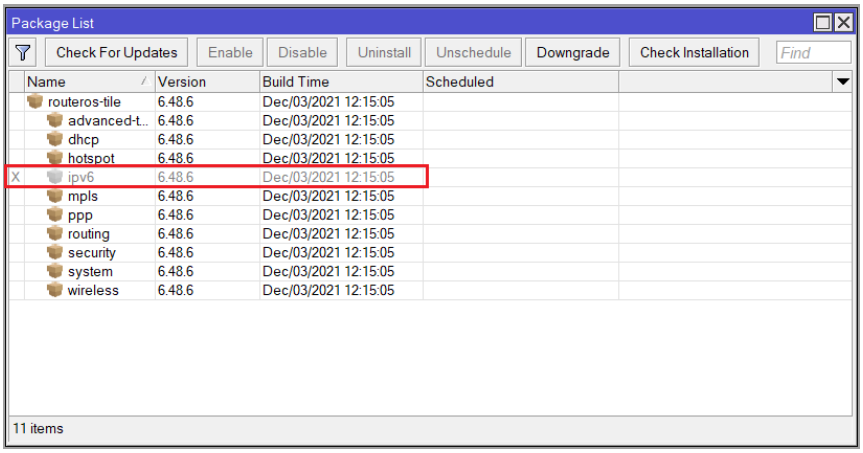


Figura 13. Comprobación protocolo IPv6.

Seleccionamos IPv6 y posteriormente activamos la opción “Enable”.

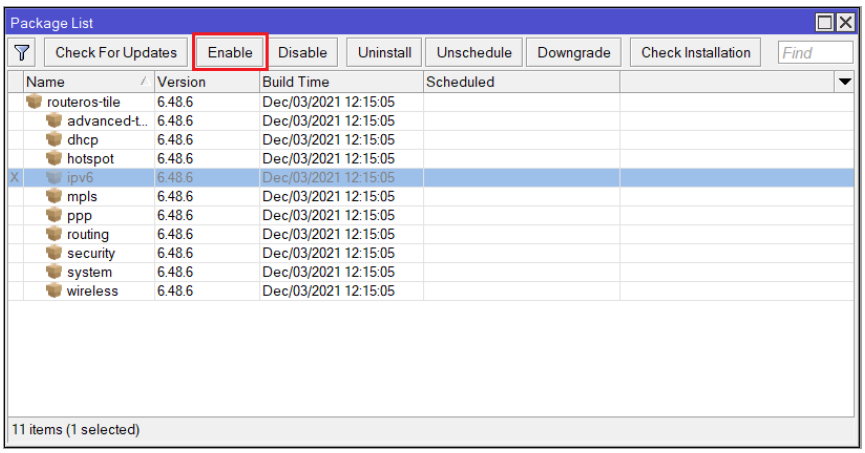


Figura 14. Activación mediante la opción "Enable".

Una vez que hayamos completado los procedimientos previos en el menú “System”, debemos seleccionar la opción “Reboot” y posteriormente confirmar la solicitud de reinicio con el propósito de reiniciar el enrutador.

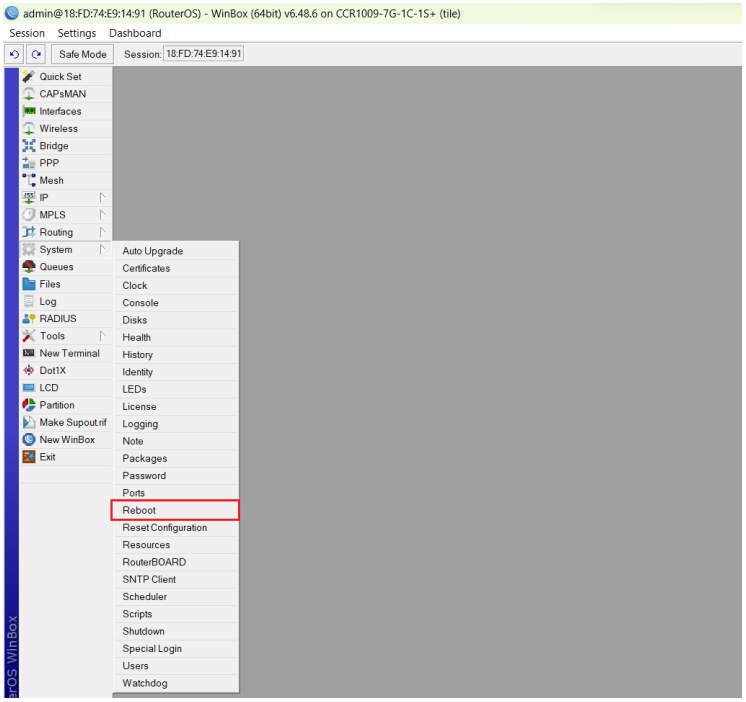


Figura 15. Reset del Router.

Una vez completados estos procedimientos, procedemos a verificar nuevamente si IPv6 está habilitado, lo cual debería ya estar activado.

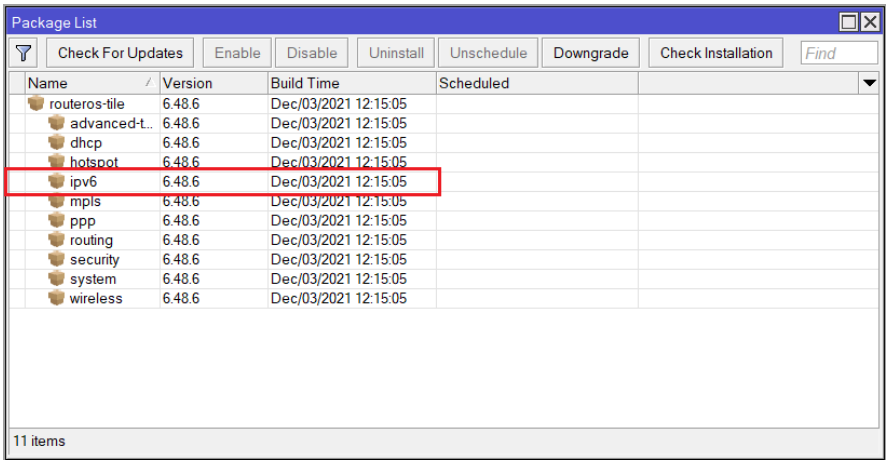


Figura 16. Verificar si IPv6 ya se encuentra habilitado.

A continuación, dentro de la interfaz, acceda a la opción “New Terminal” con el fin de proceder a la configuración de las interfaces del Router.

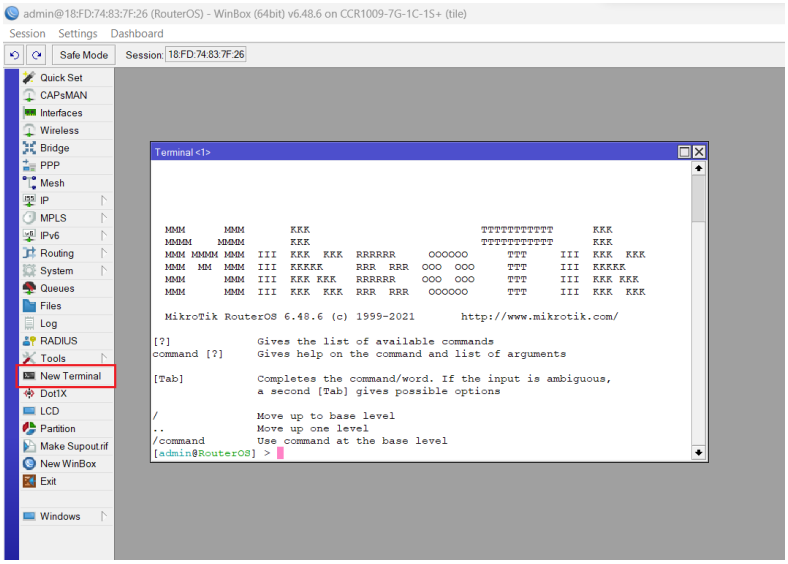


Figura 17. Interfaz, "Nuevo Terminal".

4. Configuración de direcciones IPv6.

Las interfaces se configurarán utilizando las direcciones presentadas en la **Tabla 3** de direccionamiento de este laboratorio.

Equipos	Interfaz	Direccion	Mask	Gateway
Router	ether1	2002:db8:5555:1::1	/64	NA
	ether2	2002:db8:6666:2::1	/64	NA

Tabla 3. Tabla de direcciones IPv6.

Para configurar el direccionamiento IPv6 en la interfaz “New Terminal”, debes ejecutar el siguiente comando: “***/ipv6 address add address=[dirección IPv6]/[*prefijo de red*] interface=[interfaz]”***

Donde:

- **[dirección IPv6]** es la dirección IPv6 de la red de destino a la que deseas enrutar el tráfico. No debes usar corchetes alrededor de la dirección IPv6.
- **[prefijo de red]** es la máscara de subred expresada en notación de prefijo (por ejemplo, "/64" para una red típica).
- **[interfaz]** es el nombre de la interfaz que se va a configurar.

A continuación, se muestra el comando de configuración para la interfaz **ether1** :

```
[admin@RouterOS] >/ipv6 address add address=2002:db8:5555:1::1/64 interface=ether1
```

Repita el comando para configurar la interfaz **ether2**, sustituyendo la dirección IPv6 y la interfaz que desee configurar.

Estos pasos te permitirán configurar las interfaces Ethernet con direcciones IPv6 en el Router. Asegúrese de adaptar los nombres de las interfaces y las direcciones IPv6 según los requisitos de esta práctica.

5. Configuración de direcciones IPv6 en los terminales.

Configurar en cada terminal la dirección IPv6 y la puerta de enlace correspondiente.

Equipos	Interfaz	Direccion	Mask	Gateway
PC1	NIC	2002:db8:5555:1::2	/64	2002:db8:5555:1::1

PC2	NIC	2002:db8:6666:2::2	/64	2002:db8:6666:2::1

Tabla 4. Asignación de direcciones IPv6 en los hosts.

NOTA: Ejecutar los procedimientos de la **práctica 1** en caso de que surjan complicaciones.
RECOMENDACIÓN: Es necesario verificar que las configuraciones de seguridad o antivirus estén desactivadas en el terminal o PC, lo que incluye tanto el Firewall de Windows como cualquier software antivirus, ya que podrían surgir problemas durante la ejecución de pruebas de conectividad.

6. Verificación de conectividad en IPv6.

En un Router Mikrotik, para verificar el comportamiento de las interfaces IPv6, utilizar el siguiente comando: ***/ipv6 route print***

```
[admin@RouterOS] >/ipv6 route print
```

Debe existir conectividad exitosa entre el dispositivo final y el enrutador. Para esta práctica, puede comprobarse la conectividad entre el enrutador y cada uno de los hosts PC1 y PC2, y entre ellos. **Usted deberá realizar un análisis de la práctica en lo que respecta a las pruebas de conectividad y adjuntar evidencia de los resultados obtenidos en la parte final de la misma.**

NOTA: Ejecutar los procedimientos de la práctica previa en caso de que surjan complicaciones.

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. **¿Cuáles son los pasos específicos para habilitar las interfaces Ethernet con direcciones IPv6 en un router Mikrotik?**
2. **¿Qué herramientas o comandos se pueden utilizar para realizar pruebas de conectividad IPv6 en un router MikroTik?**
3. **¿Cuáles son los posibles desafíos o problemas comunes que podrían surgir al realizar estas configuraciones y pruebas?**

ACTIVIDADES DESARROLLADAS

(Anotar las actividades que siguió para el desarrollo de la práctica)

Verificación de las configuraciones

Router Mikrotik

Aquí usted deberá adjuntar los resultados obtenidos del comando de verificación y realizar su respectivo análisis de lo que se muestra en pantalla.

Verificación de la conectividad

Por ejemplo, entre el Router Mikrotik y PC1:

Aquí usted deberá adjuntar la evidencia de la prueba de conectividad entre los terminales.

Por ejemplo, entre la PC2 y PC1:

Aquí usted deberá adjuntar la evidencia de la prueba de conectividad entre los terminales.

Análisis:

Aquí usted deberá adjuntar un análisis de las pruebas de conectividad entre los terminales.

CONCLUSIONES:

BIBLIOGRAFIA:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN**
REALIZADO POR:		
CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**4**	**TÍTULO PRÁCTICA:** Configuración VLANs, Inter-VLANs Routing.

OBJETIVO:

- Configurar VLANs en los switches.
- Establecer modos troncales en los puertos de conexión entre switches para comunicación entre VLANs.
- Verificar la conectividad entre terminales en diferentes VLANs.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

1. (2) Switch Cisco Catalyst.
2. (4) Dispositivos con capacidad para soportar IPv6 (p. ej. computadoras).
3. (5) Cables de red Ethernet.
4. (1) Cable serial.

NOTA: Es necesario contar con 4 computadoras equipadas con interfaces Ethernet para llevar a cabo la práctica. Se brinda la opción de utilizar su propia computadora junto con la que se encuentra en la mesa de trabajo. En caso de no contar con dicha interfaz, se deberá disponer de adaptadores Ethernet, ya que la práctica se ha diseñado para ser ejecutada en cada estación de trabajo en el laboratorio de cómputo 8.

DESCRIPCIÓN GENERAL:

En esta práctica de laboratorio, se busca implementar VLANs mediante la configuración de los switches. Se establecerán modos troncales en los puertos de conexión. Se realizará pruebas de conectividad entre los terminales.

INSTRUCCIONES:

1. Descripción de equipos

Revise la **Figura 1**, para identificar los dispositivos Router Cisco 4321 y Switch Cisco Catalyst serie C1000-24P-4G-L que serán empleados para el desarrollo de la práctica.

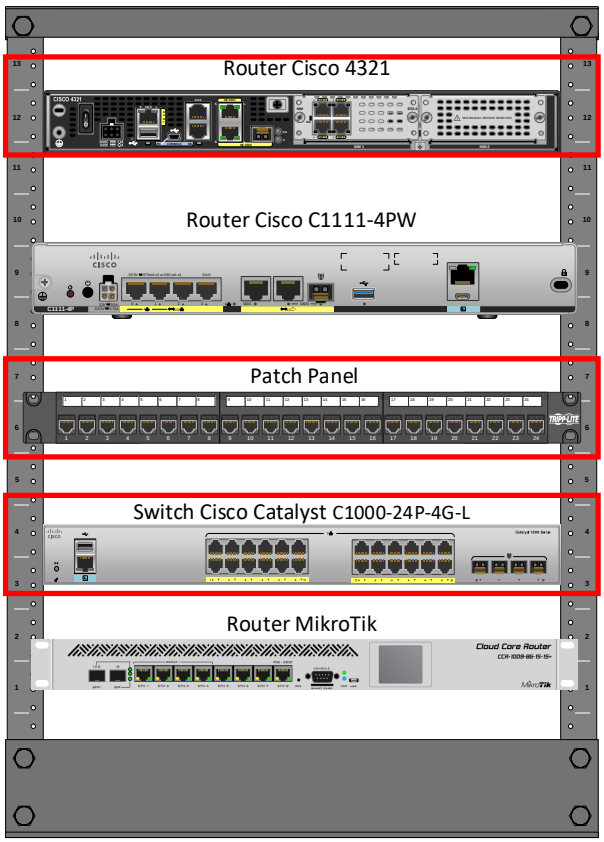


Figura 1. Diseño Rack Laboratorio de Cómputo 8.

En la **Figura 2 y 3** se muestran los equipos y cada una de sus partes, los cuales se detallan en las siguientes **Tablas 1 y 2**.

Router Cisco 4321.

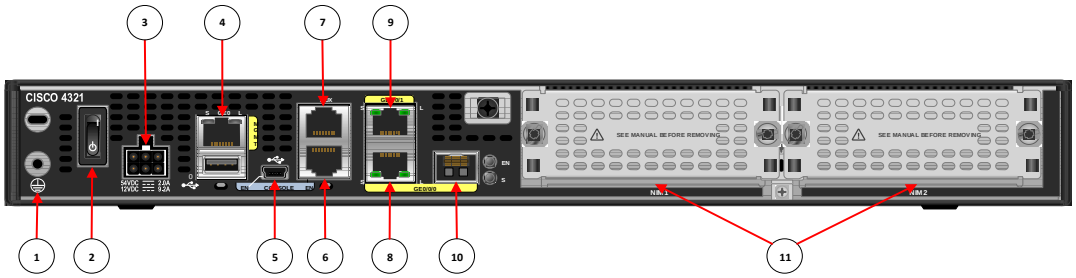


Figura 2. Router Cisco 4321.

Especificaciones del equipo

CISCO 4321			
1	Puesta a tierra	2	Interruptor de alimentación
3	Conector de entrada de alimentación	4	Puerto GE "MGMT" (con puerto USB debajo)
5	Minipuerto USB tipo B	6	Puerto de consola
7	Puerto auxiliar	8	GE 0/0/0 RJ-45 (puerto de cable)
9	GE 0/0/1 RJ-45 (puerto de cable)	10	GE 0/0/0 SFP (puerto de fibra óptica)
11	Ranuras NIM		

Tabla 1. Especificaciones Router Cisco 4321 ISR.

Switch Cisco Catalyst serie C1000-24P-4G-L.

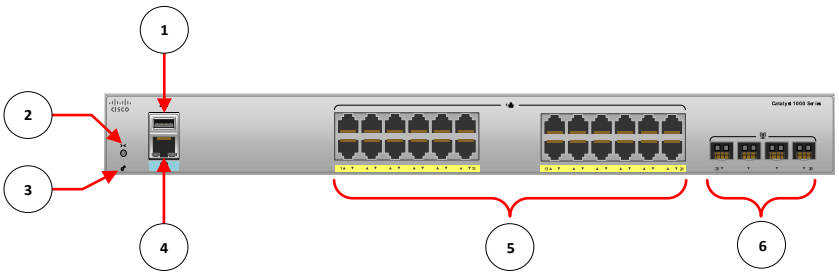


Figura 3. Switch Cisco Catalyst serie C1000-24P-4G-L.

Especificaciones del equipo

Catalyst 1000 Series C1000-24P-4G-L.			
1	Puerto USB tipo A	2	Botón de reinicio
3	LED del sistema	4	Puerto de consola RJ-45
5	24 puertos 10/100/1000 PoE+	6	Ranuras para módulos SFP

Tabla 2. Especificaciones Switch Cisco.

2. Esquema de la práctica 4.1 a desarrollar VLANs.

En esta práctica usted deberá conectar los equipos del laboratorio de red como se muestra a continuación:

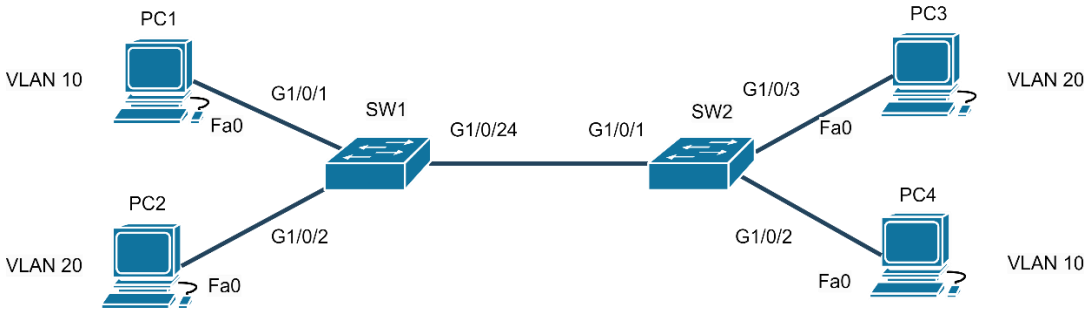


Figura 5. Topología de la red 4.1 VLANs.

3. Conexión entre racks

Observe la **Figura 5,** que representa el laboratorio de cómputo 8, los detalles específicos de dicho laboratorio se encuentran descritos en la **Tabla 3** que se presenta a continuación.

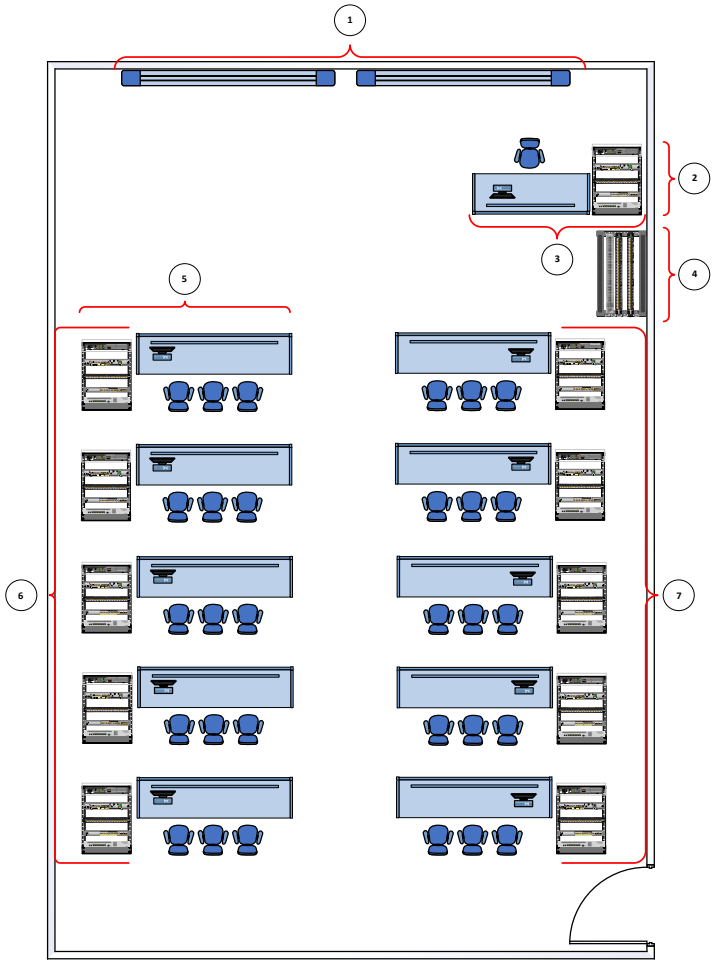


Figura 6. Laboratorio de Computo 8

Especificaciones del Laboratorio

LABORATORIO DE CÓMPUTO 8			
1	Panel táctil	2	Rack de equipos para el docente
3	Estación de trabajo para el docente	4	Rack de conexiones principal
5	Estación de trabajo para los estudiantes	6	Rack de equipos en el lado izquierdo
7	Rack de equipos en el lado derecho		

Tabla 3. Especificaciones Laboratorio Computo 8

Observar la disposición de los racks de equipos ubicados en ambos lados, dado que la disposición de los paneles de conexión (patch panel) en los racks ha sido diseñada en función de esta disposición. Se sugiere analizar el panel de conexión del rack asociado con cada estación de trabajo. Las **Figuras 3 y 4** ilustran los paneles de conexión del lado izquierdo y derecho, respectivamente.

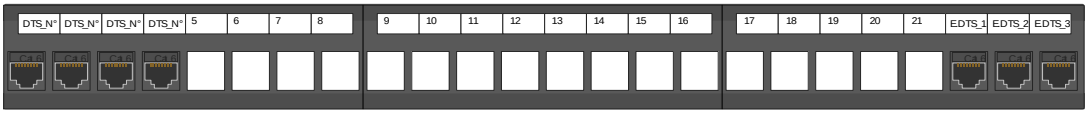


Figura 7. Panel de Conexión lado Izquierdo.

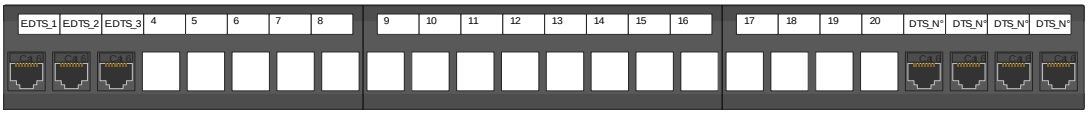


Figura 8. Panel de Conexión lado derecho.

Es esencial comprender la configuración de conexión tanto en el rack de la estación de trabajo como en el rack central del laboratorio.

Identifica el rack central, que actúa como el punto de conexión para todos los demás racks en el laboratorio.

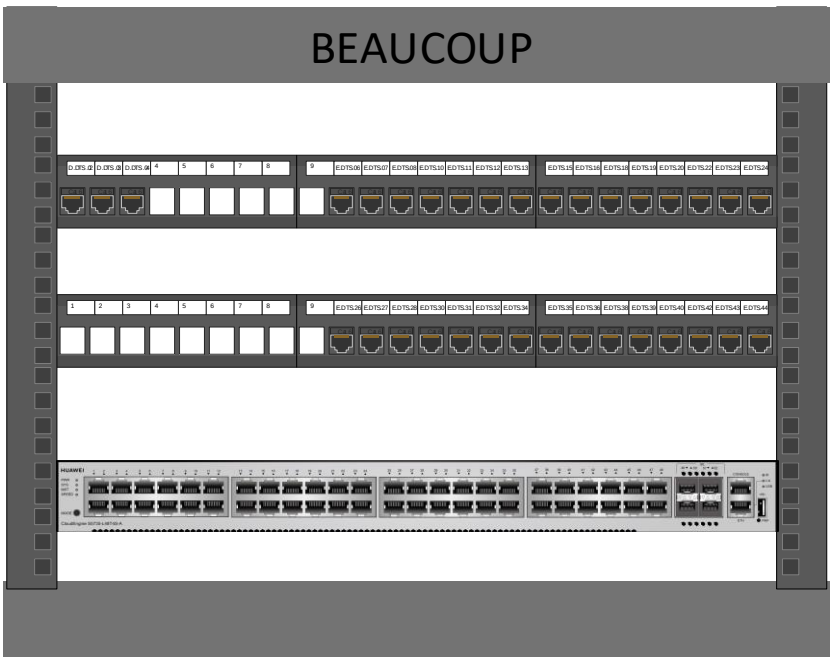


Figura 9. Rack central del Laboratorio.

Para llevar a cabo esta práctica, se requiere la interconexión entre dos switches Cisco. A continuación, se presenta un ejemplo de conexión entre un switch ubicado en el lado izquierdo del laboratorio y otro en el lado derecho.

1. Inicie conectando el cable Ethernet de acuerdo con la topología especificada para la interconexión entre los switches, utilizando el puerto FastEthernet 0/3.
2. En el patch panel del rack de equipos de la estación de trabajo, identificamos los conectores de hebra etiquetados como DTS seguido de un número. Una vez identificado, conectamos el extremo opuesto del cable a uno de estos puertos.
3. Diríjase al rack central para realizar un “pacheo” entre el puerto conectado y el puerto correspondiente del otro switch. Esto se logra identificando, en la estación de trabajo, los puertos mediante las etiquetas. Por ejemplo, supongamos que identificamos el puerto DTS 32 en una estación de trabajo y el puerto DTS 11 en la otra estación de

trabajo. En el rack central, realizamos el pacheo entre los puertos EDTS 32 y EDTS 11, donde la "E" indica estudiantes. Esto establecerá una conexión entre las estaciones de trabajo.

Siguiendo estos pasos, podrá realizar la conexión entre el rack de equipos de la estación de trabajo y el rack central de manera efectiva en el Laboratorio de Cómputo 8, garantizando un entorno de trabajo ordenado y funcional.

4. Configuración de VLANs:

Las VLANs se configurarán utilizando las direcciones presentadas en la **Tabla 3** de direccionamiento de este laboratorio.

Equipos	VLANs	Dirección de red	Mask	Gateway
Switch	VLAN 10	fd00::10:1	/64	NA
	VLAN 20	fd00::20:1	/64	NA

Tabla 4. Tabla de direcciones IPv6.

1. Entre al modo EXEC privilegiado escribiendo **"enable"**.

```
Switch>enable
```

2. En el modo EXEC privilegiado, ingrese el comando **"configure terminal"** para acceder al Modo de configuración global.

```
Switch#configure terminal
```

3. En el Modo de configuración global, asigne un nombre al switch mediante el comando **"hostname"**, seguido del nombre deseado; en este ejercicio, se empleará **"SW1"** como designación para el Switch 1 y **"SW2"** para el Switch 2 como identificador del switch.

Por ejemplo:

```
Switch (config)#hostname SW1
```

4. En el Modo de configuración global, cree las VLANs mediante el comando: ***"vlan [número de VLAN]"***.

Donde:

- **"[número de VLAN]"** representa el identificador de la VLAN que se configurará.

Por ejemplo:

```
SW1(config)#vlan 10
```

Una vez creada la VLAN le damos un nombre a la misma ingresando el siguiente comando: **"name [nombre de la VLAN]"**.

Donde:

- **"[nombre de la VLAN]"** es el nombre de la VLAN que se va a configurar.

Por ejemplo:

```
SW1(config-vlan)#name VLAN10
SW1(config-vlan)#exit
```

Nota: Repita estos pasos para la creación de una VLAN adicional (por ejemplo, VLAN 20).

Configuración de interfaces VLAN:

5. Ingrese al modo de configuración de interfaz utilizando el comando: **"*interface [Tipo de interfaz] [Número de interfaz]*"**

Donde:

- **"[Tipo de interfaz]"** se refiere al nombre de la interfaz que será utilizada, ya sea fastEthernet o gigabitEthernet.
- **"[Número de interfaz]"** corresponde al número asignado a la interfaz que se va a emplear.

Por ejemplo:

```
SW1(config)#interface gigabitEthernet 1/0/1
```

Activamos el modo acceso usando el siguiente comando: ***"switchport mode access".***

```
SW1(config-if)#switchport mode access
```

Después de haber configurado la interfaz, otorgamos permisos para acceder a la VLAN mediante el siguiente comando: **"switchport access [VLAN]"**.

Donde:

- **"[VLAN]"** se refiere al nombre de la VLAN que será utilizada.

Por ejemplo:

```
SW1(config-if)#switchport access vlan 10
SW1(config-if)#exit
```

Nota: Vuelva a ejecutar los procedimientos indicados para establecer la configuración de la interfaz en el modo de acceso VLAN, específicamente asignando la VLAN 20.

6. Una vez configurada la interfaz de VLAN, active el modo troncal. Ingrese al modo de configuración de interfaz del puerto que se conectará al otro switch en este ejercicio práctico (por ejemplo, puerto fastEthernet 1/0/24 para el Switch 1).

```
SW1(config)#interface gigabitEthernet 1/0/24
```

Activamos el modo troncal usando el siguiente comando ***"switchport mode trunk".***

```
SW1(config-if)#switchport mode trunk
SW1(config-if)#exit
```

7. Repita los pasos anteriores para crear VLANs y configurar los modos de configuración según sea necesario.

5. Configuración de direcciones IPv6 en los terminales.

Configurar en cada terminal la dirección IPv6 y la puerta de enlace correspondiente.

Equipos	Interfaz	Direccion	Mask	Gateway
PC1	NIC	fd00::10:2	/64	NA
PC2	NIC	fd00::20:2	/64	NA
PC3	NIC	fd00::20:3	/64	NA
PC4	NIC	fd00::10:3	/64	NA

Tabla 5. Asignación de direcciones IPv6 en los terminales.

NOTA: Ejecutar los procedimientos de la práctica previa en caso de que surjan complicaciones.
RECOMENDACIÓN: Es necesario verificar que las configuraciones de seguridad o antivirus estén desactivadas en el terminal o PC, lo que incluye tanto el Firewall de Windows como cualquier software antivirus, ya que podrían surgir problemas durante la ejecución de pruebas de conectividad.

6. Verificación de conectividad en IPv6.

Al igual que en IPv4, existen una serie de comandos tipo show que permiten verificar el comportamiento de las interfaces conectadas. Estos comandos te permitirán verificar que las interfaces y las VLAN se han configurado correctamente.

El siguiente comando muestra una lista de todas las VLANs configuradas en el switch y la información asociada, como los puertos asignados a cada VLAN.

```
enable
Router# show vlan
```

El siguiente comando proporciona un resumen de todas las VLANs configuradas en el switch, mostrando también los puertos asociados a cada VLAN.

```
enable
Router# show vlan brief
```

El siguiente comando muestra una lista de la VLAN específica con el identificador proporcionado y la información asociada, como los puertos asignados a esa VLAN.

```
enable
Router# show vlan id [ID de la Vlan]
```

Reemplaza **"[ID de la Vlan]"** con el número de identificación de la VLAN que deseas consultar.

El siguiente comando muestra una lista de todas las VLANs configuradas en el switch junto con su nombre y la información asociada, incluyendo los puertos asignados a cada VLAN.

```
enable
Router# show vlan name [Nombre de la Vlan]
```

Reemplaza **"[Nombre de la Vlan]"** con el nombre de la VLAN que deseas consultar.

Debe existir conectividad exitosa entre las VLANs del dispositivo final. Para esta práctica, puede comprobarse la conectividad entre las VLANs 10 y VLANs 20. **Usted deberá realizar un análisis de la práctica en lo que respecta a las pruebas de conectividad y adjuntar evidencia de los resultados obtenidos en la parte final de la misma.**

7. Esquema de la práctica 4.2 a desarrollar Inter-VLANs Routing.

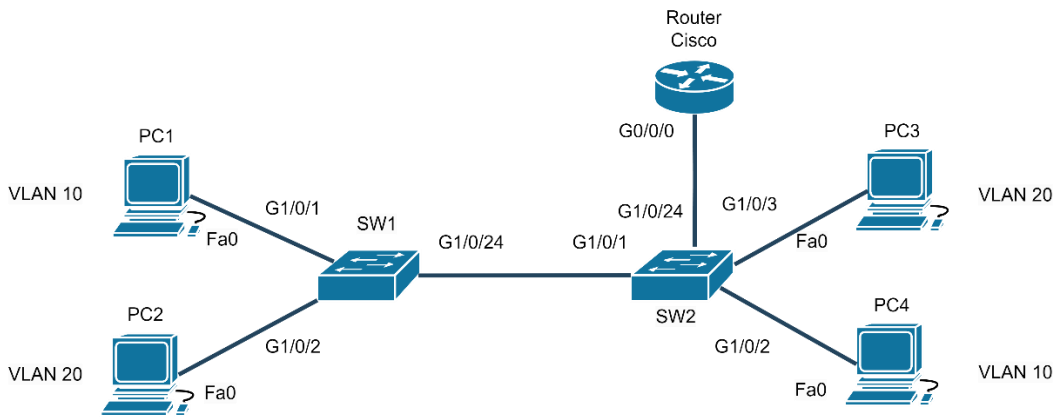


Figura 10. Topología de la red 4.2 Inter-VLANs Routing.

8. Configuración de Inter-VLANs Routing:

Después de completar la configuración de VLANs y verificar su correcto funcionamiento, procederemos a realizar la implementación del enrutamiento Inter-VLAN. Para llevar a cabo este procedimiento, se llevará a cabo la creación de subinterfaces, ya que una interfaz única solo puede tener asignada una dirección IP. Dado que contamos con varias subredes vinculadas a sus respectivas VLAN a las que deseamos acceder, será necesario crear subinterfaces y asociarles direcciones IP. Los pasos a seguir son los siguientes:

1. En el switch siguiendo la topología, ingrese al modo de configuración de interfaz del puerto en este ejercicio práctico.

```
SW1(config)#interface gigabitEthernet 1/0/24
```

Configuraremos la interfaz del switch en modo troncal (trunk) el cual se conectará al router, Activamos el modo troncal usando el siguiente comando ***"switchport mode trunk".***

```
SW1(config-if)#switchport mode trunk
SW1(config-if)#exit
```

2.En el Router dentro del Modo de configuración global, asigne un nombre al Router mediante el comando **"hostname"**, seguido del nombre deseado; en este ejercicio, se empleará **"R1"** como designación para el Router.
Por ejemplo:

```
Router(config)#hostname R1
```

3. En el Modo de configuración global, habilite el enrutamiento IPv6 en el router ingresando el siguiente comando **"*ipv6 unicast-routing*"**.

```
R1(config)#ipv6 unicast-routing
```

4.Habilitamos la interfaz usando el comando **"no shutdown"**.

```
R1(config)# interface gigabitEthernet 0/0/0
no shutdown
```

5. Utiliza el comando ***"interface gigabitEthernet [interfaz].[SudInterfaz]"*** donde La sintaxis para la subinterfaz es la interfaz física seguida de un punto y un número de subinterfaz. El número de subinterfaz es configurable en el modo de configuración global con el fin de generar una subinterfaz única para cada VLAN que requiera enrutamiento.
Donde:

- **"[interfaz]"** es el nombre de la interfaz que se va a configurar.
- ***"[SudInterfaz]"*** Es el nombre de la subinterfaz esta se refiere a una interfaz virtual creada en un router para permitir la comunicación entre diferentes VLANs. En lugar de asignar una interfaz física separada para cada VLAN, se utiliza una sola interfaz física que se divide en varias subinterfaces, cada una asociada con una VLAN específica.

Por ejemplo:

```
R1(config)#interface gigabitEthernet 0/0/0.10
```

Creamos el encapsulamiento para la VLAN 10

```
R1(config-if)#encapsulation dot1Q 10
R1(config-if)#ipv6 address fd00::10:1/64
R1(config-if)#exit
```

NOTA: Repita el proceso de creación de subinterfaces con los valores apropiados para la VLAN 20.

```
R1(config)#interface gigabitEthernet 0/0/0.10
R1(config-if)#encapsulation dot1Q 10
R1(config-if)#ipv6 address fd00::10:1/64
R1(config-if)#exit
```

9. Configuración de direcciones IPv6 en los terminales.

Ajustar la configuración de la dirección IPv6 y la puerta de enlace respectiva en cada terminal es imperativo para llevar a cabo esta práctica. En este contexto, es necesario incorporar la puerta de enlace predeterminada en los terminales mediante la implementación del protocolo de enrutamiento Inter VLANs.

Equipos	Interfaz	Direccion	Mask	Gateway
PC1	NIC	fd00::10:2	/64	fd00::10:1
PC2	NIC	fd00::20:2	/64	fd00::20:1
PC3	NIC	fd00::20:3	/64	fd00::20:1
PC4	NIC	fd00::10:3	/64	fd00::10:1

Tabla 6. Asignación de direcciones IPv6 en los terminales.

RECOMENDACIÓN: Para llevar a cabo la verificación de la conectividad en Inter VLAN Routing, es necesario consultar la sección 6 de esta práctica.

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. **¿Qué es una VLAN y cuál es su propósito en una red?**
2. **¿Por qué se utiliza el enrutamiento entre VLANs y cuál es el dispositivo comúnmente utilizado para realizar esta función?**
3. **¿Qué es un trunk link y por qué es necesario en una configuración de VLANs?**
4. **¿Cómo se evita la interferencia de broadcast en una red con VLANs?**
5. **¿Cuál es la diferencia entre VLAN nativa y VLAN predeterminada?**

ACTIVIDADES DESARROLLADAS

(Anotar las actividades que siguió para el desarrollo de la práctica)

Verificación de la conectividad

Incluya los resultados adquiridos en las pruebas de conectividad, acompañados de un análisis.

Prueba de Conectividad, entre las VLANs 10:

Aquí usted deberá adjuntar los resultados obtenidos del comando de verificación y realizar su respectivo análisis de lo que se muestra en pantalla.

Prueba de Conectividad, entre las VLANs 20:

Aquí usted deberá adjuntar los resultados obtenidos del comando de verificación y realizar su respectivo análisis de lo que se muestra en pantalla.

Adjuntar evidencia de los resultados obtenidos al configurar Inter-VLANs Routing y realizar un análisis:

Aquí usted deberá adjuntar los resultados obtenidos del comando de verificación y realizar su respectivo análisis de lo que se muestra en pantalla.

CONCLUSIONES:

BIBLIOGRAFIA:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN.**
REALIZADO POR:		
CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**5**	**TÍTULO PRÁCTICA:** Configurar el Protocolo de Troncalización de VLAN (VTP, por sus siglas en inglés)

OBJETIVO:

- Establecer el modo VTP en cada switch (Server, Client o Transparent) según los requisitos de la red.
- Definir y configurar el nombre del dominio VTP para asegurar la consistencia en toda la red.
- Verificar que la información de VLAN se sincronice correctamente entre los switches VTP en el dominio.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

1. (3) Switch Cisco Catalyst.
2. (2) Cables de red Ethernet.
3. (1) Cable serial.

DESCRIPCIÓN GENERAL: En esta práctica de laboratorio, se procederá a la configuración del protocolo de Troncal de VLAN (VTP) que opera en tres modos diferentes. Se realizará la configuración individual de cada uno de estos modos, posibilitando la creación, eliminación y modificación de VLANs. Esto resulta en una reducción de la necesidad de configurar la misma VLAN en todos los nodos.

INSTRUCCIONES:

1. Esquema de la práctica a desarrollar VLANs.

En esta práctica usted deberá conectar los equipos del laboratorio de red como se muestra a continuación:

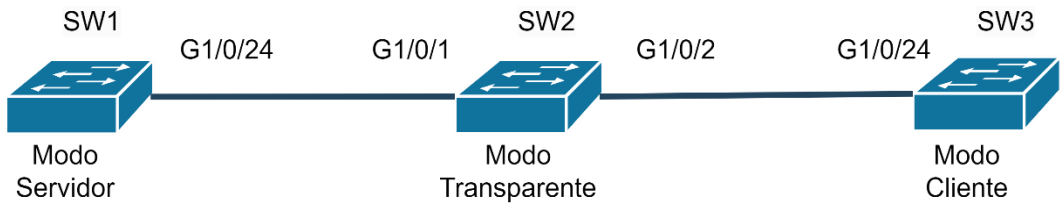


Figura 1. Topología de la red VLANs.

2. Configuración del protocolo VTP (VLAN Trunking Protocol).

VTP funciona en tres modos distintos:

- Modo Servidor
- Modo Cliente
- Modo Transparente

En esta práctica, se configuran las diferentes modalidades, para ello usted debe realizar las siguientes instrucciones:

Configuración Switch 1

1. En el Modo de configuración global, asigne un nombre al switch mediante el comando **"hostname"**, seguido del nombre deseado para esta práctica será SW1.

2.En el Modo de configuración global, configurar el switch en modo servidor y asigna un nombre de dominio VTP utilizando los comandos correspondientes, que son **"vtp mode server"** y ***"vtp domain [dominio]"***.

Donde:

- **"[dominio]"** representa el nombre de un dominio que se desea configurar.

Por ejemplo:

```
SW1(config)# vtp mode server
```

```
SW1(config)# vtp domain laboratorio
```

3. Para incrementar la seguridad, se recomienda asignar una contraseña VTP, si bien es opcional, se aconseja su implementación para fortalecer las medidas de seguridad. A modo de ejercicio práctico, se realizará la configuración correspondiente mediante el uso del comando **"vtp password [contraseña]"** con la contraseña designada como **"UPS"**.

Donde:

- **"[contraseña]"** representa la contraseña que se desea configurar.

Por ejemplo:

```
SW1(config)# vtp password UPS
```

Configuración de interfaces VLAN:

4. En el Modo de configuración global, cree las VLANs mediante el comando: ***"vlan [número de VLAN]"***.

Donde:

- **"[número de VLAN]"** representa el identificador de la VLAN que se configurará.

Por ejemplo:

```
SW1(config)#vlan 10
```

Una vez creada la VLAN le damos un nombre a la misma ingresando el siguiente comando: **"name [nombre de la VLAN]"**.

Donde:

- **"[nombre de la VLAN]"** es el nombre de la VLAN que se va a configurar.

Por ejemplo:

```
SW1(config-vlan)#name VLAN10
SW1(config-vlan)#exit
```

Nota: Repita estos pasos para la creación de una VLAN adicional (por ejemplo, VLAN 20).

5. Acceda al modo de configuración de interfaz correspondiente al puerto que se desea habilitar como troncal mediante la ejecución del comando ***"switchport mode trunk".***

```
SW1(config)# interface gigabitEthernet 1/0/24
SW1(config-if)#switchport mode trunk
SW1(config-if)#exit
```

Configuración Switch 2

6. En el Modo de configuración global, asigne un nombre al switch mediante el comando **"hostname"**, seguido del nombre deseado.

7.En el Modo de configuración global, configurar el switch en modo transparente y asigne el mismo nombre de dominio VTP utilizando los comandos correspondientes, que son ***"vtp mode transparent"*** y ***"vtp domain [dominio]".***

Por ejemplo:

```
SW1(config)# vtp mode transparent
SW1(config)# vtp domain laboratorio
```

8. Para incrementar la seguridad, se recomienda asignar una contraseña VTP, si bien es opcional, se aconseja su implementación para fortalecer las medidas de seguridad. A modo de

ejercicio práctico, se realizará la configuración correspondiente mediante el uso del comando **"vtp password [contraseña]"** con la contraseña designada como **"UPS"**.

Por ejemplo:

```
SW1(config)# vtp password UPS
```

9. Acceda al modo de configuración de interfaz correspondiente a los puertos que se desea habilitar mediante el comando ***"interface range [Tipo de interfaz] [Número de interfaz]"*** este comando permite seleccionar un conjunto de puertos que se configuraran como troncal mediante la ejecución del comando ***"switchport mode trunk".***

```
SW1(config)# interface range gigabitEthernet 1/0/1-2
SW1(config-range-if)#switchport mode trunk
SW1(config-range-if)#exit
```

Configuración Switch 3

10. En el Modo de configuración global, asigne un nombre al switch mediante el comando **"hostname"**, seguido del nombre deseado.

11.En el Modo de configuración global, configurar el switch en modo cliente y asigne el mismo nombre de dominio VTP utilizando los comandos correspondientes, que son ***"vtp mode client"*** y ***"vtp domain [dominio]".***

Por ejemplo:

```
SW1(config)# vtp mode client
SW1(config)# vtp domain laboratorio
```

12. Para incrementar la seguridad, se recomienda asignar una contraseña VTP, si bien es opcional, se aconseja su implementación para fortalecer las medidas de seguridad. A modo de ejercicio práctico, se realizará la configuración correspondiente mediante el uso del comando **"vtp password [contraseña]"** con la contraseña designada como **"UPS"**.

Por ejemplo:

```
SW1(config)# vtp password UPS
```

13. Acceda al modo de configuración de interfaz correspondiente al puerto que se desea habilitar como troncal mediante la ejecución del comando ***"switchport mode trunk".***

```
SW1(config)# interface gigabitEthernet 1/0/24
SW1(config-if)#switchport mode trunk
SW1(config-if)#exit
```

3. Verificación de conectividad en IPv6.

Estos comandos te permitirán verificar que las interfaces y las VLAN se han configurado correctamente.

El siguiente comando despliega el estado y la información resumida del Protocolo de Troncales VLAN (VTP). Es imperativo encontrarse en el modo EXEC privilegiado previo a la ejecución de este comando.

```
enable
show vtp status
```

El siguiente comando muestra la configuración de VLAN en el dispositivo. Puedes utilizarlo para ver las VLAN configuradas, sus nombres, estados, etc. Este comando te dará una lista de VLAN configuradas en el dispositivo.

```
enable
show vlan
```

El siguiente comando despliega el resumen informativo de las interfaces troncales, ofreciendo detalles respecto a las VLAN permitidas y activas en dichas interfaces. Al ejecutar esta instrucción, se accede a información detallada acerca de las interfaces troncales, proporcionando datos específicos acerca de las VLAN permitidas y activas en cada interfaz respectiva.

```
enable
show interfaces trunk
```

Usted deberá comprobar que las vlans creadas en el switch servidor se puedan verificar en el switch cliente, llevando a cabo un análisis. Realizar un análisis sobre lo que ocurre en el switch transparente.

Usted deberá adjuntar evidencia de los resultados obtenidos en la parte final de la misma.

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. **¿Cuál es el propósito de utilizar VTP en una red?**
2. **¿Cuáles son los modos de operación de VTP y cuál es la diferencia entre ellos?**
3. **¿Cuál es el riesgo asociado con el uso indiscriminado del modo servidor en VTP?**
4. **¿Cómo se puede mitigar el riesgo de configuraciones incorrectas al utilizar VTP?**

ACTIVIDADES DESARROLLADAS

(Anotar las actividades que siguió para el desarrollo de la práctica)

Verificación de la conectividad

Adjuntar evidencia de los resultados obtenidos al configurar VTP y realizar un análisis:

Switch 1

Aquí usted deberá adjuntar los resultados obtenidos del comando de verificación y realizar su respectivo análisis de lo que se muestra en pantalla.

Switch 2

Aquí usted deberá adjuntar los resultados obtenidos del comando de verificación y realizar su respectivo análisis de lo que se muestra en pantalla.

Switch 3

Aquí usted deberá adjuntar los resultados obtenidos del comando de verificación y realizar su respectivo análisis de lo que se muestra en pantalla.

Incluya los resultados adquiridos en las pruebas de conectividad, acompañados de un análisis.

Verificación, Switch Servidor:

Aquí usted deberá adjuntar los resultados obtenidos del comando de verificación y realizar su respectivo análisis de lo que se muestra en pantalla.

Verificación, Switch Transparente:

Aquí usted deberá adjuntar los resultados obtenidos del comando de verificación y realizar su respectivo análisis de lo que se muestra en pantalla.

Verificación, Switch Cliente:

Aquí usted deberá adjuntar los resultados obtenidos del comando de verificación y realizar su respectivo análisis de lo que se muestra en pantalla.

CONCLUSIONES:

BIBLIOGRAFIA:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN**
REALIZADO POR:		
CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**6**	**TÍTULO PRÁCTICA:** Configuración y Pruebas de Spanning Tree Protocol (STP) y PER VLAN Spanning Tree (PVST) en IPv6.

OBJETIVO:

- Familiarizarse con los conceptos básicos de STP y PVST.
- Configurar y verificar STP y PVST en IPv6 en un switch Cisco.
- Realizar pruebas para garantizar la redundancia y la eficiencia en la red.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

1. (3) Switch Cisco Catalyst.
2. (3) Cables de red Ethernet.
3. (1) Cable serial.

DESCRIPCIÓN GENERAL: En esta práctica de laboratorio, se procederá a la configuración del Protocolo Spanning Tree (STP) y el Per VLAN Spanning Tree (PVST) utilizando direcciones IPv6 en un switch Cisco. Esto asegurará la redundancia en la red y evitará bucles de red.

1. Esquema de la práctica a desarrollar

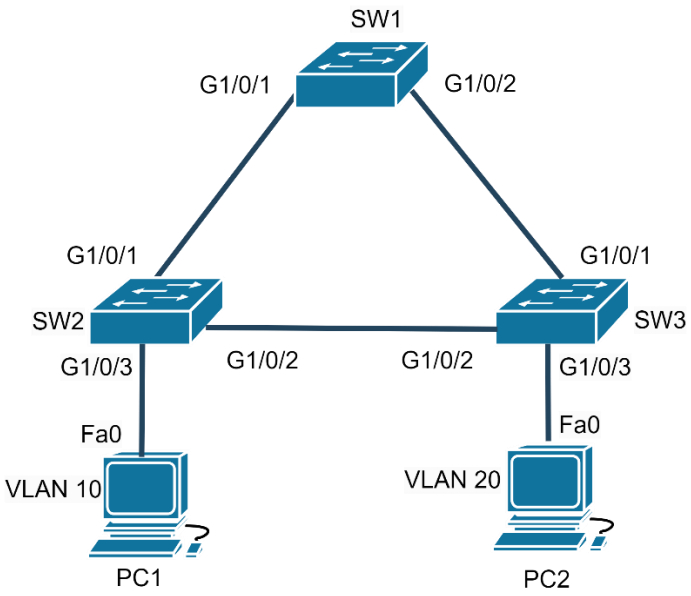


Figura 1. Topología de la Red.

2. Direccionamiento Terminales

En la siguiente tabla 1 se muestra las direcciones IPv6 que se deben asignar a los Terminales (PC1 y PC2).

Equipos	Interfaz	Direccion	Mask	Gateway
PC1	NIC	2023:c8:1::1	/64	NA
PC2	NIC	2023:c8:1::2	/64	NA

Tabla 1. Direcciones IPv6

3. Configuración de STP

1. Entre al modo EXEC privilegiado escribiendo **“enable”**.

```
Switch>enable
```

2. En el modo EXEC privilegiado, ingrese el comando **"configure terminal"** para acceder al Modo de configuración global.

```
Switch#configure terminal
```

3. En el Modo de configuración global, asigne un nombre al switch mediante el comando **"hostname"**, seguido del nombre deseado; en este ejercicio, se empleará **"SW1"** como designación para el Switch 1 y **"SW2"** para el Switch 2 como identificador del switch.

Por ejemplo:

```
Switch (config)#hostname SW1
```

En el switch el protocolo STP ya se encuentra habilitado por defecto con la versión de RSTP , a continuación, se muestra los comandos de verificación para revisar los parámetros del protocolo.

4. En el modo EXEC privilegiado de SW1, ingrese el comando "show spanning-tree", a continuación, se muestra lo que deberá observar:
La información puede variar de acuerdo a la elección de SPT para la elección del Bridge Root.

```
SW1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
         Address     5c3e.0609.1880
         Cost        4
         Port        2 (GigabitEthernet1/0/2)
         Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
         Address     5c3e.0609.1b80
         Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
         Aging Time  300 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/2          Root FWD 4         128.2    P2p


SW1#
```

A continuación, se muestra a detalle los parámetros de SPT para SW1:

1. **Configuración Global de Spanning Tree:**
   - **Protocolo y VLAN:** Rapid Spanning tree está habilitado y utiliza el protocolo IEEE. La información presentada es para la VLAN 1.
   - **Root Bridge:** Este switch tiene la ID de raíz con prioridad 32769 y la dirección MAC 5c3e.0609.1b80. Es el puente raíz para esta VLAN.
2. **Información del Bridge Actual:**
   - **ID del Bridge:** El ID del bridge de este switch es 32769 (prioridad 32768 + extensión de identificación del sistema 1) con la dirección 5c3e.0609.1b80.
3. **Información de la Topología de la Red:**
   - **Interfaz y Estado:** Muestra las interfaces del switch y su estado actual en la topología del Spanning Tree.

- **Role (Papel):** Indica el papel del switch en cada interfaz (Root, Designated, etc.).
- **Estado:** Indica si la interfaz está en el estado de escucha (Listening), aprendizaje (Learning), o reenvío (Forwarding).

5. Verificar los parámetros para SW2 y SW3 e identificar entre los 3 switch el Root Bridge designado.

Switch 2

```
SW2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     5c3e.0609.1880
             Cost        4
             Port        2 (GigabitEthernet1/0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     d009.c85e.0380
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1          Altn BLK 4         128.1    P2p
Gi1/0/2          Root FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p


SW2#
```

Switch 3

```
SW3#show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     5c3e.0609.1880
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     5c3e.0609.1880
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p


SW3#
```

Se observa que el SW3 ha sido designado como puente raíz (root bridge), por lo tanto, en todos los switches se muestra la información de la dirección MAC y prioridad correspondiente al SW3 en el Root ID.

6. Una vez identificado el Root Bridge modificar la prioridad para otro switch. Para este caso se cambiará al switch 2, usted deberá elegir a que switch cambiar.
Con el siguiente comando dentro del modo de configuración se asigna una prioridad mas alta para que se designe como root bridge.

```
SW2(config)#spanning-tree vlan 1 priority 4096
```

Nota: El Root Bridge se elegirá por el ID mas alto.

7. Ingresar el comando de verificación en el switch 2 para observar el cambio del Root Bridge.

```
SW2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     d009.c85e.0380
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     d009.c85e.0380
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p


SW2#
```

4. Verificación de STP

Usted deberá realizar un análisis de la práctica en lo que respecta a las pruebas de conectividad y adjuntar evidencia de los resultados obtenidos en la parte final de la misma.

1. Utilizando el comando de verificación “show spanning-tree”, proporcione evidencia que indique cuál es el switch designado como puente raíz (root bridge).

5. Configuración de PVST:

Para implementar PVST es necesario tener preconfigurado VLANs en los equipos. PVST permite configurar el protocolo en cada VLAN creada como si fueran capas. A continuación, se muestra los pasos de configuración para la topología de la figura 1.

1. En el Modo de configuración global, cree las VLAN 10 en SW2 y VLAN 20 en SW3 mediante el comando: ***“vlan [número de VLAN]”.***

Donde:

- **[número de VLAN]** representa el identificador de la VLAN que se configurará.

Por ejemplo, para SW2:

```
SW2(config)#vlan 10
```

Una vez creada la VLAN le damos un nombre a la misma ingresando el siguiente comando: **“name [nombre de la VLAN]”**.

Donde:

- **[nombre de la VLAN]** es el nombre de la VLAN que se va a configurar.

Por ejemplo:

```
SW2(config-vlan)#name VLAN10
SW2(config-vlan)#exit
```

Nota: Repita estos pasos para la creación de una VLAN adicional (por ejemplo, VLAN 20).

Configuración de interfaces VLAN:
5. Ingrese al modo de configuración de interfaz utilizando el comando: **"*interface [Tipo de interfaz] [Número de interfaz]*"**

Donde:

- **[Tipo de interfaz]** se refiere al nombre de la interfaz que será utilizada, ya sea fastEthernet o gigabitEthernet.
- **[Número de interfaz]** corresponde al número asignado a la interfaz que se va a emplear.

Por ejemplo:

```
SW2(config)#interface gigabitEthernet 1/0/3
```

Activamos el modo troncal usando el siguiente comando: ***"switchport mode access".***

```
SW2(config-if)#switchport mode access
```

Después de haber configurado la interfaz, otorgamos permisos para acceder a la VLAN mediante el siguiente comando: **"switchport access [VLAN]"**.

Donde:

- **[VLAN]** se refiere al nombre de la VLAN que será utilizada.

Por ejemplo:

```
SW2(config-if)#switchport access vlan 10
SW2(config-if)#exit
```

Nota: Repita estos pasos para configurar la interfaz de VLAN con la VLAN 20.

6. Una vez configurada la interfaz de VLAN, active el modo troncal. Ingrese al modo de configuración de interfaz del puerto que se conectará al otro switch en este ejercicio práctico (por ejemplo, puerto gigabitEthernet 1/0/2 para el Switch 2).

```
SW2(config)#interface gigabitEthernet 1/0/2
```

Activamos el modo troncal usando el siguiente comando ***"switchport mode trunk".***

```
SW2(config-if)#switchport mode trunk
SW2(config-if)#exit
```

7. Repita los pasos anteriores para crear y configurar nuevas VLANs según sea necesario.

Previa a la configuración de las VLANs, es necesario declarar en todos los switchs las VLANS creadas para evitar problemas en la habilitación del protocolo PVST.

8. Ingresar los siguientes comandos para cada Switch.

SW1

```
SW1(config)#vlan 10
SW1(config-vlan)#name VLAN10
SW1(config-vlan)#exit
```

```
SW1(config)#vlan 20
SW1(config-vlan)#name VLAN20
SW1(config-vlan)#exit
```

SW2

```
SW2(config)#vlan 20
SW2(config-vlan)#name VLAN20
SW2(config-vlan)#exit
```

SW3

```
SW3(config)#vlan 10
SW3(config-vlan)#name VLAN10
SW3(config-vlan)#exit
```

Al igual que STP, el protocolo PVST se encuentra habilitado por defecto, a continuación, se muestra los comandos de verificación para revisar los parámetros del protocolo.

9. En los 3 Switch ingresar el comando "show spanning-tree" e identificar el root bridge para VLAN20 y VLAN10.

```
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    32778
             Address     5c3e.0609.1880
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     5c3e.0609.1880
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/2          Desg FWD 4         128.2    P2p



VLAN0020
  Spanning tree enabled protocol rstp
  Root ID    Priority    32788
             Address     5c3e.0609.1880
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     5c3e.0609.1880
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p


SW3#
```

En este caso el root bridge designado es SW3 para las 2 VLANS.

10. Configurar como root bridge para la VLAN 20 en SW1 y para la VLAN10 en SW2.

Configuración para SW1

```
SW1(config)#spanning-tree vlan 20 root primary
SW1(config)#spanning-tree vlan 10 root secondary
```

Configuración para SW2

```
SW2(config)#spanning-tree vlan 10 root primary
SW2(config)#spanning-tree vlan 20 root secondary
```

6. Verificación de conectividad en IPv6.

Usted deberá realizar un análisis de la práctica en lo que respecta a las pruebas de conectividad y adjuntar evidencia de los resultados obtenidos en la parte final de la misma.

1. Utilizando el comando de verificación “show spanning-tree”, proporcione evidencia de la configuración obtenida en SW1 y SW2.

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. **¿Cuál es el propósito principal del Protocolo Spanning Tree (STP) en una red?**
2. **¿Cuál es la diferencia entre STP y PVST (Per VLAN Spanning Tree)?**
3. **¿Qué características adicionales ofrece RSTP (Rapid Spanning Tree Protocol) en comparación con STP?**
4. **¿Cuál es el papel del Bridge Protocol Data Unit (BPDU) en el funcionamiento del Spanning Tree Protocol (STP)?**

ACTIVIDADES DESARROLLADAS

(Anotar las actividades que siguió para el desarrollo de la práctica)

Verificación de la conectividad

STP

1. Utilizando el comando de verificación “show spanning-tree”, proporcione evidencia que indique cuál es el switch designado como puente raíz (root bridge).

.

Aquí usted deberá adjuntar la evidencia de las configuraciones.

Análisis. - *Aquí usted deberá realizar el análisis.*

PVST

2. Utilizando el comando de verificación “show spanning-tree”, proporcione evidencia de la configuración obtenida en SW1 y SW2.

SW1

Aquí usted deberá adjuntar la evidencia de la verificación.

Análisis. - *Aquí usted deberá realizar el análisis.*

SW2

Aquí usted deberá adjuntar la evidencia de la verificación.

Análisis. - *Aquí usted deberá realizar el análisis.*
CONCLUSIONES:
BIBLIOGRAFIA:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN**
REALIZADO POR:		
CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**7**	**TÍTULO PRÁCTICA:** Configuración de DHCPv6 con Estado.

OBJETIVO:

- Configurar un servidor DHCPv6 con estado en un Router.
- Configurar servidores DNS y un nombre de dominio en la asignación de direcciones IPv6.
- Establecer un rango de direcciones IPv6 disponibles para asignación.
- Habilitar el enrutamiento IPv6 en el Router.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

1. (1) Router Cisco
2. (1) Switches Cisco
3. (1) Dispositivos con capacidad para soportar IPv6 (p. ej. computadoras)
4. (2) Cables de red Ethernet
5. (1) Cable serial

NOTA: Es necesario contar con 1 computadora equipadas con interfaces Ethernet para llevar a cabo la práctica. Se brinda la opción de utilizar su propia computadora o la que se encuentra en la mesa de trabajo. En caso de no contar con dicha interfaz, se deberá disponer de adaptadores Ethernet, ya que la práctica se ha diseñado para ser ejecutada en cada estación de trabajo en el laboratorio de cómputo 8.

DESCRIPCIÓN GENERAL:

En este laboratorio, se realizará la configuración de un servidor DHCPv6 con estado en un Router Cisco. El servidor DHCPv6 permitirá asignar direcciones IPv6 a dispositivos en la red, facilitando la gestión de direcciones en la infraestructura.

INSTRUCCIONES:

1. Descripción de equipos

Revise la **Figura 1**, para identificar los dispositivos Router Cisco 4321 y Switch Cisco Catalyst serie C1000-24P-4G-L que serán empleados para el desarrollo de la práctica.

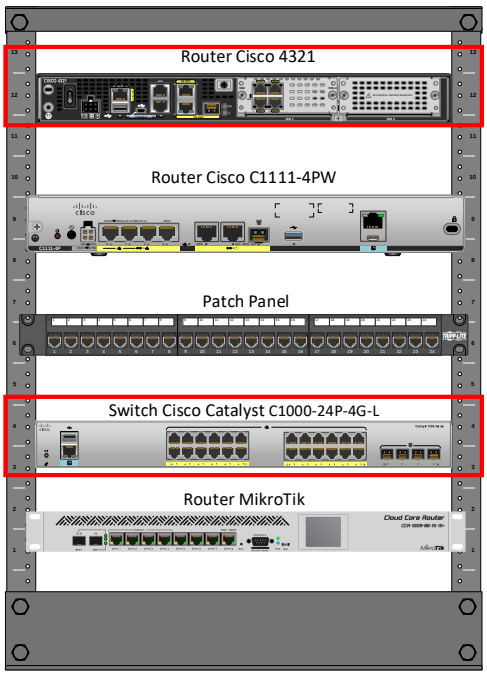


Figura 1. Diseño Rack Laboratorio de Cómputo 8.

En la **Figura 2 y 3** se muestran los equipos y cada una de sus partes, los cuales se detallan en las siguientes **Tablas 1 y 2**.

Router Cisco 4321.

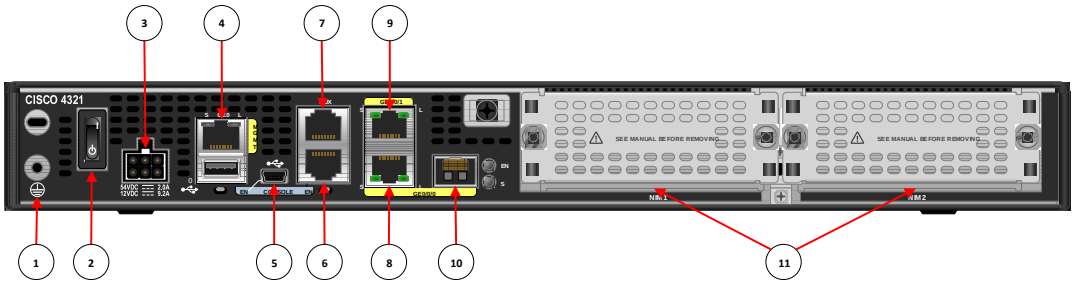


Figura 2. Router Cisco 4321.

Especificaciones del equipo

CISCO 4321			
1	Puesta a tierra	2	Interruptor de alimentación
3	Conector de entrada de alimentación	4	Puerto GE "MGMT" (con puerto USB debajo)
5	Minipuerto USB tipo B	6	Puerto de consola
7	Puerto auxiliar	8	GE 0/0/0 RJ-45 (puerto de cable)
9	GE 0/0/1 RJ-45 (puerto de cable)	10	GE 0/0/0 SFP (puerto de fibra óptica)
11	Ranuras NIM		

Tabla 1. Especificaciones Router Cisco 4321 ISR.

Switch Cisco Catalyst serie C1000-24P-4G-L.

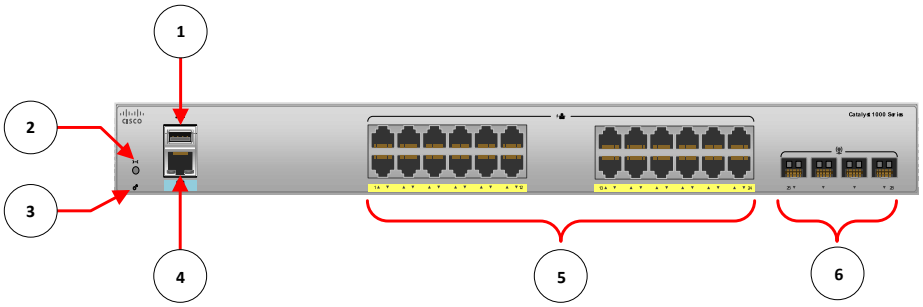


Figura 3. Switch Cisco Catalyst serie C1000-24P-4G-L.

Especificaciones del equipo

Catalyst 1000 Series C1000-24P-4G-L.			
1	Puerto USB tipo A	2	Botón de reinicio
3	LED del sistema	4	Puerto de consola RJ-45
5	24 puertos 10/100/1000 PoE+	6	Ranuras para módulos SFP

Tabla 2. Especificaciones Switch Cisco.

2. Esquema de la práctica a desarrollar.

En esta práctica usted deberá conectar los equipos del laboratorio de red como se muestra a continuación:

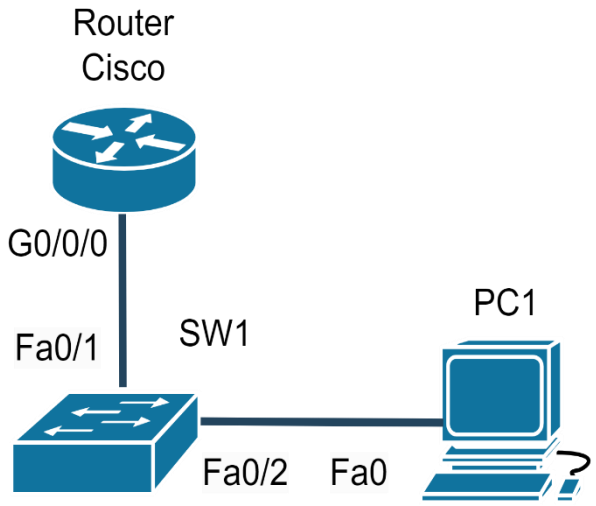


Figura 4. Topología de la red.

3. Configuración de direcciones IPv6.

Las interfaces se configurarán utilizando las direcciones presentadas en la **Tabla 3** de direccionamiento de este laboratorio, para ello realizar las siguientes instrucciones:

Equipos	Interfaz	Direccion	Mask	Gateway
Router	G0/0/0	2001:db8:0:1::1	/64	NA
	Servidor DNS	AAAA:BBBB:CCCC:DDDD::1	NA	NA

Tabla 3. Tabla de direcciones IPv6.

1. Entre al modo EXEC privilegiado escribiendo **"enable"**.

```
Router>enable
```

2. Una vez en el modo EXEC privilegiado, ingrese el comando **"configure terminal"** para acceder al Modo de configuración global.

```
Router#configure terminal
```

3. En el Modo de configuración global, habilitaremos el enrutamiento IPv6 en el router ingresando comando ***"ipv6 unicast-routing"***.

```
Router(config)#ipv6 unicast-routing
```

4. Ahora, configuremos la dirección IPv6 en la interfaz Gigabit Ethernet. Para hacerlo, primero ingrese al modo de configuración de interfaz utilizando el siguiente comando ***"interface gigabitEthernet [Nombre de la interfaz]".***

```
Router(config)#interface gigabitEthernet 0/0/0
```

5. Una vez dentro del modo de configuración de interfaz, configure la dirección IPv6 en la interfaz usando el siguiente comando: ***"ipv6 address [direccion Ipv6]/[mascara de subred] "***.

```
Router(config-if)#ipv6 address 2001:db8:0:1::1/64
```

6. Asegúrese de que la interfaz esté habilitada usando el comando ***"no shutdown"***.

```
Router(config-if)#no shutdown
```

7. Salga del modo de configuración de interfaz escribiendo ***"exit"***.

```
Router(config-if)#exit
```

8. A continuación, procederemos a la configuración de un servidor DHCP para IPv6 mediante el uso del comando **"*ipv6 dhcp pool [nombre del identificador]*"**. Puede elegir cualquier valor para el nombre del identificador.

```
Router(config)#ipv6 dhcp pool LAN1
```

9. Una vez se haya asignado el nombre para el identificador ingresamos el comando **"address prefix [prefijo de la subred]"** seguido del prefijo de la de la subred IPv6 que se asignará a los clientes. Esto establece el rango de direcciones IPv6 que el servidor DHCPv6 puede asignar.

En este ejercicio, se emplea la dirección IPv6 2001:db8:0:1::1/64, donde el prefijo de la red se obtiene al contar los primeros 64 bits de la dirección.

```
Router(config-dhcpv6)#address prefix 2001:db8:0:1::/64
```

10. A continuación, procederemos a configurar los servidores DNS utilizando el comando ***"dns-server"***, seguido de la dirección correspondiente al servidor.

```
Router(config-dhcpv6)#dns-server AAAA:BBBB:CCCC:DDDD::1
```

11. Procedemos a registrar un nombre de dominio, como ejemplo ***"lab_computo8.com".***

```
Router(config-dhcpv6)#domain-name lab_computo8.com
```

12. Salga del modo de configuración de interfaz escribiendo **"exit"**.

```
Router(config-dhcpv6)#exit
```

13. Ahora ingresaremos nuevamente a la interfaz GE 0/0/0 para habilitar a esta interfaz DHCPv6 con el siguiente comando **"ipv6 dhcp server [nombre del identificador]"** el nombre del identificador debe ser el mismo que se uso en el paso 8.

```
Router(config)# interface gigabitEthernet 0/0/0
Router(config-if)#ipv6 dhcp server LAN1
```

14. El siguiente comando se usa para cambiar la bandera M de "0" a "1" para indicar el uso del DHCPv6 con estado:

```
Router(config-if)#ipv6 nd managed-config-flag
```

Con la finalización de estos pasos, el router está configurado para asignar direcciones IPv6 a dispositivos en la red.

4. Verificación de conectividad en IPv6.

En IPv6, al igual que en IPv4, se dispone de comandos de tipo **"show"** que simplifican la validación de la operatividad de las interfaces conectadas. Estos comandos permiten obtener datos relevantes, como el nombre del grupo de direcciones (pool) configurado, el prefijo vinculado al pool y el recuento de dispositivos a los que se les han asignado direcciones. Para llevar a cabo estas tareas, se emplea el siguiente comando: ***"show ipv6 dhcp pool"***.

1. **¿Qué información se puede obtener mediante el comando "show ipv6 dhcp pool"?**

Ejemplo de uso del comando:

```
Router#show ipv6 dhcp pool
```

Este comando posibilita la evaluación de la información de cada una de las direcciones asignadas a través de una interfaz específica, así como la identificación del DUID (Identificador Único del Cliente DHCP), que representa la dirección física de los equipos a los que se les están asignando direcciones.

Otro comando relevante para la gestión de IPv6 en este contexto es el siguiente:

```
Router# show ipv6 dhcp binding
```

2. **¿Cuál es el propósito del comando "show ipv6 dhcp binding" en la gestión de IPv6?**

3. **¿Cuáles es la dirección IPv6 asignada a la computadora por el servidor DHCP?**
   Para esta práctica, es fundamental verificar la conectividad exitosa entre el enrutador y el host, es decir, entre PC1 y Router Cisco.

Usted deberá realizar un análisis de la práctica en lo que respecta a las pruebas de conectividad y adjuntar evidencia de los resultados obtenidos en la parte final de la misma.

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. **¿Qué es DHCPv6 y cuál es su propósito en una red IPv6?**

2. **¿Qué diferencia existe entre un servidor DHCPv6 con estado y uno sin estado?**

3. **¿Por qué es importante la configuración de servidores DNS y un nombre de dominio en el servidor DHCPv6?**

4. **¿Cuál es la importancia del enrutamiento IPv6 en el router en el contexto de DHCPv6 con estado?**

5. **¿Cuál es la ventaja de utilizar DHCPv6 con estado en comparación con la autoconfiguración de direcciones IPv6?**

ACTIVIDADES DESARROLLADAS

(Anotar las actividades que siguió para el desarrollo de la práctica)

1. **PRUEBAS DE CONECTIVIDAD**

Router Cisco

Aquí usted deberá adjuntar la evidencia conectividad del comando "show ipv6 dhcp pool"

¿Qué información se puede obtener mediante el comando "show ipv6 dhcp pool"?
Aquí su respuesta

Router Cisco

Aquí usted deberá adjuntar la evidencia conectividad del comando "show ipv6 dhcp binding"

¿Cuál es el propósito del comando "show ipv6 dhcp binding" en la gestión de IPv6?
Aquí su respuesta

Conectividad entre PC1 y Router Cisco

Aquí usted deberá adjuntar la evidencia de la prueba de conectividad.

¿Cuáles es la dirección IPv6 asignada a la computadora por el servidor DHCPv6?

Aquí usted deberá adjuntar la evidencia de la dirección IPv6 asignada en el terminal.

La dirección asignada por DHCPv6 para este host es: *Aquí su respuesta*

CONCLUSIONES:

BIBLIOGRAFIA:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN**
REALIZADO POR:		
CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**8**	**TÍTULO PRÁCTICA:** Enrutamiento Estático Router Cisco.

OBJETIVO:

- Configurar direcciones IPv6 en las interfaces de los dispositivos de red.
- Configurar enrutamiento estático IPv6 en dispositivos de red.
- Verificar la conectividad IPv6 entre dispositivos de red.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

1. (2) Router Cisco.
2. (1) Switch Cisco Catalyst.
3. (3) Dispositivos con capacidad para soportar IPv6 (p. ej. computadoras).
4. (5) Cables de red Ethernet.
5. (1) Cable serial.

NOTA: Es necesario contar con 3 computadoras equipadas con interfaces Ethernet para llevar a cabo la práctica. Se brinda la opción de utilizar su propia computadora junto con la que se encuentra en la mesa de trabajo. En caso de no contar con dicha interfaz, se deberá disponer de adaptadores Ethernet, ya que la práctica se ha diseñado para ser ejecutada en cada estación de trabajo en el laboratorio de cómputo 8.

DESCRIPCIÓN GENERAL:

En esta práctica se configura y gestiona el enrutamiento estático en una red IPv6. Esto implica la configuración de rutas estáticas en los enrutadores para dirigir el tráfico IPv6 hacia sus destinos correspondientes.

INSTRUCCIONES:

1. Descripción de equipos

Revise la **Figura 1**, para identificar los dispositivos Router Cisco 4321 y Switch Cisco Catalyst serie C1000-24P-4G-L que serán empleados para el desarrollo de la práctica.

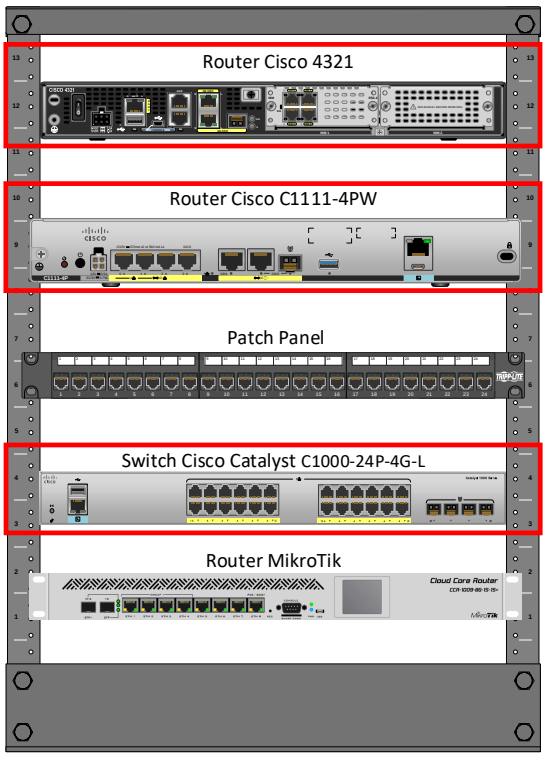


Figura 1. Diseño Rack Laboratorio de Cómputo 8.

En la **Figura 2 y 3** se muestran los equipos y cada una de sus partes, los cuales se detallan en las siguientes **Tablas 1 y 2**.

Router Cisco 4321.

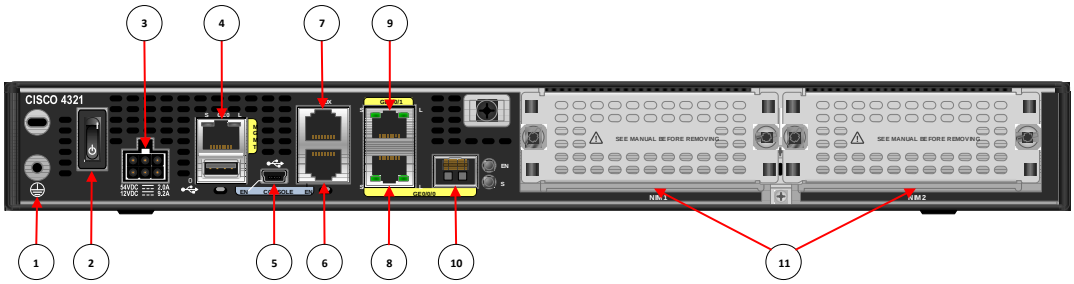


Figura 2. Router Cisco 4321.

Especificaciones del equipo

CISCO 4321			
1	Puesta a tierra	2	Interruptor de alimentación
3	Conector de entrada de alimentación	4	Puerto GE "MGMT" (con puerto USB debajo)
5	Minipuerto USB tipo B	6	Puerto de consola
7	Puerto auxiliar	8	GE 0/0/0 RJ-45 (puerto de cable)
9	GE 0/0/1 RJ-45 (puerto de cable)	10	GE 0/0/0 SFP (puerto de fibra óptica)
11	Ranuras NIM		

Tabla 1. Especificaciones Router Cisco 4321 ISR.

Router Cisco C1111-4PW

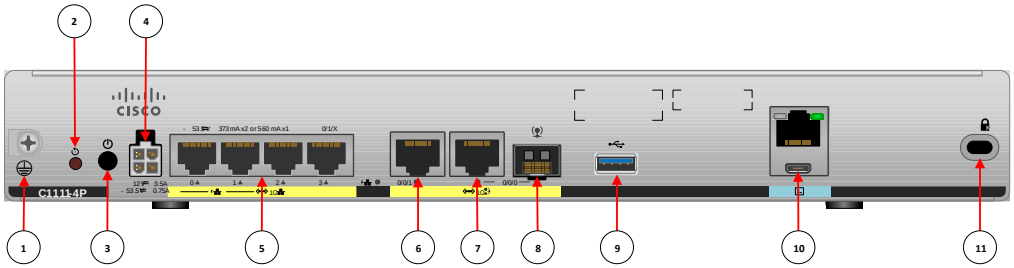


Figura 3. Router Cisco C1111-4PW.

Especificaciones del equipo

1	Puesta a tierra	2	Botón de restablecimiento
3	Interruptor de alimentación eléctrica	4	Conector de alimentación de 4 patillas
5	Switch Ethernet 6 GE 0/0/1	6	GE 0/0/1
7	GE 0/0/0: RJ45	8	GE 0/0/0: SFP
9	USB3.0	10	RJ45/consola de Micro USB
11	Ranura para candado Kensingto		

Tabla 2. Router Cisco C1111-4PW.

Switch Cisco Catalyst serie C1000-24P-4G-L.

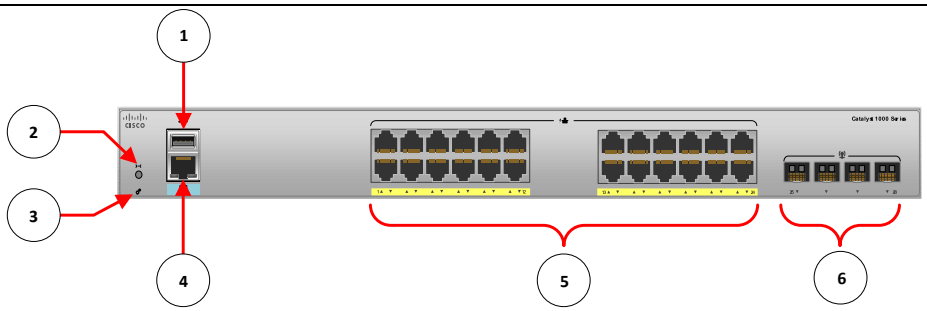


Figura 4. Switch Cisco Catalyst serie C1000-24P-4G-L.

Especificaciones del equipo

Catalyst 1000 Series C1000-24P-4G-L.			
1	Puerto USB tipo A	2	Botón de reinicio
3	LED del sistema	4	Puerto de consola RJ-45
5	24 puertos 10/100/1000 PoE+	6	Ranuras para módulos SFP

Tabla 3. Especificaciones Switch Cisco.

2. Esquema de la práctica a desarrollar.

En esta práctica usted deberá conectar los equipos del laboratorio de red como se muestra a continuación:

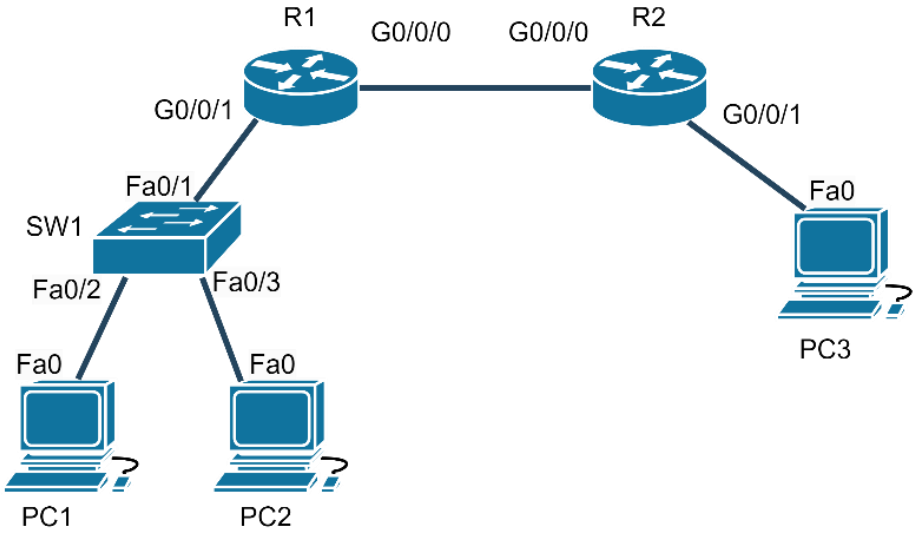


Figura 5. Topología de la red.

3. Configuración de direcciones IPv6.

Las interfaces se configurarán utilizando las direcciones presentadas en la **Tabla 4** de direccionamiento de este laboratorio, para ello realizar las siguientes instrucciones:

Equipos	Interfaz	Direccion	Prefijo de red	Gateway
R1	G0/0/0	2023:c8:1::1	/64	NA
	G0/0/1	2023:c8:0:1::1	/64	NA
R2	G0/0/0	2023:c8:1::2	/64	NA
	G0/0/1	2023:c8:0:2::1	/64	NA

Tabla 4. Tabla de direcciones IPv6.

1. Entre al modo EXEC privilegiado escribiendo **"enable"**.

```
Router>enable
```

2. En el modo EXEC privilegiado, ingrese el comando **"configure terminal"** para acceder al Modo de configuración global.

```
Router#configure terminal
```

3. En el Modo de configuración global, asigne un nombre al router ingresando el siguiente comando **"hostname",** seguido del nombre que desee para el enrutador, en este ejercicio práctico se utilizara "R1" y "R2" como nombres para identificar cada uno de los routers, respectivamente.

```
Router(config)#hostname R1
```

4. En el Modo de configuración global, habilite el enrutamiento IPv6 en el router ingresando el siguiente comando **"*ipv6 unicast-routing*"**.

```
Router(config)#ipv6 unicast-routing
```

Este comando permite habilitar el protocolo IPv6 a nivel global en el router.

5. Ahora, configure la dirección IPv6 en la interfaz Gigabit Ethernet. Para hacerlo, primero ingrese al modo de configuración de interfaz utilizando el siguiente comando ***"interface gigabitEthernet [Nombre de la Interfaz]"***.

```
Router(config)#interface gigabitEthernet 0/0/0
```

6. Una vez dentro del modo de configuración de interfaz, configure la dirección IPv6 en la interfaz usando el siguiente comando ***"ipv6 address [dirección IPv6] / [máscara de subred]"*** (sustituya la dirección IPv6 y la máscara de subred deseada):

```
Router(config-if)#ipv6 address 2023:c8:1:1::1/64
```

7. Asegúrese de que la interfaz esté habilitada usando el comando **"no shutdown"**.

```
Router(config-if)#no shutdown
```

8. Salga del modo de configuración de interfaz escribiendo **"exit"**.

```
Router(config-if)#exit
```

9. Una vez que las direcciones IPv6 se han configurado en las interfaces GigabitEthernet, el siguiente paso implica establecer enrutamiento estático. Esta configuración permite al administrador de red establecer manualmente las rutas que deben seguir los paquetes para alcanzar diferentes áreas de la red. Esto se logra mediante el ingreso del siguiente comando: **"ipv6 route [Dirección de red a alcanzar/prefijo de red] [Dirección de la interfaz a través de la cual se alcanzará la red]".**

En R1, ejecutar el siguiente comando:

```
R1(config)#ipv6 route 2023:c8:0:2::/64 2023:c8:1::2
```

Este comando indica que cualquier tráfico destinado a la red 2023: c8:0:2::/64 debe ser enviado al siguiente salto 2023:c8:1::2, que corresponde a la dirección IPv6 de la interfaz GigabitEthernet 0/0/0 del Router R2.

En R2, ejecutar el siguiente comando:

```
R2(config)#ipv6 route 2023:c8:0:1::/64 2023:c8:1::1
```

10. Repita los pasos del 5 al 9 para cada interfaz Gigabit Ethernet que desee configurar con una dirección IPv6.

Con la finalización de estos pasos, el router está configurado para asignar direcciones IPv6 a dispositivos en la red.

4. Configuración de direccionamiento IPv6 en los terminales.

Configurar en cada host la dirección IPv6 y la puerta de enlace correspondiente.

Equipos	Interfaz	Direccion	Mask	Gateway
PC1	NIC	2023:c8:0:1::10	/64	2023:c8:0:1::1
PC2	NIC	2023:c8:0:1::11	/64	2023:c8:0:1::1
PC3	NIC	2023:c8:0:2::10	/64	2023:c8:0:2::1

Tabla 5. Asignación de direcciones IPv6 en los hosts.

RECOMENDACIÓN: Es necesario verificar que las configuraciones de seguridad o antivirus estén desactivadas en el terminal o PC, lo que incluye tanto el Firewall de Windows como cualquier software antivirus, ya que podrían surgir problemas durante la ejecución de pruebas de conectividad.

5. Verificación de conectividad en IPv6.

Para confirmar la efectividad de las rutas estáticas, es necesario examinar la tabla de enrutamiento utilizando el comando **"show ipv6 route"** en el enrutador.

Una vez realizada la configuración del enrutamiento estático en ambos enrutadores, se debe verificar que la conectividad IPv6 se ha establecido correctamente realizando ping entre los terminales y en caso de falla verifique las configuraciones y conexiones físicas. **Usted deberá realizar un análisis de la práctica en lo que respecta a las pruebas de conectividad y adjuntar evidencia de los resultados obtenidos en la parte final de la misma.**

6. Actividad en casa.

Mediante el software GNS3, realizar la topología de la Figura 6. Asegúrese de asignar direcciones propias IPv6 a los dispositivos. Proporcione evidencia de la verificación de conectividad.

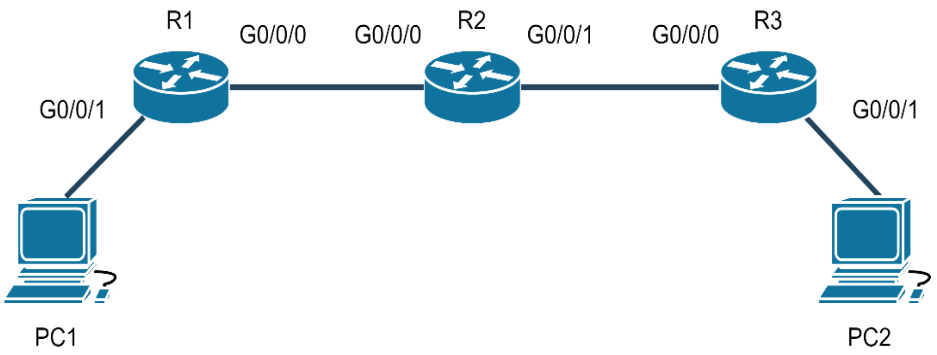


Figura 6. Topología de la Red.

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. **¿Cuál es el propósito de implementar enrutamiento estático?**
2. **¿Cuáles son los requisitos de red que deben cumplirse para utilizar enrutamiento estático de manera efectiva?**
3. **¿Cuáles son los pasos necesarios para configurar el enrutamiento estático en un enrutador?**

ACTIVIDADES DESARROLLADAS

(Estimado docente, a continuación, se detallan los pasos a cumplir en las instrucciones por los estudiantes)

1. **Verificación de Conectividad**

   Prueba de conectividad:

   Entre R1 y PC3

Aquí usted deberá adjuntar la evidencia de la prueba de conectividad.

Entre R2 y PC1

Aquí usted deberá adjuntar la evidencia de la prueba de conectividad.

Entre PC1 y PC3

Aquí usted deberá adjuntar la evidencia de la prueba de conectividad entre los terminales.

2. Actividad en casa

Tabla de Direccionamiento

Equipos	Interfaz	Direccion	Prefijo de red	Gateway
R1				
R2				
R3				
PC1				
PC2				

Tabla 6. Direcciones Ipv6.

Topología implementada en el Software GNS3

Aquí usted deberá adjuntar la evidencia de la topología implementada en el Software GNS3 etiquetada con las direcciones propias IPv6 a los dispositivos.

- **Configuración Direccionamiento y Routing**

Configuración PC1 y PC2

Aquí usted deberá adjuntar las configuraciones.

Configuración Router R1

Aquí usted deberá adjuntar las configuraciones.

Configuración Router 2

Aquí usted deberá adjuntar las configuraciones.

Configuración Router R3

Aquí usted deberá adjuntar las configuraciones.

- **Verificación de Conectividad**

Capturas de Conectividad:
PC1 a PC2

Aquí usted deberá adjuntar la evidencia de la prueba de conectividad.

PC2 a PC1

Aquí usted deberá adjuntar la evidencia de la prueba de conectividad.

Tabla de Enrutamiento Router R1

Aquí usted deberá adjuntar la evidencia de la prueba de conectividad

CONCLUSIONES:
BIBLIOGRAFIA:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN.**
REALIZADO POR:		
CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**9**	**TÍTULO PRÁCTICA:** Enrutamiento estático equipos Cisco y MikroTik.

OBJETIVO:

- Configurar direcciones IPv6 en las interfaces de los dispositivos de red.
- Configurar enrutamiento estático IPv6 en dispositivos de red.
- Verificar la conectividad IPv6 entre dispositivos de red.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

6. (2) Router Cisco.
7. (1) Router MikroTik.
8. (5) Cables de red Ethernet.
9. (1) Cable serial.

DESCRIPCIÓN GENERAL:

En esta práctica se configura y gestiona el enrutamiento estático en una red IPv6, que incluye dispositivos de Router Cisco y MikroTik. Esto implica la configuración de rutas estáticas en los enrutadores para dirigir el tráfico IPv6 hacia sus destinos correspondientes.

NOTA: Para llevar a cabo la práctica, es esencial contar con habilidades específicas, como la asignación de direcciones IPv6 en un router MikroTik y la configuración de enrutamiento estático mediante un router Cisco.

INSTRUCCIONES:

1. Esquema de la práctica a desarrollar.

En esta práctica usted deberá conectar los equipos del laboratorio de red como se muestra a continuación:

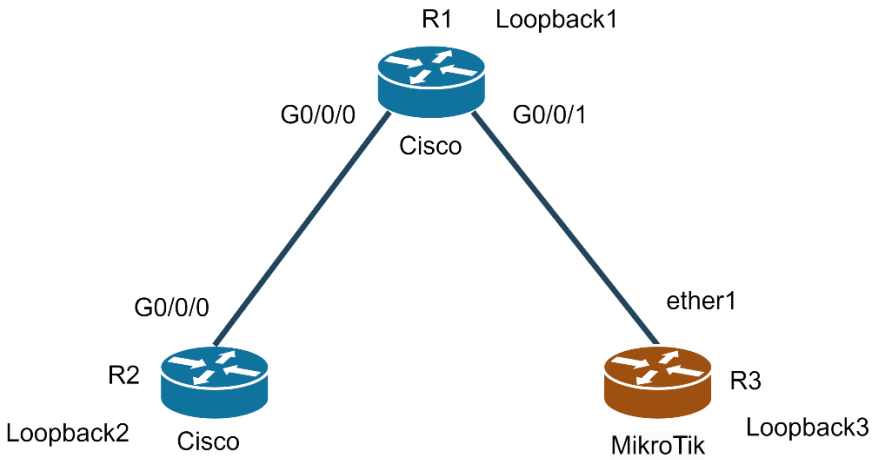


Figura 1.Topología de la Red

2. Configuración de direcciones IPv6.

Las interfaces se configurarán utilizando las direcciones presentadas en la **Tabla 4** de direccionamiento de este laboratorio, para ello realizar las siguientes instrucciones:

Equipos	Interfaz	Direccion	Mask	Gateway
R1(Cisco)	G0/0/0	2023:ae:c8:1::1	/64	NA
	G0/0/1	2023:ae:c8:2::1	/64	NA
	LoopBack1	2023:ae:c8:3::2	/64	NA
R2(Cisco)	G0/0/0	2023:ae:c8:1::2	/64	NA
	LoopBack2	2023:ae:c8:4::2	/64	NA
	ether1	2023:ae:c8:2::2	/64	NA

R3 (Mikrotik)	LoopBack3	2023:ae:c8:5::2	/64	NA

Tabla 1. Tabla de direcciones IPv6.

Ejemplo de configuración para Router Cisco R1

1. Entre al modo EXEC privilegiado escribiendo **"enable"**.
2. En el modo EXEC privilegiado, ingrese el comando **"configure terminal"** para acceder al Modo de configuración global.
3. En el Modo de configuración global, asigne un nombre al Router según la **Figura 1**
4. En el Modo de configuración global, habilite el enrutamiento IPv6 en el Router ingresando el siguiente comando **"*ipv6 unicast-routing*"**.
5. Para establecer una interfaz de Loopback, se debe emplear el comando **"interface loopback [número]"**. El parámetro **[número]** admite un rango de valores desde 0 hasta 4294967295. Por ejemplo, para crear una interfaz de Loopback con el número 1, ingresa:

```
R1(config)#interface loopback 1
```

6. Para asignar una dirección IPv6 a la interfaz de Loopback, utiliza el comando "**ipv6 address [dirección/prefijo de red]"**. Reemplaza la **[dirección/ prefijo de red]** con la dirección IPv6 y la longitud del prefijo especificado en la **Tabla1**:

```
R1(config-if)#ipv6 address 2023:ae:c8:3::2/64
```

7. Asegúrate de que la interfaz de Loopback esté habilitada con el comando **"no shutdown"**:

```
R1(config-if)#no shutdown
R1(config-if)#exit
```

8. Repita los pasos 5 a 7 para cada interfaz de Loopback que se encuentra especificado en la **Tabla 1**.

9. Ahora, configure la dirección IPv6 en la interfaz Gigabit Ethernet. Para hacerlo, primero ingrese al modo de configuración de interfaz utilizando el siguiente comando **"*interface gigabitEthernet [Nombre de la Interfaz]*"**.

```
R1(config)#interface gigabitEthernet 0/0/0
```

10. Una vez dentro del modo de configuración de interfaz, configure la dirección IPv6 en la interfaz usando el siguiente comando ***"ipv6 address [dirección IPv6] / [*prefijo de red*]"*** (sustituya la dirección IPv6 y la máscara de subred deseada):

```
R1(config-if)#ipv6 address 2023:ae:c8:1::1/64
```

11. Asegúrese de que la interfaz esté habilitada usando el comando **"no shutdown"**.

```
R1(config-if)#no shutdown
```

12. Salga del modo de configuración de interfaz escribiendo **"exit"**.

```
R1(config-if)#exit
```

13. Repita los pasos del 9-12 para la asignación de direcciones IPv6 a cada Router Cisco que se encuentra especificado en la **Tabla 1.**

Nota: Si surgen complicaciones en la asignación de direcciones Ipv6 en los enrutadores se recomienda revisar practicas previas.

14. Una vez que las direcciones IPv6 se han configurado en las interfaces GigabitEthernet, el siguiente paso implica establecer enrutamiento estático. Esta configuración permite al administrador de red establecer manualmente las rutas que deben seguir los paquetes para alcanzar diferentes áreas de la red.

Esto se logra mediante el ingreso del siguiente comando: **"ipv6 route [Dirección de red a alcanzar/prefijo de red] [dirección IPv6 del próximo salto o interfaz de salida]".**

- **"[Dirección de red a alcanzar]"** es la dirección IPv6 de la red de destino a la que deseas enrutar el tráfico.
- **"[prefijo de red]"** es la máscara de subred de la red de destino.
- **"[dirección IPv6 del próximo salto o interfaz de salida]"** es la dirección IPv6 del siguiente salto o la interfaz de salida para enrutar el tráfico.

Por ejemplo:
En R1, ejecutar el siguiente comando:

```
R1(config)#ipv6 route 2023:ae:c8:5::/64 2023:ae:c8:2::2
```

Este comando indica que cualquier tráfico destinado a la red *2023:ae:c8:5::/64* debe ser enviado al siguiente salto *2023:ae:c8:2::2*, que corresponde a la dirección IPv6 de la interfaz ether1 del Router R3 (Mikrotik).

```
R1(config)#ipv6 route 2023:ae:c8:4::/64 2023:ae:c8:1::2
```

Este comando indica que cualquier tráfico destinado a la *2023:ae:c8:4::/64* debe ser enviado al siguiente salto *2023:ae:c8:1::2*, que corresponde a la dirección IPv6 de la interfaz GigabitEthernet 0/0/0 del Router R2.

13. Repita el paso 14 para cada **Router Cisco** que se encuentra especificado en la **Tabla 1** para la asignación de rutas estáticas.

Nota: Asegúrate de repetir los pasos para cada interfaz Gigabit Ethernet que desees configurar con IPv6, y ajusta las direcciones y rutas según la topología de la red.

Ejemplo de configuración para Router MikroTik R3
1. Para configurar el direccionamiento IPv6, ejecutar el siguiente comando: ***/ipv6 address add address=[dirección IPv6]/[*****prefijo de red*****] interface=[interfaz]***

Donde:

- **"[dirección IPv6]"** es la dirección IPv6 de la red de destino a la que deseas enrutar el tráfico. No debes usar corchetes alrededor de la dirección IPv6.
- **"[prefijo de red]"** es la máscara de subred expresada en notación de prefijo (por ejemplo, "/64" para una red típica).
- **"[interfaz]"** es el nombre de la interfaz que se va a configurar.

Por ejemplo:
En R3(Router MikroTik), ejecutar el siguiente comando:

```
[admin@MikroTik] >/ipv6 address add address=2023:ae:c8:2::2/64
interface=ether1
```

2. Para crear una interfaz de loopback en un router MikroTik, utiliza el siguiente comando con el nombre de la interfaz (por ejemplo, "Loopback3"):

/interface bridge add name= "[nombre para la interfaz loopback]"

Este comando creará una interfaz de bridge llamada "Loopback3". Ten en cuenta que, en realidad, estás creando un bridge que actúa como una interfaz de loopback.

Ejemplo:

```
/interface bridge add name=Loopback3
```

3. Para asignar una dirección IPv6 a la interfaz de loopback, usa el siguiente comando:
/ipv6 address add address="[dirección IPv6]"/"[máscara]" interface="[nombre de la interfaz loopback]"

Esto asignará la dirección IPv6 especificada a la interfaz "Loopback3".

Ejemplo:

```
[admin@MikroTik] >/ipv6 address add address=2023:ae:c8:5::2/64
interface=Loopback3
```

4. Después de configurar las direcciones IPv6 en las interfaces, se debe configurar el enrutamiento estático. Mediante el siguiente comando:

/ipv6 route add dst-address="[dirección de la red a alcanzar]"/"[mascara de la red]" gateway= "[direccion del próximo salto]"

Este comando agrega rutas estáticas para las redes especificadas con los respectivos gateways.

Ejemplo:

```
[admin@MikroTik] >/ipv6 route add dst-address=2023:ae:c8:3::/64
gateway=2023:ae:c8:2::1
[admin@MikroTik] >//ipv6 route add dst-address=2023:ae:c8:4::/64
gateway=2023:ae:c8:2::1
[admin@MikroTik] >//ipv6 route add dst-address=2023:ae:c8:1::/64
gateway=2023:ae:c8:2::1
```

3. Verificación de conectividad en IPv6.

El siguiente comando muestra una lista de todas las rutas IPv6 configuradas en el dispositivo y la información asociada, como las redes de destino y las interfaces salientes para cada ruta.

```
enable
Router# show ipv6 route
```

El siguiente comando muestra una lista de todas las rutas estáticas IPv6 configuradas en el dispositivo y la información asociada, como las interfaces de salida asignadas a cada ruta estática:

```
enable
Router# show ipv6 route static
```

Para esta práctica, es esencial verificar la conectividad exitosa entre los enrutadores y sus Loopback.

Para verificar la conectividad en el Router MikroTik, se emplean los siguientes comandos:

- **"/ipv6 route print"** para mostrar los detalles específicos de una ruta estática IPv6.
- Para utilizar "ipv6 route print" con una dirección de destino específica, se usa **"ipv6 route print where dst-address=[dirección de destino]"**.
- Para verificar la tabla de enrutamiento IPv6 completa, incluyendo la información de las rutas estáticas, se utiliza **"ipv6 route print where static=yes"**.

Usted deberá realizar un análisis de la práctica en lo que respecta a las pruebas de conectividad y adjuntar evidencia de los resultados obtenidos en la parte final de la misma.

4. Actividad en casa.

Mediante el software GNS3, Realice la configuración del enrutamiento estático en la siguiente topología de la Figura 2. Asegúrese de asignar direcciones propias IPv6 a los dispositivos. Proporcione evidencia de la verificación de conectividad. (El docente enviará el trabajo para que los estudiantes lo desarrollen, cada estudiante deberá tener la topología con su propia dirección Ipv6).

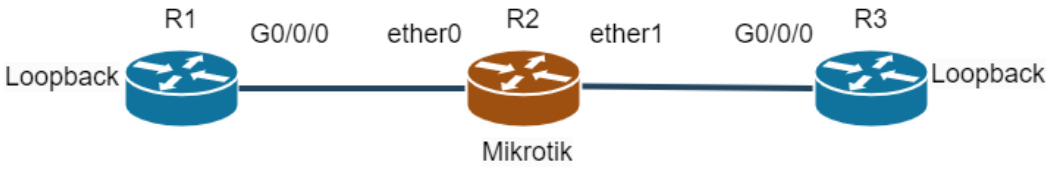


Figura 2.Topología Simulación GNS3

Nota: Es posible que se tenga confusión con la asignación de direccionamiento en GNS3 y la interfaz del router Mikrotik. Para referirse a la interfaz física ether0 en la línea de comando se tiene que digitar ether1 mientras si se tiene que referir a la interfaz física ether1 se tiene que digitar ether2.

Instalación IOS Router MikroTik en GNS3

1. Ingresar a la siguiente dirección www.mikrotik.com de la página oficial de MikroTik

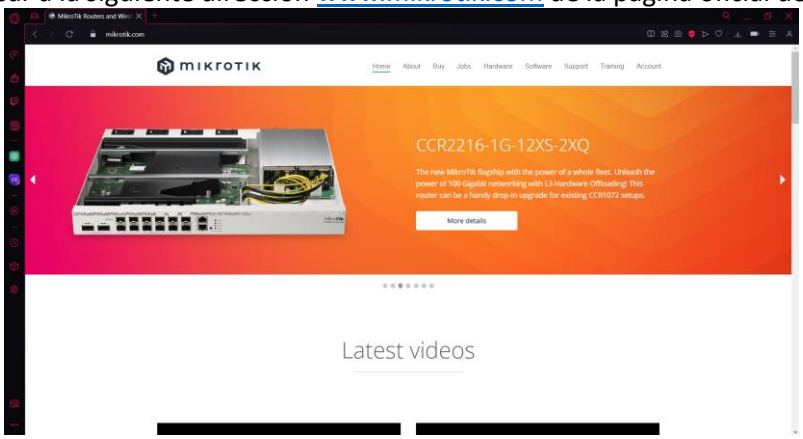


Figura 3. Página Oficial MikroTik.

2. En el menú de la página de Mikrotik damos clic en "Software". A continuación, aparecerá en pantalla las versiones más recientes del RouterOS.

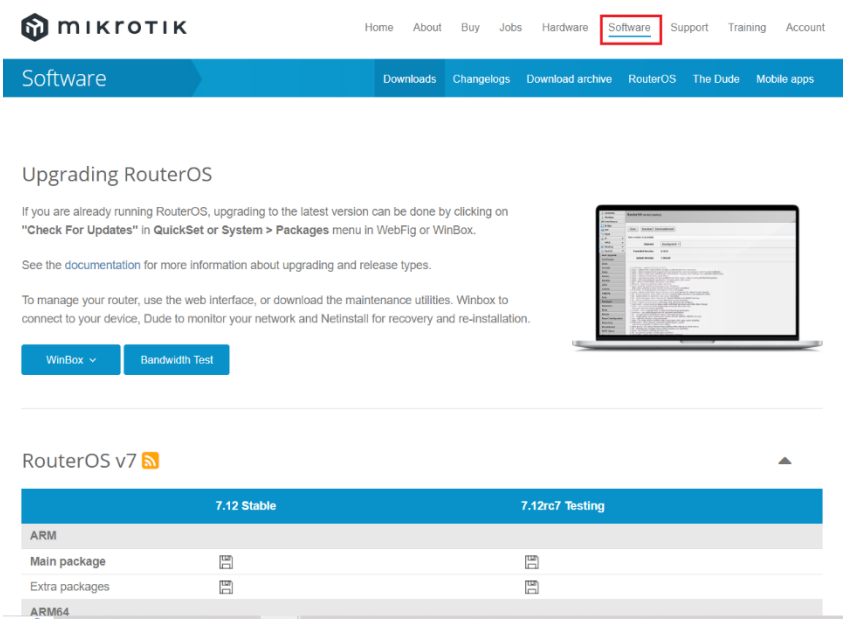


Figura 4. Software del Router OS MikroTik para GNS3.

3. Dentro de las opciones de Software daremos clic en “Download archive”. Aquí encontramos todas las versiones del RouterOS. A continuación, buscamos el “Release 6.49”.

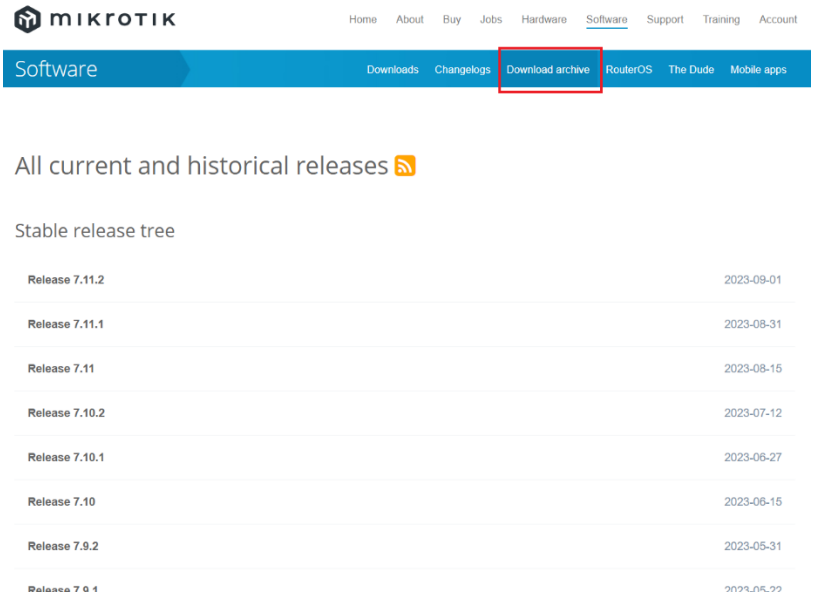


Figura 5. Versiones del Router OS Publicados por MikroTik.

4. Damos clic en “Release 6.49” seguidamente nos muestra los tipos de descarga. Buscamos “chr-6.49.img.zip” y damos clic sobre el nombre para que empiece la descarga.

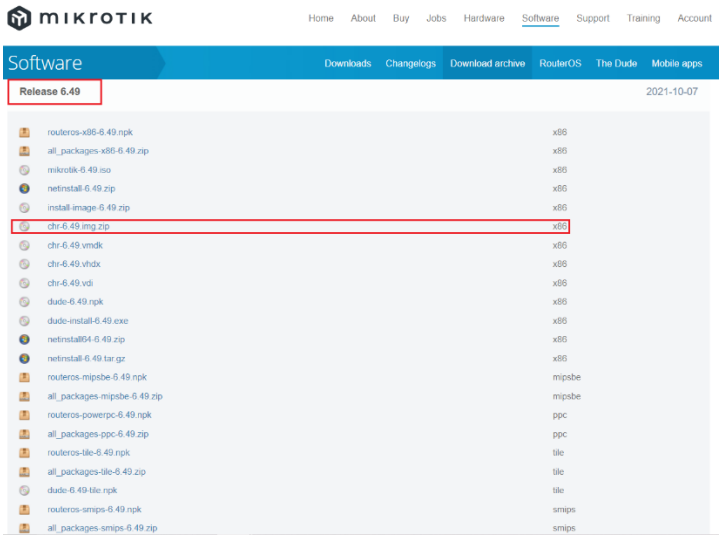


Figura 6. Versión de RouterOS utilizada para GNS3.

5. Ingresamos en GNS3 > “Edit”> “Preferences”.

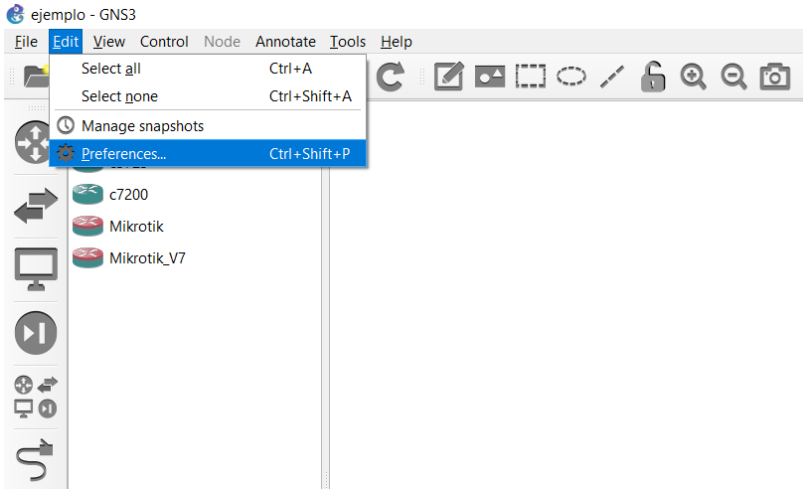


Figura 17. Ventana Edit.

6. Seleccionamos “Qemu VMs” y damos clic en “New”.

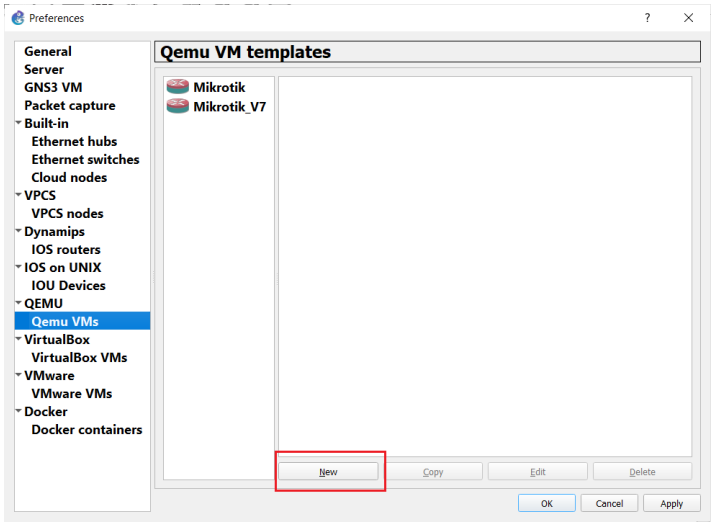


Figura 7. Selección de Qemu VMs.

7. A continuación, nos aparecerá la siguiente pantalla, seleccionamos “Run this Qemu VM on the GNS3 VM” y damos clic en “Next”.

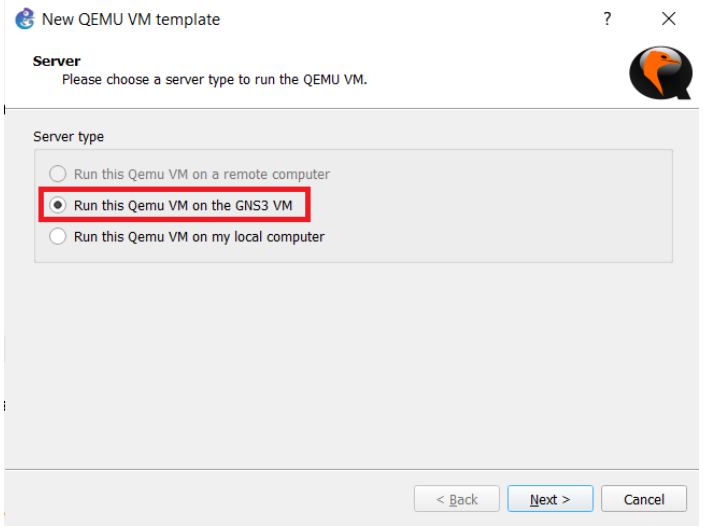


Figura 8. Selección de Run this Qemu VM on the GNS3 VM.

8. Ingresamos el nombre “chr-6.49.8” y damos clic en “Next”.

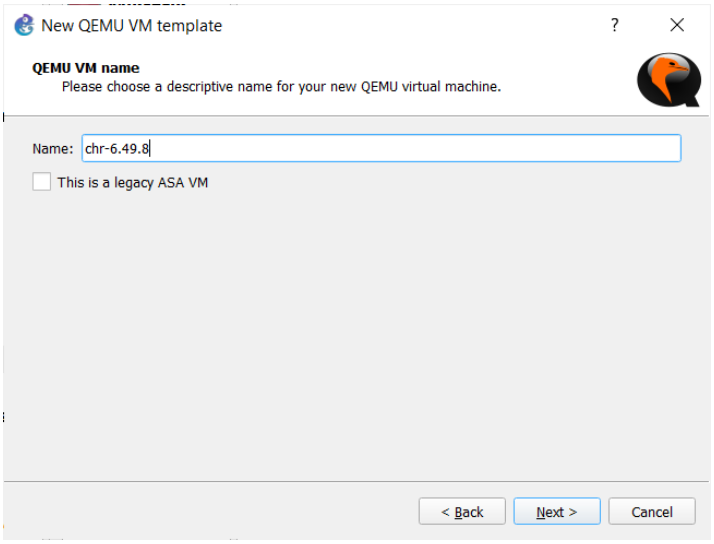


Figura 9. Agnación del nombre chr-6.49.8.

9. En las siguientes 2 pantallas que se mostraran damos clic en “Next”.

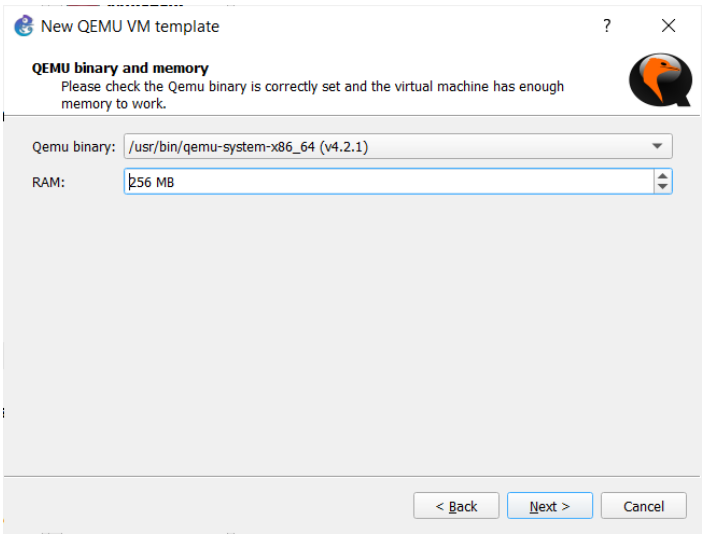


Figura 10. Seleccionar de Next.

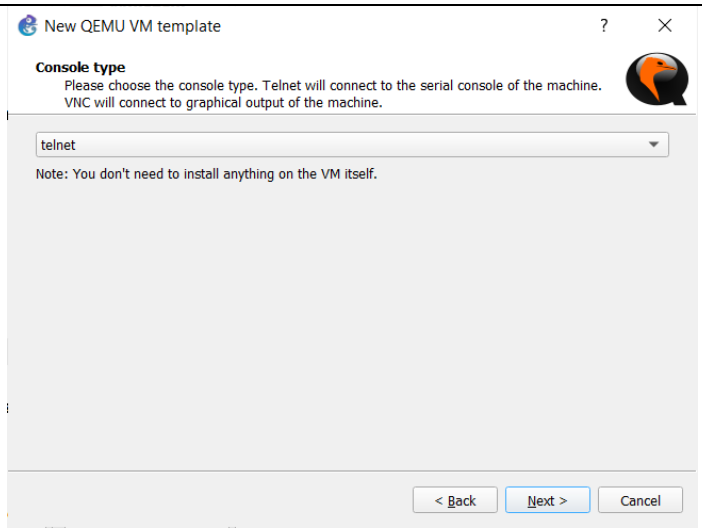


Figura 11. Seleccionar de Next.

10. Seleccionar “New Image” clic en > “Browse”.

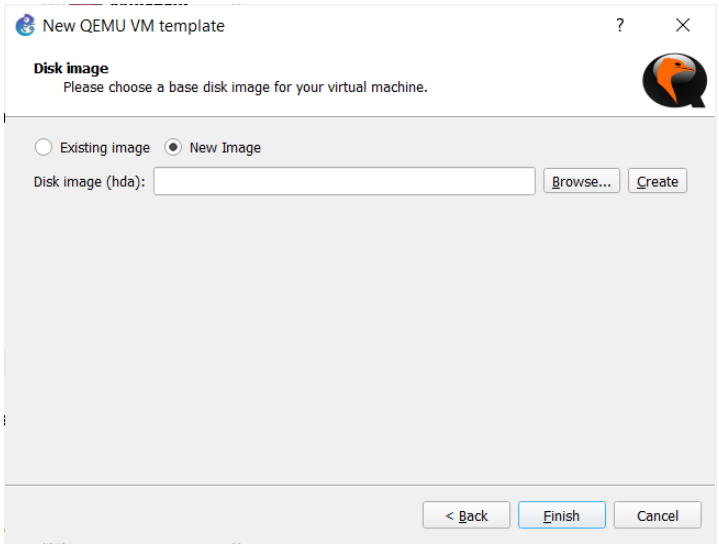


Figura 12. Seleccionar New Image.

11. Buscamos la ubicación en donde descargamos el archivo .img desde las pagina de Mikrotik. Damos clic en “Abrir”.

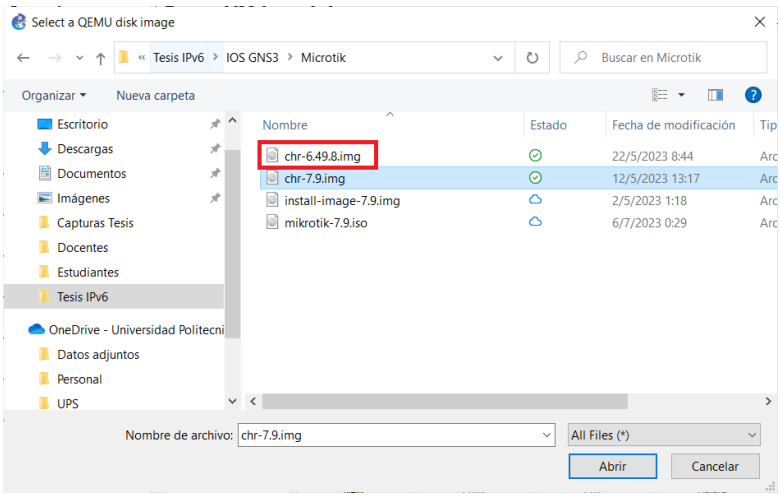


Figura 13 . archivo .img.

12. A continuación, damos clic en “Finish”.

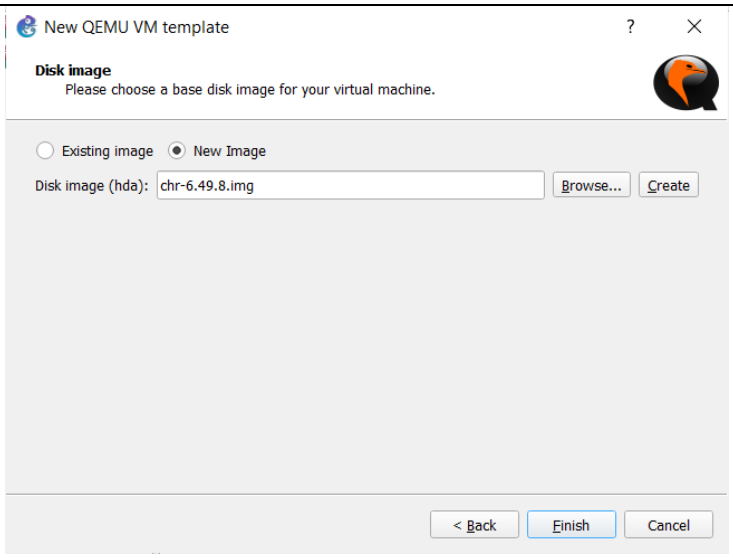


Figura 14. Seleccionar Finish.

13. Finalmente damos clic en “Apply” y “OK”.

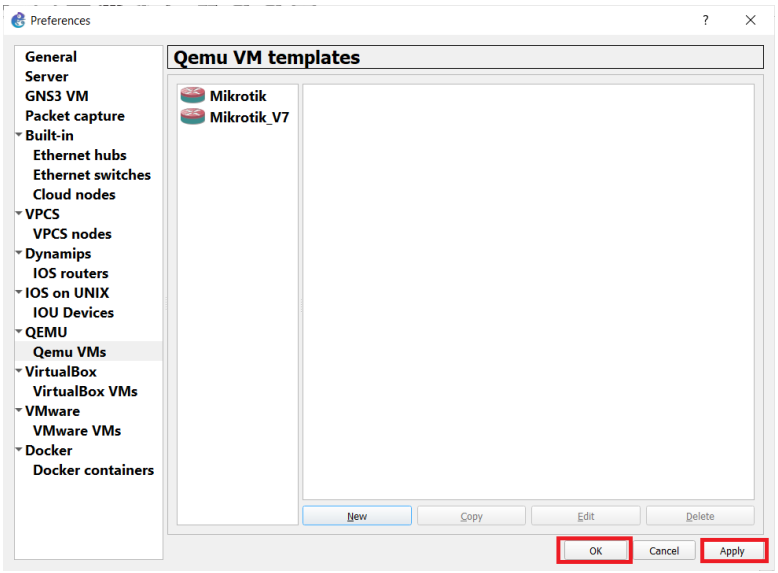


Figura 15. Seleccionar Apply y OK.

Nota: Para emular un enrutador Mikrotik a través de la interfaz de Winbox en GNS3 ver figura 17, se requiere la conexión de un conmutador (Switch) y una nube (Cloud) a una de sus interfaces para habilitar la comunicación con la interfaz de Terminal. A través de este método, es posible autenticarse en Winbox utilizando la dirección MAC del enrutador Mikrotik. Si no se puede acceder mediante la interfaz de Winbox, se puede recurrir a la consola de GNS3 para llevar a cabo la configuración como si se estuviera trabajando con un enrutador Mikrotik físico.

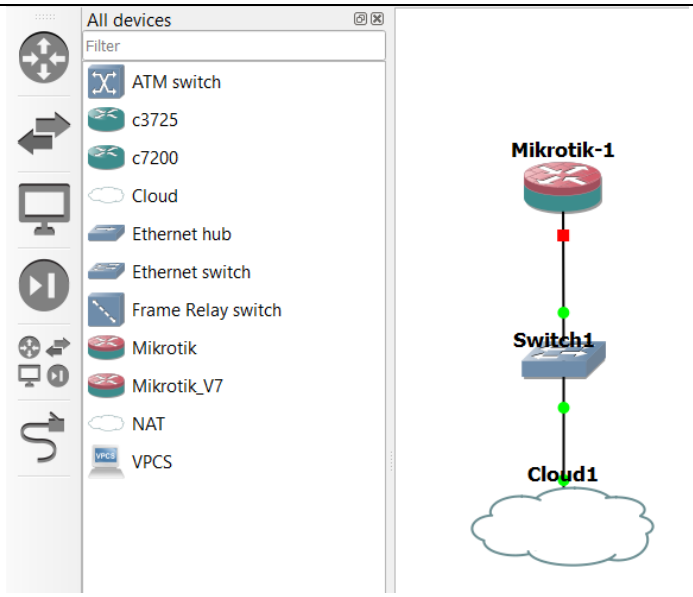


Figura 16. Topología para configurar por Winbox Router MikroTik

Nota: Para habilitar IPv6 en el Router MikroTik por consola de GNS3 ingresar los comandos *"/system package enable ipv6"* y "*system reboot*".

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. **¿Por qué es importante configurar direcciones IPv6 en las interfaces de los dispositivos de red?**
2. **¿Cuál es la importancia de verificar la conectividad IPv6 entre dispositivos de red?**

ACTIVIDADES DESARROLLADAS

(Estimado docente, a continuación, se detallan los pasos a cumplir en las instrucciones por los estudiantes)

1. **Verificación de Conectividad en Ipv6**

¿Qué información se puede obtener mediante el comando "show ipv6 route"?

Aquí usted deberá adjuntar la evidencia de la prueba de conectividad.

Respuesta:

¿Cuál es el propósito del comando "show ipv6 route static"?

Aquí usted deberá adjuntar la evidencia de la prueba de conectividad.

Respuesta:

2. **Pruebas de Conectividad**

Por ejemplo, entre el R1 y Mikrotik:

Aquí usted deberá adjuntar la evidencia de la prueba de conectividad.

Por ejemplo, entre el Mikrotik y LooKBack1:

Aquí usted deberá adjuntar la evidencia de la prueba de conectividad.

Por ejemplo, entre el LookBack2 y LoopBack3:

Aquí usted deberá adjuntar la evidencia de la prueba de conectividad.

3. **Actividad en casa**

Tabla de Direccionamiento

Equipos	Interfaz	Direccion	Prefijo de red	Gateway
R1	f0/0			
	loopback			
R2(Mikrotik)	e0			
	e1			
R3	f0/0			
	loopback			

Topología implementada en el Software GNS3

Aquí usted deberá adjuntar la evidencia de la topología implementada en el Software GNS3 etiquetada con las direcciones propias IPv6 a los dispositivos.

Nota. - *Para simular el Router Mikrotik mediante la interfaz de Winbox es necesario conectar un Switch y un Cloud a una de sus interfaces para tener salida hacia la interfaz del Terminal. Con esto mediante la Mac del Router Mikrotik se podrá loguear en Winbox tal como se muestra en la Figura 4. De no poder acceder mediante la interfaz de Winbox puede usar la consola de GNS3 para configurar como si estuviera haciendo en el Router MikroTik físico.*

Configuración Equipos

Direccionamiento y Routing **Router 1**

Aquí usted deberá adjuntar las evidencias

Direccionamiento y Routing **Router Mikrotik**

Aquí usted deberá adjuntar las evidencias

Direccionamiento y Routing **Router 3**

Aquí usted deberá adjuntar las evidencias

Verificación Conectividad

Prueba de conectividad desde Router 1 hacia Router 3

Aquí usted deberá adjuntar las evidencias

Prueba de conectividad desde Router 3 hacia Router 1

Aquí usted deberá adjuntar las evidencias

CONCLUSIONES:

BIBLIOGRAFIA:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN**
REALIZADO POR:		
CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**10**	**TÍTULO PRÁCTICA:** Enrutamiento Dinámico RIPng Router Cisco.

OBJETIVO:

- Realizar tareas de configuración básicas en un enrutador.
- Configurar direcciones IPv6 en interfaces de red de dispositivos de red.
- Activar RIPng en los Routers.
- Verificar la conectividad IPv6 y tráfico entre dispositivos de red.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

10. (3) Router Cisco
11. (2) Dispositivos con capacidad para soportar IPv6 (p. ej. computadoras)
12. (4) Cables de red Ethernet
13. (1) Cable serial

NOTA: Es necesario contar con 3 computadoras equipadas con interfaces Ethernet para llevar a cabo la práctica. Se brinda la opción de utilizar su propia computadora junto con la que se encuentra en la mesa de trabajo. En caso de no contar con dicha interfaz, se deberá disponer de adaptadores Ethernet, ya que la práctica se ha diseñado para ser ejecutada en cada estación de trabajo en el laboratorio de cómputo 8.

DESCRIPCIÓN GENERAL:

INSTRUCCIONES:

1. Esquema de la práctica a desarrollar.

En esta práctica usted deberá conectar los equipos del laboratorio de red como se muestra en la figura 1:

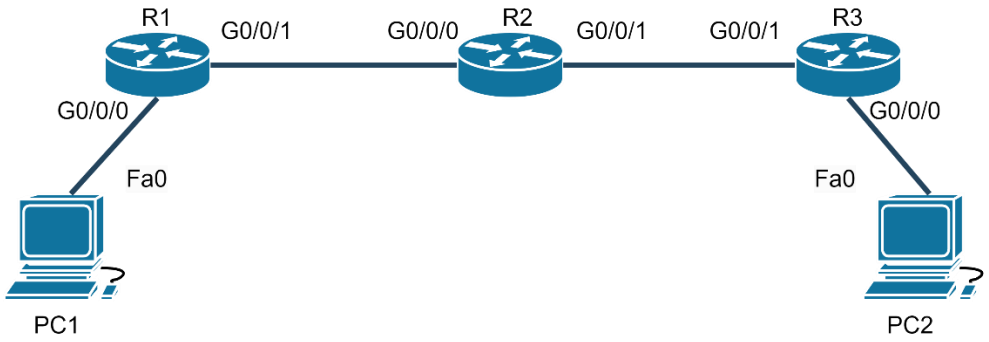


Figura 1. Topología de la red

2. Configuraciones Básicas de los Routers

1. Borre las configuraciones previas en cada uno de los Routers y reinícielos.

```
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
Router#
*Mar  1 00:01:43.367: %SYS-7-NV_BLOCK_INIT: Initialized the geometry
of nvram
Router#reload
```

2. En el Modo de configuración global, asigne un nombre al router mediante el comando **"hostname"**, seguido del nombre deseado; en este ejercicio, se empleará **"R1"** como designación para el Router 1 y **"R2"** para el Router 2 como identificador del router.

3. Configuración de direccionamiento IPv6.

Las interfaces se configurarán utilizando las direcciones presentadas en la **Tabla 1** de direccionamiento de este laboratorio, para ello realizar las siguientes instrucciones:

1. Habilite el protocolo de enrutamiento IPv6.

Nota: Es importante habilitar el protocolo de enrutamiento Ipv6 en los Routers para evitar complicaciones en el desarrollo de la práctica. Si no recuerda cómo hacerlo, se recomienda revisar practicas previas.

2. Realice la configuración de las interfaces de los Routers, asignando direcciones IPv6 de acuerdo con el direccionamiento especificado en la **Tabla 1**.

Equipos	Interfaz	Direccion	Mask	Gateway
R1	G0/0/0	2023:c8:3:3::1	/64	NA
	G0/0/1	2023:c8:1:1::1	/64	NA
R2	G0/0/0	2023:c8:1:1::2	/64	NA
	G0/0/1	2023:c8:2:2::1	/64	NA
R3	G0/0/0	2023:c8:4:4::1	/64	NA
	G0/0/1	2023:c8:2:2::2	/64	NA

Tabla 1. Tabla de direcciones IPv6

4. Configuración enrutamiento Dinámico RIPng

Una vez realizada la configuración de las direcciones IPv6 en las interfaces GigabitEthernet, configure el enrutamiento dinámico RIPng. Esta configuración permite que los routers intercambien información de enrutamiento y actualicen automáticamente sus tablas de enrutamiento para adaptarse a cambios en la topología de la red.

Para habilitar el enrutamiento RIPng en cada interfaz conectada de un enrutador, ejecute el siguiente comando: ***"ipv6 rip [proceso RIPng] enable"***

Donde:

- ***[proceso RIPng]*** se refiere al nombre del proceso que será utilizado. **En esta práctica, se designará como "ups".**

1. A continuación, se muestra la configuración para **R1**.

```
R1(config)#interface gigabitEthernet 0/0/0
R1(config-if)#ipv6 rip ups enable
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)#ipv6 rip ups enable
```

2. Repita el paso anterior, para habilitar el enrutamiento RIPng en R2 y R3.

Nota: Recuerde que para habilitar RIPng debe ingresar a cada interfaz física del Router que desee configurar**.**

5. Configuración de direcciones IPv6 en los hosts.

Configurar en cada host la dirección IPv6 y la puerta de enlace correspondiente.

Equipos	Interfaz	Direccion	Mask	Gateway
PC1	NIC	2023:c8:3:3::2	/64	2023:c8:3:3::1
PC2	NIC	2023:c8:4:4::2	/64	2023:c8:4:4::1

Tabla 2. Asignación de direcciones IPv6 en los hosts.

RECOMENDACIÓN: Es necesario verificar las configuraciones de seguridad estén desactivadas, lo que incluye tanto el Firewall de Windows como el software antivirus ya que podría surgir problemas durante la ejecución de pruebas de conectividad.

Nota: Al configurar enrutamiento dinámico RIPng se asignarán automáticamente las direcciones a los terminales (PCs). Para visualizar la dirección asignada entre al cmd del terminal e ingrese "ipconfig". Recuerde que la opción "Obtener automáticamente dirección IPv6" debe estar habilitada dentro de las propiedades del protocolo de versión 6 del terminal.

6. Verificación de conectividad en IPv6.

Realice las siguientes instrucciones y proporcione evidencia de su respuesta en la sección de Actividades Desarrolladas.

Una vez realizada la configuración del enrutamiento entre los enrutadores, se deberá verificar que la conectividad IPv6 se ha establecido correctamente realizando ping entre los terminales y verificando la tabla de enrutamiento de los routers.

1. Utilice los comandos **"show ipv6 route" y "ping" para** verificar las configuraciones y el tráfico entre los Routers.

Nota: Usted deberá realizar un análisis de la práctica en lo que respecta a las pruebas de conectividad y adjuntar evidencia de los resultados obtenidos en la parte final de la misma.

7. Actividad para el hogar

Mediante el software GNS3, realizar la topología de la Figura 2. Asegúrese de asignar direcciones propias IPv6 a los dispositivos. Proporcione evidencia de la verificación de conectividad.

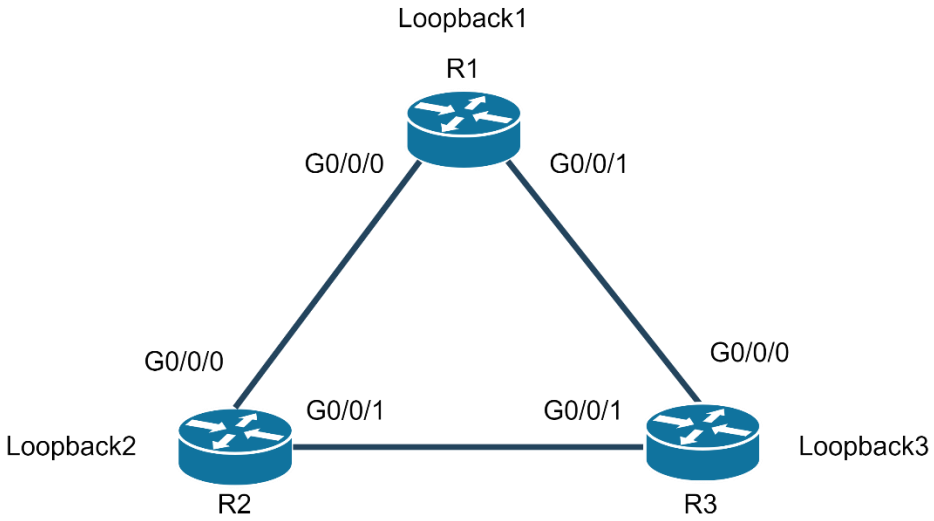


Figura 2. Topología de la Red.

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. **¿Qué ventajas tiene el enrutamiento estático en comparación con el enrutamiento dinámico?**
2. **¿Qué información se puede obtener al utilizar el comando "*show ipv6 route*"?**
3. **¿Cuándo es más apropiado utilizar enrutamiento dinámico en lugar de enrutamiento estático?**

ACTIVIDADES DESARROLLADAS

(Anotar las actividades que siguió para el desarrollo de la práctica)

1. Verificación de la conectividad

Incluya los resultados adquiridos en las pruebas de conectividad, acompañados de un análisis.

Ruta mostrada R1

Aquí usted deberá adjuntar las evidencias

Ruta mostrada R3

Aquí usted deberá adjuntar las evidencias

2. Actividad para el hogar.

Topología implementada en el Software GNS3

Configuración Router R1

Aquí usted deberá adjuntar las evidencias

Configuración Router R2

Aquí usted deberá adjuntar las evidencias

Configuración Router R3

Aquí usted deberá adjuntar las evidencias

Verificación de Conectividad

Prueba de conectividad:

Prueba de conectividad desde Router 1 hacia Router 2 y Router 3 respectivamente.

Prueba de conectividad desde Router 2 hacia Router 1 y Router 3 respectivamente.

Prueba de conectividad desde Router 3 hacia Router 1 y Router 2 respectivamente.

CONCLUSIONES:

BIBLIOGRAFIA:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN**
REALIZADO POR:		
CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**11**	**TÍTULO PRÁCTICA:** Enrutamiento Dinámico RIPng Cisco y Mikrotik

OBJETIVO:

- Configurar direcciones IPv6 en interfaces de red de dispositivos de red.
- Configurar enrutamiento Dinámico IPv6 en dispositivos de red.
- Activar RIPng en los Routers.
- Verificar la conectividad IPv6 entre dispositivos de red.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

1. (2) Routers Cisco
2. (1) Router Mikrotik
3. (2) Cables de red Ethernet
4. (1) Cable Serial

DESCRIPCIÓN GENERAL:

En esta práctica, se lleva a cabo la configuración del enrutamiento dinámico RIPng en una red IPv6, con un enfoque específico en la configuración del Router MikroTik. Este proceso implica establecer y gestionar rutas automáticamente a través del protocolo RIPng en el entorno de IPv6, facilitando la comunicación eficiente entre los dispositivos en la red.

Conocimientos Requeridos para el desarrollo de la práctica: Configuración Enrutamiento Dinámico RIPng con Router Cisco.

INSTRUCCIONES:

1. Esquema de la práctica a desarrollar.

En esta práctica usted deberá conectar los equipos del laboratorio de red como se muestra en la **Figura 1.**

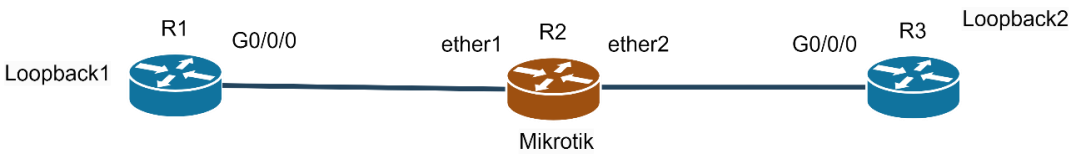


Figura 1. Topología de la red

2. Configuraciones Básicas de los Routers

1. Borre las configuraciones previas en cada uno de los Routers y reinícielos.
2. Cambie los nombres de los Routers según la Topología de la **Figura 1.**

3. Configuración de direccionamiento IPv6.

Las interfaces se configurarán utilizando las direcciones presentadas en la **Tabla 1** de direccionamiento de este laboratorio, para ello realizar las siguientes instrucciones:

1. Habilite el protocolo de enrutamiento IPv6 para los **Routers Cisco** y revise si se encuentra habilitado en el **Router Mikrotik** de no ser así, habilítelo.
Nota: Es importante habilitar el protocolo de enrutamiento Ipv6 en los Routers para evitar complicaciones en el desarrollo de la práctica. Si no recuerda cómo hacerlo, se recomienda revisar practicas previas.
2. Realice la configuración de las interfaces de los Routers, asignando direcciones IPv6 de acuerdo con el direccionamiento especificado en la **Tabla 1**.

Tabla de Direccionamiento

Equipos	Interfaz	Direccion	Prefijo de red	Gateway

R1	G0/0/0	2023:ae:c8:1::1	/64	NA
	Loopback1	2023:ae:c8:3::1	/64	NA
R2(Mikrotik)	ether1	2023:ae:c8:1::2	/64	NA
	ether2	2023:ae:c8:2::1	/64	NA
R3	G0/0/0	2023:ae:c8:2::2	/64	NA
	Loopback2	2023:ae:c8:4::1	/64	NA

Tabla 1. Direcciones IPv6

4. Configuración enrutamiento Dinámico RIPng

1. En los **Routers Cisco** configure el enrutamiento dinámico RIPng con el nombre del proceso "ups". Si tiene complicaciones con las configuraciones se recomienda revisar practicas previas.
2. Para configurar RIPng en el **Router MikroTik** debe ingresar el siguiente comando:

"/routing ripng interface add interface= [interfaz correspondiente]"

A diferencia del Router Cisco, en Mikrotik no se debe ingresar en cada interfaz para habilitar RIPng. Se asigna el direccionamiento Ipv6 y luego se habilita el enrutamiento RIPng indicando el nombre de la interfaz.
3. Identificar la interfaz ether para la habilitación de RIPng.
En la **Figura 1** se observa que el Router MikroTik tiene conectadas sus interfaces **ether1** y **ether2**. Estas interfaces serán habilitadas con RIPng.
4. Habilitar RIPng en el Router Mikrotik.

Habilitación RIPng

*[admin@MikroTik] > /routing ripng interface add interface=**ether1***
*[admin@MikroTik] > /routing ripng interface add interface=**ether2***

5. Verificación de conectividad en IPv6.

Realice las siguientes instrucciones y proporcione evidencia de su respuesta en la sección de Actividades Desarrolladas.
1. Haga un ping con carga entre R1 y R2 y diga que diferencias encuentra entre el ping normal.
2. Mediante el comando "show ipv6 neighbors" identifique los neighbors IPv6 que encontraron los Routers Cisco. Para ver los neighbors en el Router Mikrotik utilice el comando "/ipv6 neighbor print".
3. Ingresa el comando "show ipv6 protocols" y responde ¿Qué puedes observar?
4. Ingresa el comando" /ipv6 route print" en el Router MikroTik e indica en qué estado se encuentran las interfaces.
Nota: Recuerde que usted deberá realizar un análisis de la práctica en lo que respecta a las pruebas de conectividad y adjuntar evidencia de los resultados obtenidos en la parte final de la misma.

6. Actividad en Casa

1. Realice la configuración en GNS3 del enrutamiento RIPng, proponga una topología usando dos Routers Mikrotik y un Router Cisco. Realizar su propia tabla de direccionamiento.
2. Realice ping desde los terminales, para ello instale máquinas virtuales de los terminales para simular en GNS3, puede utilizar Virtual Box o VMware.
3. Proporcione evidencia de la configuración y verificación de conectividad.
4. Analice el ping con carga para 100000 bytes y 10000 bytes y diga que sucede según su resultado.

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. **Explique brevemente cómo habilitaría RIPng en un Router Cisco y qué comandos usaría para verificar la información de enrutamiento.**
2. **¿Cuál es la diferencia clave entre RIPng y RIP?**
3. **¿Por qué podría optar por usar RIPng en lugar de OSPFv3 en una red IPv6?**

4. Explique el propósito de la métrica en RIPng.

ACTIVIDADES DESARROLLADAS

(Anotar las actividades que siguió para el desarrollo de la práctica)

1. Verificación de conectividad en IPv6

Router 1

Aquí las evidencias de la verificación de conectividad y comandos.

Router 2

Aquí las evidencias de la verificación de conectividad y comandos.

Router 3

Aquí las evidencias de la verificación de conectividad y comandos.

Análisis. –

Aquí el análisis de los comandos ejecutados en los Routers

2. Actividad en Casa

Topología implementada en el Software GNS3

Aquí su topología

Tabla de Direccionamiento
(Si es necesario, usted puede modificar la tabla conforme a su topología)

Equipos	Interfaz	Direccion	Mask	Gateway
R1				
R2				
R3				

Tabla 2. Tabla Direccionamiento IPv6

Configuraciones

Aquí las configuraciones realizadas en el simulador de GNS3

Pruebas de Conectividad

Pruebas de conectividad desde Terminal de Windows hacia el Terminal Ubuntu y Loopback Router 2

Aquí las pruebas de conectividad

Análisis ping con carga

Aquí colocar una captura de una terminal virtual que usted prefiera con el ping de carga para 100,000 bytes y 10,000 bytes. No olvide realizar el respectivo análisis.

CONCLUSIONES:

BIBLIOGRAFIA:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN**
REALIZADO POR:		
CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**12**	**TÍTULO PRÁCTICA:** Enrutamiento Estático y Dinámico RIPng Router Cisco y Mikrotik.

OBJETIVO:

- Configurar direcciones IPv6 en interfaces de red de dispositivos de red.
- Configurar enrutamiento estático IPv6 en dispositivos de red.
- Activar RIPng en los Routers.
- Activar Rutas Estáticas
- Verificar la conectividad IPv6 entre dispositivos de red.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

5. (2) Routers Cisco
6. (1) Router MikroTik
7. (4) Cables de red Ethernet
8. (1) Cable Serial

DESCRIPCIÓN GENERAL: En esta práctica se realizará la asignación de direcciones IPv6 y la configuración de rutas dinámicas utilizando el protocolo RIPng, así como rutas estáticas, en Routers Cisco y MikroTik. Además, se llevará a cabo la verificación del tráfico en las rutas configuradas. El objetivo principal es proporcionar una experiencia práctica en la implementación de configuraciones de enrutamiento IPv6, tanto estático como dinámico, y evaluar el funcionamiento del tráfico en estas rutas.

Conocimientos Requeridos para el desarrollo de la práctica: Configuración Enrutamiento Estático y Dinámico con Routers Cisco y MikroTik.

INSTRUCCIONES:

1. Esquema de la práctica a desarrollar.

En esta práctica usted deberá conectar los equipos del laboratorio de red como se muestra en la **Figura 1.**

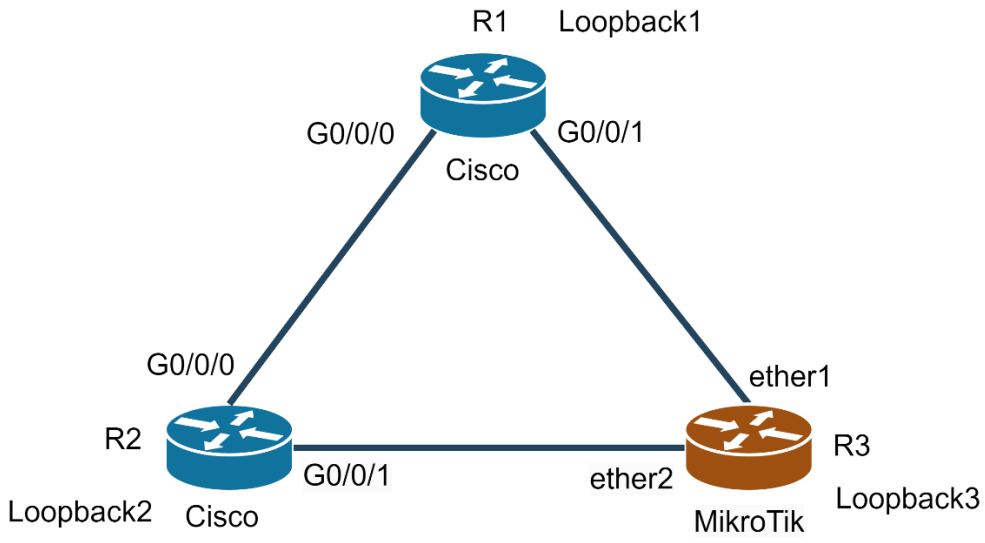


Figura 1. Topología de la red

2. Configuraciones Básicas de los Routers

1. Borre las configuraciones previas en cada uno de los Routers y reinícielos.
2. Cambie los nombres de los Routers según la Topología de la **Figura 1.**

3. Configuración de direccionamiento IPv6

Las interfaces se configurarán utilizando las direcciones presentadas en la **Tabla 1** de direccionamiento de este laboratorio. Para ello realizar las siguientes instrucciones:

1. Habilite el protocolo de enrutamiento IPv6 para los **Routers Cisco** y revise si se encuentra habilitado en el **Router Mikrotik** de no ser así, habilítelo.
2. Realice la configuración de las interfaces de los Routers, asignando direcciones IPv6 de acuerdo con el direccionamiento especificado en la **Tabla 1**.

Tabla de direccionamiento

Equipos	Interfaz	Direccion	Mask	Gateway
R1	G0/0/0	2001:db8:1:1::1	/64	NA
	G0/0/1	2001:db8:2:2::1	/64	NA
R2	G0/0/0	2001:db8:1:1::2	/64	NA
	G0/0/1	2001:db8:3:3::1	/64	NA
R3(Mikrotik)	ether1	2001:db8:2:2::2	/64	NA
	ether2	2001:db8:3:3::2	/64	NA
LoopBack1	R1	2001:db8:4:4::2	/64	
LoopBack2	R2	2001:db8:5:5::2	/64	
LoopBack3	R3	2001:db8:6:6::2	/64	

Tabla 1. Direcciones IPv6

4. Configuración Enrutamiento Estático

Para el enrutamiento estático usted deberá configurar una ruta estática sin redistribución de rutas entre el Router 2 (Cisco) y el Router 3 (Mikrotik). A continuación, se indica el procedimiento:

1. Configure **enrutamiento estático** en el Router 2(Cisco) hacia el Router 3 (MikroTik).
Nota: Recuerde que para realizar la configuración usted debe ingresar la red de destino y el siguiente salto para llegar a la red de destino. Esto permite al Router establecer una ruta específica y fija para dirigir el tráfico hacia esa red en particular.
Router Cisco (R2)

```
R2(config)#ipv6 route 2001:db8:6:6::/64 2001:db8:3:3::2
```

2.Configure **enrutamiento estático** en el Router 3 (Mikrotik) hacia el Router 2 (Cisco)
Router Mikrotik

```
[admin@MikroTik] >/ipv6 route add dst-address=2001:db8:5:5::/64
gateway=2001:db8:3:3::1
```

5. Configuración Enrutamiento Dinámico

1. En los **Routers Cisco 1 y 2** configure el enrutamiento dinámico RIPng con el nombre del proceso "ups". Si tiene complicaciones con las configuraciones se recomienda revisar las practicas previas.
2. Configure enrutamiento RIPng en el Router 3 (Mikrotik).

6. Verificación de conectividad en IPv6.

Realice las siguientes instrucciones y proporcione evidencia de su respuesta en la sección de Actividades Desarrolladas.

1. Verificar la ruta del tráfico del enrutamiento estático mediante el comando "traceroute (*dirección IPv6*)".
2. Realice ping sostenido desde R2 hacia R1. Ahora desconecte la interfaz G0/0/0 de R1 y responda: ¿Por qué no tiene respuesta de R1 sabiendo que R2 se encuentra conectado a R3 y R3 a R1?

7. Actividad en Casa

1. En el software de GNS3 simule la topología de la Figura 1., cambie las loopbacks 1 y 3 por terminales Virtuales. Realice ping con carga y analice el tiempo de convergencia entre la ruta por RIPng y Enrutamiento Estático.

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. En qué escenario se recomienda usar enrutamiento estático con enrutamiento dinámico.

2. **¿Cuándo elegiría utilizar enrutamiento dinámico RIPng en lugar de enrutamiento estático en una red IPv6?**
3. **¿Cuáles son las ventajas y desventajas de utilizar enrutamiento dinámico (RIPng) en comparación con enrutamiento estático?**
4. **Explique las diferencias clave entre enrutamiento estático y dinámico y proporcione un escenario en el que sería más apropiado utilizar enrutamiento estático.**

ACTIVIDADES DESARROLLADAS

(Anotar las actividades que siguió para el desarrollo de la práctica)

1. **Verificación de Conectividad**

Ruta del enrutamiento estático

Aquí las evidencias de la verificación y ruta del enrutamiento estático

Análisis. – *Aquí el análisis del resultado del comando "traceroute"*

¿Por qué no tiene respuesta de R1 sabiendo que R2 se encuentra conectado a R3 y este a R1?

2. **Actividad en Casa**

Topología implementada en el Software GNS3

Aquí la topología en GNS3

Configuraciones

Aquí las configuraciones realizadas en el simulador de GNS3

Asignación Direcciones IPv6 a los Terminales

Aquí capturas del direccionamiento IPv6 en los Terminales Virtuales

Pruebas de Conectividad

Analizas de los tiempos de convergencia entre la ruta por RIPng y Enrutamiento Estático.

Aquí las pruebas de conectividad por ruta estática y ruta dinámica RIPng

Análisis

Aquí el análisis de lo obtenido en las pruebas de conectividad.

CONCLUSIONES:

BIBLIOGRAFIA:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN**
REALIZADO POR:		
CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**13**	**TÍTULO PRÁCTICA:** Enrutamiento Dinámico OSPFv3 Router Cisco.

OBJETIVO:

- Configurar direcciones IPv6 en interfaces de red de dispositivos de red.
- Configurar enrutamiento dinámico IPv6 en dispositivos de red.
- Activar OSPFv3 en los Routers.
- Análisis de Paquetes OSPFv3 mediante Wireshark.
- Verificar la conectividad IPv6 entre dispositivos de red.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

9. (3) Routers Cisco
10. (3) Cables de red Ethernet
11. (1) Cable Serial
12. Dispositivos con capacidad para soportar IPv6 (p. ej. computadoras)

DESCRIPCIÓN GENERAL:

Esta práctica se centra en el Enrutamiento Dinámico mediante OSPFv3 en Routers Cisco. Incluye la implementación y análisis detallado de este protocolo, destacando la configuración y el seguimiento del tráfico mediante herramientas como Wireshark en el entorno simulado de GNS3.

Conocimientos Requeridos para el desarrollo de la práctica: Asignación de Direcciones IPv6 con Router Cisco y conexión física entre dos estaciones de trabajo.

INSTRUCCIONES:

1. Esquema de la práctica a desarrollar.

En esta práctica usted deberá conectar los equipos del laboratorio de red como se muestra en la **Figura 1** utilizando dos estaciones de trabajo para conectar **3 Routers Cisco.**

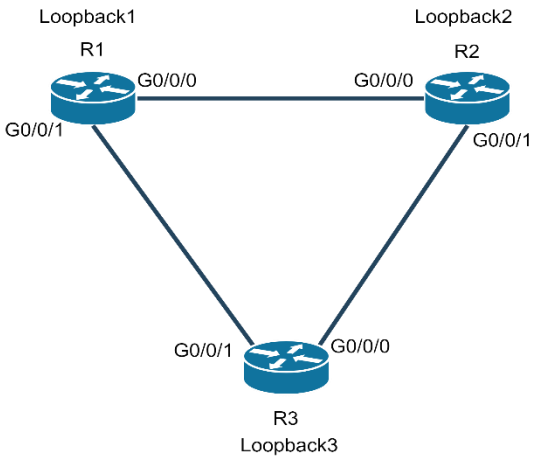


Figura 1. Topología de la red

2. Configuraciones Básicas de los Routers

1. Borre las configuraciones previas en cada uno de los Routers y reinícielos.

2. Cambie los nombres de los Routers según la Topología de la **Figura 1.**

3. Configuración de direccionamiento IPv6.

Las interfaces se configurarán utilizando las direcciones presentadas en la **Tabla 1** de direccionamiento de este laboratorio, para ello realizar las siguientes instrucciones:

1. Habilite el protocolo de enrutamiento IPv6.

Nota: Es importante habilitar el protocolo de enrutamiento Ipv6 en los Routers para evitar complicaciones en el desarrollo de la práctica. Si no recuerda cómo hacerlo, se recomienda revisar practicas previas.

2. Realice la configuración de las interfaces y Loopbacks de los Routers, asignando direcciones IPv6 de acuerdo con el direccionamiento especificado en la **Tabla 1**.

Tabla de Direccionamiento IPv6

Equipos	Interfaz	Direccion	Mask	Gateway
R1	G0/0/0	2023:ae:c8:1::1	/64	NA
	G0/0/1	2023:ae:c8:3::1	/64	NA
	Loopback1	2023:ae:c8:4::1	/64	NA
R2	G0/0/0	2023:ae:c8:1::2	/64	NA
	G0/0/1	2023:ae:c8:2::1	/64	NA
	Loopback2	2023:ae:c8:5::1	/64	NA
R3	G0/0/0	2023:ae:c8:2::2	/64	NA
	G0/0/1	2023:ae:c8:3::2	/64	NA
	Loopback3	2023:ae:c8:6::1	/64	NA

Tabla 1. Direcciones IPv6

4. Configuración enrutamiento Dinámico OSPFv3

Una vez realizada la configuración de las direcciones IPv6 en las interfaces GigabitEthernet, se debe realizar la configuración del enrutamiento OSPFv3. Esta configuración permite a los Routers realizar el intercambio de paquetes "Hello" OSPF, actualización de enlace y la creación de una base de datos topológica. Esto proporciona la capacidad de determinar las rutas más eficientes a través de la red y actualizar sus tablas de enrutamiento en consecuencia.

Los comandos que se utilizan para la configuración de OSPFv3 son los siguientes:

Este comando permite acceder al modo de configuración de OSPFv3
Router(config)# "ipv6 router ospf [Número de proceso de 1 - 65535]"

Donde

- **Numero de proceso:** Este proceso permite identificar el número de proceso que será asignado a la topología, permitiendo al enrutamiento dinámico OSPFv3 reconocer en qué Routers está habilitado. El número de proceso es un valor que oscila entre 1 y 65535. Este número actúa como un identificador único para el proceso OSPFv3 en la configuración de enrutamiento de los Routers, lo que facilita la gestión y la identificación en el entorno de la red.

Router(config-rtr)#"router-id [Identificador de enrutador] "
Router(config-rtr)# "no shutdown"

Donde

- **Identificador de enrutador:** corresponde al identificador único del Router que se está configurando. Este identificador puede ser una dirección IPv4 en formato decimal con puntos (por ejemplo, 192.168.1.1) o un valor decimal (por ejemplo, 1.1.1.1).
  Es esencial señalar que el Router ID debe ser único en todo el dominio OSPF. Si no se especifica manualmente un Router ID, OSPFv3 seleccionará automáticamente uno basado en las direcciones IP de las interfaces del Router. Se recomienda configurar manualmente el Router ID para tener un control más preciso sobre su valor y evitar cambios inesperados.

Router(config)# "interface gigabitEthernet [interfaz]"
Router(config-if)# "ipv6 ospf [Número de proceso] área [número de área]"

Donde

- **Interfaz:** Pertenece a cada interfaz GigabitEthernet y loopback de los Routers.
- **Numero de proceso:** Es el identificador único para el proceso OSPFv3 que se asignó al habilitar por primera vez el enrutamiento dinámico OSPFv3.
- **Numero de área:** OSPFv3 segmenta la red en áreas con el objetivo de mejorar la escalabilidad. Cada área funciona de manera semi-independiente, lo que disminuye la carga de información de enrutamiento que cada Router necesita procesar.

Para esta práctica, **el número de proceso utilizado será de 1**, un **router-id en formato ip (1.1.1.1)** y el número de **área 0.**

A continuación, se detalla los pasos para la configuración de OSPFv3 en el **Router Cisco R1**:

1. Ingresar al modo de configuración global y acceder al modo de configuración de OSPFv3. No olvidar elegir el número de proceso para la configuración de OSPFv3.

```
R1(config)#ipv6 router ospf 1
```

2. Asignar el Router ID, recuerde que el router-id es único para cada router, se recomienda usar para **R1= 1.1.1.1** para **R2=2.2.2.2** para **R3=3.3.3.3**

```
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#no shutdown
R1(config-rtr)#exit
```

3. Ingresar a cada interfaz gigabitEthernet y loopback según la **tabla 1** para configurar cada interfaz con OSPFv3. Aquí se asignará el **número de proceso de 1** y el **número de área de 0**.

```
R1(config)#interface loopback 0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#exit
R1(config)#interface gigabitEthernet 0/0/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#exit
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#exit
```

4. Configurar para cada Router Cisco el enrutamiento dinámico OSPFv3 siguiendo los pasos 1-3.

5. Verificación de conectividad en IPv6.

Realice las siguientes instrucciones y proporcione evidencia de su respuesta en la sección de Actividades Desarrolladas.

Después de haber configurado el enrutamiento OSPFv3, es necesario comprobar que la conectividad IPv6 se ha establecido correctamente.

1. Ingrese el comando “Traceroute” desde el Router 1 con dirección a la loopback del Router 3. Identifique la ruta del tráfico para llegar desde la Loobpack1 hacia la Loopback3.

2. Desconectar la interfaz G0/0/1 del Router 3 y vuelva a repetir el paso anterior.

3. Conecte la interfaz G0/0/1 del Router 3 y en la topología de la **Figura 1** identifique los Routers BD, BDR y en caso de existir el Router DROther. Utilice los comandos " show ipv6 ospf neighbor " y “show ipv6 ospf interface”.

6. Actividad en casa

1. Mediante el Software de GNS3 realizar la topología de la red de la **Figura 1.,** use las direcciones IPv6 de la práctica y habilite el enrutamiento dinámico OSPFv3.

2.Descargue e Instale la herramienta Wireshark para ello siga los siguientes pasos:

- Abra el navegador y escriba "Wireshark Download", luego acceda a la página.

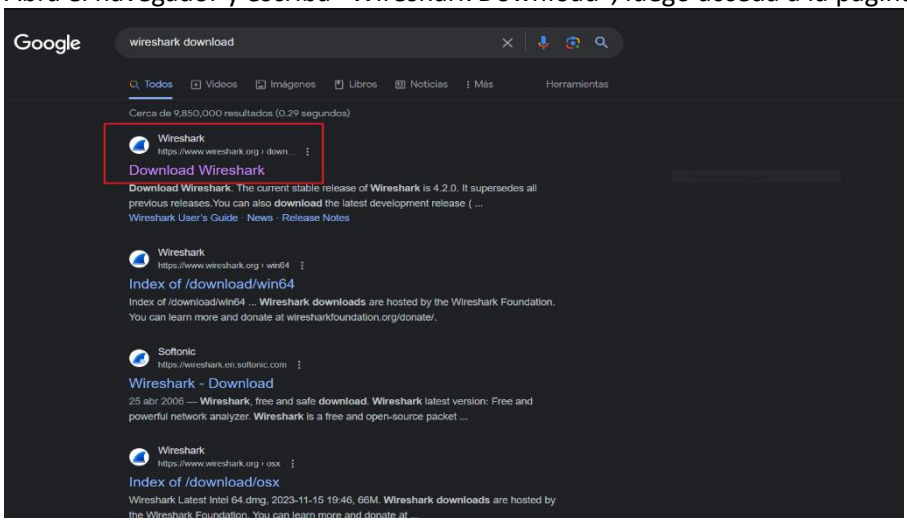


Figura 2. Pagina de instalación de Wireshark

- Seleccione la opción “Windows x64 Installer” para Windows.

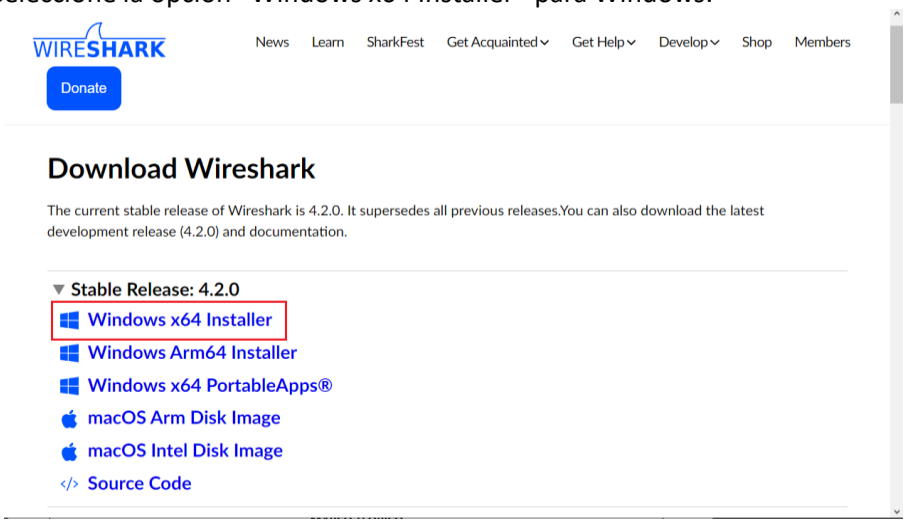


Figura 3.Instalador para Windows

- En la pantalla se presentará una ventana donde se descargará el instalador. Haga clic en "Guardar".

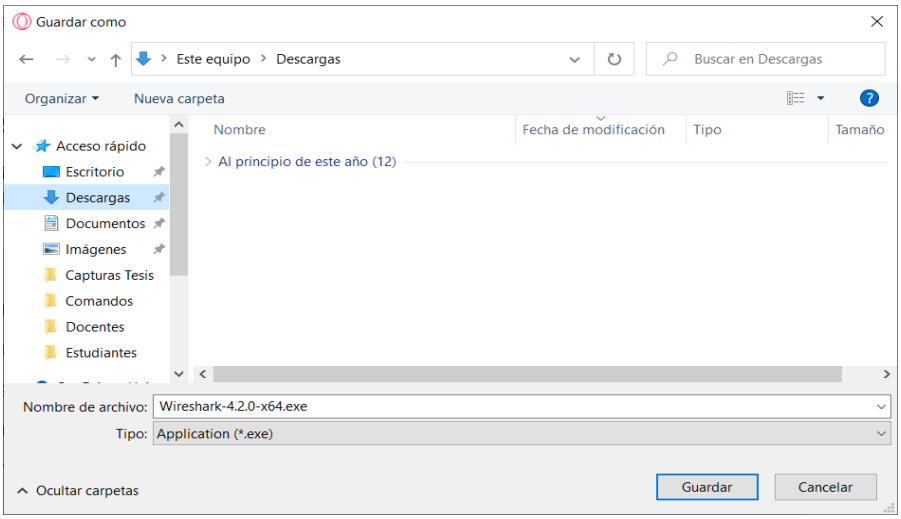


Figura 4.Ubicacion de Instalador de Wireshark

- Haga doble clic en el instalador de Wireshark e instale siguiendo los pasos sugeridos por el asistente de instalación de Wireshark.

3. Mediante Wireshark **analice e identifique los paquetes OSPFv3** en cualquier enlace de la topología de la **Figura 1.** Usted podrá identificar los paquetes OSPF “Hello” , paquete LS con la información de los costes y los neighbords. Para ello siga los siguientes pasos:

- Dar clic izquierdo sobre un enlace y seleccionar la opción “start capture”. Para analizar los paquetes OSPFv3 en la topología de GNS3.

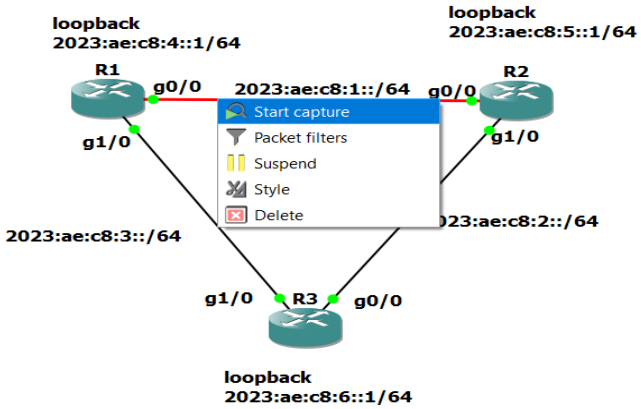


Figura 5.Configuracion de captura de tráfico con Wireshark

- En pantalla se presentará la siguiente ventana indicando el tipo de interfaz a capturar y el nombre del archivo. Dar clic en “OK”

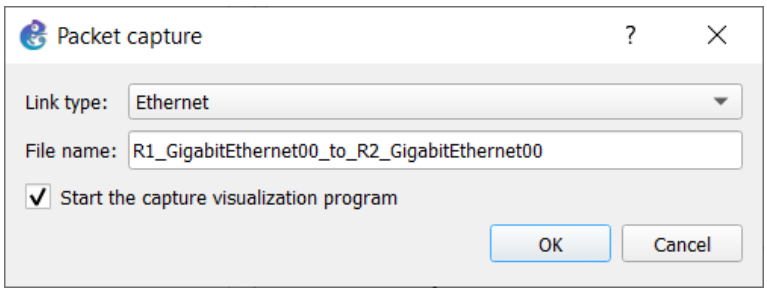


Figura 6. Configuración Captura de Trafico

- En la pantalla se abrirá la ventana de Wireshark y comenzará a capturar el tráfico a través del enlace seleccionado. Para evitar problemas al capturar el tráfico se recomienda configurar la captura de tráfico de GNS3 como “Wireshark Traditional Capture”. Esto se puede realizar dentro del software GNS3, haciendo clic en “Edit>Preferences>Packet Capture> Wireshark Traditional Capture>Set>Apply>OK”.

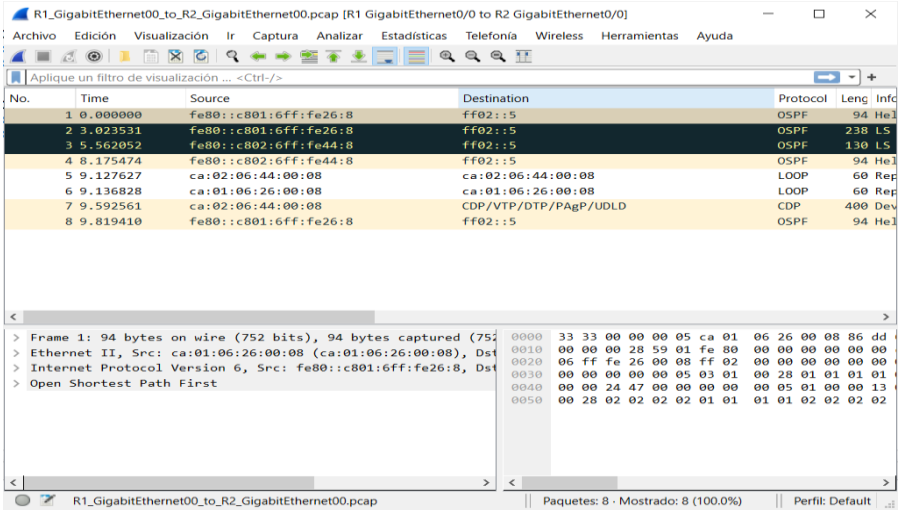


Figura 7. Captura de Trafico con Wireshark

- Hacer clic en "Recargar este archivo" en la interfaz del software Wireshark. Para actualizar la visualización del tráfico de los paquetes OSPFv3 y los paquetes ICMPv6.

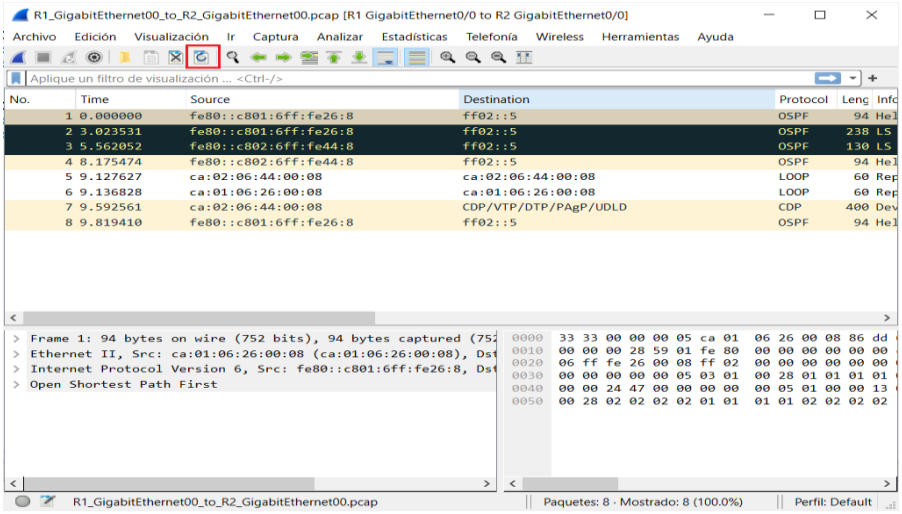


Figura 8. Actualización de Trafico en Wireshark

- Hacer doble clic sobre un paquete, se abrirá una ventana que presenta toda la información detallada del paquete.

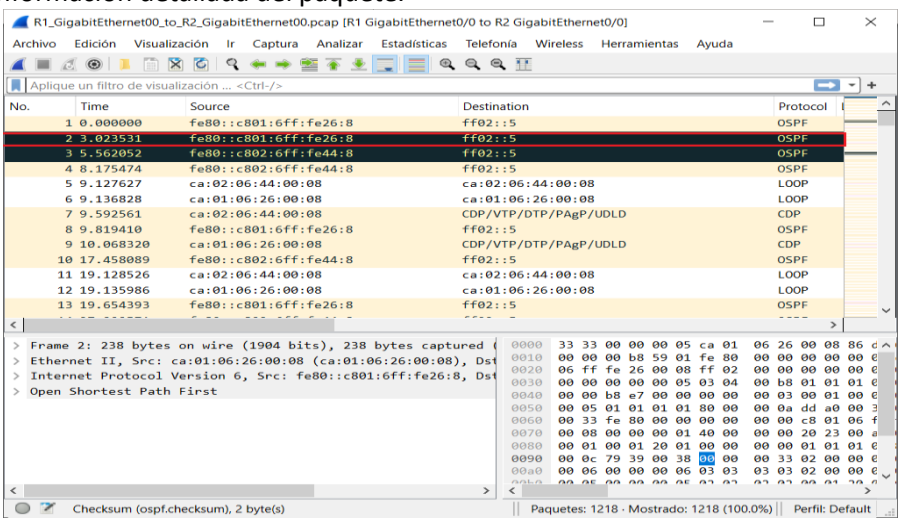


Figura 9. Selección de Paquete OSPF

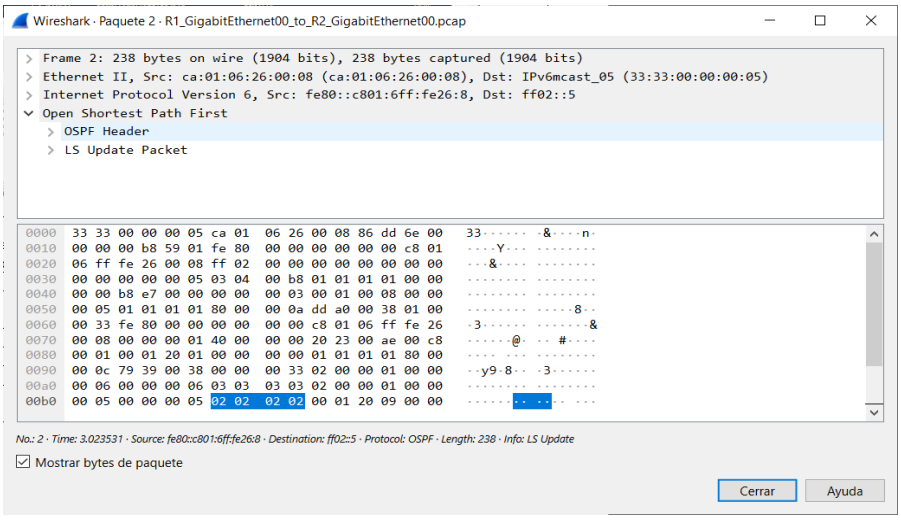


Figura 10. Detalles del Paquete OSPF seleccionado

Con estos pasos usted puede realizar el análisis del tráfico de cualquier topología implementada en GNS3.

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. **¿Cuál es el propósito principal del protocolo OSPFv3 en una red IPv6 y cuáles son los beneficios clave que ofrece?**
2. **Explica la función del Router ID en OSPFv3 y cómo se puede configurar en un Router Cisco.**
3. **¿Cuáles son las principales diferencias entre OSPFv2 y OSPFv3 en términos de enrutamiento IPv6?**
4. **Describe el proceso de elección del DR y BDR en OSPFv3 y su importancia en redes con segmentos de broadcast.**

ACTIVIDADES DESARROLLADAS

(Anotar las actividades que siguió para el desarrollo de la práctica)

1. **Verificación de Conectividad en Ipv6**

Captura de ruta desde Loopback1 hacia Loopback3

Aquí las pruebas de conectividad

Análisis:

Aquí el análisis de las pruebas de conectividad

Captura de ruta desde Loopback1 hacia Loopback3 con la interfaz G0/0/1 de R3 desconectada.

Aquí las pruebas de conectividad

Análisis:

Aquí el análisis de las pruebas de conectividad

Captura de los Routers BD y BDR

Aquí las pruebas de conectividad

Análisis:

Aquí el análisis de las pruebas de conectividad

2. **Actividad en Casa**

Aquí la topología de la red implementada en GNS3

Tabla de Direccionamiento

Equipos	Interfaz	Direccion	Mask	Gateway

Tabla 2. Tabla de Direcciones IPv6

Configuraciones

Router 1

Aquí las configuraciones del Router

Router 2

Aquí las configuraciones del Router

Router 3

Aquí las configuraciones del Router

Análisis Paquetes OSPF con Wireshark *Aquí las capturas de los paquetes en Wireshark y análisis.*
CONCLUSIONES:
BIBLIOGRAFIA:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN**
REALIZADO POR:		
CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**14**	**TÍTULO PRÁCTICA:** Enrutamiento Dinámico OSPFv3 Router Cisco y Mikrotik.

OBJETIVO:

- Configurar direcciones IPv6 en interfaces de red de dispositivos de red.
- Configurar enrutamiento estático IPv6 en dispositivos de red.
- Activar OSPFv3 en los Routers.
- Verificar la conectividad IPv6 entre dispositivos de red.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

13. (1) Router MikroTik
14. (2) Routers Cisco
15. (4) Cables de red Ethernet
16. (1) Cable Serial
17. (2) Dispositivos con capacidad para soportar IPv6 (p. ej. computadoras)

DESCRIPCIÓN GENERAL:

En esta práctica de Enrutamiento Dinámico OSPFv3 con Routers Cisco y MikroTik, se llevó a cabo la configuración y análisis de rutas dinámicas utilizando el protocolo OSPFv3. La actividad incluyó pruebas de conectividad entre Routers de diferentes fabricantes y la observación de la interacción entre ellos.

Conocimientos Requeridos para el desarrollo de la práctica: Asignación de Direcciones IPv6 con Router Cisco y Configuración Enrutamiento Dinámico OSPFv3 en Router Cisco.

INSTRUCCIONES:

1. Esquema de la práctica a desarrollar.

En esta práctica usted deberá conectar los equipos del laboratorio de red como se muestra en la **Figura 1.**

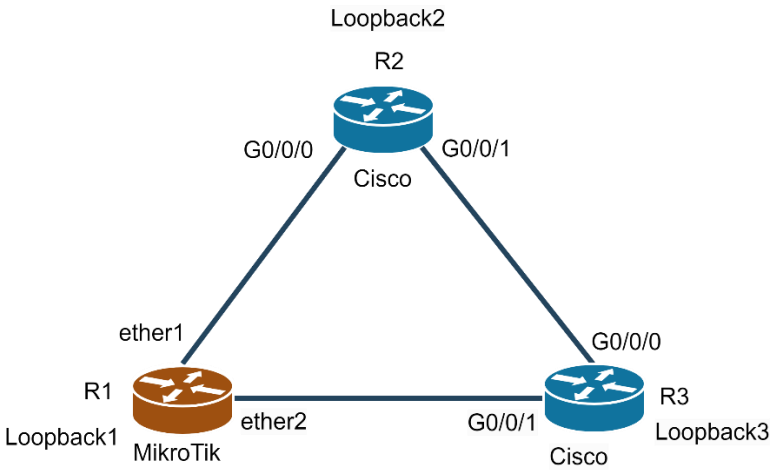


Figura 1. Topología de la red

2. Configuraciones Básicas de los Routers

1. Borre las configuraciones previas en cada uno de los Routers y reinícielos.

2. Cambie los nombres de los Routers según la Topología de la **Figura 1.**

3. Configuración de direccionamiento IPv6.

Las interfaces se configurarán utilizando las direcciones presentadas en la **Tabla 1** de direccionamiento de este laboratorio. para ello realizar las siguientes instrucciones:

1. Habilite el protocolo de enrutamiento IPv6 para los **Routers Cisco** y revise si se encuentra habilitado en el **Router Mikrotik** de no ser así, habilítelo.

Nota: Es importante habilitar el protocolo de enrutamiento Ipv6 en los Routers para evitar complicaciones en el desarrollo de la práctica. Si no recuerda cómo hacerlo, se recomienda revisar practicas previas.

2. Realice la configuración de las interfaces y Loopbacks de los Routers, asignando direcciones IPv6 de acuerdo con el direccionamiento especificado en la **Tabla 1**.

Tabla de Direccionamiento

Equipos	Interfaz	Direccion	Mask	Gateway
R1(Mikrotik)	ether1	2023:ae:c8:1::1	/64	NA
	ether2	2023:ae:c8:6::1	/64	NA
	Loopback1	2023:ae:c8:3::1	/64	NA
R2(Cisco)	G0/0/0	2023:ae:c8:1::2	/64	NA
	G0/0/1	2023:ae:c8:2::1	/64	NA
	Loopback2	2023:ae:c8:5::1	/64	NA
R3(Cisco)	G0/0/0	2023:ae:c8:2::2	/64	NA
	G0/0/1	2023:ae:c8:6::2	/64	NA
	Loopback3	2023:ae:c8:4::1	/64	NA

Tabla 1. Tabla de Direccionamiento IPv6

4. Configuración enrutamiento Dinámico OSPFv3

Para esta práctica, **el número de proceso utilizado será de 1**, un **router-id en formato ip (1.1.1.1)** y el número de **área 0.**

Configuración en Router Cisco.

A continuación, se detalla los pasos para la configuración de OSPFv3 en los **Routers Cisco:**

5. Ingresar al modo de configuración global y acceder al modo de configuración de OSPFv3. No olvidar elegir el número de proceso para la configuración de OSPFv3.

```
R2(config)#ipv6 router ospf 1
```

6. Asignar el Router ID, recuerde que el router-id es único para cada Router, se recomienda usar para **R1= 1.1.1.1** para **R2=2.2.2.2** para **R3=3.3.3.3**

```
R2(config-rtr)#R1-id 2.2.2.2
R2(config-rtr)#no shutdown
R2(config-rtr)#exit
```

7. Ingresar a cada interfaz gigabitEthernet y loopback según la **tabla 1** para configurar cada interfaz con OSPFv3. Aquí se asignará el **número de proceso de 1** y el **número de área de 0**.

```
R2(config)#interface loopback 2
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#exit
R2(config)#interface gigabitEthernet 0/0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#exit
R2(config)#interface gigabitEthernet 0/0/1
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#exit
```

8. Configurar para cada Router Cisco el enrutamiento dinámico OSPFv3 siguiendo los pasos 1-3.

Configuración en Router MikroTik.

Para habilitar OSPFv3 en los Routers MikroTik se utilizan los siguientes comandos:

```
"/routing ospf-v3 instance set [ find default=yes] redistribute-connected=as-type-1 router-id=[identificador de enrutador]"
```

Donde:

- **"/routing ospf-v3 instance":** Indica que se está trabajando con la configuración del proceso OSPFv3.
- **"set [find default=yes]"**: Establece la configuración para la instancia de OSPFv3 que está marcada como predeterminada (default). Es decir, modifica la configuración de la instancia OSPFv3 que se utiliza de manera predeterminada en el Router.
- **"redistribute-connected=as-type-1":** Configura la redistribución de las rutas conectadas al OSPFv3. as-type-1 se refiere al tipo de área de OSPFv3, y en este caso, indica que las rutas conectadas se redistribuirán como rutas de tipo 1 en OSPFv3.
- **"router-id=[identificador de enrutador]":** Establece el ID del Router OSPFv3. Cada Router en un dominio OSPFv3 debe tener un ID único. El ID del Router es importante para la identificación única del Router en el área OSPFv3.

```
"/routing ospf-v3 interface add interface=[interfaz] area=backbone"
```

Donde:

- **"/routing ospf-v3 interface add":** Agrega una interfaz al proceso OSPFv3.
- **"interface=[interfaz]":** Especifica la interfaz a la que se va a aplicar la configuración OSPFv3. Debes reemplazar "[interfaz]" con el nombre de la interfaz específica, por ejemplo, "ether1".
- **"area=backbone":** Asigna la interfaz al área llamada "backbone". En OSPF, un área es una parte lógica de la topología de la red, y el área de backbone (área 0) es fundamental en la jerarquía de áreas.

A continuación, se detalla los pasos para la configuración de OSPFv3 en el **Router MikroTik:**

1. Habilitar el protocolo OSPFv3 y el Router ID sugerido para R1=1.1.1.1.

```
[admin@MikroTik] > /routing ospf-v3 instance set [ find default=yes ] redistribute-connected=as-type-1 router-id=1.1.1.1
```

2. Para cada interfaz de R1(MikroTik) configurar OSPFv3 y designar el área 0 (backbone)

```
[admin@MikroTik] > /routing ospf-v3 interface add interface=Loopback1 area=backbone
[admin@MikroTik] >/routing ospf-v3 interface add interface=ether1 area=backbone
[admin@MikroTik] >/routing ospf-v3 interface add interface=ether2 area=backbone
```

5. Verificación de conectividad en IPv6.

Realice las siguientes instrucciones y proporcione evidencia de su respuesta en la sección de Actividades Desarrolladas.

1. En la topología de la **Figura 1 para los Routers Cisco** identifique los Routers BD, BDR. Utilice los comandos " show ipv6 ospf neighbor " y "show ipv6 ospf interface".

6. Actividad para el hogar

1. Mediante el Software de GNS3 realizar la siguiente topología de la **figura 2** usando únicamente Routers Mikrotik y máquinas virtuales, puede usar cualquier sistema operativo (Windows o Linux) para simular las máquinas virtuales. Asigne direccionamiento IPv6 y configure enrutamiento dinámico OSPFv3.

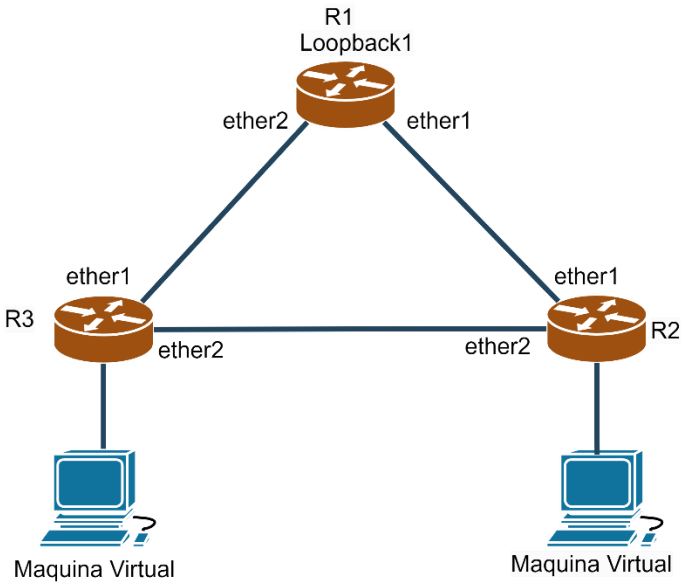


Figura 2. Topología de implementación en GNS3

3. Investigue los comandos para visualizar la información del enrutamiento dinámico OSPv3 (DR,BDR,area) para el Router MikroTik.
2. Mediante Wireshark capture el tráfico entre las máquinas virtuales y analice los paquetes OSPFv3.

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. **¿Cuáles son las diferencias clave entre OSPFv2 y OSPFv3 en relación al enrutamiento IPv6?**
2. **¿Cuáles son los tipos de área admitidos por OSPFv3?**
3. **¿Cómo se configura OSPFv3 para el enrutamiento IPv6 en un router? Describe los pasos clave involucrados.**
4. **¿Cómo se verifica y soluciona problemas en el enrutamiento OSPFv3 para el enrutamiento IPv6? Menciona algunas herramientas o comandos útiles para el diagnóstico.**

ACTIVIDADES DESARROLLADAS

(Anotar las actividades que siguió para el desarrollo de la práctica)

7. **Verificación de Conectividad en Ipv6**

Captura de los Routers BD y BDR

Aquí las pruebas de conectividad

Análisis:

Aquí el análisis de las pruebas de conectividad

8. **Actividad en Casa**

Aquí la tipología de la red implementada en GNS3

Tabla de Direccionamiento

Equipos	Interfaz	Direccion	Mask	Gateway

Tabla 2. Tabla de Direcciones

Configuraciones

Router 1

Aquí las configuraciones del Router

Router 2

Aquí las configuraciones del Router

Router 3

Aquí las configuraciones del Router

Comandos para verificación de OSPFv3 en MikroTik

- ¿Qué comando encontró para verificar los Routers BD, DBR y el Área?

Aquí su respuesta

[admin@MikroTik] > Aquí el resultado de los comandos de verificación para Routers BD, BDR y Área.

Análisis Paquetes OSPF con Wireshark

Aquí las capturas de los paquetes en Wireshark y su respectivo análisis.

CONCLUSIONES:

BIBLIOGRAFIA:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN**
REALIZADO POR:		
CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**15**	**TÍTULO PRÁCTICA:** Enrutamiento Dinámico EIGRPv3 Router Cisco.

OBJETIVO:

- Configurar direcciones IPv6 en interfaces de red de dispositivos de red.
- Configurar enrutamiento estático IPv6 en dispositivos de red.
- Activar EIGRPv3 en los Routers.
- Verificar la conectividad IPv6 entre dispositivos de red.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

18. (3) Routers Cisco
19. (2) Cables de red Ethernet
20. (1) Cable Serial

DESCRIPCIÓN GENERAL:

En esta práctica, se configurará aspectos específicos de EIGRPv3, adaptado para el soporte de IPv6, proporcionando una solución eficaz para el enrutamiento dinámico en redes que emplean este protocolo. La actividad incluyó pruebas de conectividad entre Routers Cisco.

Conocimientos Requeridos para el desarrollo de la práctica: Asignación de Direcciones IPv6 con Router Cisco y conexión física entre los puestos de trabajo.

INSTRUCCIONES:

1. Esquema de la práctica a desarrollar.

En esta práctica usted deberá conectar los equipos del laboratorio de red como se muestra en la **Figura 1.**

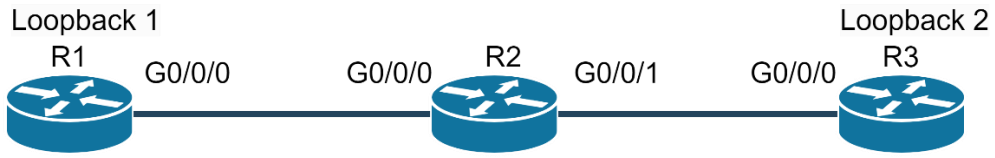


Figura 1. Topología de la red

2. Configuraciones Básicas de los Routers

1. Borre las configuraciones previas en cada uno de los Routers y reinícielos.

2. Cambie los nombres de los Routers según la Topología de la **Figura 1.**

3. Configuración de direccionamiento IPv6.

Las interfaces se configurarán utilizando las direcciones presentadas en la **Tabla 1** de direccionamiento de este laboratorio. para ello realizar las siguientes instrucciones:

1. Habilite el protocolo de enrutamiento IPv6

Nota: Es importante habilitar el protocolo de enrutamiento Ipv6 en los Routers para evitar complicaciones en el desarrollo de la práctica. Si no recuerda cómo hacerlo, se recomienda revisar practicas previas.

2. Realice la configuración de las interfaces y Loopbacks de los Routers, asignando direcciones IPv6 de acuerdo con el direccionamiento especificado en la **Tabla 1**.

Tabla de Direccionamiento IPv6

Equipos	Interfaz	Direccion	Mask	Gateway
R1	G0/0/0	2023:ae:c8:1::1	/64	NA
	Loopback1	2023:ae:c8:3::1	/64	NA
R2	G0/0/0	2023:ae:c8:1::2	/64	NA
	G0/0/1	2023:ae:c8:2::1	/64	NA
R3	G0/0/0	2023:ae:c8:2::2	/64	NA

	Loopback2	2023:ae:c8:4::1	/64	NA

Tabla 1. Direccione IPv6

4. Configuración enrutamiento dinámico EIGRPv3

Los comandos que se utilizan para la configuración de OSPFv3 son los siguientes:

```
Router(config)# ipv6 router eigrp [Número del sistema autónomo 1 – (2^32 – 1)]
```

Donde

- **Número del sistema autónomo:** Permite proporcionar el número de sistema autónomo (AS) para EIGRPv6. El número de sistema autónomo es un valor único que identifica a un sistema autónomo en una red EIGRP. Debe coincidir en todos los routers dentro del mismo dominio de enrutamiento EIGRPv6 para que puedan intercambiar información de enrutamiento.

```
Router(config-rtr)#eigrp router-id [Identificador de enrutador como una dirección IPv4]
Router(config-rtr)# no shutdown
```

Donde

- **Identificador de enrutador como una dirección IPv4:** Aquí debes proporcionar un identificador de enrutador, que generalmente es una dirección IPv4. Este identificador se utiliza para distinguir un router EIGRP de otros en el mismo sistema autónomo.
  Es importante destacar que el Router ID debe ser único dentro del sistema autónomo EIGRP y, si no se configura manualmente, el router elegirá automáticamente uno basado en la interfaz más alta de dirección IPv4. Configurar manualmente el Router ID es útil en escenarios donde se necesita un control específico sobre el ID del router.

```
Router(config)# "interface gigabitEthernet [interfaz]"
Router(config-if)# "ipv6 eigrp [Numero del sistema autónomo]"
```

Donde

- **Interfaz:** Pertenece a cada interfaz GigabitEthernet y loopback de los Routers.
- **Número del sistema autónomo:** Es el identificador que se configuro previamente para distinguir un Router EIGRP de otros en el mismo sistema autónomo.

Para esta práctica, el proceso de enrutamiento utilizará un **sistema autónomo de 100** y un **router-id en formato ip (1.1.1.1)**

A continuación, se detalla los pasos para la configuración de OSPFv3 en el **Router Cisco R1**:

9. Ingresar al modo de configuración global y acceder al modo de configuración de EIGRPv3. No olvidar elegir el **número del sistema autónomo** para la configuración de EIGRPv3.

```
R1(config)#ipv6 router eigrp 100
```

10. Asignar el Router ID, recuerde que el router-id es único para cada router, se recomienda usar para **R1= 1.1.1.1** para **R2=2.2.2.2** para **R3=3.3.3.3**

```
R1(config-rtr)#eigrp router-id 1.1.1.1
R1(config-rtr)#no shutdown
R1(config-rtr)#exit
```

11. Ingresar a cada interfaz gigabitEthernet y loopback según la **tabla 1** para configurar cada interfaz con EIGRPv3. Aquí se asignará el **número del sistema autónomo configurado previamente.**

```
R1(config)#interface loopback 0
R1(config-if)#ipv6 eigrp 100
R1(config-if)#exit
R1(config)#interface gigabitEthernet 0/0/0
R1(config-if)# ipv6 eigrp 100
```

```
R1(config-if)#exit
```

12. Configurar para cada Router Cisco el enrutamiento dinámico EIGRPv3 siguiendo los pasos 1-3.

5. Verificación de conectividad en IPv6.

Realice las siguientes instrucciones y proporcione evidencia de su respuesta en la sección de Actividades Desarrolladas.

- Una vez el protocolo de enrutamiento es activado en cada enrutador y converge, la red es completamente operativa. Utilice el comando **"show IPv6 route" para verificar** que todas las redes sean conocidas por todos los enrutadores de la red. Debe haber conectividad exitosa entre el dispositivo final y el enrutador. Utilice el comando **ping para verificar el correcto funcionamiento de la red.**

6. Actividad para el hogar

Mediante el Software de GNS3 realizar la topología de la Red de la Figura 2. Asignar Direccionamiento IPv6 dada la siguiente tabla 2.

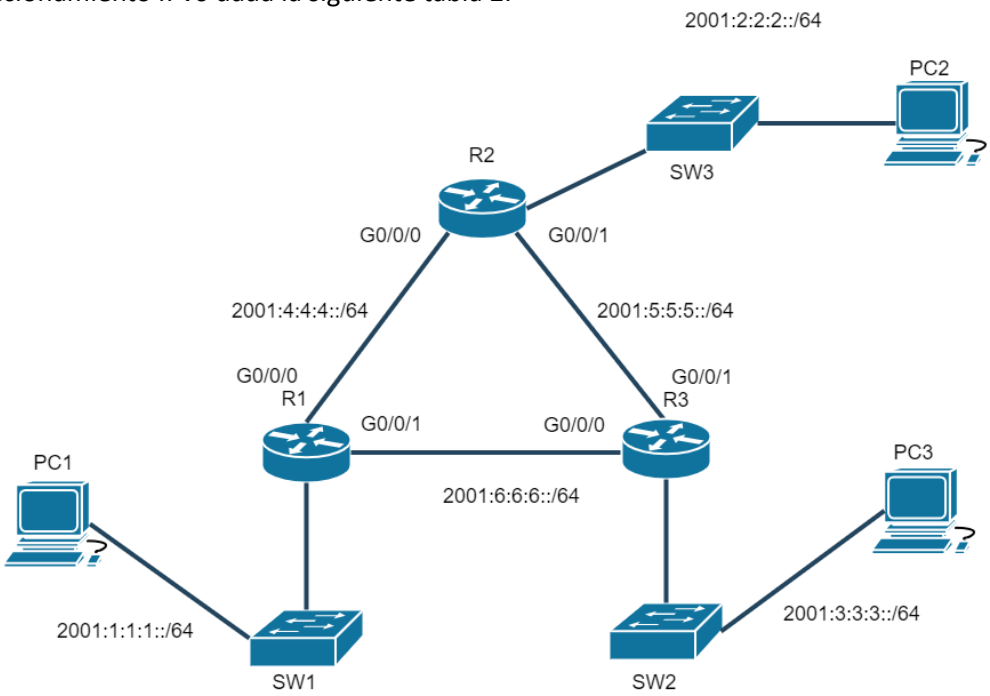


Figura 2. Topología de la red

Equipos	Interfaz	Direccion	Mask	Gateway
R1	Fa0/0	2001:4:4:4::1	/64	NA
	Fa0/1	2001:6:6:6::1	/64	NA
	Fa1/0	2001:1:1:1::1	/64	NA
R2	Fa0/0	2001:4:4:4::2	/64	NA
	Fa0/1	2001:5:5:5::1	/64	NA
	Fa1/0	2001:2:2:2::1	/64	NA
R3	Fa0/0	2001:6:6:6::2	/64	NA
	Fa0/1	2001:5:5:5::2	/64	NA
	Fa1/0	2001:3:3:3::1	/64	NA
PC1		2001:1:1:1::2	/64	2001:1:1:1::1
PC2		2001:2:2:2::2	/64	2001:2:2:2::1
PC3		2001:3:3:3::2	/64	2001:3:3:3::1

Tabla 2. Tablas de direccionamiento IPv6.

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. **¿Cuál es el propósito de utilizar la palabra clave "no auto-summary" al configurar EIGRPv3 en un router Cisco?**
2. **¿Cuál es la diferencia entre EIGRPv3 y EIGRPv4?**
3. **¿Por qué es importante configurar el ID de proceso EIGRPv3 al configurar el enrutamiento dinámico en un router Cisco?**

ACTIVIDADES DESARROLLADAS

Anotar las actividades que siguió para el desarrollo de la práctica)

1. **Verificación de Conectividad**

Ping desde Loopback1 hacia Loopback2

Aqui las pruebas de conectividad

Ping desde Loopback2 hacia Loopback1

Aquí las pruebas de conectividad

2. **Actividad para el Hogar**

Aquí la topología de la Red implementada en GNS3

Configuración R1

Aquí las configuraciones respectivas del Router

Configuración R2

Aquí las configuraciones respectivas del Router

Configuración R3

Aquí las configuraciones respectivas del Router

Verificación de Conectividad

Prueba de conexión desde PC1 hacia PC2 y PC3

Aquí las pruebas de conectividad

Prueba de conexión desde PC2 hacia PC1 y PC3

Aquí las pruebas de conectividad

Prueba de conexión desde PC3 hacia PC1 y PC3

Aquí las pruebas de conectividad

CONCLUSIONES:

BIBLIOGRAFIA:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN**
REALIZADO POR:		
CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**16**	**TÍTULO PRÁCTICA:** Enrutamiento Dinámico IS-IS Router Cisco.

OBJETIVO:

- Configurar direcciones IPv6 en interfaces de red de dispositivos de red.
- Configurar enrutamiento dinámico IS-IS.
- Configurar Intra-area e Inter-area según la topología.
- Verificar la conectividad IPv6 entre dispositivos de red.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

1. (2) Routers Cisco
2. (1) Cables de red Ethernet
3. (1) Cable Serial

DESCRIPCIÓN GENERAL:

En esta práctica, se abordarán aspectos clave, como la configuración de IS-IS en el router, la definición de áreas y la interconexión con otros routers. Además, se explorará cómo el protocolo IS-IS se adapta y reacciona a cambios en la topología de la red, proporcionando una visión detallada de cómo se establecen y mantienen las rutas dinámicamente.

Conocimientos Requeridos para el desarrollo de la práctica: Asignación de Direcciones IPv6 con Router Cisco.

INSTRUCCIONES

1. Esquema de la práctica a desarrollar.

En esta práctica usted deberá conectar los equipos del laboratorio de red como se muestra en la figura 1:

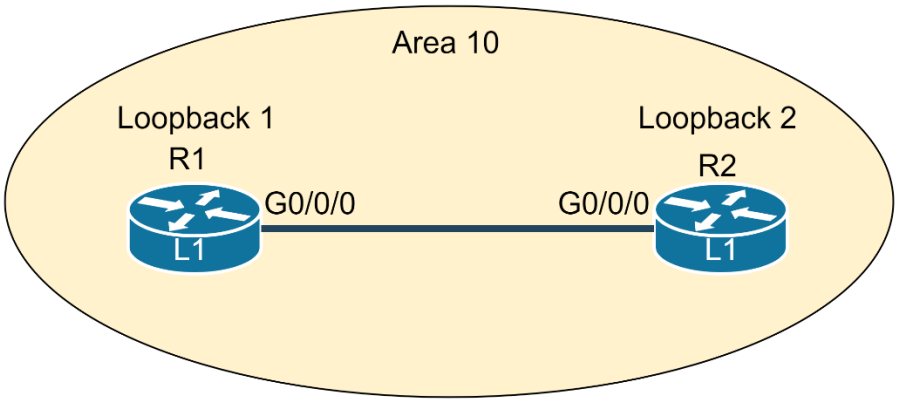


Figura 1. Topología de la red

2. Configuraciones Básicas de los Routers

1. Borre las configuraciones previas en cada uno de los Routers y reinícielos.

2. En el Modo de configuración global, asigne un nombre al router mediante el comando **"hostname"**, seguido del nombre deseado; en este ejercicio, se empleará **"R1"** como designación para el Router 1 y **"R2"** para el Router 2 como identificador del router.

3. Configuración de direccionamiento IPv6.

Las interfaces se configurarán utilizando las direcciones presentadas en la **Tabla 1** de direccionamiento de este laboratorio, para ello realizar las siguientes instrucciones:

1. Habilite el protocolo de enrutamiento IPv6.

Nota: Es importante habilitar el protocolo de enrutamiento Ipv6 en los Routers para evitar complicaciones en el desarrollo de la práctica. Si no recuerda cómo hacerlo, se recomienda revisar practicas previas.

2. Realice la configuración de las interfaces de los Routers, asignando direcciones IPv6 de acuerdo con el direccionamiento especificado en la **Tabla 1**.

Equipos	Interfaz	Direccion	Mask	Gateway
R1(L1)	G0/0/0	2023:c8:1:1::1	/64	NA
	Loopback1	2023:c8:4:4::1	/64	NA
R2(L1)	G0/0/0	2023:c8:1:1::2	/64	NA
	Loopback2	2023:c8:5:5::1	/64	NA

Tabla 1. Tabla de direcciones IPv6

4. Configuración enrutamiento Dinámico IS-IS

Una vez que se ha completado la configuración de las direcciones IPv6 en las interfaces GigabitEthernet, se procede a llevar a cabo la configuración del enrutamiento IS-IS. Este paso implica establecer y ajustar los parámetros necesarios para que el protocolo IS-IS (Intermediate System to Intermediate System) pueda gestionar y distribuir información de enrutamiento de manera eficiente en la red IPv6 configurada.

A continuación, se detallan los comandos para habilitar el enrutamiento IS-IS:

"router isis [etiqueta]"

Donde:

- ***[etiqueta]:*** Este es un parámetro opcional. Puede especificar una etiqueta para el proceso ISIS. Es un identificador alfanumérico significativo localmente que ayuda a distinguir entre múltiples instancias de IS-IS en el mismo Router.

"net <NET_ID> <AREA_ID>"

Donde:

- **NET_ID(IDP)**: Este campo representa la identificación de red. Es un valor hexadecimal que identifica de manera única una red IS-IS.
- **AREA_ID(DSP)**: Este campo especifica el ID del área a la que pertenece la red.

En IS-IS, se emplea el formato NSAP (Network Service Access Point) que consta de dos partes: IDP (Initial Domain Part) y DSP (Domain-Specific Part). Este formato se utiliza para identificar cada nodo, es decir, para diferenciar los Routers en la red. La estructura del formato es la siguiente:

IDP	**DSP**		
AFI	Área	System ID	NSEL
49	0200	0000.0100.0000	00

Tabla 2. Formato NSAP

IDP: **49** es el identificador privado utilizado para definir IS-IS.
DSP: se especifica el **área de la red**, un **ID para el sistema** y **NSEL** que para TCP/IP siempre es **00**.

"metric-style wide"

Donde:

- **metric-style-wide:** este comando permite habilitar una métrica extendida de 32 bits para proporcionar una mayor precisión en la representación de los costos de ruta.

"is-type level-1"
ó

	"is-type level-2-only" ***ó*** ***"is-type level-1-2"*** Donde: • **is-type level-1:** Al utilizar el comando is-type level-1, estás configurando el router para que sea de tipo Nivel-1 en una red IS-IS de múltiples niveles. Esto implica que el router se centrará en la información de enrutamiento dentro de su área local y no se preocupa por la topología más allá de esa área. • **is-type level-2-only:** Al utilizar el comando is-type level-2-only, estás configurando el router para que opere como un router de nivel 2. Esto implica que el router se centrará en el enrutamiento entre áreas IS-IS y proporcionará conectividad entre ellas. • **is-type level-1-2:** Al utilizar el comando is-type level-1-2, se está configurando el router para el nivel 1 como el nivel 2 de IS-IS. Esto significa que el router puede funcionar como un router de nivel 1 dentro de un área IS-IS y también puede intercambiar información de enrutamiento con routers fuera del área en el nivel 2. ***"interface GigabitEthernet[interfaz]"*** ***"ipv6 router isis [etiqueta]"*** **Nota: Es importante este comando ya que permite habilitar IS-IS en cada interfaz física del Router que se desee configurar.** Donde: • **interfaz:** Pertenece a cada interfaz GigabitEthernet y loopback de los Routers. • **etiqueta:** Es el nombre de la etiqueta del proceso IS-IS que se configuro previamente. ***"isis network point-to-point"*** **Este comando permite configurar el tipo de red como Point to Point (P2P), es importante configurar correctamente en cada interfaz física del Router.** **Nota**: No es necesario ingresar ningún comando para configurar el tipo de red como **Broadcast en un router Cisco**, ya que la configuración predeterminada suele ser Broadcast. Si la red requiere específicamente el tipo de red Broadcast, generalmente se detecta automáticamente, y el comando mencionado puede no ser necesario en este caso. Donde: • **point-to-point:** Este comando indica que la interfaz se conecta directamente a otro router sin la presencia de un dispositivo de red intermedio, como un switch. Además, en IS-IS, si se configura un enlace point to point, no hay necesidad de realizar la elección de un Designated Router (DR) o Backup Designated Router (BDR), ya que estos conceptos suelen aplicarse en enlaces de difusión. ***"isis circuit-type [level-1]"*** ***ó*** ***"isis circuit-type [level-2-only]"*** **Donde:** • **level-1:** Este comando configura la interfaz para participar únicamente en el nivel 1 de IS-IS. En IS-IS, hay dos niveles jerárquicos: nivel 1 (intra-área) y nivel 2 (inter-área). Configurar una interfaz como level-1 significa que esta interfaz participará solo en el nivel 1 y no intercambiará información de nivel 2. • **Level-2-only:** Este es un parámetro opcional que indica que el circuito se utilizará solo para el nivel 2 de IS-IS. Si no se proporciona esta opción, la interfaz admitirá tanto el nivel 1 como el nivel 2.

A continuación, se muestra la configuración para **R1:**

1. Ingresar al modo configuración del protocolo IS-IS. **En esta práctica, el nombre del proceso se designará como "ups" para ambos Routers.**

```
R1(config)#router isis ups
```

2. Configurar el número de red IS-IS, Área, ID para el sistema y NSEL para TCP/IP. **En esta práctica se configura en el área 10 y un ID de sistema 1 para R1. Para el ID de R2 configure como 2.**

Según el formato NSAP el formato es el siguiente:

Red ISIS	*Area*	*ID Sistema*	*NSEL*
49.	0010.	0000.0000.0001.	00

```
R1(config-router)# net 49.0010.0000.0000.0001.00
```

Nota: Recuerde, que el ID del sistema es único y deberá respetar el formato NSAP.

3. Establecer el estilo métrico como "wide".

```
R1(config-router)#metric-style wide
```

4. Configurar el tipo de IS-IS como nivel 1, en la figura 1 se observa que los 2 routers serán configurados como L1(nivel1).

```
R1(config-router)#is-type level-1
R1(config-router)#exit
```

5. Acceder al modo de configuración de la interfaces GigabitEthernet y Loopback del router para configurar y habilitar cada interfaz con IS-IS.

Router 1

Habilitación y Configuración de IS-IS en interfaz G0/0/0

- Habilitar IS-IS en la interfaz

```
R1(config)#interface gigabitEthernet 0/0/0
R1(config-if)#ipv6 router isis ups
```

- Configurar en esta topología el enlace como una red P2P

```
R1(config-if)#isis network point-to-point
```

Nota: Dependiendo de la topología que usted vaya a configurar puede modificar el tipo de red a su conveniencia, ya sea P2P o Broadcast. **Para esta práctica el tipo de red elegido es P2P para ambos Routers.**

- Configurar la interfaz como nivel 1 (intra-área)

```
R1(config-if)#isis circuit-type level-1
```

Habilitación de IS-IS en interfaz loopback

- Habilitar IS-IS en la interfaz

```
R1(config)#interface loopback 0
R1(config-if)#ipv6 router isis ups
```

6. Repita los pasos anteriores (1-5), para habilitar el enrutamiento IS-IS en R2.

5. Verificación de conectividad en IPv6.

Realice las siguientes instrucciones y proporcione evidencia de su respuesta en la sección de Actividades Desarrolladas.

Una vez realizada la configuración del enrutamiento entre los enrutadores, se deberá verificar que la conectividad IPv6 se ha establecido correctamente realizando ping entre las interfaces de loopback y verificando configuración del enrutamiento IS-IS en los routers.

1. Utilice los comandos **"show ipv6 route" y "ping"** para verificar las configuraciones y el tráfico entre los Routers.
2. Utilice los siguientes comandos para la verificación de IS-IS. Proporcione evidencia del resultado de cada comando:

```
"show isis topology"
```

Función: Este comando mostrará la tabla de enrutamiento IS-IS para IPv6, que lista las rutas aprendidas por IS-IS.

"show isis neighbors"

Función: Este comando mostrará información sobre los vecinos IS-IS para IPv6, incluyendo el estado de la relación y otra información relevante.

Nota: Recuerde que usted deberá realizar un análisis de la práctica en lo que respecta a las pruebas de conectividad y adjuntar evidencia de los resultados obtenidos en la parte final de la misma.

6. Actividad para el hogar

1. Mediante el software GNS3, realizar la topología de la Figura 2. Asignar direcciones IPv6 de acuerdo con la información especificada en la Tabla 3.

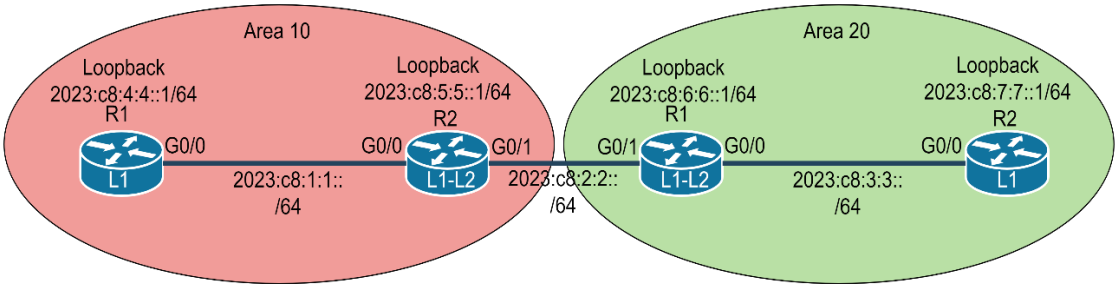


Figura 2. Topología de la Red.

Equipos	Interfaz	Direccion	Mask	Area
R1	G0/0	2023:c8:1:1::1	/64	10
	Loopback	2023:c8:4:4::1	/64	10
R2	G0/0	2023:c8:1:1::2	/64	10
	G0/1	2023:c8:2:2::1	/64	10
	Loopback	2023:c8:5:5::1	/64	10
R1	G0/0	2023:c8:3:3::1	/64	20
	G0/1	2023:c8:2:2::2	/64	20
	Loopback	2023:c8:6:6::1	/64	20
R2	G0/0	2023:c8:3:3::2	/64	20
	Loopback	2023:c8:7:7::1	/64	20

Tabla 3. Direcciones IPv6

2. Habilitar y configurar el protocolo IS-IS según el tipo de sistema (Intra-area y Inter-area) para cada Router de acuerdo a la topología de la red de la Figura 2. El tipo de red para la topología será de Broadcast.

3. Mediante Wireshark realizar un análisis de los paquetes IS-IS de la topología de la Figura 2. A continuación se muestra un ejemplo del análisis en Wireshark de los paquetes IS-IS para la topología de la Figura 1:

- En la figura 3, se pueden observar los encabezados de los mensajes de ISIS, que siguen el estándar ISO 10589 con un ID de protocolo de 0x83 asociado a ISIS. Todos los encabezados incluyen el tipo de PDU (Protocol Data Unit) que se está transmitiendo. El PDU en este encabezado específico tiene un tipo de mensaje 17, correspondiente a un PDU de tipo P2P Hello.

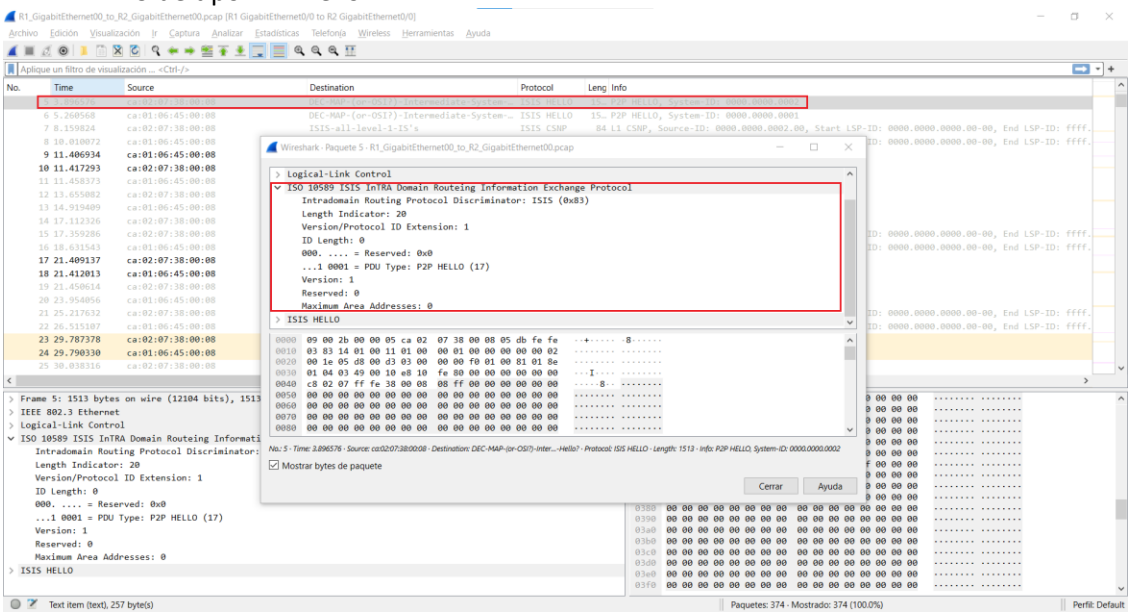


Figura 3. Mensajes y Encabezados ISIS

- En la Tabla 4 que se presenta a continuación, se detallan los tipos de Unidades de Datos de Protocolo (PDU). En el contexto de la topología representada en la Figura 1, el tipo de PDU es 17. Esto se debe a que, al configurar ISIS, se seleccionó la topología de red como punto a punto (P2P).

Tipo de PDU	Nombre
15	Level 1 LAN Hello
16	Level 2 LAN Hello
17	P2P Hello
18	Level 1 Link State PDU
20	Level 2 Link State PDU
24	Level 1 CSNP
25	Level 2 CSNP
26	Level 1 PSNP
27	Level 2 PSNP

Tabla 4. Tipos de PDU

- Los intercambios de mensajes que se llevan a cabo al configurar ISIS son de la siguiente manera:

R1 envía un mensaje IIH (IS-IS Hello)
R2 envía un mensaje IIH (IS-IS Hello)
R1 envía su base de datos con un CNSP
R2 envía su base de datos con un CNSP
R1 envía actualizaciones con un PSNP
R2 envía actualizaciones con un PSNP

Tabla 5. Intercambios mensajes ISIS

- En la Figura 4, se pueden visualizar los intercambios de mensajes IS-IS Hello y CNSP entre los routers. El mensaje de actualización PSNP se enviará en cuando haya modificaciones en las topologías, con el propósito de que los routers actualicen sus bases de datos.

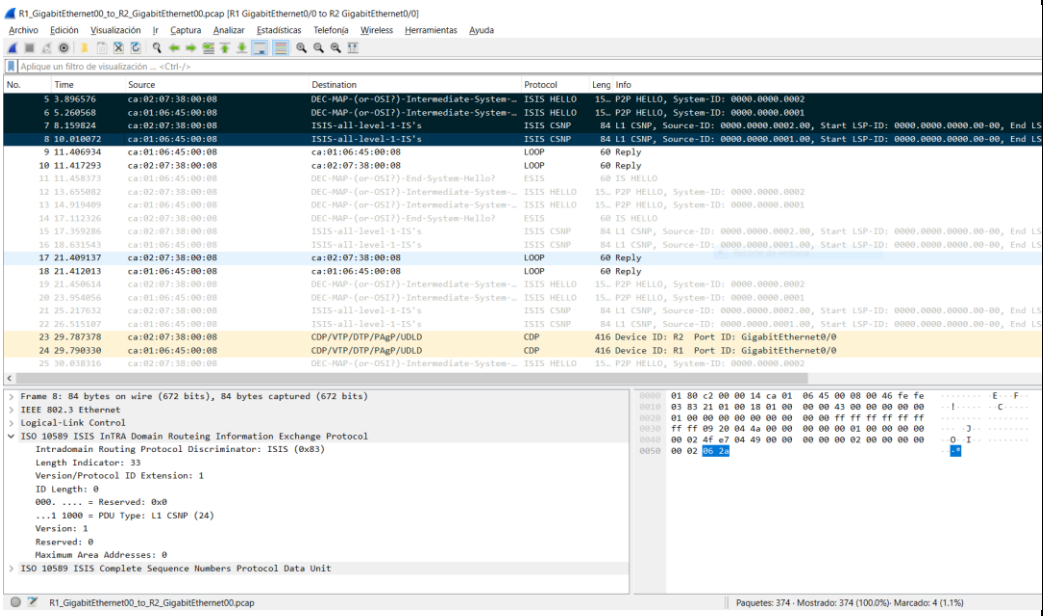


Figura 4. Intercambio de mensajes IS-IS entre R1 y R2

- En la Figura 5, se evidencia el contenido del primer mensaje Hello con un tipo de circuito de nivel 1 (0x1). Este intercambiará mensajes únicamente con routers de nivel 1. Se incluye el ID del sistema, la configuración 2P2 (TLV info de 240), el protocolo soportado, que en este caso es para IPv6 (TLV info de 129), la dirección del área 49.0010 (área 10 con TLV info de 1), y los campos de relleno (padding) que se utilizan para completar el tamaño mínimo del mensaje.

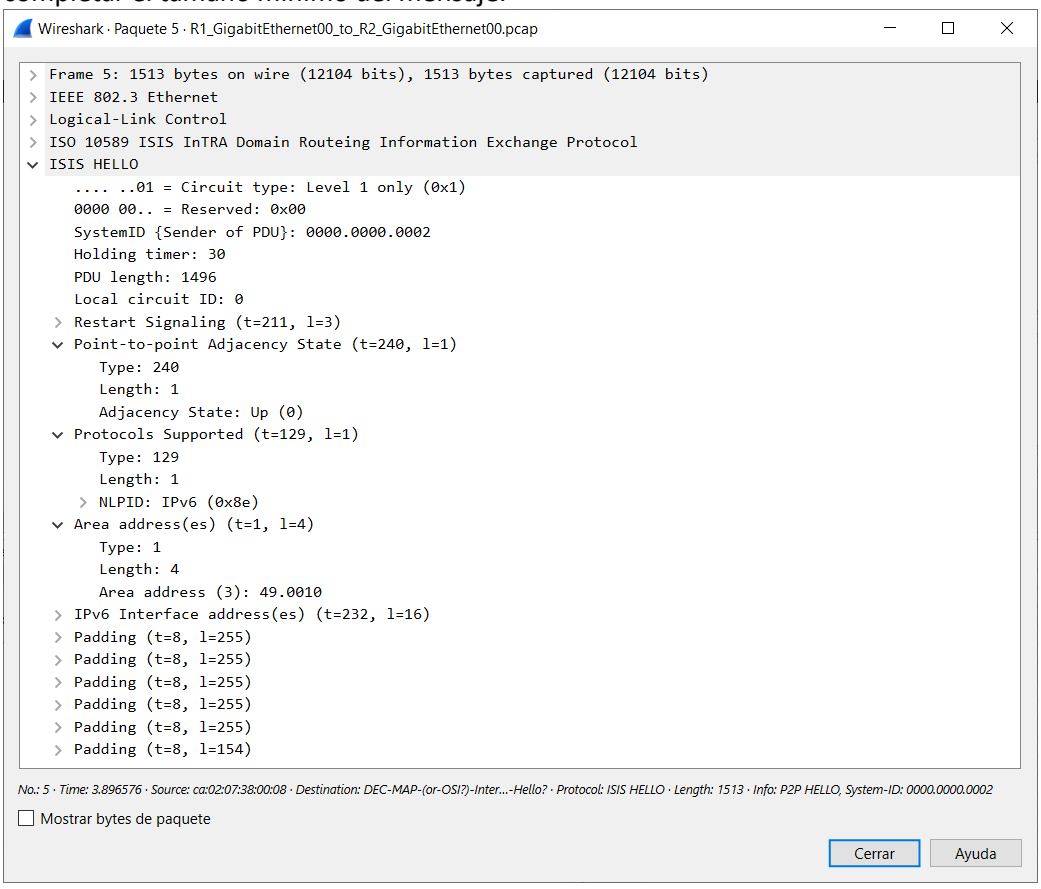


Figura 5. Mensaje ISIS Hello

- En IS-IS los TLVs son importantes por que permiten enviar una cantidad de información extensa, abarcan desde el 1 hasta el 255, sin embargo, no todos los TLVs han sido desarrollados o están en uso. Uno de los usos de estos TLVs permiten enviar etiquetas MPLs . Algunos de los TLVs son los siguientes:

TLV info	
1	Area Address
2	Metric
6	IS neighbor
8	Padding
10	Authentication
129	Protocol supported
132	IP outgoing interface address
135	Wide Metric
240	Adjacency state

Tabla 6. Detalles de TLVs

4. Proporcione evidencia de la verificación de conectividad.

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. **¿Cómo se diferencia IS-IS de otros protocolos de enrutamiento dinámico, como OSPF?**
2. **Describe los pasos clave para configurar IS-IS en un router Cisco.**
3. **¿Por qué es importante diseñar áreas en IS-IS? Proporciona ejemplos.**
4. **¿Cuáles son algunas herramientas y comandos útiles para la solución de problemas en IS-IS?**

ACTIVIDADES DESARROLLADAS

(Anotar las actividades que siguió para el desarrollo de la práctica)

Verificación de la conectividad

Incluya los resultados adquiridos en las pruebas de conectividad, acompañados de un análisis.

1. Utilice los comandos **“show ipv6 route” y “ping”** para verificar las configuraciones y el tráfico entre los Routers.

   Tabla de rutas Ipv6

   Aquí las pruebas de conectividad

   Análisis. -

   Ping desde Loopback1 hacia Loopback2

   Aquí las pruebas de conectividad

2. Utilice los siguientes comandos para la verificación de IS-IS. Proporcione evidencia del resultado de cada comando:

   Aquí las pruebas de conectividad

   Análisis. –

   Aquí las pruebas de conectividad

   Análisis. -

Actividad para el hogar.

1. **Topología implementada en el Software GNS3**

Aquí la topología de la Red implementada en GNS3

Configuración Router R1

Aquí las pruebas de conectividad

Configuración Router R2

Aquí las pruebas de conectividad

Configuración Router R3

Aquí las pruebas de conectividad

Configuración Router R4

Aquí las pruebas de conectividad

2. **Análisis en Wireshark**

Aquí el análisis con Wireshark

3. **Verificación de Conectividad**

Prueba de conectividad:

Prueba de conexión desde R1 hacia R3 Y R4

Aquí las pruebas de conectividad

Prueba de conexión desde R4 hacia R1 y R2

Aquí las pruebas de conectividad

CONCLUSIONES:

BIBLIOGRAFIA:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN - PARA DOCENTES**
REALIZADO POR:		
CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**17**	**TÍTULO PRÁCTICA:** Configuración BGP (Protocolo de Puerta de Enlace de Borde) en IPv6.

OBJETIVO:

- Establecer la conectividad y mejorar la eficiencia en entornos de redes avanzadas mediante la implementación y optimización de la configuración BGP en el contexto de IPv6.
- Ajustar parámetros de configuración BGP para optimizar el rendimiento y la eficiencia de la red IPv6.
- Realizar pruebas de conectividad para verificar la correcta propagación de las rutas IPv6 a través de la configuración de BGP.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

1. (3) Router Cisco
2. (2) Dispositivos con capacidad para soportar IPv6 (p. ej. computadoras)
3. (1) Cable Serial
4. (5) Cables de red Ethernet

DESCRIPCIÓN GENERAL:

En esta práctica de laboratorio, se busca llevar a cabo la implementación del Protocolo de Puerta de Enlace de Borde (BGP), específicamente diseñado para la versión 6 del Protocolo de Internet (IPv6), mediante la configuración apropiada de los dispositivos de conmutación.

INSTRUCCIONES:

1. Esquema de la práctica a desarrollar.

En esta práctica usted deberá conectar los equipos del laboratorio de red como se muestra a continuación:

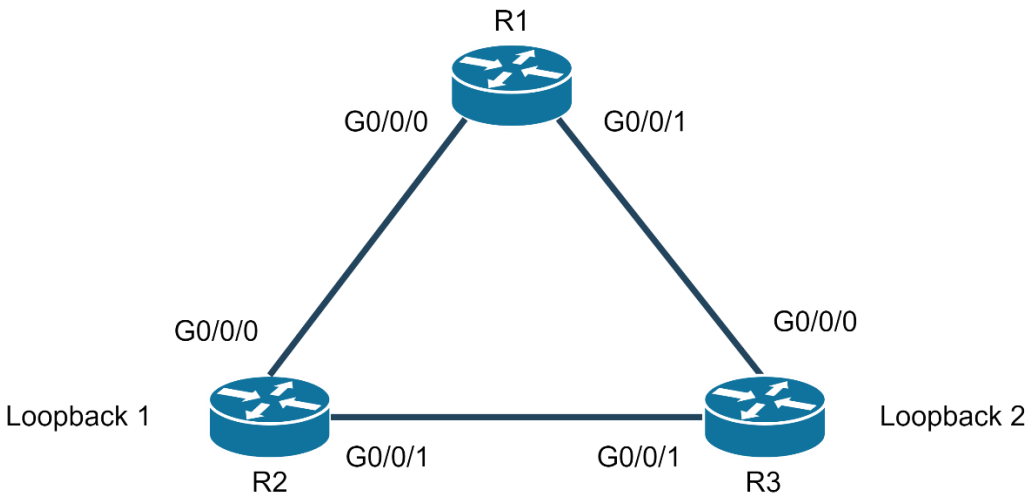


Figura 1. Topología de la red.

2. Configuración del Protocolo de Puerta de Enlace de Borde (BGP).

Las interfaces se configurarán utilizando las direcciones presentadas en la **Tabla 1** de direccionamiento de este laboratorio.

Equipos	Interfaz	Direccion	Mask	Gateway
R1	G0/0/0	fd00:1::1	/64	NA
	G0/0/1	fd00:2::1	/64	NA
R2	G0/0/0	fd00:1::2	/64	NA
	G0/0/1	fd00:3::1	/64	NA

R3	G0/0/0	fd00:2::2	/64	NA
	G0/0/1	fd00:3::2	/64	NA

Tabla 1. Tabla de direcciones IPv6.

En esta práctica, se configura el protocolo de Puerta de Enlace de Borde (BGP) versión 6, para ello usted debe realizar las siguientes instrucciones:

1. En el modo de configuración global, proceda a asignar un nombre al enrutador. Para esta práctica específica, se sugiere utilizar los nombres **R1**, **R2** y **R3** para cada uno de los dispositivos, conforme a la topología proporcionada.

2. Configure las direcciones IPv6 en la interfaz Gigabit Ethernet correspondientes.

Nota: Es imperativo considerar que, para implementar esta topología de red, se utilizará el módulo de interfaz de red del conmutador de capa 2 con 4 puertos GE Switch en el Router Cisco 4321, el cual funciona como un dispositivo de expansión de puertos. En relación a los puertos de esta interfaz, se emplearán los puertos G0/1/0, G0/1/1, G0/1/2 y G0/1/3 con el propósito de su identificación.

En el contexto del router R1, por ejemplo:

```
interface GigabitEthernet0/0/0
ipv6 address [dirección IPv6] / [prefijo de red]
exit

interface GigabitEthernet0/0/1
ipv6 address [dirección IPv6] / [prefijo de red]
exit
```

En el contexto de los routers R2 y R3, por ejemplo:

```
interface GigabitEthernet0/0/0
ipv6 address [dirección IPv6] / [prefijo de red]
exit

interface GigabitEthernet0/0/1
ipv6 address [dirección IPv6] / [prefijo de red]
exit

interface GigabitEthernet0/1/0
ipv6 address [dirección IPv6] / [prefijo de red]
exit
```

Sustituya "*[dirección IPv6] / [prefijo de red]*" con la dirección IPv6 y el prefijo red correspondiente.

3. Asegúrese de que la interfaz esté habilitada usando el comando **"no shutdown"**.

4.Ingresamos en el modo de configuración de BGP y configuramos los procesos

Por ejemplo:

```
router bgp <Número_de_ASA>
address-family ipv6 unicast
network <Red_IPv6/Longitud_prefijo>
neighbor <Dirección_IP_vecino> remote-as <Número_AS_vecino>
```

5.Repita los pasos anteriores en cada uno de los enrutadores para establecer la configuración del Protocolo de Puerta de Enlace de Borde (BGP) en su versión 6.

3. Configuración de direcciones IPv6 en los terminales.

Configurar en cada terminal la dirección IPv6 y la puerta de enlace correspondiente.

Equipos	Interfaz	Direccion	Mask
Loopback1	NIC	fd00:10::1	/64
Loopback2	NIC	fd00:20::1	/64
Loopback3	NIC	fd00:30::1	/64

Tabla 2. Asignación de direcciones IPv6 en los hosts.

RECOMENDACIÓN: Es necesario verificar que las configuraciones de seguridad o antivirus estén desactivadas en el terminal o PC, lo que incluye tanto el Firewall de Windows como cualquier software antivirus, ya que podrían surgir problemas durante la ejecución de pruebas de conectividad.

4. Verificación de conectividad BGP en IPv6.

Estos comandos mostrarán información sobre las interfaces IPv6, el estado de las sesiones BGP y las rutas BGP IPv6 aprendidas.

El siguiente comando proporciona información rápida sobre las interfaces IPv6, como las direcciones IPv6 configuradas y el estado de la interfaz.

```
enable
show ipv6 interface brief
```

El siguiente comando es útil para obtener información general sobre las sesiones BGP IPv6, como el número de vecinos BGP, el estado de las sesiones y estadísticas resumidas.

```
enable
show bgp ipv6 unicast summary
```

El siguiente comando se utiliza para obtener detalles específicos sobre las rutas IPv6 anunciadas por vecinos BGP, incluyendo métricas, caminos y otra información relacionada con el enrutamiento BGP IPv6.

```
enable
show bgp ipv6 unicast
```

Debe existir conectividad exitosa entre los terminales y el enrutador. Para esta práctica, puede comprobarse la conectividad entre el enrutador y cada uno de los terminales PC1 y PC2, y entre ellos. **Usted deberá realizar un análisis de la práctica en lo que respecta a las pruebas de conectividad y adjuntar evidencia de los resultados obtenidos en la parte final de la misma.**

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. **¿Cuál es el propósito principal del protocolo BGP en una red IPv6?**
2. **¿Cuáles son los pasos básicos para configurar BGP en un router Cisco para IPv6?**
3. **¿Cuál es la diferencia entre el enrutamiento BGP interno (IBGP) y el enrutamiento BGP externo (EBGP)?**
4. **¿Por qué es importante utilizar BGP en IPv6 en lugar de otros protocolos de enrutamiento interno?**

ACTIVIDADES DESARROLLADAS

(Anotar las actividades que siguió para el desarrollo de la práctica)

1. Verificación de la conectividad

Incluya los resultados adquiridos en las pruebas de conectividad, acompañados de un análisis.

Capturas de Conectividad:

Router 1

```
Aquí las pruebas de conectividad
```

Router 2

Aquí las pruebas de conectividad

Router 3

Aquí las pruebas de conectividad

Prueba de Conectividad, entre el R1, la Loopback1 y Loopback 2:

Aquí las pruebas de conectividad

Prueba de Conectividad, entre el R2 y R1:

Aquí las pruebas de conectividad

Prueba de Conectividad, entre el R3, la Loopback1 y Loopback 2:

Aquí las pruebas de conectividad

CONCLUSIONES:

BIBLIOGRAFIA:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN**
REALIZADO POR:		
CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**18**	**TÍTULO PRÁCTICA:** ACLs for IPv6 Router Cisco.

OBJETIVO:

- Configurar direcciones IPv6 en interfaces de red de dispositivos de red.
- Configurar enrutamiento dinámico RIPng.
- Configurar ACls según la topología.
- Verificar las reglas configuradas.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

4. (2) Routers Cisco
5. (3) Cables de red Ethernet
6. (3) Terminales (Computadoras)
7. (1) Cable Serial

DESCRIPCIÓN GENERAL:

En esta práctica, se centrará en la configuración de las Listas de Control de Acceso (ACLs) en un Router Cisco para IPv6. Esto incluirá la comprensión de la sintaxis y la estructura de las ACL para IPv6, así como la aplicación de estas reglas para gestionar el tráfico en la red. La práctica ofrecerá una visión práctica de cómo utilizar las ACLs para controlar selectivamente el paso de paquetes, lo que es crucial para mejorar la seguridad y la eficiencia en redes IPv6.

Conocimientos Requeridos para el desarrollo de la práctica: Asignación de Direcciones IPv6 con Router Cisco y Configuración Enrutamiento Dinámico RIPng.

INSTRUCCIONES

1. Esquema de la práctica a desarrollar Parte 1.

En esta práctica usted deberá conectar los equipos del laboratorio de red como se muestra en la figura 1:

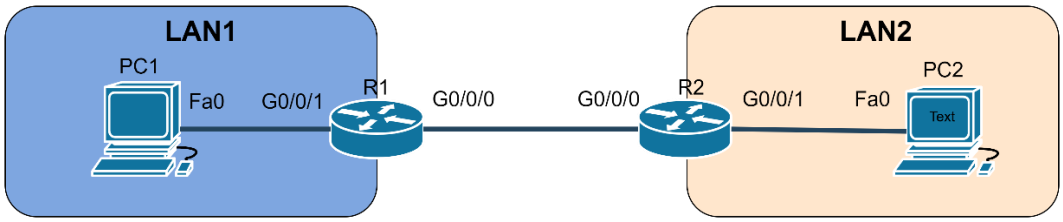


Figura 1. Topología de la red

2. Configuraciones Básicas de los Routers

1. Borre las configuraciones previas en cada uno de los Routers y reinícielos.

2. En el Modo de configuración global, asigne un nombre al router mediante el comando **"hostname"**, seguido del nombre deseado; en este ejercicio, se empleará **"R1"** como designación para el Router 1 y **"R2"** para el Router 2 como identificador del router.

3. Configuración de direccionamiento IPv6.

Las interfaces se configurarán utilizando las direcciones presentadas en la **Tabla 1** de direccionamiento de este laboratorio, para ello realizar las siguientes instrucciones:

1. Habilite el protocolo de enrutamiento IPv6.

Nota: Es importante habilitar el protocolo de enrutamiento Ipv6 en los Routers para evitar complicaciones en el desarrollo de la práctica. Si no recuerda cómo hacerlo, se recomienda revisar practicas previas.

2. Realice la configuración de las interfaces de los Routers, asignando direcciones IPv6 de acuerdo con el direccionamiento especificado en la **Tabla 1**.

Equipos	Interfaz	Direccion	Mask	Gateway
R1	G0/0/0	2023:c8:1:1::1	/64	NA
	G0/0/1	2023:c8:2:2::1	/64	NA
R2	G0/0/0	2023:c8:1:1::2	/64	NA
	G0/0/1	2023:c8:3:3::1	/64	NA

Tabla 1. Tabla de direcciones IPv6

4. Configuración enrutamiento Dinámico RIPng

1. Configurar RIPng en cada Router Cisco. **En esta práctica, el nombre del proceso se designará como "ups".**

Recuerde que para habilitar RIPng debe ingresar a cada interfaz física del Router que desee configurar**. Si presenta problemas en la configuración se recomienda revisar practicas previas.**

Nota: Al configurar enrutamiento dinámico RIPng se asignarán automáticamente las direcciones a los terminales (PCs). Para visualizar la dirección asignada entre al cmd del terminal e ingrese "ipconfig". Recuerde que la opción "Obtener automáticamente dirección IPv6" debe estar habilitada dentro de las propiedades del protocolo de versión 6 del terminal.

5. Configuración ACLs for IPv6

Para crear una Lista de Control de Acceso se utilizan los siguientes comandos:

*"**ipv6 access-list** [nombre de la ACL]"*

Donde:

- **"ipv6 access-list" :** Este es el comando base para crear una lista de control de acceso IPv6.
- **Nombre de la ACL:** Debes proporcionar un nombre único para la lista de control de acceso. Este nombre es utilizado para identificar la ACL.

*"**permit** protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [port-number] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [port-number] [dscp value] [log] [log-input] [sequence value]"*

Donde:

- **"permit":** Este comando establece condiciones de permiso para la ACL de IPv6

*"**deny** protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [port-number] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [port-number] [dscp value] [log] [log-input] [sequence value]"*

Donde:

- **"deny":** Este comando establece condiciones de denegación para la ACL de IPv6

Para aplicar una Lista de Control de Acceso a una interfaz física se utilizan los siguientes comandos:

*"**interface** [nombre de la interfaz]"*

Donde:

- **"Interface":** Este comando permite ingresar a la interfaz fisca de los Routers.
- **nombre de la interfaz:** Es el nombre de la interfaz física a la que deseamos ingresar.

*"**ipv6 traffic-filter** [nombre de la ACL] **[in | out]**"*

Donde:

- **"ipv6 traffic-filter":** Este comando indica al router que aplique una lista de control de acceso específica.
- **"in | out"**: Este comando determina la dirección del tráfico al que se aplicará la ACL.
  "in" se refiere al tráfico que entra en la interfaz.
  "out" se refiere al tráfico que sale de la interfaz.

En la topología de la **figura 1**, se aplicará la siguiente regla:
Crear una lista de acceso con el nombre PING y denegar el tráfico desde LAN2 hacia LAN1, para ello realizar las siguientes configuraciones:

1. Ingresar al modo configuración en la consola de R2 y crear la ACL con el nombre PING

```
R2(config)# ipv6 access-list PING
```

2. Crear un permiso para negar el tráfico desde la LAN2. Usar el protocolo ipv6, seguido ingresamos la ipv6 de origen con su prefijo y la dirección de destino con su prefijo. Con este comando se esta denegando toda la Red de LAN 2.

```
R2(config-ipv6-acl)# deny ipv6 2023:c8:3:3::/64 2023:c8:2:2::/64
R2(config-ipv6-acl)# exit
```

Nota: No olvide probar conectividad entre los terminales (PC1 y PC2) antes de configurar ACLs.
3. Ingresar a la interfaz G0/0/0 y aplicar la regla en modo "in". Es decir que el trafico que ingrese por esa interfaz será verificada por la regla creada.

```
R2(config)#interface gigabitEthernet 0/0/0
R2(config-if)# ipv6 traffic-filter PING in
```

6. Verificación de ACL.

1. Utilice el comando **"show access-lists"** para verificar las reglas en el Router. ¿Cuál es el resultado obtenido del comando?

2. Utilice el comando **"ping"** desde PC1 hacia PC2 ¿Cuál es el resultado obtenido del comando?

7. Esquema de la práctica a desarrollar Parte 2

Agregue un switch y un terminal (PC) a la topología de la red figura 1, usted deberá conectar los equipos de la siguiente manera:

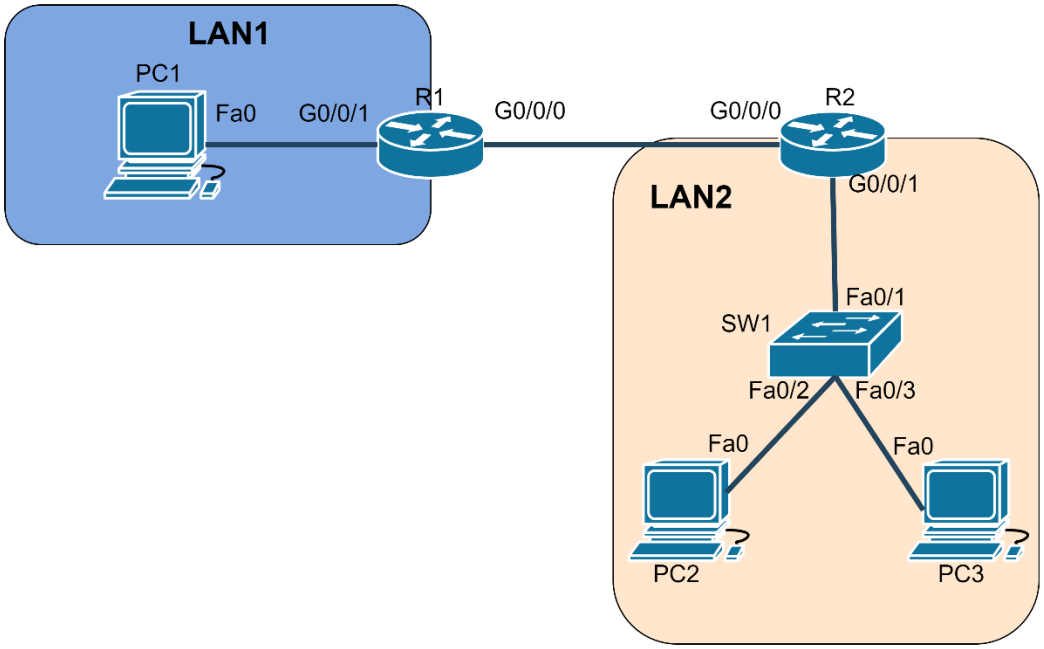


Figura 2. Topología de la Red

8. Configuración ACls for IPv6

Antes de Configurar, ingresar los siguientes comandos para eliminar las configuraciones de ACL previas:

1. Ingrese al modo configuración de consola en R2 y elimine la regla previamente creada en R2.

```
R2(config)# no ipv6 access-list PING
```

2. Ingrese a la interfaz G0/0/0 de R2 y elimine regla implementada en la interfaz.

```
R2(config)# no ipv6 traffic-filter PING in
```

3. Verifique la conectividad entre los terminales (PCs). Al usar enrutamiento dinámico RIPng a los terminales se les asignara automáticamente una dirección Ipv6.

Nota: En caso de experimentar dificultades con la conectividad, proceda a cambiar los puertos conectados al switch y valide la presencia de la luz indicadora para confirmar la conexión. Además, es fundamental desactivar tanto el firewall como el antivirus en las terminales correspondientes caso contrario pruebe la conexión con otra terminal.

En la topología de la **figura 2**, se aplicará las siguientes reglas:

Crear una lista de acceso con el nombre HOST2 y denegar trafico desde la LAN1 hacia la la LAN2.

1. Ingresar al modo configuración en la consola de R1 y crear la ACL con el nombre HOST2

```
R1(config)# ipv6 access-list host2
```

2. Crear un permiso para denegar el tráfico desde la LAN1 hacia la LAN2. Usar el protocolo ipv6, seguido ingresamos la ipv6 de origen con su prefijo y el host de destino.

```
R1(config-ipv6-acl)# deny ipv6 2023:C8:2:2::/64 host 2023:c8:3:3:20dc:cb7d:7e4f:f325
R1(config-ipv6-acl)# exit
```

Nota: La dirección ipv6 *2023:c8:3:3:20dc:cb7d:7e4f:f325* es la dirección asignada al terminal 3 (PC3) por RIPng de manera automática. Usted deberá modificar esta dirección conforme a la dirección que se asigne automáticamente al realizar las configuraciones en el laboratorio.

3. Ingresar a la interfaz G0/0/1 y aplicar la regla en modo "in". Es decir que el tráfico que ingrese por esa interfaz será verificada por la regla creada.

```
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)# ipv6 traffic-filter host2 in
```

Crear una lista de acceso con el nombre **NO_HTTP**. Denegar a la LAN2 acceso a http del Router R2

1. Ingresar al modo configuración en la consola de R2 y habilitar el server con nombre de usuario y password de "**nla"**.

```
R2(config)# ip http server
R2(config)# username nla privilege 15 password nla
R2(config)# ip http authentication local
```

2. Ingresar en el navegador de internet de terminal 3(PC3) e ingresar la siguiente dirección http:

```
http://[2023:c8:3:3::1]/
```

Al acceder a la dirección HTTP del servidor, se solicitará el nombre de usuario y la contraseña. Al ingresar las credenciales, se visualizará la pantalla siguiente:

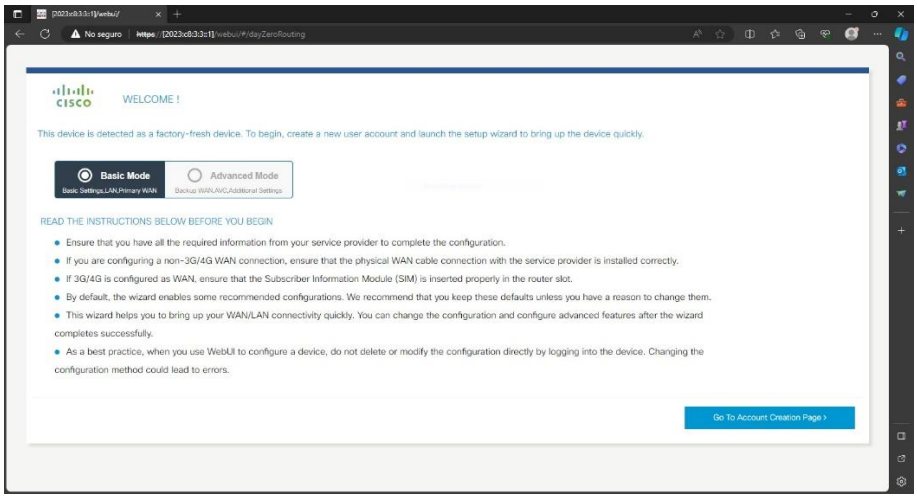


Figura 3. Servidor Router Cisco R2

3. Ingresar al modo configuración en la consola de R2 y crear la ACL con el nombre NO_HTTP

```
R2(config)# ipv6 acces-list NO_HTTP
```

4. Crear un permiso para denegar tcp desde la LAN2 la red de la interfaz G0/0/1 de R2. Usar el protocolo tcp, seguido ingresamos la red de origen con su prefijo y la red de destino solo cuando sea 80(www).

```
R2(config-ipv6-acl)# deny tcp 2023:c8:3:3::/64 2023:c8:3:3::/64 eq 80
```

5. Crear un permiso para permitir el tráfico ipv6 desde cualquier origen a cualquier destino.

```
R2(config-ipv6-acl)# permit ipv6 any any
R2(config-ipv6-acl)# exit
```

6. Ingresar a la interfaz G0/0/1 y aplicar la regla en modo "in". Es decir que el tráfico que ingrese por esa interfaz será verificado por la regla creada.

```
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)# ipv6 traffic-filter NO_HTTP in
```

9. Verificación de ACLs

1. Utilice el comando **"show access-lists"** para verificar las reglas en los Routers. ¿Cuál es el resultado obtenido del comando?

2. Utilice el comando **"ping"** desde PC1 hacia PC2 ¿Cuál es el resultado obtenido del comando?

3. Utilice el comando **"ping"** desde PC1 hacia PC3 ¿Cuál es el resultado obtenido del comando?

4. Ingresar en el navegador de internet de terminal 3(PC3) e ingresar la siguiente dirección http:

http://[2023:c8:3:3::1]/

¿Cuál es el resultado obtenido del comando?

10. Actividad para el hogar

1. Mediante el software GNS3, realizar la topología de la Figura 5. Asignar sus propias direcciones IPv6.

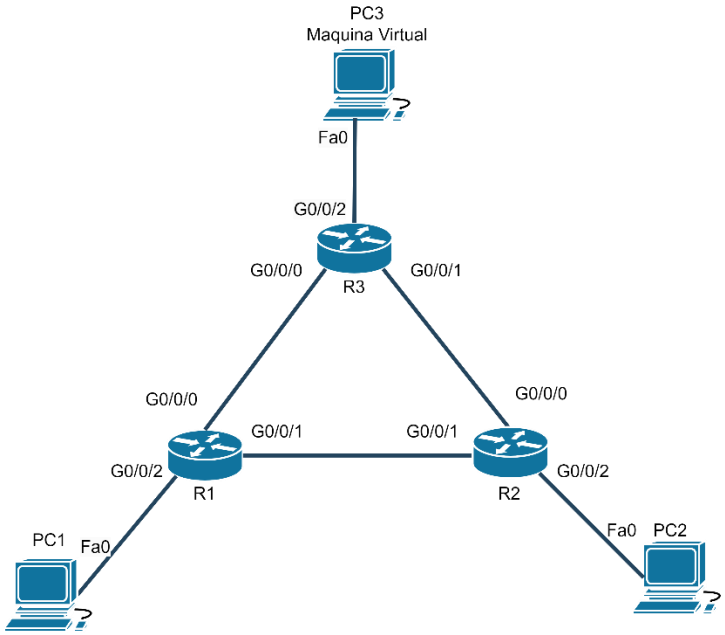


Figura 4. Topología de la Red.

2. En la topología de la figura 4, se configurará con direccionamiento y enrutamiento que usted prefiera, todos los terminales deben tener conectividad entre si antes de comenzar con la configuración de ACL. Usted puede asignar cualquier credencial para la creación del servidor.

3. Deberá crear los siguientes ACLs

- El PC2 debe responder PINGs solamente desde LAN R3
- El PC de la LAN de R3 debe acceder solamente al servidor de R3. Para todos los otros servidores, el acceso debe estar bloqueado.
- PC1 no debe poder acceder de ningún modo a la LAN de R3

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. **¿Cuál es el propósito principal de las listas de control de acceso (ACLs) en un router Cisco IPv6?**
2. **Describe la diferencia clave entre una ACL estándar y una ACL extendida en el contexto de IPv6.**
3. **Explica la diferencia entre aplicar una ACL en la dirección de entrada (in) y en la dirección de salida (out) de una interfaz.**
4. **¿Por qué es importante tener precaución al configurar ACLs en un router Cisco IPv6?**

ACTIVIDADES DESARROLLADAS

Anotar las actividades que siguió para el desarrollo de la práctica

Actividad para el hogar.

4. **Topología implementada en el Software GNS3**

Aquí la topología implementada en GNS3

Figura 5. Topología de la Red implementada en GNS3

Tabla de Direcciones IPv6

Equipos	Interfaz	Direccion	Mask	Gateway
R1				
R2				
R3				

Tabla 2. Tabla de Direcciones IPv6

5. **Configuración ACLs for IPv6**

- El PC2 debe responder PINGs solamente desde LAN R3

Aquí las configuraciones realizadas

- El PC de la LAN de R3 debe acceder solamente al servidor de R3. Para todos los otros servidores, el acceso debe estar bloqueado.

Aquí las configuraciones realizadas

- PC1 no debe poder acceder de ningún modo a la LAN de R3

Aquí las configuraciones realizadas

6. **Verificación de ACLs**

Prueba de conexión desde PC3 hacia PC2

Aquí las pruebas de conectividad

Prueba de conexión desde PC1 hacia PC2

Aquí las pruebas de conectividad

Prueba Conexión PC3 a servidor R3

Aquí las pruebas de conectividad

Prueba Conexión PC1 a LAN3

Aquí las pruebas de conectividad

CONCLUSIONES:
BIBLIOGRAFIA:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN - PARA DOCENTES**
REALIZADO POR:		
CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**19**	**TÍTULO PRÁCTICA:** Transición IPv4 a IPv6 Router Cisco.

OBJETIVO:

- Configurar direcciones IPv4 e IPv6 en interfaces de dispositivos de red.
- Configurar enrutamiento estático para IPv4 e IPv6.
- Configurar enrutamiento dinámico RIP para IPv4.
- Configurar enrutamiento dinámico OSPFv3.
- Configurar Dual Stack.
- Configurar Tunneling.
- Verificar las configuraciones.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

8. (3) Routers Cisco
9. (3) Cables de red Ethernet
10. (2) Terminales (Computadoras)
11. (1) Cable Serial

DESCRIPCIÓN GENERAL:

Esta practicas se enfoca en la migración de redes desde IPv4 a IPv6. Durante esta actividad, se lleva a cabo la configuración y transición de protocolos en un router Cisco para facilitar la coexistencia y adopción progresiva de IPv6. Se exploran los métodos de transición, como túneles IPv6 sobre IPv4, y se analiza cómo gestionar la transición de manera efectiva. La práctica incluye la asignación de direcciones IPv6, la configuración de túneles, y la observación del comportamiento de la red durante el proceso de migración.

Conocimientos Requeridos para el desarrollo de la práctica: Asignación de Direcciones IPv6 e IPv4 con Router Cisco, configuración Enrutamiento Estático IPv4 e IPv6, configuración Enrutamiento Dinámico RIP para IPv4 y configuración Enrutamiento Dinámico OSPFv3.

INSTRUCCIONES

1. Esquema de la práctica a desarrollar DUAL STACK.

En esta práctica usted deberá conectar los equipos del laboratorio de red como se muestra en la figura 1:

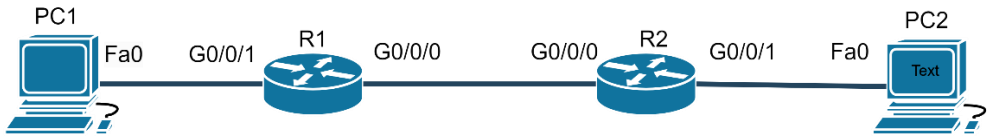


Figura 1. Topología de la red

2. Configuraciones Básicas de los Routers

1. Borre las configuraciones previas en cada uno de los Routers y reinícielos.

2. En el Modo de configuración global, asigne un nombre al router mediante el comando **"hostname"**, seguido del nombre deseado; en este ejercicio, se empleará **"R1"** como designación para el Router 1 y **"R2"** para el Router 2 como identificador del router.

3. Configuración de DUAL STACK.

Los Routers Cisco están preparados para el soporte de Dual Stack tan pronto como se configure IPv4 e IPv6. Para habilitar Dual Stack solo se necesita configurar las interfaces del Router con direcciones IPv4 e IPv6.

Las interfaces se configurarán utilizando las direcciones presentadas en la **Tabla 1** de direccionamiento de este laboratorio, para ello realizar las siguientes instrucciones:

1. Habilite el protocolo de enrutamiento IPv6.
Nota: Es importante habilitar el protocolo de enrutamiento Ipv6 en los Routers para evitar complicaciones en el desarrollo de la práctica. Si no recuerda cómo hacerlo, se recomienda revisar practicas previas.
2. Realice la configuración de las interfaces de los Routers y de los terminales (PCs), asignando direcciones IPv4 e IPv6 de acuerdo con el direccionamiento especificado en la **Tabla 1**.

Equipos	Interfaz	Direccion	Mask	Gateway
R1	G0/0/0	2023:AE:C8:1::1	/64	NA
		10.10.10.1	/30	NA
	G0/0/1	2023:C8:1:1::1	/64	NA
		192.168.172.1	/24	NA
PC1	ethernet	2023:C8:1:1::2	/64	2023:C8:1:1::1
		192.168.172.2	/24	192.168.172.1
R2	G0/0/0	2023:AE:C8:1::2	/64	NA
		10.10.10.2	/30	NA
	G0/0/1	2023:C8:2:2::1	/64	NA
		172.16.10.1	/30	NA
PC2	ethernet	2023:C8:2:2::2	/64	2023:C8:2:2::1
		172.16.10.2	/64	172.16.10.1

Tabla 1. Tabla de direcciones IPv4-IPv6

A continuación, se muestra un ejemplo de configuración para R1:
Direccionamiento IPv4-IPv6 R1

```
R1(config)#interface gigabitEthernet 0/0/0
R1(config-if)#ip address 10.10.10.1 255.255.255.252
R1(config-if)#ipv6 address 2023:AE:C8:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)#ip address 192.168.172.1 255.255.255.0
R1(config-if)#ipv6 address 2023:C8:1:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
```

El direccionamiento para R2 es similar a R1 según las direcciones de la Tabla 1.

Nota: Recuerde asignar manualmente ambas direcciones IPv4 e IPv6 en los terminales. (PC1 y PC2).

4. Configuración enrutamiento Estático

1. Configurar enrutamiento Estático IPv4 y Enrutamiento Estático Ipv6 en cada Router Cisco.
Nota: Si presenta problemas en la configuración se recomienda revisar practicas previas.

5. Verificación de DUAL STACK.

Realice las siguientes instrucciones y proporcione evidencia de su respuesta en la sección de Actividades Desarrolladas.

1. Utilice el comando **"show ip interface" (para ipv4) y "show ipv6 interface" (para ipv6)** para verificar Dual Stack en R1. ¿Cuál es el resultado obtenido del comando?

2. Utilice el comando **"ping"** desde PC1 hacia PC2 usando la dirección IPv4 y luego la dirección Ipv6 ¿Cuál es el resultado obtenido del comando?

6. Esquema de la práctica a desarrollar TUNNELING

Agregue un Router a la topología de la red, usted deberá conectar los equipos de la siguiente manera:

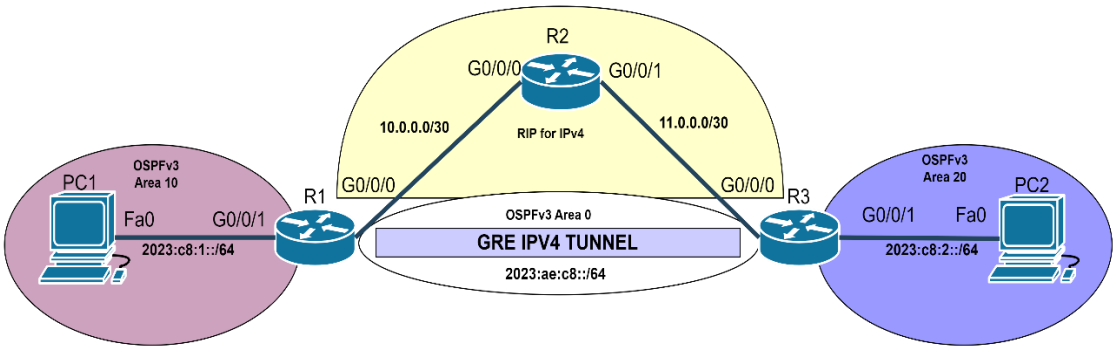


Figura 2. Topología de la Red

7. Configuraciones Básicas de los Routers

1. Borre las configuraciones previas en cada uno de los Routers y reinícielos.

2. En el Modo de configuración global, asigne un nombre al router mediante el comando **"hostname"**, seguido del nombre deseado; en este ejercicio, se empleará **"R1"** como designación para el Router 1, **"R2"** para el Router 2 y **"R3"** como identificador del Router 3.

8. Configuración Direccionamiento IPv4-Ipv6

Las interfaces se configurarán utilizando las direcciones presentadas en la **Tabla 2** de direccionamiento de este laboratorio, para ello realizar las siguientes instrucciones:

1. Habilite el protocolo de enrutamiento IPv6 para R1 y R3. En R2 no es necesario habilitar debido a que se asignara direccionamiento IPv4.

2. Realice la configuración de las interfaces de los Routers, asignando direcciones IPv4 e IPv6 de acuerdo con el direccionamiento especificado en la **Tabla 2**.

Equipos	Interfaz	Direccion	Mask	Gateway
R1	G0/0/0	10.10.10.1	/30	NA
	G0/0/1	2023:C8:1::1	/64	NA
R2	G0/0/0	10.10.10.2	/30	NA
	G0/0/1	11.11.11.1	/30	NA
R3	G0/0/0	11.11.11.2	/30	NA
	G0/0/1	2023:C8:2::1	/64	NA

Tabla 2. Tabla de direcciones IPv4-IPv6

9. Configuración Enrutamiento Dinámico RIP for IPv4

1. Ingresar al modo de configuración de R1 y habilitar enrutamiento dinámico RIP para Ipv4

```
R1(config)#router rip
```

2. Configurar RIP para la red 10.0.0.0 de la interfaz G0/0/0 de R1

```
R1(config-if)#network 10.0.0.0
```

3. Habilitar y configurar RIP para IPv4 para R2 y R3.

Nota: No olvide que, para R3 solo deberá configurar con RIP la red de la interfaz G0/0/0.

10. Configuración Tunnel GRE

Para habilitar la comunicación entre dos terminales mediante IPv6 a través de una red con IPv4, se implementa una técnica de Tunneling que consiste en encapsular el paquete IPv6 dentro de un paquete IPv4. Para establecer este túnel, es esencial configurar los routers de borde, en este caso, R1 y R3. Los comandos empleados para la configuración son los siguientes:

```
"interface tunnel [nombre del tunel]"
```

Donde:

- **"interface tunnel":** Este comando entra en el modo de configuración de interfaz para el túnel especificado.
- **Nombre del túnel:** es un identificador para el túnel en la configuración.

"no ip address"

Donde:

- **"no ip address":** este comando elimina la dirección IP asociada con la interfaz de túnel.

"ipv6 enable"

Donde:

- **"ipv6 enable":** este comando habilita el soporte de IPv6 en la interfaz tunnel creada.

"ipv6 address [dirección ipv6]"

Donde:

- **"ipv6 addres":** este comando permite asignar una dirección IPv6 a la interfaz de túnel.
- **Direccion ipv6:** es la dirección asignad a la interfaz tunnel.

"tunnel source [nombre de la interfaz]"

Donde:

1. **"tunnel source [nombre de la interfaz]":** Este comando permite configurar la interfaz del router donde se está originando el túnel.

"tunnel destination [dirección ip]"

Donde:

2. **"tunnel destination [dirección ip]":** Este comando permite especificar la dirección IP de destino del extremo del túnel para indicar a qué dirección IP deben enviarse los paquetes encapsulados a través del túnel.

A continuación, se muestra la configuración de Tunnel GRE para R1:

1. Ingresar al modo de configuración de interfaz del túnel. Como nombre de interfaz de túnel se configuro como "0".

```
R1(config)# interface tunnel 0
R1(config-if)# no ip address
```

2. Habilitar el soporte IPv6 en la interfaz del túnel.

```
R1(config-if)# ipv6 enable
```

3. Asignar una dirección IPv6 a la interfaz del túnel. El direccionamiento IPv6 para la interfaz del túnel, se observa en la siguiente tabla 3.

Equipos	Interfaz	Direccion	Mask
R1	Tunnel 0	2023:AE:C8::1	/64
R2	Tunnel 0	2023:AE:C8::2	/64

Tabla 3. Direccionamiento IPv6 Interfaz Tunnel 0

```
R1(config-if)# ipv6 address 2023:AE:C8::1/64
```

4. Especificar la fuente del túnel (source):
Este comando indica que la fuente del túnel será la interfaz GigabitEthernet0/0 indicando que el tráfico que proviene de esta interfaz se encapsulará en el túnel.

```
R1(config-if)# tunnel source GigabitEthernet0/0/0
```

5. Especificar la dirección IP del destino del túnel:
Este comando establece la dirección IP del destino del túnel en 11.11.11.2. Los paquetes encapsulados se enviarán a esta dirección.

```
R1(config-if)# tunnel destination 11.11.11.2
R1(config-if)#exit
```

6. Repita los pasos de 1-5 para configurar el tunnel "0" en R3. Asegúrese de especificar correctamente la fuente y el destino del tunnel.

7. Una vez que el Tunnel 0 ha sido configurado, mediante el comando "show interfaces tunnel 0", verifique en R1 y R3 que el Tunnel 0 esté habilitado. A continuación, se presenta la información que deberá observar en la pantalla al ejecutar el comando de verificación.

```
R1#show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.10.10.1 (GigabitEthernet0/0), destination 11.11.11.2
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255

R3#sh interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 11.11.11.2 (GigabitEthernet0/0), destination 10.10.10.1
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
```

Nota: Verifique que tanto el túnel como el protocolo estén en estado "up" (levantados). Además, examine la configuración del túnel en caso de encontrar problemas al utilizar el comando de verificación. Es fundamental que la configuración sea precisa para completar el enrutamiento y lograr la conexión entre los terminales.

11. Configuración Enrutamiento Dinámico OSPFv3

Una vez completada la configuración del Tunnel GRE, es esencial establecer la configuración de enrutamiento entre las interfaces de los túneles creados y las interfaces con IPv6 correspondientes en R1 y R3.

Para esta práctica, **el número de proceso utilizado será de 1**, un **router-id en formato ip (x.x.x.x),** el número de **área 0** para las interfaces de los túneles 0 en R1 y R3, el número de **área 10** para la interfaz G0/0/1 de R1 y el número de **área 20** para la interfaz G0/0/1 de R3.

A continuación, se detalla los pasos para la configuración de OSPFv3 en R1.

13. Ingresar al modo de configuración global y acceder al modo de configuración de OSPFv3. No olvidar elegir el número de proceso para la configuración de OSPFv3.

```
R1(config)#ipv6 router ospf 1
```

14. Asignar el Router ID, recuerde que el router-id es único para cada router, se recomienda usar para **R1= 1.1.1.1** y para **R3=3.3.3.3**

```
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#exit
```

15. Ingresar a la interfaz gigabitEthernet y tunnel correspondiente según la **tabla 1 y tabla2** para configurar cada interfaz con OSPFv3. Aquí se asignará el **número de proceso de 1** y **los números de áreas correspondiente.**

```
R1(config)#interface tunnel 0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#exit
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)#ipv6 ospf 1 area 10
R1(config-if)#exit
```

16. Configurar para R3 el enrutamiento dinámico OSPFv3 siguiendo los pasos 1-3.

```
R3(config)#ipv6 router ospf 1
R3(config-rtr)#router-id 3.3.3.3
R3(config-rtr)#exit
R3(config)#interface tunnel 0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#exit
R3(config)#interface gigabitEthernet 0/0/1
R3(config-if)#ipv6 ospf 1 area 20
R3(config-if)#exit
```

Nota: Al configurar enrutamiento dinámico OSPFv3 en una de las interfaces de R1 y R3 se asignarán automáticamente las direcciones a los terminales (PCs). Para visualizar la dirección asignada, entre al cmd del terminal e ingrese "ipconfig". Recuerde que la opción "Obtener automáticamente dirección IPv6" debe estar habilitada dentro de las propiedades del protocolo de versión 6 del terminal.

12. Verificación Tunnel GRE

Realice las siguientes instrucciones y proporcione evidencia de su respuesta en la sección de Actividades Desarrolladas.

1. Utilice el comando **"show ipv6 route"** para verificar el túnel creado. ¿Cuál es el resultado obtenido del comando?

2. Utilice el comando **"ping"** desde la dirección de PC1 configurada automáticamente hacia PC2 ¿Cuál es el resultado obtenido del comando?

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. **¿Cuáles son las principales razones para la transición de IPv4 a IPv6, y cómo aborda IPv6 las limitaciones de IPv4?**
2. **Describe el proceso de configuración de enrutamiento dual-stack en un router Cisco y explica cómo permite la coexistencia de IPv4 e IPv6.**
3. **¿Cuáles son las diferencias entre el túnel NAT-PT y NAT64 para la transición de IPv4 a IPv6?**

ACTIVIDADES DESARROLLADAS

(Anotar las actividades que siguió para el desarrollo de la práctica)

1. Verificación de DUAL STACK.

1. Utilice el comando **“show ip interface brief” (para ipv4) y “show ipv6 interface brief” (para ipv6)** para verificar Dual Stack en R1. ¿Cuál es el resultado obtenido del comando?

Aquí las pruebas de conectividad

2. Utilice el comando **“ping”** desde PC1 hacia PC2 usando la dirección IPv4 y luego la dirección Ipv6 ¿Cuál es el resultado obtenido del comando?

Aquí las pruebas de conectividad

2. Verificación Tunnel GRE

1. Utilice el comando **“show ipv6 route”** para verificar el túnel creado. ¿Cuál es el resultado obtenido del comando?

Aquí las pruebas de conectividad

2. Utilice el comando **“ping”** desde la dirección de PC1 configurada automáticamente hacia PC2 ¿Cuál es el resultado obtenido del comando?

Aquí las pruebas de conectividad

CONCLUSIONES:

BIBLIOGRAFIA:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR	FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO/TALLERES/CENTROS DE SIMULACIÓN - PARA DOCENTES

REALIZADO POR:

CARRERA:		**ASIGNATURA:**
NRO. PRÁCTICA:	**20**	**TÍTULO PRÁCTICA:** MPLS.

OBJETIVO:

- Configurar direcciones IPv6 e Ipv4 en interfaces de red de dispositivos de red.
- Configurar enrutamiento dinámico OSPFv3, OSPFv2.
- Configurar Tunnel GRE.
- Configurar MPLS.
- Verificar la conectividad IPv6 entre dispositivos de red.

HERRAMIENTAS:

Herramientas necesarias para realizar la práctica.

12. (3) Routers Cisco
13. (4) Cables de red Ethernet
14. (1) Cable Serial

DESCRIPCIÓN GENERAL:

La práctica de MPLS (Multiprotocol Label Switching) con IPv6 e IPv4 implica la implementación y configuración de MPLS en una red que utiliza tanto IPv6 como IPv4 para el enrutamiento. MPLS, un protocolo avanzado de conmutación de etiquetas, permite la creación de rutas más eficientes y flexibles en redes IP. Esta práctica específica se centra en la integración de MPLS con los protocolos IPv6 e IPv4, explorando cómo MPLS mejora el rendimiento y la gestión del tráfico en una red dual-stack.

Conocimientos Requeridos para el desarrollo de la práctica: Asignación de Direcciones IPv6 e IPv4 con Router Cisco, Configuración OSPFv2 y OSPFv3, Configuración Tunneling.

INSTRUCCIONES

8. Esquema de la práctica a desarrollar.

En esta práctica usted deberá conectar los equipos del laboratorio de red como se muestra en la figura 1:

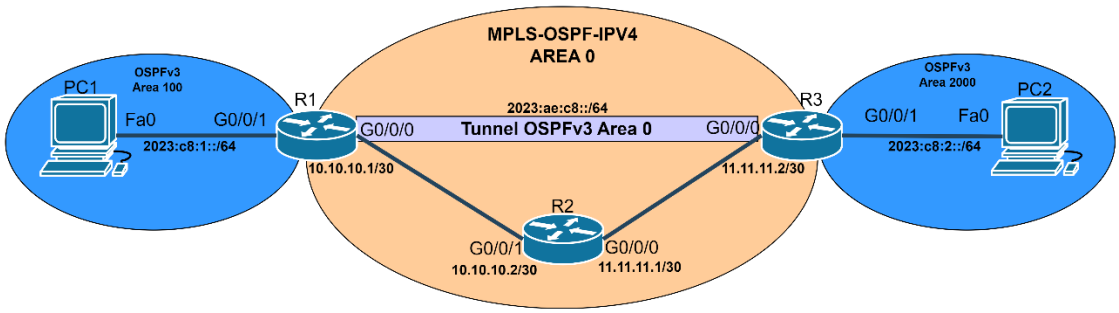


Figura 1. Topología de la red

9. Configuraciones Básicas de los Routers

1. Borre las configuraciones previas en cada uno de los Routers y reinícielos.

2. En el Modo de configuración global, asigne un nombre al router mediante el comando **"hostname"**, seguido del nombre deseado; en este ejercicio, se empleará **"R1"** como designación para el Router 1, **"R2"** para el Router 2 y **"R3"** para Router 3 como identificador del router.

10. Configuración de direccionamiento IPv6 e IPv4.

Las interfaces se configurarán utilizando las direcciones presentadas en la **Tabla 1** de direccionamiento de este laboratorio, para ello realizar las siguientes instrucciones:

1. Habilite el protocolo de enrutamiento IPv6 en R1 y R3.

Nota: Es importante habilitar el protocolo de enrutamiento Ipv6 en los Routers para evitar complicaciones en el desarrollo de la práctica. Si no recuerda cómo hacerlo, se recomienda revisar practicas previas.

2. Realice la configuración de las interfaces de los Routers, asignando direcciones IPv6 e IPv4 de acuerdo con el direccionamiento especificado en la **Tabla 1**.

Equipos	Interfaz	Dirección	Mask	Gateway
R1	G0/0/0	10.10.10.1	/30	NA
	G0/0/1	2023:c8:1::1	/64	NA
R2	G0/0/0	10.10.10.2	/30	NA
	G0/0/1	11.11.11.1	/30	NA
R3	G0/0/0	11.11.11.2	/30	NA
	G0/0/1	2023:c8:2::1	/64	NA

Tabla 1. Tabla de direcciones IPv6 e IPv4

11. Configuración Enrutamiento Dinámico OSPF para IPv4

Para la configuración de OSPF en IPv4, **el número de proceso utilizado será de 10**, un **router-id en formato ip (x.x.x.x),** el número de **área 0.**

En la siguiente tabla 2. Se especifica la configuración para cada Router:

Configuraciones	**R1**	**R2**	**R3**
Numero Proceso	10	10	10
ID Router	10.10.10.10	20.20.20.20	30.30.30.30
área	0	0	0
Networks	10.10.10.0	11.11.11.0	11.11.11.0
		10.10.10.0	

Tabla 2. Configuraciones OSPF para IPv4

A continuación, se detalla los pasos para la configuración de OSPF en R1.

17. Ingresar al modo de configuración global y acceder al modo de configuración de OSPF. No olvidar el número de proceso.

```
R1(config)#router ospf 10
```

18. Asignar el Router ID, recuerde que el router-id es único para cada Router.

```
R1(config-router)#router-id 10.10.10.10
```

19. Configurar las redes IPv4 a las que está conectado cada router. En el caso de R1, según la Tabla 2, está conectado a la red 10.10.10.0. Se debe introducir la información de la red junto con su máscara de wildcard y el área correspondiente.

```
R1(config-router)#network 10.10.10.0 0.0.0.3 area 0
R1(config-router)#exit
```

20. Configurar para R2 y R3 el enrutamiento dinámico OSPF siguiendo los pasos 1-3.

Nota: Al configura OSPF en los Routers usted podrá comprobar conectividad entre ellos haciendo ping entre sus direcciones IPv4 asignadas previamente.

12. Configuración Tunnel GRE

A continuación, se muestra la configuración de Tunnel GRE para R1:

1. Ingresar al modo de configuración de interfaz del túnel. Como nombre de interfaz de túnel se configuro como "0".

```
R1(config)# interface tunnel 0
R1(config-if)# no ip address
```

2. Habilitar el soporte IPv6 en la interfaz del túnel.

```
R1(config-if)# ipv6 enable
```

3. Asignar una dirección IPv6 a la interfaz del túnel. El direccionamiento IPv6 para la interfaz del túnel, se observa en la siguiente tabla 3.

Equipos	Interfaz	Direccion	Mask
R1	Tunnel 0	2023:AE:C8::1	/64
R2	Tunnel 0	2023:AE:C8::2	/64

Tabla 3. Direccionamiento IPv6 Interfaz Tunnel 0

```
R1(config-if)# ipv6 address 2023:AE:C8::1/64
```

4. Especificar la fuente del túnel (source):
Este comando indica que la fuente del túnel será la interfaz GigabitEthernet0/0 indicando que el tráfico que proviene de esta interfaz se encapsulará en el túnel.

```
R1(config-if)# tunnel source GigabitEthernet0/0/0
```

5. Especificar la dirección IP del destino del túnel:
Este comando establece la dirección IP del destino del túnel en 11.11.11.2. Los paquetes encapsulados se enviarán a esta dirección.

```
R1(config-if)# tunnel destination 11.11.11.2
R1(config-if)#exit
```

6. Repita los pasos de 1-5 para configurar el tunnel "0" en R3. Asegúrese de especificar correctamente la fuente y el destino del tunnel.

13. Configuración Enrutamiento Dinámico OSPFv3

Para esta práctica, **el número de proceso utilizado será de 1**, un **router-id en formato ip (x.x.x.x),** el número de **área 0** para las interfaces de los túneles 0 en R1 y R3, el número de **área 100** para la interfaz G0/0/1 de R1 y el número de **área 200** para la interfaz G0/0/1 de R3.

A continuación, se detalla los pasos para la configuración de OSPFv3 en R1.

21. Ingresar al modo de configuración global y acceder al modo de configuración de OSPFv3. No olvidar elegir el número de proceso para la configuración de OSPFv3.

```
R1(config)#ipv6 router ospf 1
```

22. Asignar el Router ID, recuerde que el router-id es único para cada router, se recomienda usar para **R1= 1.1.1.1** y para **R3=3.3.3.3**

```
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#exit
```

23. Ingresar a la interfaz gigabitEthernet y tunnel correspondiente según la **tabla 1 y tabla 3** para configurar cada interfaz con OSPFv3. Aquí se asignará el **número de proceso de 1** y **los números de áreas correspondiente.**

```
R1(config)#interface tunnel 0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#exit
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)#ipv6 ospf 1 area 100
```

```
R1(config-if)#exit
```

24. Configurar para R3 el enrutamiento dinámico OSPFv3 siguiendo los pasos 1-3.

```
R3(config)#ipv6 router ospf 1
R3(config-rtr)#router-id 3.3.3.3
R3(config-rtr)#exit
R3(config)#interface tunnel 0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#exit
R3(config)#interface gigabitEthernet 0/0/1
R3(config-if)#ipv6 ospf 1 area 200
R3(config-if)#exit
```

Nota: Al configurar enrutamiento dinámico OSPFv3 en una de las interfaces de R1 y R3 se asignarán automáticamente las direcciones a los terminales (PCs). Para visualizar la dirección asignada, entre al cmd del terminal e ingrese "ipconfig". Recuerde que la opción "Obtener automáticamente dirección IPv6" debe estar habilitada dentro de las propiedades del protocolo de versión 6 del terminal.

14. Configuración MPLS

Para habilitar MPLS en IPv4, es necesario asegurarse de que los routers tienen activada la licencia que permite utilizar los comandos de configuración MPLS. Los comandos utilizados para la configuración son los siguientes:

"mpls ip"

Donde:

- **"mls ip":** Este comando habilita MPLS para paquetes IPv4 en el modo configuración global.

"mpls label protocol ldp"

Donde:

- **"mpls label protocol ldp":** Este comando se utiliza en el modo de configuración global para especificar que el protocolo LDP será el método utilizado para distribuir las etiquetas MPLS.

"mpls label range"

Donde:

- **"mpls label range":** Este comando permite realizar ajustes de los valores del rango de etiquetas MPLS según los requisitos específicos de la red.

"interface <tipo interfaz>"
"mpls ip"

Donde:

- **"interface <tipo interfaz> ":** Selecciona la interfaz específica donde se habilitará MPLS.
- **"mpls ip":** Este comando habilito MPLS para paquetes IPv4 en la interfaz seleccionada.

A continuación, se muestra los pasos para activar la licencia de MPLS ("appxk9") en caso de que el router ya este activado omitir estos pasos (verificar con el comando "show licence all").

LICENCIA APPXK9
HABILITACIÓN DE COMANDOS PARA MPLS

Los pasos descritos a continuación son válidos para el Router Cisco 4321 y Router Cisco C1111-4PW.

- Para el Router Cisco 4321 se activará automáticamente la licencia: appxk9 (ISR_4321_Application)

- Para el Router Cisco C1111-4PW se activará automáticamente la licencia: appxk9 (ISR_1100_4P_Application)

1. Ingresar al modo configuración del Router
2. Digitar el comando **"license boot level appxk9"**

```
Router(config)#license boot level appxk9
% use 'write' command to make license boot config take effect on next boot
Router(config)#
```

3. Salir del modo configuración y digitar el comando **"write"** para guardar la configuración.

```
Router#
*Jan 25 17:22:14.265: %SYS-5-CONFIG_I: Configured from console by console
Router#write
Building configuration...
[OK]
Router#
*Jan 25 17:22:32.235: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully
encrypted private config file
Router#
```

4. Digitar el comando "**reload**" para reiniciar el Router y actualizar la configuración.

```
Router#reload
WARNING:
Boot variable either does not exist or buffer is too small
This may impact autoboot of the router. Proceed with caution
```

5. Confirmar 2 veces para proceder a reiniciar el Router.

```
Do you wish to proceed with reload anyway[confirm]
Proceed with reload? [confirm]
```

6. Luego del reinicio, ingresar el comando **"show license all"** para verificar la licencia.

```
Router#show license all
License Usage
=============

appxk9 (ISR_4321_Application):
  Description: appxk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: appxk9
  Feature Description: appxk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual
```

A continuación, se detalla los pasos para la configuración de MLS en R1.

1. Acceder al modo de configuración global y activar MPLS.

```
R1(config)#mpls ip
```

2. Habilitar el protocolo LDP para la asignación de etiquetas.

```
R1(config)#mpls label protocol ldp
```

3. Establecer el intervalo de etiquetas. La tabla 4 proporciona la información detallada sobre el rango de cada interfaz para cada router.

Router	Rango
R1	16 99
R2	100 199
R3	200 299

Tabla 4. Rango de etiquetas para cada Router.

```
R1(config)#mpls label range 16 99
```

4. Acceder a las interfaces del router y activar MPLS.

```
R1(config)#int g0/0/0
R1(config-if)#mpls ip
R1(config-if)#exit
```

5. Repetir los pasos 1-4 para la configuración de R2 y R3.

```
Configuración MPLS R2
R2(config)#int g0/0/0
R2(config-if)#mpls ip
R2(config-if)#exit
R2(config)#int g0/0/1
R2(config-if)#mpls ip
R2(config-if)#exit

Configuración MPLS R3
R3(config)#int g0/0/0
R3(config-if)#mpls ip
R3(config-if)#exit
```

15. Verificaciones

Realice las siguientes instrucciones y proporcione evidencia de su respuesta en la sección de Actividades Desarrolladas.

Una vez realizada la configuración del enrutamiento entre los enrutadores, se deberá verificar que la conectividad IPv6 se ha establecido correctamente realizando ping entre las interfaces de loopback y verificando configuración del enrutamiento IS-IS en los routers.

1. Utilice en R1 el comando **"show ipv6 route"** y **"show ip route"**. ¿Cuál es el resultado obtenido de los comandos?

2. Utilice en R1 el comando **"show mpls interfaces" y "show mpls ldp discovery".** ¿Cuál es el resultado obtenido de los comandos?

3. Utilice el comando **"ping"** desde la dirección de PC1 configurada automáticamente hacia PC2 ¿Cuál es el resultado obtenido del comando?

4. Mediante Wireshark analice el tráfico en la interfaz G0/0/1 de R1 al realizar ping sostenido desde PC1 hacia PC2 y responda: ¿Por qué solo se visualiza ICMPv6?, ¿Qué podría hacer para visualizar el tráfico en R2?

Nota: Recuerde que usted deberá realizar un análisis de la práctica en lo que respecta a las pruebas de conectividad y adjuntar evidencia de los resultados obtenidos en la parte final de la misma.

16. Actividad para el hogar

1. Mediante el software GNS3, realizar nuevamente la topología de la Figura 1 y asignar su propio direccionamiento.

	2. Realizar las configuraciones realizadas en la práctica del laboratorio. **3.** Mediante Wireshark analizar el tráfico en G0/0/0 de R2 al realizar ping desde PC1 a PC2. Usted deberá observar en el análisis del tráfico el protocolo LDP y la encapsulación por la configuración del tunnel.

MARCO TEORICO

(Investigar los siguientes conceptos para el desarrollo de la práctica)

1. **¿Qué es MPLS y cuál es su propósito en las redes?**
2. **Explique el proceso de conmutación de etiquetas en MPLS y cómo contribuye a la eficiencia del enrutamiento.**
3. **¿Cuál es la diferencia entre LER y LSR en el contexto de MPLS en un router Cisco?**

ACTIVIDADES DESARROLLADAS

(Anotar las actividades que siguió para el desarrollo de la práctica)

Verificación de la conectividad

Incluya los resultados adquiridos en las pruebas de conectividad, acompañados de un análisis.

1. Utilice en R1 el comando **"show ipv6 route"** y **"show ip route"**. ¿Cuál es el resultado obtenido de los comandos?

Tabla de rutas IPv6

Aquí las pruebas de conectividad

Análisis. -

Tabla de rutas IPv4

Aquí las pruebas de conectividad

Análisis. -

2. Utilice en R1 el comando **"show mpls interfaces" y "show mpls ldp discovery".** ¿Cuál es el resultado obtenido de los comandos?

Aquí las pruebas de conectividad

Aquí las pruebas de conectividad

Análisis. -

3. Utilice el comando **"ping"** desde la dirección de PC1 configurada automáticamente hacia PC2 ¿Cuál es el resultado obtenido del comando?

Aquí las pruebas de conectividad

Análisis. –

4. Mediante Wireshark analice el tráfico en la interfaz G0/0/1 de R1 al realizar ping sostenido desde PC1 hacia PC2 y responda: ¿Por qué solo se visualiza ICMPv6?, ¿Qué podría hacer para visualizar el tráfico en R2?

Aquí colocar la captura del trafico mediante Wireshark

Análisis. –

Actividad para el hogar

7. Topología implementada en el Software GNS3

Aquí colocar la topología implementada en GNS3

Configuración Router R1

Aquí las pruebas de conectividad

Configuración Router R2

Aquí las pruebas de conectividad

Configuración Router R3

Aquí las pruebas de conectividad

8. Análisis en Wireshark

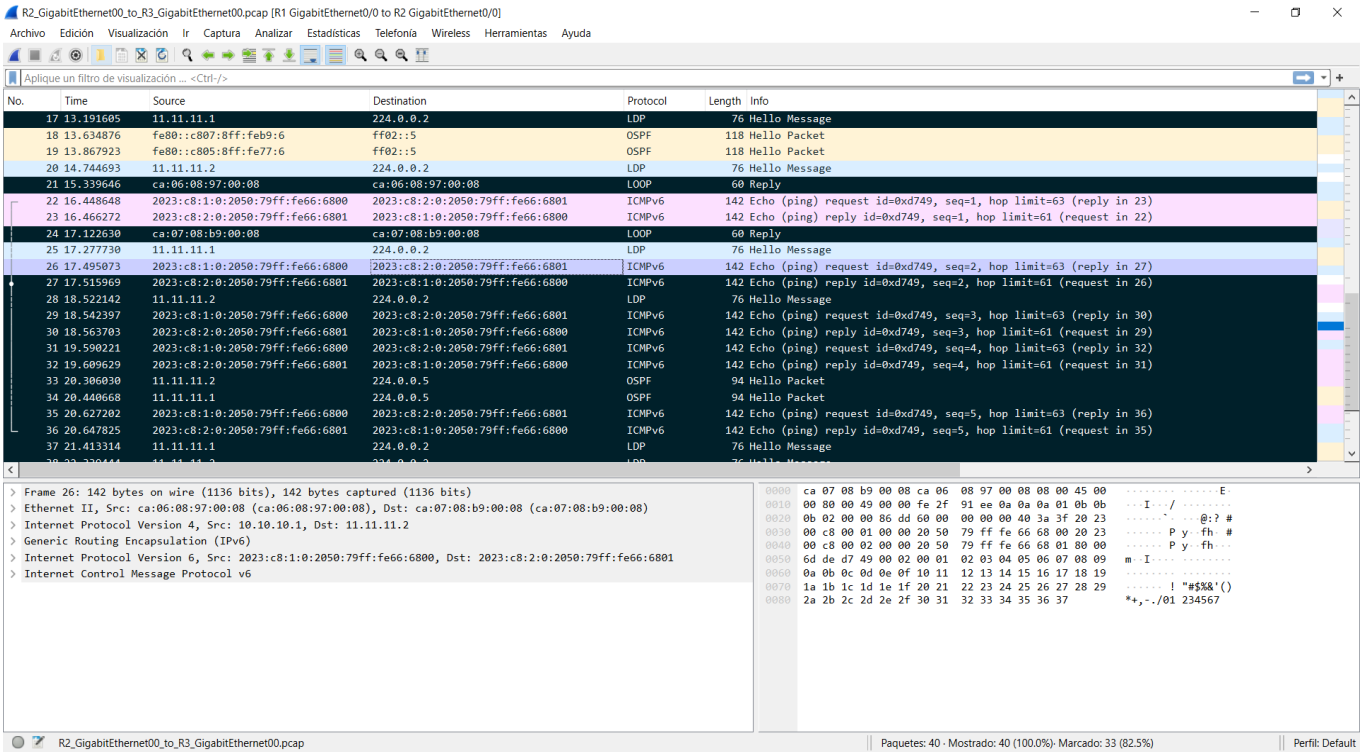


Figura 2. Análisis de Trafico de GNS3 en Wireshark

Análisis. -

9. Verificación de Conectividad

Prueba de conectividad:

Prueba de conexión desde PC1 hacia PC3

Aquí las pruebas de conectividad

CONCLUSIONES:

BIBLIOGRAFIA: