ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

IMPLEMENTACIÓN DE PRÁCTICAS DE ENRUTAMIENTO CON EQUIPOS VIRTUALIZADOS DE NETWORKING DE HUAWEI EN GNS3 Y ENSP

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO SUPERIOR EN REDES Y TELECOMUNICACIONES

Zurita Maldonado Israel Alexander
israel.zurita@epn.edu.ec

DIRECTOR: ING. FERNANDO VINICIO BECERRA CAMACHO, MSc.
fernando.becerrac@epn.edu.ec

CODIRECTOR: ING. FABIO MATÍAS GONZÁLEZ GONZÁLEZ, MSc.
fabio.gonzalez@epn.edu.ec

Quito, enero 2022

CERTIFICACIÓN

Certificamos que el presente trabajo fue desarrollado por el Sr. Zurita Maldonado Israel Alexander como requerimiento parcial a la obtención del título de TECNÓLOGO SUPERIOR EN REDES Y TELECOMUNICACIONES, bajo nuestra supervisión:

Fernando Vinicio Becerra Camacho
DIRECTOR DEL PROYECTO

Fabio Matías González González
CODIRECTOR DEL PROYECTO

DECLARACIÓN

Yo Zurita Maldonado Israel Alexander con CI: 172355585-8 declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

Sin prejuicio de los derechos reconocidos en el primer párrafo del artículo 144 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación– COESC-, soy titular de la obra en mención y otorgo una licencia gratuita, intransferible y no exclusiva de uso con fines académicos a la EscuelaPolitécnica Nacional.

Entrego toda la información técnica pertinente, en caso de que hubiese una explotación comercial de la obra por parte de la EPN, se negociará los porcentajes de los beneficios conforme lo establece la normativa nacional vigente.

Zurita Maldonado IsraelAlexander

DEDICATORIA

Con su apoyo que se fomentó en mí, con su amor, paciencia y conocimiento que ahora son plasmados en extraordinarios párrafos llenos de inspiración y por haber marcado en mí el camino a un gran futuro lleno de esfuerzos en los cuales habrá obstáculos para llegar a alcanzar el éxito. Con todo mi agradecimiento se la dedico a ustedes:

A Dios por darme la bendición, paciencia y conocimiento.
A mi querido abuelo César Maldonado y a mi querida mamá Patricia Maldonado.
A mi papá Víctor Zurita y a mi tío César Maldonado, al igual que, a toda mi familia.

Israel

AGRADECIMIENTO

Culminando esta fase estudiantil, agradezco de manera muy sincera y cordial a mis licenciados, familia y autoridades que me brindaron todo su apoyo y sabiduría, que bajo su guía me permitió crecer como estudiante y aún más como persona.

Israel

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El área de las Tecnologías de la Información y las Comunicaciones (TICs) ha tenido cambios exponenciales en temas de desarrollo de las redes de información, por lo tanto, estos cambios se ven sujetos en el proceso de aprendizaje para su respectiva implementación en el campo laboral.

En el primer capítulo se comienza con la introducción hacia la importancia del manejo de los programas eNSP y GNS3 para los alumnos de la Escuela de Formación de Tecnólogos de la EPN enfocada en el área de la información, al igual que, se detalla los objetivos planteados para el presente proyecto.

En el segundo capítulo se establece la metodología utilizada para el desarrollo del proyecto de titulación, además de ser utilizada en la elaboración de las cinco hojas guías propuestas para prácticas de laboratorio las cuales aportarán con la información adecuada para configurar los equipos virtualizados de la marca Huawei.

El tercer capítulo establece los protocolos y tecnologías a utilizar que son estudiados en las materias de TCP/IP y Redes de Computadoras y configurados en el programa de Cisco. Esto a su vez ha permitido relacionar al estudiante con las bases necesarias para configurar las topologías de red propuestas para las 5 prácticas de laboratorio con equipos virtualizados de la marca Huawei.

El cuarto capítulo presenta las conclusiones y recomendaciones obtenidas durante la elaboración del proyecto de titulación.

Y finalmente, el último capítulo corresponde a las referencias bibliográficas utilizadas en el presente proyecto.

PALABRAS CLAVE: Enrutamiento, GNS3, eNSP, Redes.

ABSTRACT

The area of Information and Communication Technologies (ICT) has had exponential changes in the development of information networks; therefore, these changes are subject to the learning process for their respective implementation in the labor field.

The first chapter begins with the introduction to the importance of using the eNSP and GNS3 programs for the students of the EPN Technologist Training School focused on the information area, as well as the objectives raised for this project.

The second chapter establishes the methodology used for the development of the degree project, in addition to being used in the elaboration of the five proposed guide sheets for laboratory practices, which will provide adequate information to configure the virtualized equipment of the Huawei brand.

The third chapter establishes the protocols and technologies to be used that are studied in the subjects of TCP / IP and Computer Networks and configured in the Cisco program that in turn has allowed the student to relate to the necessary bases to configure network topologies proposals for the 5 laboratory practices with virtualized equipment of the Huawei brand.

The fourth chapter presents the conclusions and recommendations obtained during the development of the degree project.

And finally, the last chapter corresponds to the bibliographic references used in this project.

KEYWORDS: *Routing, GNS3, eNSP, Networking.*

1. INTRODUCCIÓN

Ecuador cuenta con un sistema educativo que se basa en normativas y reglamentos que garantizarán el éxito de los estudiantes que a futuro serán profesionales calificados, competitivos y productivos. Los logros de aprendizaje del alumno son indicadores de desempeño y calidad dentro del sector educativo, pero fundamentalmente se enfocan en el desarrollo del país [1].

El régimen educativo es eficiente, aunque basándose en procesos repetitivos con programas que se orientan más a la parte teórica que a la práctica. El proceso de aprendizaje educativo se fomenta en la utilización de programas orientados a la configuración de equipos con un alto grado de similitud con los equipos existentes, añadiendo que son *softwares* libres que ofrecen ambientes flexibles e intuitivos como es el caso de los programas GNS3 y eNSP [2].

El presente proyecto de titulación tiene como objetivo la implementación de prácticas de *networking* a base de equipos virtualizados de la marca Huawei, y se orientará a la carrera de Tecnología Superior en Redes y Telecomunicaciones de la Escuela de Formación de Tecnólogos, en donde, solo se utiliza programas de la marca Cisco. Por esta razón, como herramienta de estudio para futuros estudiantes que cursarán la carrera los programas eNSP y GNS3 serán utilizados en los laboratorios virtuales propuestos para este proyecto.

Por lo tanto, se garantizará el dejar a un lado la dependencia de enseñanza de manejo de una sola marca de equipo de *networking* dentro de la formación de los futuros profesionales en el sector de las redes de la información.

1.1 Objetivo general

Implementar prácticas de enrutamiento con equipos virtualizados de *networking* de la marca HUAWEI en GNS3 y eNSP.

1.2 Objetivos específicos

- Realizar un estudio de emuladores a utilizar eNSP y GNS3.
- Establecer las tecnologías y los protocolos que se van a utilizar con una topología base con equipos *networking* Huawei.
- Desarrollar las topologías de red utilizando los equipos Huawei.
- Realizar pruebas de las topologías implementadas.
- Realizar las hojas guías tanto para los profesores como estudiantes.

1.3 Fundamentos

Con la introducción de nuevas marcas de dispositivos, tecnologías, protocolos y programas en el mercado de las redes y telecomunicaciones, el uso de hipervisores por parte de los futuros especialistas en el área de las redes de información se ha visto envuelto en resultados favorables al momento de configurar dichos equipos [3].
El uso de estos programas de virtualización ha permitido que los estudiantes logren familiarizarse con la configuración de equipos de *networking* reales [4].

Simulación de redes

Compañías como Cisco y Huawei han ampliado su mercado a nivel global con la introducción de equipos de red a nivel LAN (Red de Área Local) y WAN (Red de Área Amplia) [3].
La simulación de una red se utiliza como herramienta de apoyo ante los procesos de configuración de diferentes dispositivos de *networking* con el equipo final [3]. Además, permite evaluar el desempeño del sistema sin la necesidad de adquirir el equipo real. Lo cual genera, la reducción y la prevención de errores al momento de configurar en el ámbito laboral [3].
Huawei ha crecido progresivamente en Ecuador [3], satisfaciendo el requerimiento de equipos de conectividad en áreas de mayor demanda de servicios. Por lo cual, diseñó el programa eNSP *(Enterprise Network Simulation Platform)* que es la plataforma de simulación de gran utilidad para estudiantes en la rama de las redes de información [5].

GNS3 y eNSP como herramientas fundamentales en las redes de información

En el área de las redes de información, existen diversas herramientas que permiten simular el comportamiento de equipos de red como es el caso de *AdventNET, ns2, Packet Tracer, Boson, H3C Cloud*; sin embargo, estos programas no cumplen con el procesamiento y configuración para generar topologías con un ambiente de mayor complejidad [6].

Plataformas como GNS3 y eNSP presentan grandes ventajas respecto a las demás plataformas de simulación, entre las que resalta el alto grado de semejanza y compatibilidad con dispositivos de *networking* reales. Además de ser programas con licenciamiento libre, y con gran aceptación por parte de marcas como Fortinet, Cisco, Huawei, Avaya para su utilización en los cursos de certificación [6].

GNS3

Permite reproducir con precisión dispositivos reales del área de *networking* por medio de su plataforma local que se accede por aplicación o por servicio remoto mediante la *web*. Implementa una plataforma para el diseño de topologías de red idónea para que el estudiante logre familiarizarse con los dispositivos de red configurando los equipos virtualizados [3].

Lo que caracteriza a este simulador es la interoperabilidad que tiene con dispositivos de diferentes marcas presentes en el área de las redes y telecomunicaciones [3].

eNSP

Es una plataforma de simulación de dispositivos reales que permite a los usuarios familiarizarse con los dispositivos de red de la marca Huawei. Al mismo tiempo, permite realizar pruebas experimentales con los dispositivos virtualizados en donde el estudiante logra simular una red configurando equipos de la marca mencionada, ayudando a mejorar las habilidades de configuración y despliegue de redes con mayor eficiencia [3].

2. METODOLOGÍA

2.1 Descripción de la metodología usada

El impacto de nuevos mecanismos de enseñanza orientados a la práctica, ha generado como resultado el uso de laboratorios virtuales que abarcan beneficios en el proceso de aprendizaje para el alumno, permitiéndoles el acceso a recursos de configuración de equipos virtualizados.

El proyecto de titulación se basará en la creación de cinco guías de estudio orientadas a las prácticas de laboratorio que se utilizarán en los cursos de Redes de Computadoras que se imparten en la carrera de Tecnología Superior en Redes y Telecomunicaciones.

Por lo cual, se elaboró hojas guía de configuración de equipos virtualizados de la marca Huawei, comenzando con el estudio de los programas a utilizar como son eNSP y GNS3 en los cuales cabe resaltar la alta similitud de configuración con dispositivos reales, de manera gratuita en un ambiente flexible e intuitivo para el alumno [2].

Una vez establecida la introducción de estudio de los programas a utilizar, se procede a configurar los protocolos y tecnologías a emplear, que son estudiados y analizados previamente en las materias de TCP/IP y Redes de Computadoras y puestos a práctica en el programa Cisco Packet Tracer, que a su vez ha permitido relacionar al estudiante con las bases necesarias para el establecimiento de enlaces en una topología tanto a nivel WAN como LAN.

Finalmente, se procede a desarrollar y configurar las respectivas topologías de red en donde se mostrará el comportamiento de protocolos de enrutamiento como RIP (Routing Information Protocol), OSPF (Open Shortest Path First) y IS-IS (Intermediate System to intermediate System) y a nivel de enlace como PPP (Point-to-Point Protocol), HDLC (High-Level Data Link Control). Al igual que, su respectiva configuración mediante comandos y desarrollo de la misma en los diferentes ambientes de redes y tecnologías establecidas para las guías de estudio, en donde se encuentra el establecimiento de servicios de seguridad como la implementación de firewall básico, ejecución de DHCP (protocolo de configuración dinámica de host), configuración Frame Relay como sistema de transporte de datos dentro de una red.

3. RESULTADOS Y DISCUSIÓN

La elaboración de hojas guía de laboratorio permitirá poner en práctica los conocimientos adquiridos en el área de las redes de información. Por lo tanto, se planteó la elaboración de cinco prácticas de laboratorio, donde se detalla paso a paso las actividades a realizar para una mejor comprensión del tema a estudiar.

3.1 Estudio de los programas eNSP y GNS3

Los programas eNSP y GNS3 permiten el manejo de equipos virtualizados de red, además de configurarlos sin tener que adquirirlos físicamente [4]. Estos programas han hecho posible que el ambiente de laboratorios virtuales se convierta en la herramienta principal para la formación de los estudiantes [5].

Programas orientados a las redes de la información

Con la evolución exponencial de las redes de información se ha producido el desarrollo de programas capaces de demostrar la conducta de las diversas configuraciones asumidas por dispositivos de red de forma virtual, sin la necesidad de adquirir los equipos reales [7]. Programas como eNSP y GNS3 han permitido establecer un alto grado de similitud de comportamiento de dispositivos a nivel de *networking* [2].

Por lo tanto, para este trabajo de titulación se realizó un análisis de las plataformas eNSP y GNS3, que serán los programas principales de configuración para los equipos virtualizados de Huawei. Por lo cual, se pretende que el estudiante configure los equipos de red basándose en comandos ya utilizados en Cisco, con el objetivo de que el alumno relacione el conocimiento adquirido en las materias de TCP/ IP y Redes de Computadoras con equipos de la marca Huawei.

Arquitectura de eNSP

El programa eNSP presenta una arquitectura particular que se asemeja a GNS3, por lo tanto, requerirá de un hipervisor que permitirá ejecutar los dispositivos de *networking* de Huawei [5]. Por lo cual, se considera que eNSP posee una arquitectura de dos capas:

- **eNSP:** Interfaz de desarrollo de Huawei
- **Hipervisor:** *VirtualBox* de Oracle.

Arquitectura de GNS3

GNS3 trabaja de forma local mediante su aplicación de escritorio y de manera remota a través de su servidor *web*. Utiliza hipervisores como *VirtualBox* o *VMware* para lograr el funcionamiento de los diferentes dispositivos virtualizados que permitirán analizar el comportamiento tanto de la red como de los mismos dispositivos de *networking* [2]. Consta de dos componentes:

- **GUI de GNS3:** Es la interfaz gráfica del usuario que permite crear topologías y agregar dispositivos en un mismo espacio de trabajo.
- **Máquina virtual GNS3:** Permite la ejecución de máquinas virtuales en el ordenador, utilizando el programa *VirtualBox* o *VMware Workstation*.

GNS3 permite simular el comportamiento de los diferentes dispositivos de red existentes en el mercado de las redes de información, añadiendo que la simulación de los dispositivos virtualizados en este programa conlleva al consumo de recursos del ordenador lo cual puede afectar al rendimiento del mismo [8].

Protocolos de enrutamiento dinámico RIP, OSPF e IS-IS

Los protocolos de enrutamiento son mecanismos de transferencia de paquetes existentes entre redes de comunicación [2]. Los equipos de red de capa 3 admiten rutas directas, estáticas y dinámicas en su procesamiento para el envío y recepción de paquetes dentro de una intranet o fuera de la misma.

Los protocolos de enrutamiento son reglas establecidas en los enrutadores con el objetivo de descubrir nuevas rutas hacia un destino establecido dentro de una red, generando tablas de enrutamiento mediante el conocimiento de métricas, caminos o rutas a una nueva red generando una guía de apoyo para el reenvío de paquetes [9].
Conforme el establecimiento de la tabla de enrutamiento se puede generar diferentes tipos de rutas que se clasifican según su origen:

- **Rutas directas:** son descubiertas mediante el mismo enrutador.
- **Rutas estáticas:** se configuran manualmente por los administradores de red.
- **Rutas dinámicas:** son descubiertas mediante protocolos de enrutamiento dinámico.

El proceso de enrutamiento dinámico incluye protocolos como:

RIP: Es un protocolo *Internal Gateway Protocol* (IGP) de vector de distancia. En comparación con otros protocolos de enrutamiento, RIP utiliza los saltos como métrica por defecto, es decir, los saltos son la cantidad de enrutadores a través de los cuales pasa un paquete para llegar a su destino y se registra en la tabla de enrutamiento del *router* [10].

La métrica de RIP comprende un valor de hasta 15 saltos para llegar a un destino. Una métrica de 16 indicaría que el ordenador al cual se pretende establecer la comunicación es inalcanzable [11].

La evolución que ha tenido RIP como protocolo de enrutamiento se ha visto mejorada con base a mecanismos de transporte de información, autenticación y Máscara de Subred de Longitud Variable (VLSM). En su comienzo, este protocolo de enrutamiento se incorporó al mercado de las telecomunicaciones como protocolo *classfull* (RIP versión 1), hasta evolucionar en un protocolo *classless* (RIP versión 2) mejorando las características del protocolo [10].

OSPF: Es un protocolo de enrutamiento jerárquico IGP utilizado en redes de gran tamaño. *OSPF distribuye la información entre* todos los enrutadores que formen parte del mismo Sistema Autónomo (AS). Usa el costo de un enlace como métrica por defecto y mediante el algoritmo de Dijkstra calcula la ruta óptima de comunicación entre nodos [10].

Elabora una base de datos de estado de enlace en donde identifica a todos los enrutadores pertenecientes a la misma área mediante el *Link State Advertisement* (LSA) que son los paquetes que tienen la información de los vecinos y costos de cada enlace [10].

Por defecto, todos los enrutadores en OSPF se encuentran ubicados en el área cero dependiendo de la segmentación realizada por el administrador de red. Al implementar este protocolo de enrutamiento se reduce la sobrecarga de procesamiento en los *routers* y ante un cambio de topología recalcula las rutas en un periodo de tiempo corto [11].

IS-IS: Es un protocolo IGP desarrollado para la transmisión de paquetes por la mejor ruta mediante el algoritmo *Shortest Path First* (SPF) para entregar el paquete respectivo a su destino en el menor tiempo posible.

Utiliza una jerarquía de enrutamiento de dos niveles para dominios de enrutamiento de gran alcance y dividirlos en áreas pequeñas [11].

El enrutamiento dentro de una misma área se lo conoce como enrutamiento de nivel 1 y el enrutamiento entre áreas como de nivel 2. Un sistema que está tanto en el nivel 1 como en el nivel 2 se denomina de nivel 1-2 [10].
Por lo tanto, es implementado para la difusión de la información de manera eficaz dentro de un dominio administrativo como lo es el Proveedor del Servicio de Internet (ISP).

Servicios en red

Los servicios de red son utilizados para integrar la comunicación entre diferentes ordenadores de una red [2]. Estos servicios son complementarios para la mayoría de pequeñas y grandes empresas, por lo tanto, es una herramienta ideal tanto a nivel de seguridad como de configuración. Todo lo mencionado fue desarrollado con el objetivo de facilitar la comunicación, fortalecer la estabilidad y seguridad del envío de información [2].

Los servicios de red son configurados en la LAN de las empresas para conservar la estabilidad de una operación delegando automáticamente diversos servicios que contribuyen a la red local sin problemas [2].

En la actualidad existen diversos tipos de servicios de red, para este trabajo de titulación se va a utilizar solo DHCP y la implementación de un *firewall* básico.

Protocolo de configuración dinámica de *host* (DHCP)

DHCP fue creado para poder simplificar la asignación de direcciones IP de forma dinámica facilitando el trabajo del administrador de red [2]. En cuanto al proceso de ejecución de este protocolo frecuentemente se lleva a cabo de manera automática siempre que los ordenadores:

- Solicitan información TCP/IP al DHCP.
- Ante la gestión y asignación de direccionamiento IP para el ordenador.

Cortafuegos o *Firewall*

Es un *software* o *hardware* que bloquea la entrada no autorizada de dispositivos o servicios a la red. Los cortafuegos buscan la estabilidad informática implementando políticas de acción y denegación de servicios [3].

La política de denegación bloquea todo el tráfico no autorizado a nivel de red como bloqueo de puertos y protocolos. Para la protección de los sistemas informáticos, se cuenta con métodos de control de acceso o *Access Control List* (ACL) en donde se implementa la utilización de *las* listas blancas que permiten el acceso de sistemas basados en su dirección *Internet Protocol* (IP) o *Media Access Control* (ACL) y las listas negras que es el sistema de registro de acceso no autorizado de dispositivos en la red.

Tecnologías de transporte dentro de una red

***Frame Relay*:** Es una tecnología de transporte de alta velocidad orientada a la conexión, por lo tanto, en un sistema de transmisión de información a través de una Red de Área Extendida (WAN). *Frame Relay* divide la información en paquetes, en donde, cada trama tiene una etiqueta que la red usa para dictaminar el destino de la misma [10].
Puede transportar diversos protocolos de capa de red (incluido IP) con una calidad de servicio determinada.

MPLS: Es una tecnología de transporte de etiquetas conmutadas que puede transportar múltiples protocolos de red a nivel de capa 3 y capa 2 orientada a la conexión. Esta tecnología de transporte de alta velocidad envía información a través de etiquetas donde contiene la información de los mismos enrutadores *Multiprotocol Label Switching* (MPLS) con el objetivo de determinar el destino de los paquetes [10].
Cada paquete cuenta con su respectiva etiqueta dentro de la red para resolver el destino de la trama. En una red MPLS se puede definir rutas por el administrador o dejar que el enrutamiento IP decida la ruta. Las redes MPLS pueden utilizar *Frame Relay* o *Asyncronous Transfer Mode* (ATM) lo que hace posible que sea prolongable a muchos entornos, incluidas *Synchronous Digital Hierarchy* (SDH) y redes ópticas.
Para que exista la comunicación entre las etiquetas de MPLS, los enrutadores usan protocolos como *Border Gateway Protocol* (BGP) o *Resource Reservation Protocol* (RSPV), pero específicamente utilizan el protocolo de distribución de etiquetas como es *Label Distribution Protocol* (LDP) que usa TCP para el establecimiento de sesiones en donde se informa a los otros enrutadores de MPLS el mapeo de etiquetas existente [10].

Implementación de topología entre GNS3 y eNSP

A continuación, se describe la conexión entre GNS3 y eNSP, en donde los dispositivos de red correspondientes a Cisco y Huawei trabajan bajo los mismos sistemas estandarizados a nivel de equipos de red, lo cual permite conectarse entre sí [10].

En la Figura 3.1 se visualiza los equipos correspondientes para la interconexión entre los dos programas en donde se utilizó un enrutador virtualizado de la marca Cisco modelo C3600 y uno de la marca Huawei modelo AR3200. También, se utilizó como puente de interconexión la *cloud* de cada simulador. Con esta herramienta se establece la conexión mediante puertos UDP entre estos dos programas.

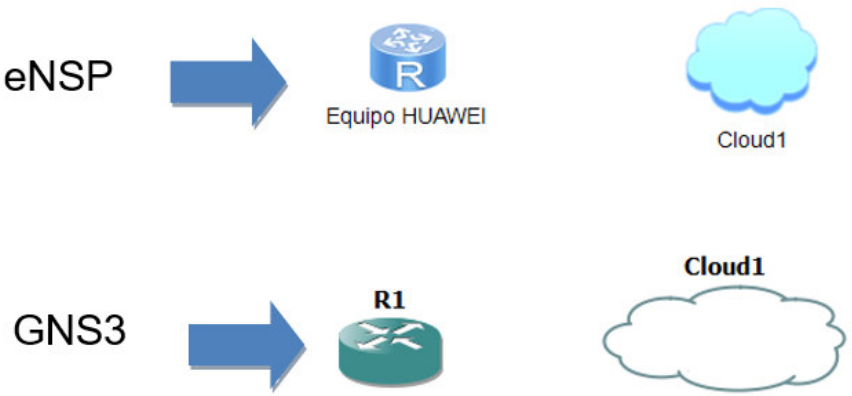


Figura 3.1 Equipos de conexión entre eNSP y GNS3

En la Figura 3.2 y Figura 3.3 se visualiza la configuración respectiva de puertos UDP para la conexión entre los diferentes programas a integrar, para ello, en la hoja guía 5 del instructor se puede observar detalladamente el proceso de configuración realizado.

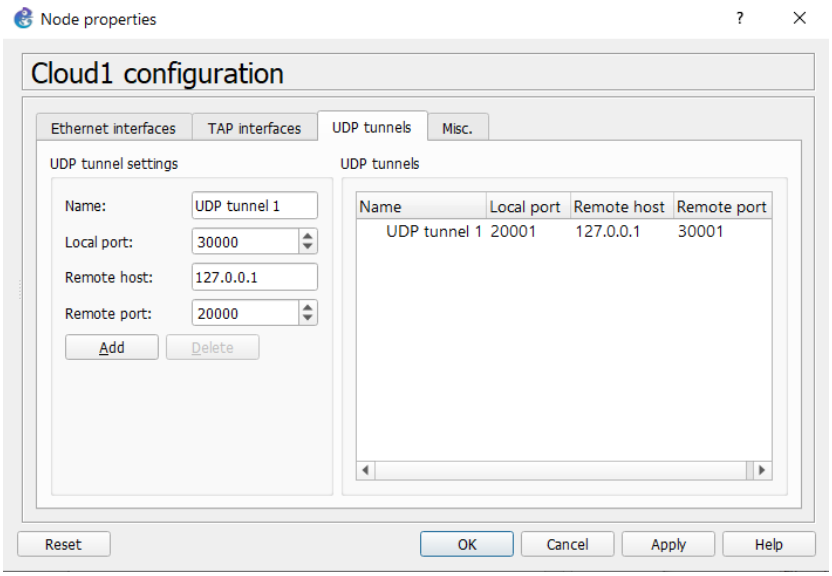


Figura 3.2 Agregación de puerto UDP en GNS3

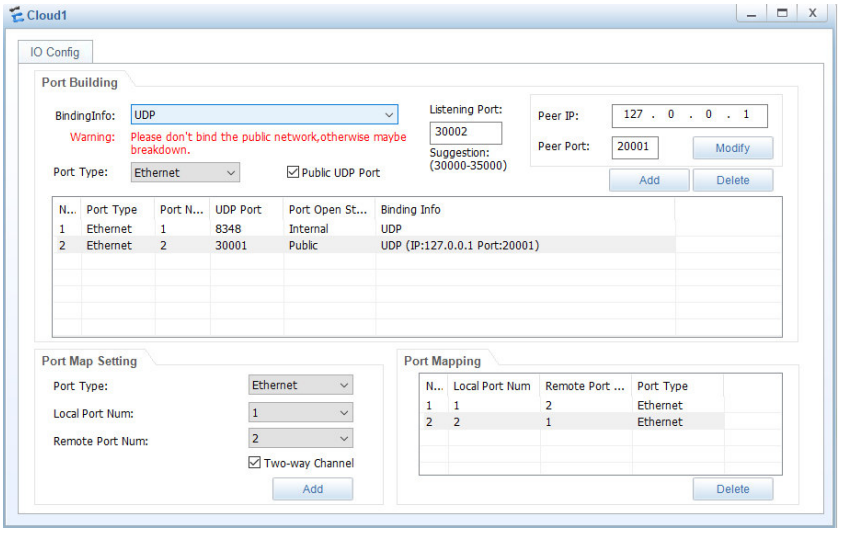


Figura 3.3 Agregación de puertos UDP en eNSP

En la Figura 3.4 se puede visualizar el enlace de los equipos hacia la respectiva nube, los cuales previamente fueron configurados con base a sus puertos UDP de conexión para generar el puente de conexión entre estos dos programas.

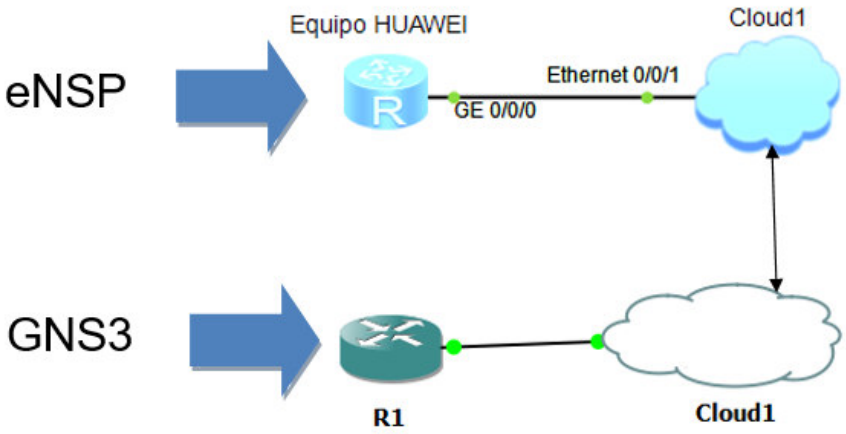


Figura 3.4 Conexión entre enrutadores y programas mediante un túnel UDP

Comandos de configuración en equipos Huawei y su equivalente en Cisco

Tabla 3.1 Comandos básicos de Cisco y su equivalente en Huawei [8] [12]

Cisco	Huawei
ping	ping
traceroute	tracert
show	display
show interfaces	display interface
show ip route	display routing-table
show ip interface	display ip interface
show version	display versión
show ip “protocolo”	display “protocolo” routing-table
show clock	display clock
show port	display port-mapping
show users	display users
exit	quit
end	return
show running config	display currrent-configuration
show startup-config	display saved-configuration
erase startup	delete saved-configuration
write mem – wr – copy run start	save
telnet	telnet
no	undo
terminal monitor	terminal monitor
reload	reboot
router (rip, ospf, is-is)	“protocol”
show mac address-table	display mac address-table
redistribute	import route

En la Tabla 3.1 se puede visualizar una recopilación de comandos utilizados en el programa de Cisco para la configuración de los equipos, por lo tanto, con base a estos comandos se elaboró una lista básica de los mismos, pero con su equivalente en Huawei. Con el objetivo de que el estudiante logré configurar equipos de esta marca con el conocimiento ya adquirido en configurar equipos virtualizados en Cisco.

3.2. Establecer las tecnologías y los protocolos que se van a utilizar con una topología base con equipos de *networking* Huawei

eNSP permite la utilización de ordenadores, enrutadores y conmutadores de la marca mencionada y deja llevar a cabo pruebas experimentales con el objetivo de involucrarse con las tecnologías de la red sin utilizar dispositivos reales de Huawei.

A continuación, se presentan las diferentes topologías previstas para el proyecto de titulación, en donde se detalla la configuración respectiva de los diferentes dispositivos de red utilizados al igual que los protocolos de enrutamiento, servicios de red y direccionamiento.

Red 1: Topología de red con enrutamiento dinámico en base a RIP, OSPF, IS-IS

En la siguiente topología de red presentada en la Figura 3.5 se establece la utilización de protocolos de enrutamiento dinámico como RIP, OSPF y IS-IS en equipos virtualizados de Huawei. Los enrutadores AR3200 serán los equipos en donde se configurará la respectiva conexión entre los dispositivos mediante la utilización del comando *import route* que permitirá ejecutar la redistribución de diferentes rutas mediante protocolos de enrutamiento.

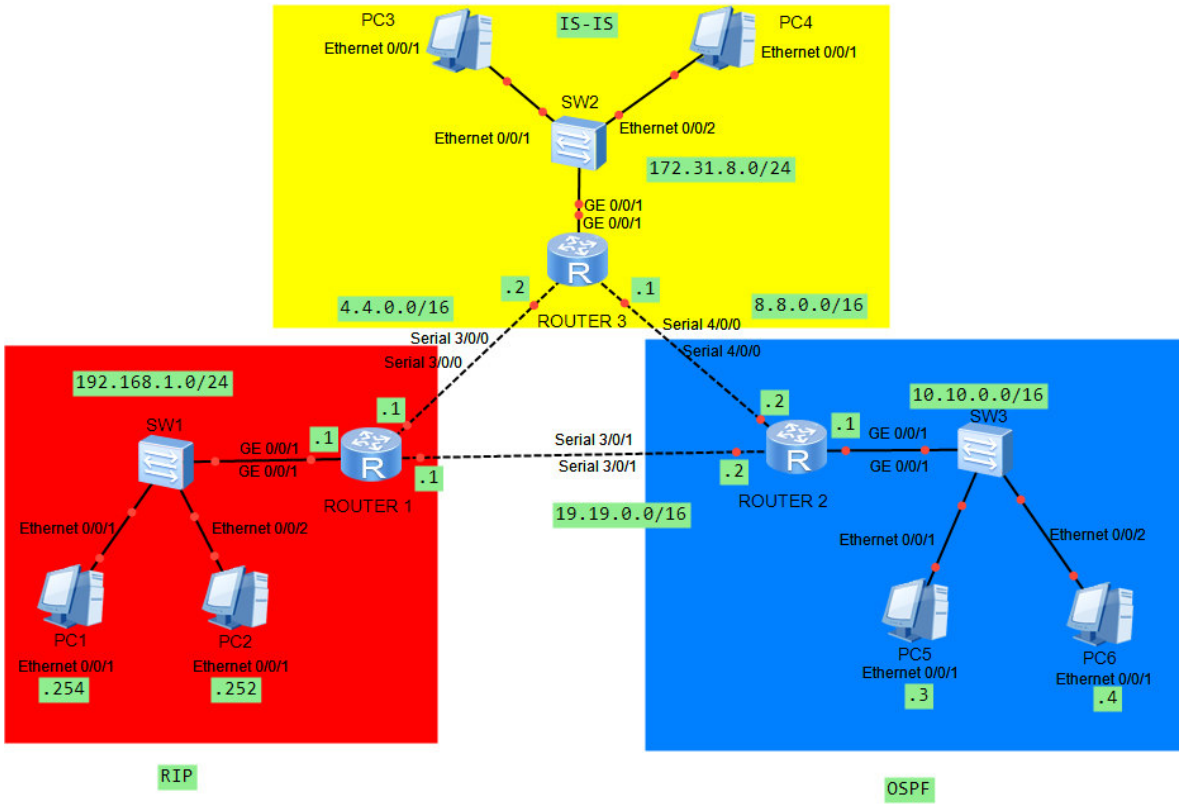


Figura 3.5 Topología base para realizar enrutamiento dinámico

Configuración de enrutamiento en dispositivos Huawei

- **Configuración básica del sistema**

En la Figura 3.6 se muestra la configuración básica realizada de cada enrutador, en donde se estableció mecanismos básicos para la identificación de cada dispositivo mediante el comando *sysname* y se añadió una cabecera de texto con el comando *header shell information.*

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sys
[Huawei]sysname Router_1
[Router_1]he
[Router_1]header s
[Router_1]header shell i
[Router_1]header shell information "BIENVENIDO AL ROUTER 1"
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sys
[Huawei]sysname ROUTER_2
[ROUTER_2]hea
[ROUTER_2]header sh
[ROUTER_2]header shell in
[ROUTER_2]header shell information "BIENVENIDO AL ROUTER 2"
[ROUTER_2]quit
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sys
[Huawei]sysname ROUTER_3
[ROUTER_3]head
[ROUTER_3]header s
[ROUTER_3]header shell i
[ROUTER_3]header shell information "BIENVENIDOS AL ROUTER 3"
```

Figura 3.6 Modificación de cabecera de bienvenida y cambio de nombre en el enrutador

- **Configuración de autenticación**

En la Figura 3.7 se muestra el proceso de configuración de un mecanismo de autenticación por contraseña mediante la utilización del comando *authentication-mode password.* Al establecer el requerimiento de contraseña encriptada se lo añade mediante el comando *set autentication password cipher.*

```
[Router_1]user-interface console 0
[Router_1-ui-console0]au
[Router_1-ui-console0]authentication-mode pas
[Router_1-ui-console0]authentication-mode password
Please configure the login password (maximum length 16):123456
[ROUTER_2]user-interface console 0
[ROUTER_2-ui-console0]au
[ROUTER_2-ui-console0]authentication-mode pas
[ROUTER_2-ui-console0]authentication-mode password
Please configure the login password (maximum length 16):123456
[ROUTER_3]user-interface console 0
[ROUTER_3-ui-console0]au
[ROUTER_3-ui-console0]authentication-mode pas
[ROUTER_3-ui-console0]authentication-mode password
Please configure the login password (maximum length 16):123456
```

Figura 3.7 Establecimiento de sistema de autenticación por contraseña

- **Asignación de direccionamiento IP en cada enrutador**

Tabla 3.2 Direccionamiento IP asignado para diferentes dispositivos

Direccionamiento	Protocolo de enrutamiento a utilizar
192.168.1.0/24	RIP
172.31.8.0/24	IS-IS
10.10.0.0/16	OSPF
4.4.0.0/16	Enlace serial 1 RIP - IS-IS
19.19.0.0/16	Enlace serial 2 RIP - OSPF
8.8.0.0/16	Enlace serial 3 OSPF - IS-IS

En la Tabla 3.2 se muestra el direccionamiento establecido para los protocolos de enrutamiento e interfaces seriales que utilizará cada dispositivo.

En las Figura 3.8 y Figura 3.9 se muestra la configuración realizada para la asignación de direccionamiento IP en cada interfaz de los enrutadores. Esta asignación de direccionamiento se realiza entrando a cada interfaz de los dispositivos mediante el comando *interface GigabitEthernet* o Serial en cada enrutador y se asigna las direcciones IP a cada interfaz mediante el comando *ip address*.

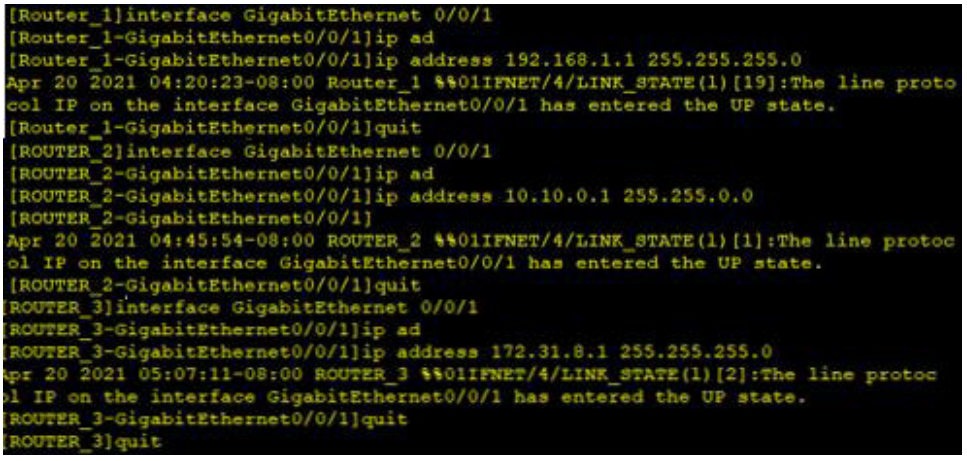


Figura 3.8 Establecimiento de direccionamiento IP a la interfaz GigabitEthernet

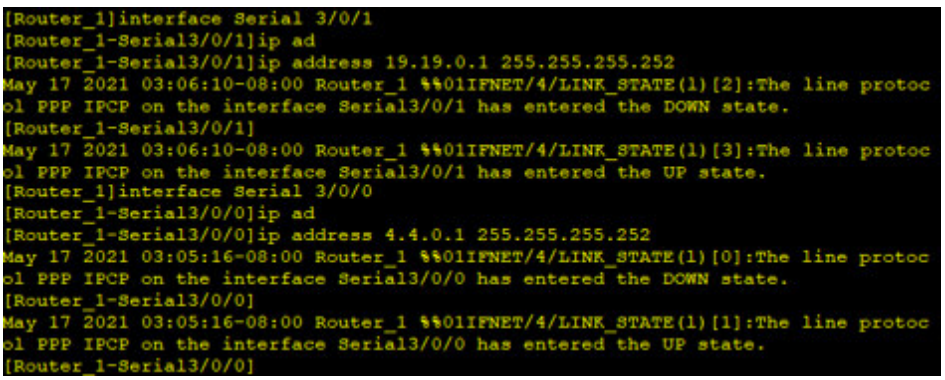


Figura 3.9 Establecimiento de direccionamiento IP a la interfaz Serial en cada enrutador

Establecido el direccionamiento IP en cada interfaz se procede a configurar el protocolo de enrutamiento dinámico asignado en cada enrutador

- **Protocolo de enrutamiento RIP**

En la Figura 3.10 se muestra los comandos utilizados para establecer RIP, el cual se determina estableciendo la versión del protocolo a utilizar y las redes que se encuentran conectadas al enrutador y se lo añade mediante el comando *network.*

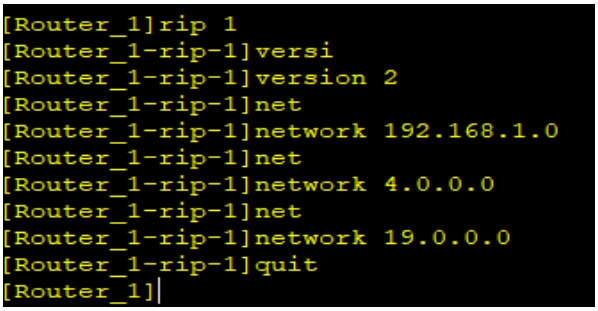


Figura 3.10 Configuración de protocolo de enrutamiento RIP

- **Protocolo de enrutamiento OSPF**

En la Figura 3.11 se muestra el proceso de establecimiento de OSPF, el cual se determina con base al sistema autónomo y el área en donde el protocolo de enrutamiento establecerá el envío de paquetes. Al igual que en RIP, se añade las redes conectadas al enrutador mediante el comando *network.*

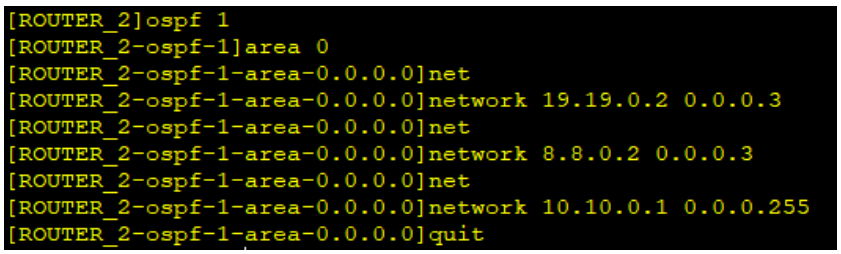


Figura 3.11 Configuración de OSPF

- **Protocolo de enrutamiento IS-IS**

En la

Figura **3.12** se muestra el proceso de establecimiento del protocolo IS-IS el cual se determina mediante un identificador de red con el comando *network-entity* y estableciéndolo en cada interfaz del enrutador con el comando *isis enable.*

```
[ROUTER_3] isis 1
[ROUTER_3-isis-1]net
[ROUTER_3-isis-1]network-entity 10.0001.0000.0000.1111.00
May 17 2021 03:53:30-08:00 ROUTER_3 %%01ISIS/4/START_ENABLE_ISIS(l)[0]:ISIS 256
enabled all ISIS modules.
[ROUTER_3-isis-1]
[ROUTER_3-isis-1]quit
[ROUTER_3]in
[ROUTER_3]interface serial 4/0/0
[ROUTER_3-Serial4/0/0]isis enable
[ROUTER_3-Serial4/0/0]quit
[ROUTER_3]interface serial 3/0/0
[ROUTER_3-Serial3/0/0]isis enable
[ROUTER_3-Serial3/0/0]quit
```

Figura 3.12 Configuración de protocolo de enrutamiento RIP

En la Figura 3.13 se muestra el establecimiento de la redistribución de protocolos de enrutamiento, lo cual se realiza mediante el comando *import route* con la siguiente sintaxis:

```
import-route:
   -  rip [ process-id-rip] [ cost cost | type type | tag tag | route-
      policy route-policy-name
   -  static [ cost cost | type type | tag tag | route-policy route-
      policy-name
   -  isis [ process-id-isis] [ cost cost | type type | tag tag |
      route-policy route-policy-name
   -  ospf [ process-id-ospf] [ cost cost | type type | tag tag |
      route-policy route-policy-name]}
```

Figura 3.13 Sintaxis del comando *import route* para protocolos de enrutamiento

Red 2: Topología de red con servicios DHCP y *Firewall*

En la Figura 3.14 se muestra una topología base para el establecimiento de un *firewall* básico en el enrutador AR3260 de Huawei, en donde se establece una lista de control de denegación o lista negra. Además, se configura el servicio de DHCP para la asignación automática de direccionamiento IP.

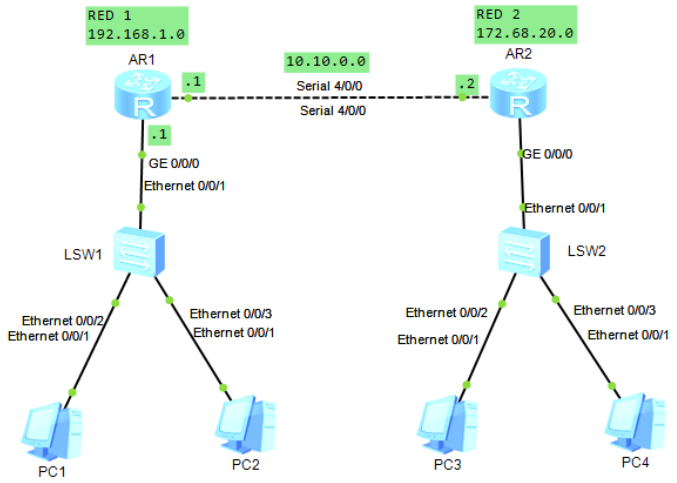


Figura 3.14 Topología implementada para ejecutar DHCP y servicio de Firewall

- **Configuración de DHCP en el enrutador AR3260**

En la Figura 3.15 se establece la configuración dinámica de asignación de direccionamiento IP en cada enrutador de la red. Con el comando *dhcp enable* se habilita este servicio y con el comando *ip pool* se especifica el nombre de la pila de direcciones en donde contiene la dirección IP de la red que se establece por el comando *network*, la dirección de salida o *gateway* con el comando *gateway-list,* la dirección de Sistema de Nombres de Dominio (DNS) con el comando *dns-list*.

```
<R1>system-view
Enter system view, return user view with Ctrl+Z.
[R1]dhcp enable
Info: The operation may take a few seconds. Please
[R1]ip pool R1
Info: It's successful to create an IP address pool.
[R1-ip-pool-R1]network 192.168.1.0
[R1-ip-pool-R1]gateway-list 192.168.1.1
[R1-ip-pool-R1]dns-list 4.2.2.2
[R1-ip-pool-R1]quit
[R2]dhcp enable
[R2]ip pool R2
[R2-ip-pool-R2]network 172.68.20.0
[R2-ip-pool-R2]gateway-list 172.68.20.1
[R2-ip-pool-R2]dns-list 4.2.2.2
[R2-ip-pool-R2]quit
```

Figura 3.15 Configuración del servicio DHCP en los enrutadores Huawei AR3260

Establecidos los parámetros de DHCP, se habilita en cada interfaz del enrutador el servicio de asignación dinámica con el comando *dhcp select global* como se muestra en la Figura 3.16.

```
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]ip address 192.168.1.1 24
Jun  9 2021 04:30:34-08:00 R1 %%01IFNET/4/LINK_STATE(l)[1
on the interface GigabitEthernet0/0/1 has entered the UP
[R1-GigabitEthernet0/0/1]dhcp sel
[R1-GigabitEthernet0/0/1]dhcp select g
[R1-GigabitEthernet0/0/1]dhcp select global
[R1-GigabitEthernet0/0/1]quit
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]ip address 172.68.20.1 24
Jun 11 2021 05:43:43-08:00 R2 %%01IFNET/4/LINK_STATE(l)[0]:The
on the interface GigabitEthernet0/0/1 has entered the UP state.
[R2-GigabitEthernet0/0/1]quit
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]dhcp select global
[R2-GigabitEthernet0/0/1]quit
```

Figura 3.16 Establecimiento de DHCP en cada interfaz del enrutador

Establecido el servicio de asignación dinámica de direccionamiento IP en las interfaces de los enrutadores, se procede a habilitar este servicio en los ordenadores de la red. En la Figura 3.17 se muestra el establecimiento del DHCP en los ordenadores, lo cual se realiza entrando a las configuraciones de las computadoras virtualizadas y habilitando el servicio.

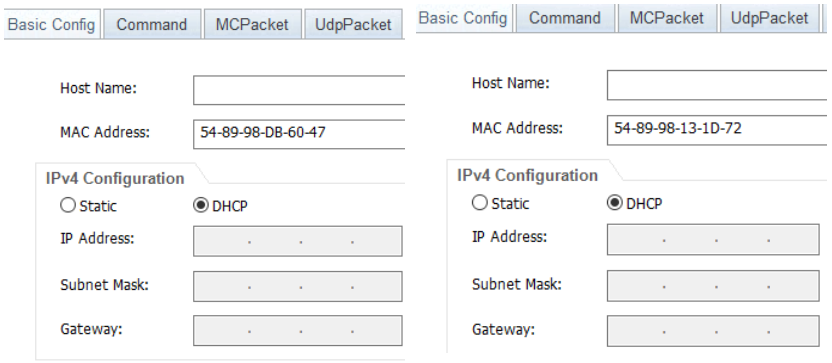


Figura 3.17 Establecimiento de DHCP en cada ordenador

- **Configuración de *firewall* en el enrutador AR3260**

En la Figura 3.18 se muestra la configuración de un cortafuegos que por defecto viene preinstalado en los enrutadores de red y se ejecuta mediante el comando *firewall* agregando el mecanismo de seguridad a ejecutar como *blacklist* o lista negra lo cual impide la conexión entre el enrutador y ordenador.

```
[Huawei]firewall ?
  black-white-list  Black-white-list
  blacklist         Blacklist
  defend            Firewall attack defend
  interzone         Enter interzone view
  log               Log information
  statistics        Traffic-statistics
  whitelist         Whitelist
  zone              Specify security zone configuration
<R1>system-view
Enter system view, return user view with Ctrl+Z.
[R1]firewall blacklist 192.168.1.253
<R2>system-view
Enter system view, return user view with Ctrl+Z.
[R2]firewall blacklist 172.68.20.2
```

Figura 3.18 Establecimiento de la lista negra en cortafuegos de la Red 1 y 2

3.3. Desarrollar las topologías de red utilizando los equipos Huawei

Al implementar topologías de red, el estudiante logra desarrollar las destrezas necesarias para la administración y control de los dispositivos que forman parte de la misma. En esta sección se implementa la configuración de *Frame Relay* como mecanismo de transporte, se configuran protocolos de encapsulación como PPP y HDLC, y se agrega la implementación de una red de área local virtual o VLAN.

Configuración de *Frame Relay* en eNSP

En eNSP se procedió a realizar el establecimiento de una red *Frame Relay* (FR), para visualizar una detallada configuración de los dispositivos utilizados en esta red consultar en la hoja guía 4 del instructor.

En la Figura 3.19 se puede visualizar un escenario de prueba de topología de una red *Frame Relay* formada por tres enrutadores modelo AR2220 los cuales constituyen una red WAN. Los *routers* AR1, AR2 y AR3 se conectarán al conmutador *Frame Relay Switch* (FRSW) mediante una interfaz serial.

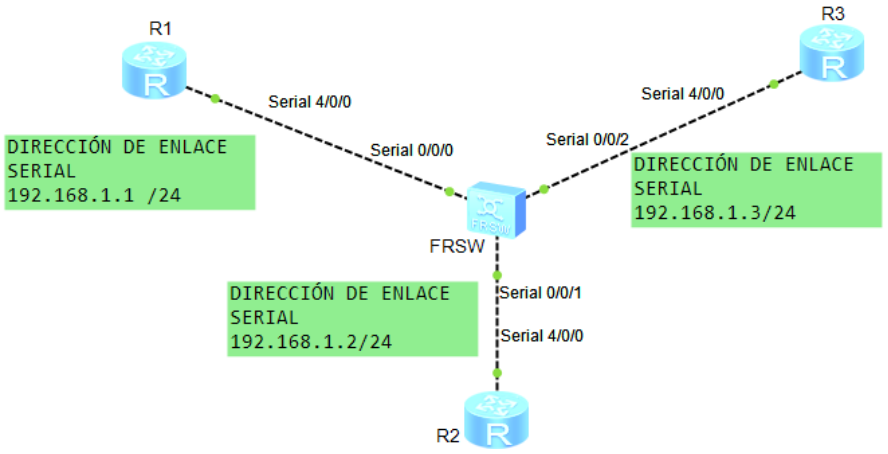


Figura 3.19 Escenario de una red *Frame Relay* en eNSP

En la Figura 3.20 se visualiza la configuración que se realiza en el enrutador FRSW que es el dispositivo virtualizado de conmutación de paquetes de *Frame Relay*. En este conmutador se establece los enlaces conectados directamente a los enrutadores mediante enlaces seriales y se configura el *Data Link Connection Identifier* (DLCI) que es el identificador que contiene la ruta establecida de los datos enviados.

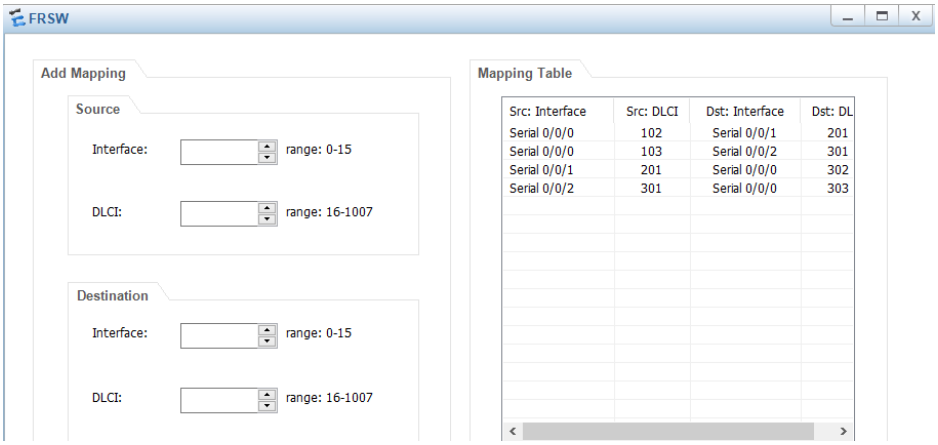


Figura 3.20 Configuración de interfaces en el conmutador *Frame Relay*

Configuración de *Frame Relay en los* enrutadores R1, R2 y R3

En la Figura 3.21 se muestra la configuración establecida en los enlaces conectados al conmutador FRWS. Al ingresar a las interfaces conectadas al conmutador, con el comando *link-protocol fr* se define el protocolo de encapsulación de *Frame Relay.*

Con el comando *fr-class* (opcional), se establece la identificación de la red que usa FR y se establece con el comando *fr map ip* la dirección IP de destino con el DLCI que le corresponde al mismo. Con el comando *undo fr inarp* elimina mapas FR creados dinámicamente mediante Protocolo de Resolución de Direcciones Inversa (INARP).

```
interface Serial4/0/0
 link-protocol fr
 fr-class 1
 undo fr inarp
 fr map ip 192.168.1.2 102
 fr map ip 192.168.1.3 103
 ip address 192.168.1.1 255.255.255.0
interface Serial4/0/0
 link-protocol fr
 undo fr inarp
 fr map ip 192.168.1.1 201
 ip address 192.168.1.2 255.255.255.0
interface Serial4/0/0
 link-protocol fr
 undo fr inarp
 fr map ip 192.168.1.1 301
 ip address 192.168.1.3 255.255.255.0
```

Figura 3.21 Establecimiento de *Frame Relay* en los enrutadores de la red

Configuración de protocolos de encapsulamiento

Se procede a la elaboración de una red que se configurará en base a protocolos de encapsulamiento a nivel de capa 2. La conexión WAN usa protocolos de capa a nivel de enlace para encapsular la información, entre los más conocidos son:

- **Protocolo Punto a Punto (PPP)**
  Establece un estándar de asignación y control de direcciones IP funcionando con diversos protocolos a nivel de capa 3 como IPv4 e IPv6 estableciendo conexiones punto a punto.
- **Control de enlace de datos de alto nivel (HDLC)**
  Establece un método de encapsulación establecido en las conexiones seriales síncronas. Además, PPP síncrono nace de HDLC que utilizan varios servidores para conectarse a una WAN, principalmente a Internet.

En la

Figura **3.22** se establece una topología de red a nivel WAN en donde se establece la configuración del protocolo de encapsulación PPP. La red contiene tres enrutadores AR3260 conectados mediante enlaces seriales y configurados con el protocolo RIP para la conexión de los dispositivos.

Para visualizar una configuración detallada del protocolo de encapsulación en los dispositivos enrutadores consultar en la hoja guía 4 del instructor.

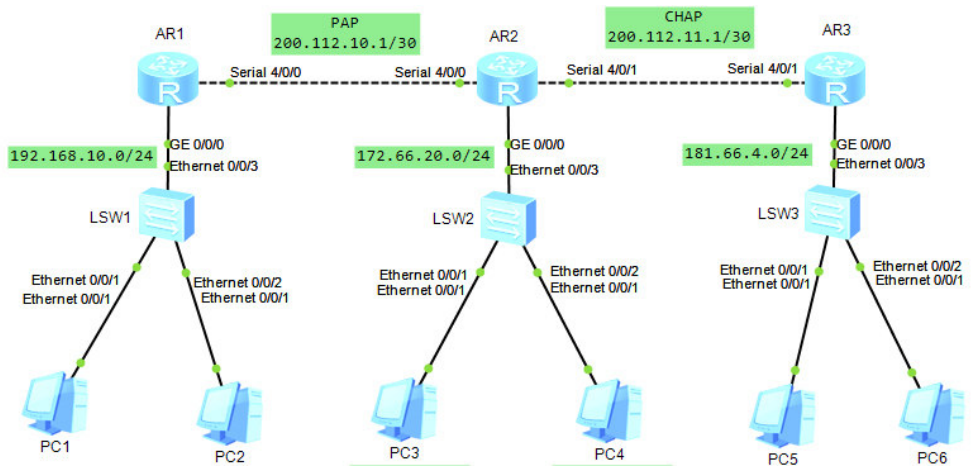


Figura 3.22 Topología base para la implementación de protocolos de encapsulación

Configuración del protocolo PPP en los enrutadores R1, R2, R3

En la Figura 3.23 se muestra la configuración realizada para el establecimiento de PPP en eNSP, para ello se realizó la configuración básica en los enrutadores y se estableció el direccionamiento IP establecido para cada enlace serial y ethernet. Con el comando link-protocol ppp se configura el protocolo de encapsulación PPP en los enlaces seriales. Se habilita el método de autenticación Password Authentication Protocol (PAP) o Protocolo de Autenticación por Desafío Mutuo (CHAP) mediante el comando *ppp authentication-mode*.

Figura 3.23 Configuración de protocolo PPP PAP y CHAP

Configuración de una red de área local virtual o VLAN

En la Figura 3.24 se presenta una topología base conformada por dos enrutadores AR3260, en donde se configurará la respectiva red de área local virtual o VLAN. Con la utilización de VLANs se organiza la red en segmentos pequeños, logrando agrupar lógicamente los diferentes dispositivos de toda la red, permitiendo alcanzar una mayor seguridad para los diferentes miembros de la subred lógica y dividiendo los dominios de *broadcast.*

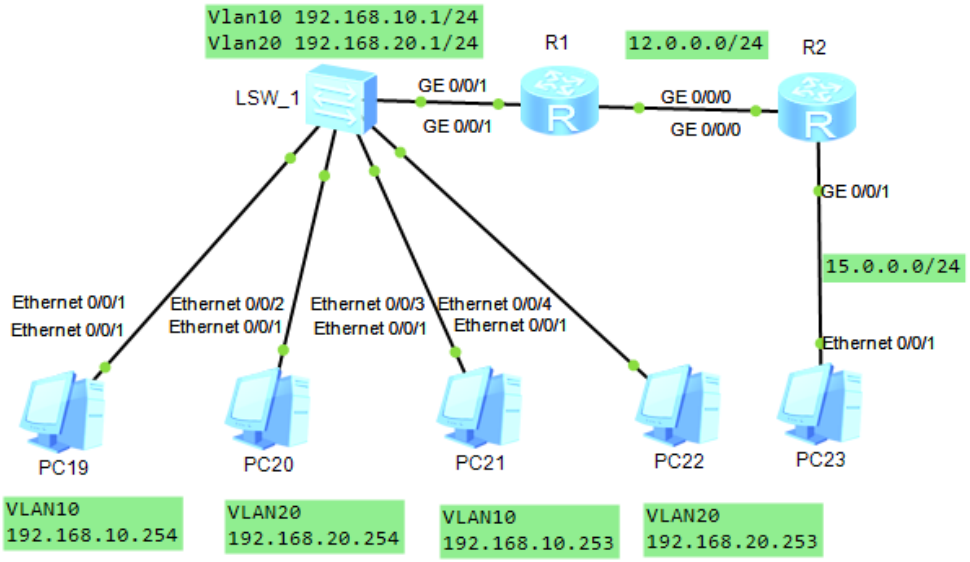


Figura 3.24 Topología base para la configuración de VLANs en eNSP

En la **Figura 3.25** se observa la asignación de VLANs correspondientes para cada subred lógica con su respectivo puerto asignado en modo acceso mediante el comando *port link-type access* o troncal mediante el comando *port link-type trunk*. Además, se define la VLAN que por defecto se configura en cada interfaz de conexión con el ordenador mediante el comando *port default vlan.*

```
interface Ethernet0/0/1
 port link-type access
 port default vlan 10
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 20
#
interface Ethernet0/0/3
 port link-type access
 port default vlan 10
#
interface Ethernet0/0/4
 port link-type access
 port default vlan 20
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 20
```

Figura 3.25 Asignación de VLANs en el *switch*

3.4. Realizar pruebas de las topologías implementadas

En esta sección se realiza pruebas de funcionamiento a las diferentes topologías de red establecidas en las secciones anteriores. Comprobando el funcionamiento de los protocolos configurados y consiguiendo una alta tasa de conectividad entre todos los equipos.

Protocolos de enrutamiento dinámico

En la

Figura **3.26** se muestra la topología propuesta para el establecimiento de diferentes protocolos de enrutamiento dinámico como IS-IS, OSPF y RIP la cual se conforma de tres enrutadores de la marca Huawei modelo AR3260, enlaces seriales, ordenadores y conmutadores de capa 2, en donde, se consiguió la conectividad entre todos los equipos que conforman la red, al igual que, el sistema de autenticación para el ingreso a los dispositivos.

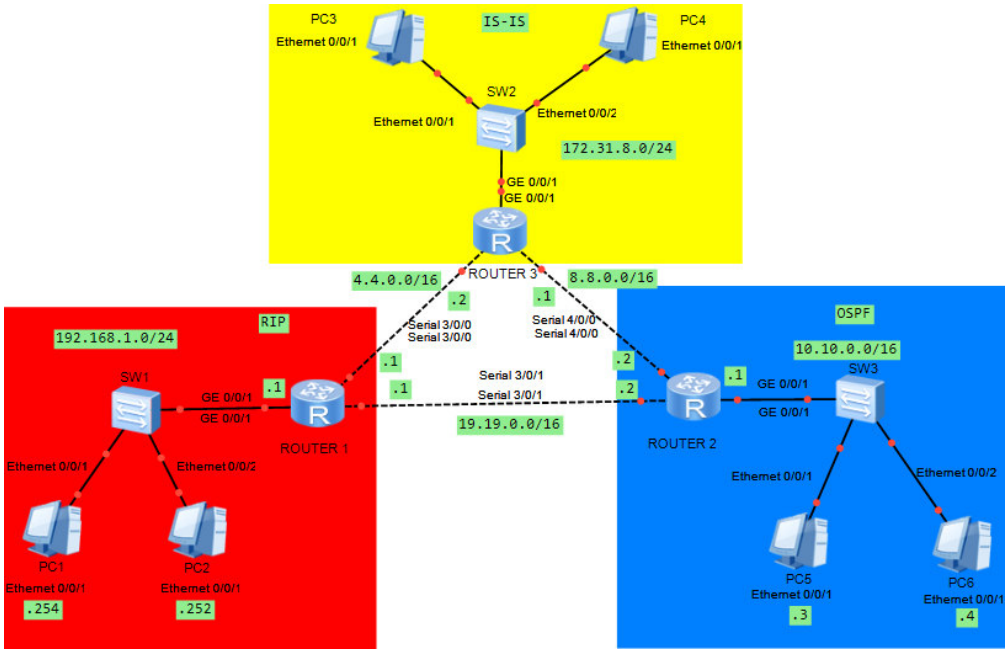


Figura 3.26 Topología de red establecida para el enrutamiento de RIP, OSPF e IS-IS

En la Figura 3.27 se muestra la comprobación del funcionamiento del sistema de autenticación y cabeceras establecidas anteriormente en los enrutadores de Huawei. Con lo que se comprueba que los parámetros de configuración básica se establecieron correctamente.

```
Login authentication


Password:
BIENVENIDO AL ROUTER 1
<Router_1>
```

Figura 3.27 Comprobación del sistema de autenticación en los enrutadores

Finalmente, en la

Figura **3.28** se muestra la comprobación de conectividad extremo a extremo entre los ordenadores de la red establecidos con distintos protocolos de enrutamiento mediante la utilización del comando *ping.*

```
PC>ping 192.168.1.252

Ping 192.168.1.252: 32 data bytes, Press Ctrl_C to break
From 192.168.1.252: bytes=32 seq=1 ttl=128 time=47 ms
From 192.168.1.252: bytes=32 seq=2 ttl=128 time=31 ms
From 192.168.1.252: bytes=32 seq=3 ttl=128 time=47 ms
From 192.168.1.252: bytes=32 seq=4 ttl=128 time=31 ms
From 192.168.1.252: bytes=32 seq=5 ttl=128 time=47 ms

--- 192.168.1.252 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 31/40/47 ms
```

Figura 3.28 Comprobación de conectividad entre distintos protocolos de enrutamiento

Servicio DHCP y *Firewall*

En la Figura 3.29 se puede observar la red establecida para la implementación del servicio DHCP y cortafuegos entre las redes establecidas. En donde se utilizó dos enrutadores AR3260 y como protocolo de enrutamiento OSPF.

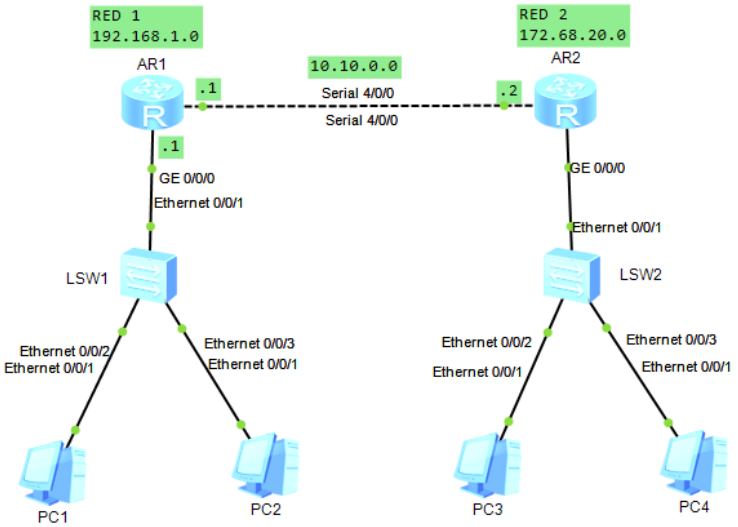


Figura 3.29 Topología prevista para el establecimiento del servicio DHCP y *Firewall*

Comprobación de asignación dinámica de dirección de *host*

En la Figura 3.30 se muestra la asignación de direccionamiento IP de forma dinámica mediante el comando *ipconfig*. Por lo tanto, se llega a establecer una dirección IP en los ordenadores de manera automática conforme a la red establecida, máscara de la red y la puerta de enlace o *gateway*.

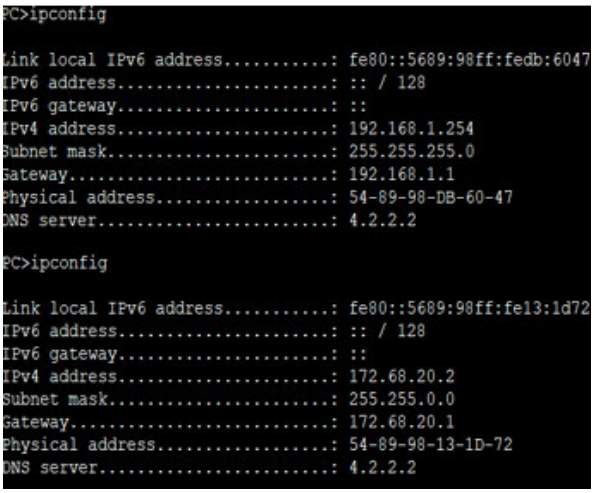


Figura 3.30 Comprobación de asignación de direcciones IP mediante el servicio DHCP

Comprobación de la implementación de un cortafuegos

En la Figura 3.31 se muestra la implementación de una lista de denegación o lista negra donde se agregó una dirección IP de los ordenadores que conforman la red con equipos virtualizados de Huawei. La lista de denegación se puede visualizar mediante el comando *display firewall blacklist all* y se demuestra el funcionamiento de este cortafuegos comprobando la conectividad extremo a extremo entre el enrutador y la máquina virtualizada mediante el comando *ping*.

```
[R1]display firewall blacklist all
 Firewall blacklist items :
-------------------------------------------------------------------------------
IP-Address      Reason        Expire-Time(m) VPN-Instance
-------------------------------------------------------------------------------
192.168.1.253   Manual        Permanent
-------------------------------------------------------------------------------
 Total number is : 1
[R1]
<R1>ping 192.168.1.253
  PING 192.168.1.253: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 192.168.1.253 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

Figura 3.31 Comprobación del sistema de cortafuegos en los enrutadores

Protocolos de encapsulación HDLC y PPP con autenticación CHAP y PAP

En la

Figura **3.32** se observa la topología de red planteada con tres enrutadores virtualizados en donde se configuró la encapsulación PPP y HDLC logrando conseguir conectividad entre los clientes. Además, al implementar el protocolo de encapsulación PPP se configuró en los extremos de la red diferentes sistemas de autenticación como CHAP y PAP.

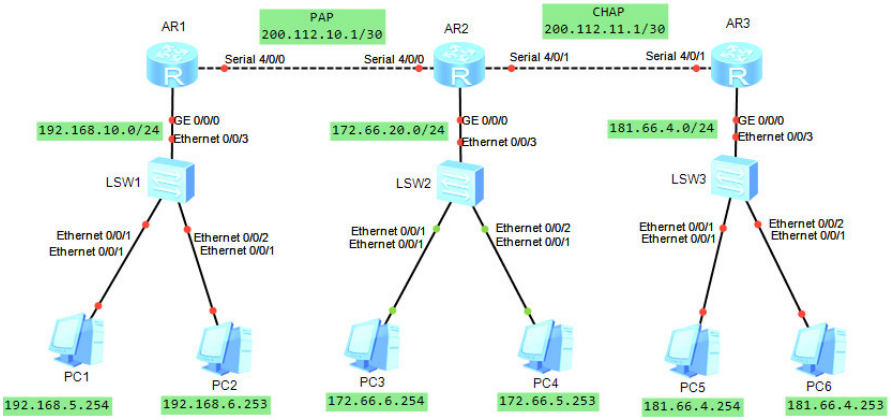


Figura 3.32 Topología planteada para el establecimiento de protocolos de encapsulación

Configurado el protocolo de encapsulación HDLC con el comando *link-protocol HDLC* en los enlaces seriales de los enrutadores, se logra evidenciar en la Figura 3.33 que mediante el comando *display interface serial* el protocolo de encapsulación se encuentra establecido en los extremos de los enlaces seriales.

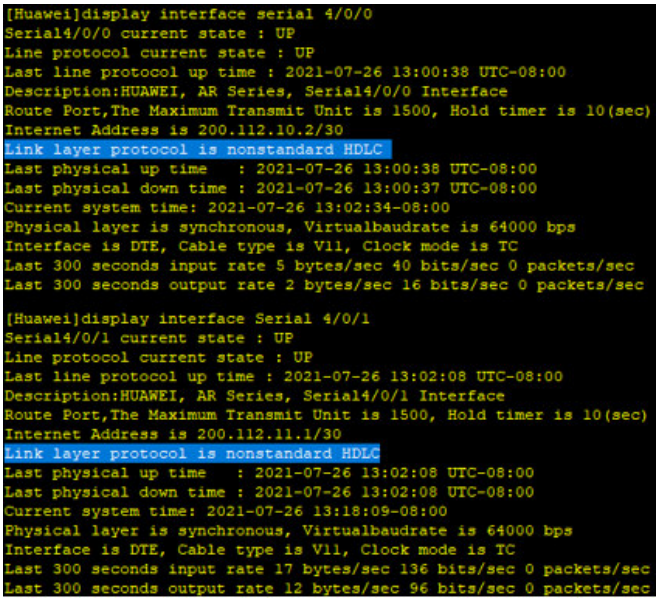


Figura 3.33 Comprobación de establecimiento del protocolo HDLC

Configurado el protocolo de encapsulación PPP con el comando *link-protocol PPP* en los extremos de los enlaces seriales de los enrutadores, se muestra en la Figura 3.34 que mediante el comando *display interface serial* el protocolo de encapsulación se encuentra establecido.

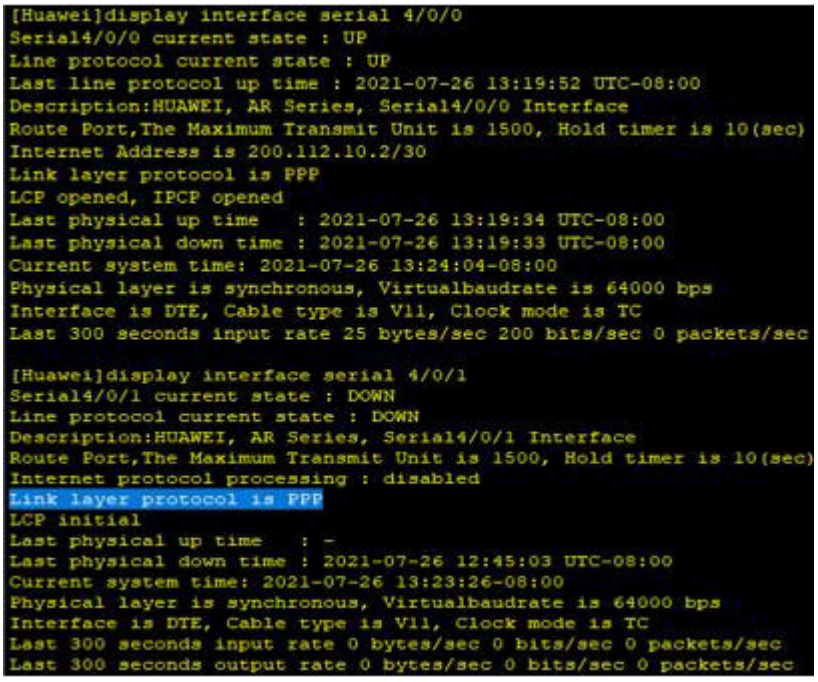


Figura 3.34 Comprobación de establecimiento del protocolo PPP

4. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- En el presente trabajo de titulación se observó que los avances en el área de las redes de información son relevantes debido a los beneficios que éstas introducen en el proceso de educación y aprendizaje.

- Con la implementación de prácticas de enrutamiento con equipos virtualizados de *networking* de Huawei, la institución lograría ahorrar gastos formidables, pues la implementación de redes basadas en equipos de la marca mencionada puede llegar a tener costos considerables para su respectiva implementación.

- Mediante el programa eNSP se logró emular varios modelos de enrutadores reales de la marca Huawei, como los equipos AR201, AR1220, AR2220, AR2240, AR3260 consiguiendo que los estudiantes de la carrera de Tecnología Superior en Redes y Telecomunicaciones consigan tener una mejor comprensión de su funcionamiento y configuración.

- De ambos programas empleados para el desarrollo del presente trabajo, GNS3 es más complejo de utilizar, sin embargo, su empleo en la rama de las redes y telecomunicaciones es muy extendido pues trabaja sobre imágenes de equipos reales.

- En cuanto al desempeño de los programas eNSP y GNS3, se consideran apropiados para emplearlos en escenarios virtuales como herramientas de apoyo educativo para el estudio de elementos básicos de transmisión de datos.

- Con la utilización de los programas eNSP y GNS3 antes mencionados, se permite que los dispositivos enrutadores de la marca Huawei se comporten con un elevado nivel de similitud con equipos reales, siendo ambos programas libres, con entornos flexibles e intuitivos para una mejor compresión del tema.

4.2. Recomendaciones

- Al utilizar eNSP y GNS3, se reduce el uso de dispositivos físicos para la realización de prácticas dentro de los laboratorios de la Escuela de Formación de Tecnólogos orientada a la carrera de Tecnología Superior en Redes y Telecomunicaciones. No obstante, se sugiere tener conocimiento previo en configuración de equipos de red independientemente de la marca.

- Se recomienda el uso de los programas como eNSP y GNS3 en el curso de Redes de Computadoras, al igual que, utilizar los principales conceptos y características mencionados en este trabajo, además de practicar en las diferentes topologías propuestas en cada hoja guía para el laboratorio.

- Se sugiere utilizar los conceptos mencionados en este trabajo de titulación sobre todo en la configuración de enrutamiento de equipos Huawei y continuar estudiando las diferentes posibilidades que eNSP y GNS3 brindan para la simulación de topologías de red.

- De los programas utilizados para el presente trabajo de titulación, se recomienda que, si se utiliza GNS3, se debe tener con anticipación las imágenes de los *softwares* de los equipos a configurar porque no todos los proveedores de terminales de red brindan gratuitamente una copia del sistema de sus dispositivos.

- Cabe resaltar que en los programas de eNSP y GNS3 demandan de una cantidad de memoria RAM significativa. Por lo tanto, para que estos programas funcionen correctamente, se recomienda tener mínimo en el ordenador una memoria RAM mayor o igual de 8 (GB).

[1] L. M. Garcés, «Instituto Nacional de Evaluación Edu,» 2018. [En línea]. Available: https://n9.cl/g4rfm.

[2] I. J. L. V. Zambrano, «Universidad Católiva de Santiago de Guayaquil.,» 05 2014. [En línea]. Available: http://repositorio.ucsg.edu.ec/bitstream/3317/1936/1/T-UCSG-POS-MTEL-17.pdf.

[3] N. J. Otero, «UNIVERSIDAD CENTRAL “Marta Abreu” DE LAS VILLAS,» 2015. [En línea]. Available: https://1library.co/document/zkw84j8z-propuesta-laboratorios-redes-ii-iii-usando-herramienta-ensp.html.

[4] J. V. C. Hernández, «Universidad Politécnica de Valencia,» [En línea]. Available: https://n9.cl/7y2s0.

[5] I. J. L. V. Zambrano, *Laboratorios virtuales para cursos de transmisión de datos,* Guayaquil, 2014.

[6] M. Domínguez, «Universidad Complutense de Madrid,» 2003. [En línea]. Available: https://www.redalyc.org/pdf/181/18100809.pdf.

[7] GNS3, «GNS3,» 2021. [En línea]. Available: https://www.gns3.com/software/download.

[8] J. Ulloa, «Escuela Politécnica Nacional,» 10 2007. [En línea]. Available: https://bibdigital.epn.edu.ec/bitstream/15000/544/1/CD-1048.pdf.

[9] L. Huawei Technologies Co., «HCNA Networking Study Guide,» China, Springer Science+Business Media Singapore, 2016, p. 119.

[10] C. H. Enterprise, « Huawei Enterprise,» 2021. [En línea]. Available: https://forum.Huawei.com/enterprise/es/forums.

[11] L. P. Z. Huang, «Universidad San Francisco de Quito,» 12 05 2017. [En línea]. Available: https://repositorio.usfq.edu.ec/bitstream/23000/6383/1/130874.pdf.

[12] R. Bejtlich, «Security networks,» de *The Tao of network security monitoring beyond intrus detection*, Londres, Librería Génesis, 2014, pp. 315-320.

[13] S. C. C. R. Brayan Bernal, «Universidad Cooperativa de Colombia,» 05 2018. [En línea]. Available: https://repository.ucc.edu.co/bitstream/20.500.12494/7048/6/2018_Dise%C3%B1o_Red_Lan.pdf.

5. REFERENCIAS BIBLIOGRÁFICAS

ANEXOS

ANEXO 1: CERTIFICADO DE FUNCIONAMIENTO

ESCUELA POLITECNICA NACIONAL

Campus Politécnico "J. Rubén Orellana R

Quito, 21 de octubre de 2021

CERTIFICADO DE FUNCIONAMIENTO DE PROYECTO DE TITULACIÓN

Yo, Fernando Vinicio Becerra Camacho, docente a tiempo completo de la Escuela Politécnica Nacional y como director de este trabajo de titulación, certifico que he constatado las prácticas de enrutamiento con equipos virtualizados de networking de HUAWEI en GNS3 y eNSP, el cual fue implementado por el estudiante Israel Alexander Zurita Maldonado

DIRECTOR

Ing. Fernando Vinicio Becerra Camacho. Msc.

Ladrón de Guevara E11-253, Escuela de Formación de Tecnólogos

email:fernando.becerrac@epn.edu.ec Quito-Ecuador

ANEXO 2: PRÁCTICAS DE LABORATORIO

ESCUELA POLITÉCNICA NACIONAL
ESCUELA DE FORMACIÓN DE TECNÓLOGOS
Tecnología Superior en Redes y Telecomunicaciones
Redes de Computadoras
Hoja Guía Práctica 1 (Instructor)

1. TEMA: Instalación de eNSP y GNS3

2. OBJETIVOS

2.1. Instalar los programas eNSP y GNS3 para las futuras prácticas de laboratorio.

2.2. Configurar GNS3 y eNSP para un correcto funcionamiento de dispositivos.

2.3. Establecer conexión de dispositivos mediante enrutamiento estático en eNSP.

3. DESARROLLO DE LA PRÁCTICA

NOTA: La presenta práctica tiene un tiempo aproximado de elaboración y ejecución de 1 hora 30 minutos.

Instalación de eNSP

3.1. Se comienza descargando el instalador del siguiente *link*: https://n9.cl/p0u15 y de prerrequisito tener programas adicionales como *Wireshark* y *VirtualBox* ya instalados, siendo *Wireshark* opcional, pero *VirtualBox* no, dado que sobre esta plataforma se ejecutan las imágenes de los diferentes dispositivos de red de la marca Huawei. Una vez que se tienen los prerrequisitos (*VirtualBox* y *Wireshark*) se comienza a instalar eNSP. Las ventas que aparecen en el proceso de instalación se muestran en las figuras A1.1 hasta la figura A1.5

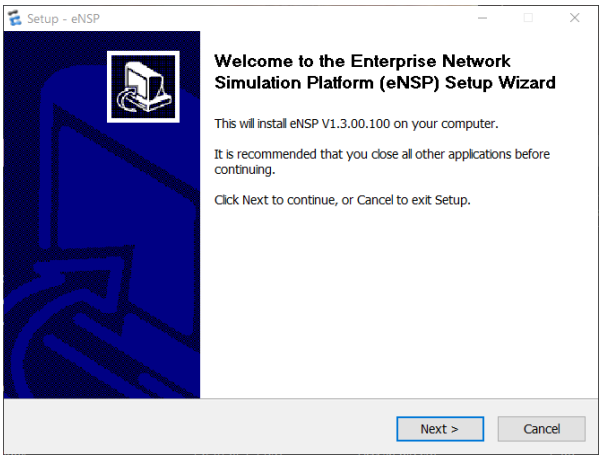


Figura A1.1 Proceso de instalación de eNSP

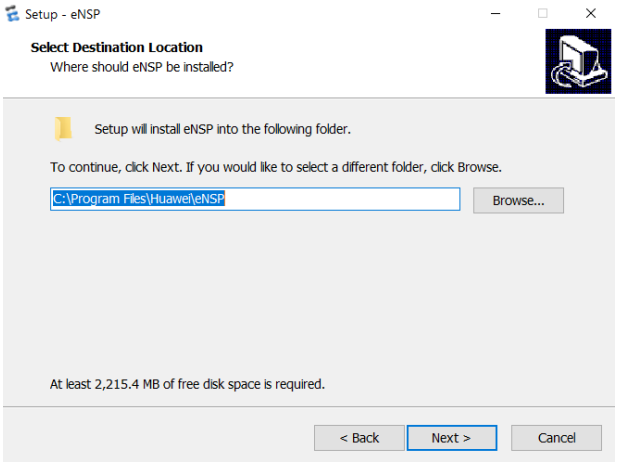


Figura A1.2 Localización de carpeta destino para la instalación

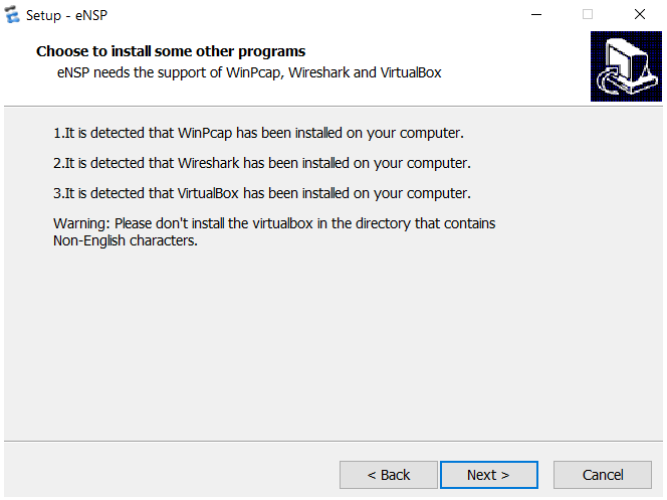


Figura A1.3 Detección de programas previamente instalados (*WinPcap*, *Wireshark*, *VirtualBox*)

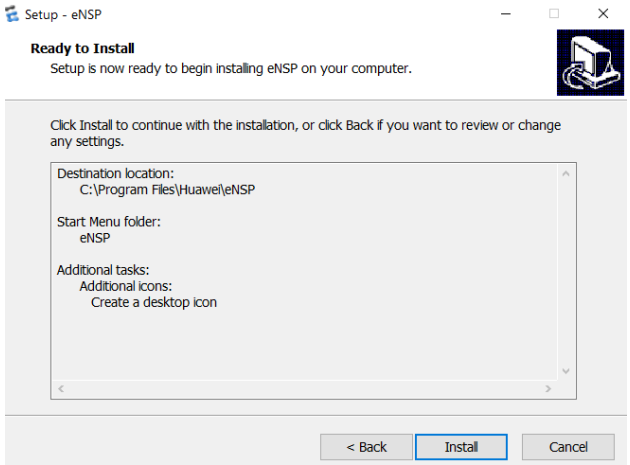


Figura A1.4 Proceso de inicio de instalación

Figura A1.5 Ejecución del Programa eNSP

Instalación de GNS3

3.2. Se comienza descargando la aplicación de la página principal y registrándose en la misma. Luego de la creación de una cuenta que a su vez permitirá entrar a la comunidad de la página, se encontrará el respectivo instalador acorde al sistema operativo sea *Windows*, *Mac* y *Linux*. Cabe resaltar que la respectiva descarga del instalador es totalmente gratis y, además, como *hypervisor* predefinido para prácticas en GNS3 se utilizará *VMware*. Las ventas que aparecen en el proceso de instalación se muestran en las figuras A1.6 hasta la figura A1.11.

Figura A1.6 Proceso de instalación de GNS3

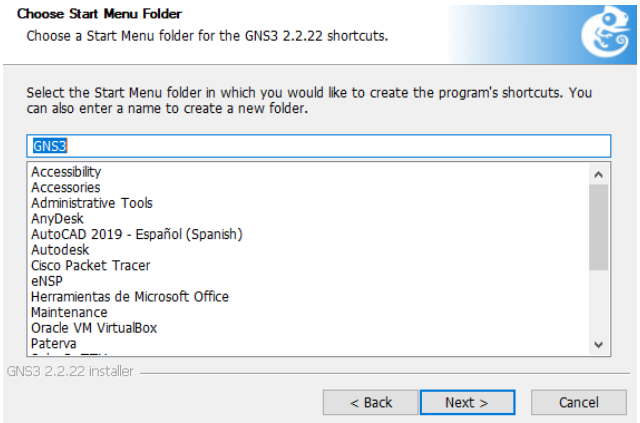


Figura A1.7 Ubicación de carpeta de instalación

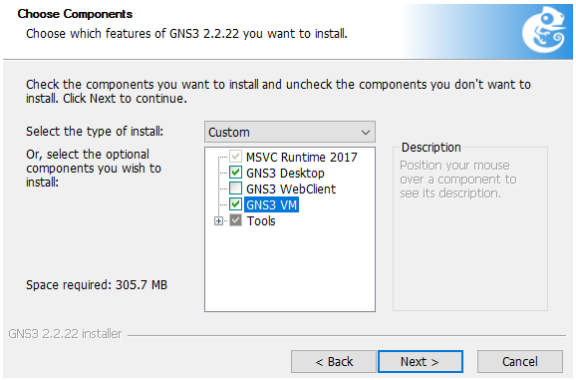


Figura A1.8 Selección de componentes para el proceso de instalación en GNS3

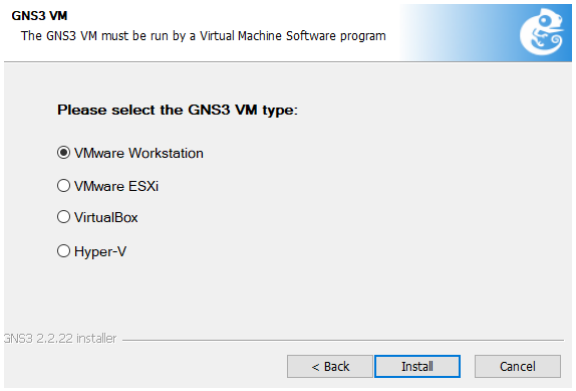


Figura A1.9 Selección de componente para el proceso de instalación en GNS3

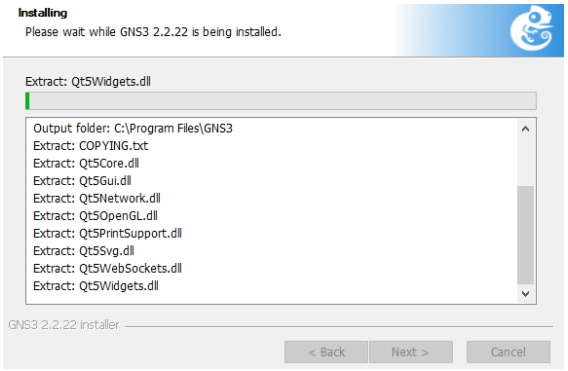


Figura A1.10 Proceso de instalación de GNS3

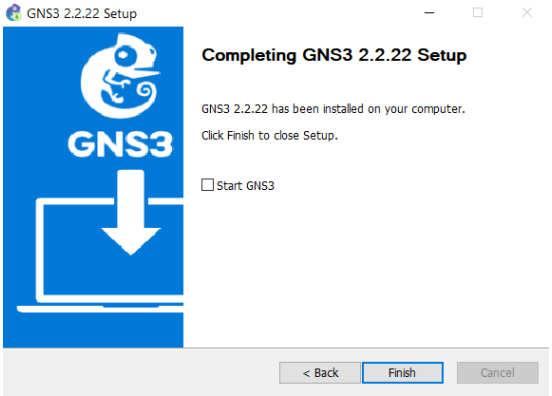


Figura A1.11 Finalización del proceso de instalación

3.3. Una vez instalados los programas, se inicia con la configuración respectiva de los mismos, por lo tanto, para eNSP se crea una nueva topología que previamente se guarda en el Escritorio para una ejecución óptima del programa, como se muestra en la figura A1.12

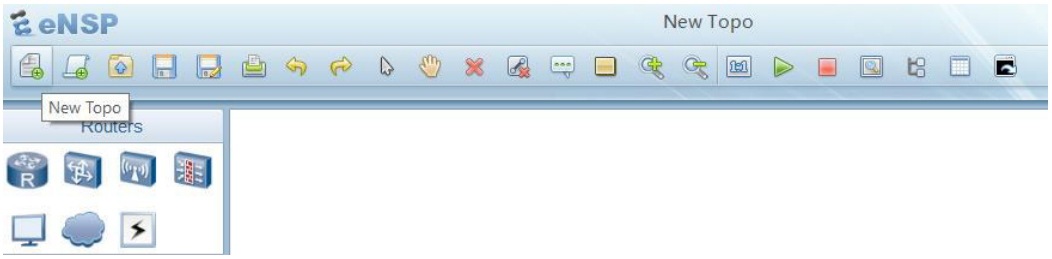


Figura A1.12 Creación de nueva topología en eNSP

3.4. En el caso de eNSP, los dispositivos de red se encuentran listos para ejecución del mismo, mientras que en GNS3 se obtendrá las ISOs correspondientes según la marca del dispositivo que se vaya a configurar. Para las futuras prácticas en GNS3 se utiliza la ISO correspondiente al *router* Cisco 3660. Cuando se obtiene la ISO correspondiente, se procede a iniciar GNS3 y en la opción de editar-preferencias se despliega la siguiente ventana, como se muestra en la figura A1.13.

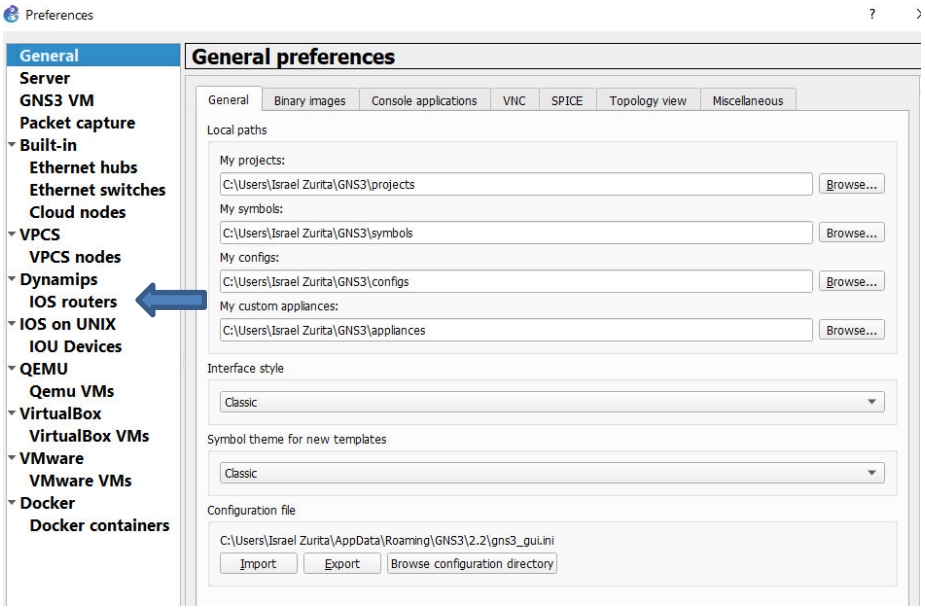


Figura A1.13 Ventana de configuración general de GNS3

3.5. Dentro de la misma, se selecciona la opción de *IOS routers,* se selecciona la opción de nuevo, como se muestra en la figura A1.14.

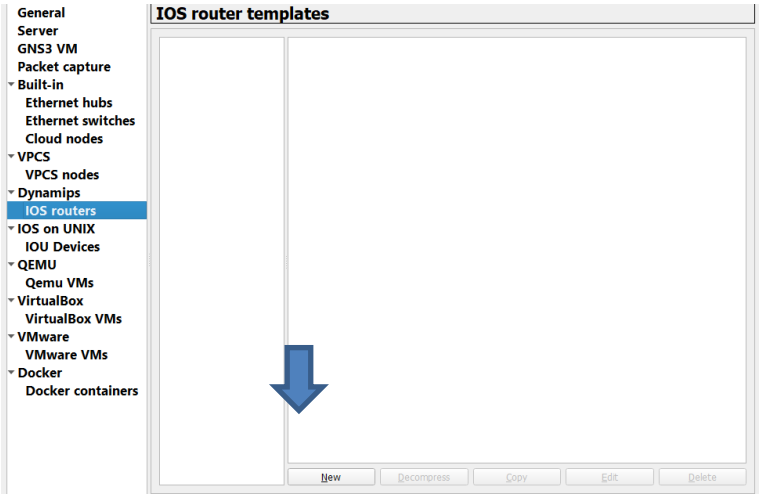


Figura A1.14 Agregación de un nuevo dispositivo

3.6 Se selecciona la opción de *New Image* y se busca la ISO correspondiente al *router* que se vaya a ejecutar, en este caso sería la ISO de *router* Cisco 3660 y se procede con la configuración respectiva del mismo, como se muestra en las figuras A1.15, A1.16.

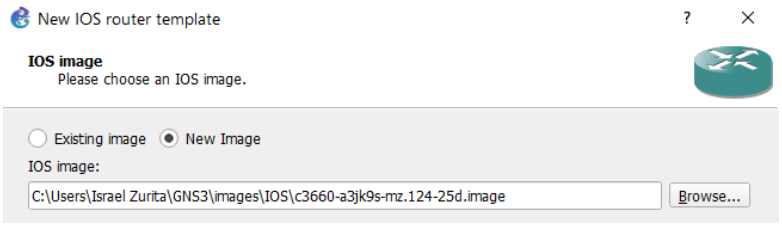


Figura A1.15 Selección de ISO

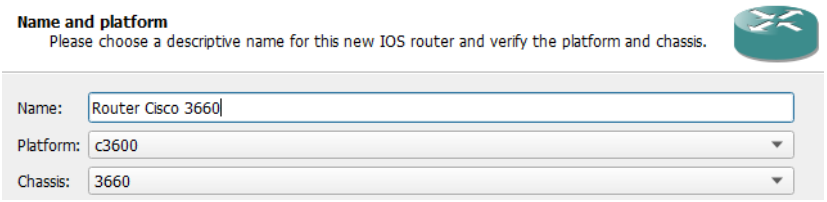


Figura A1.16 Establecimiento de nombre del dispositivo

3.7. Se establece por defecto la RAM establecida para el dispositivo como se muestra en la figura A1.17.

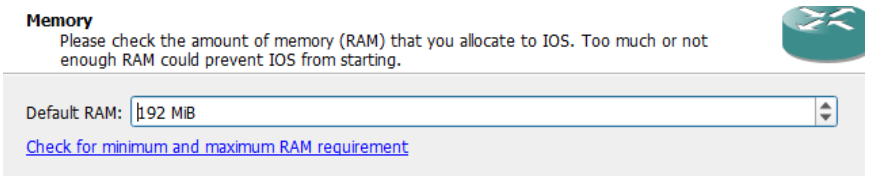


Figura A.17 Memoria RAM establecida por defecto

3.8. Se establece los adaptadores de red que va a poseer el dispositivo para cada interfaz, en esta práctica se establece 4 interfaces seriales con 3 *fast ethernet*, como se muestra en la figura A1.18.

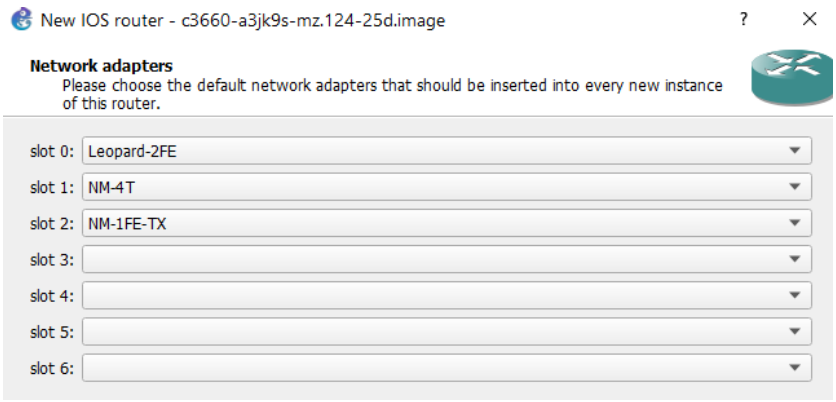


Figura A1.18 Configuración de interfaces en GNS3

3.9. Se establece por defecto la Idle-PC para la optimización de recursos del ordenador al momento de ejecutar el enrutador como se muestra en la figura A1.19.

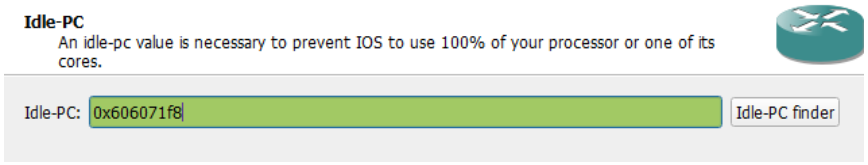


Figura A1.19 Establecimiento por defecto de GNS3 para la optimación de recursos en la PC

3.10. Una vez que se cumpla con los pasos mencionados anteriormente, el enrutador añadido aparece en el lado izquierdo en donde se encuentran diferentes dispositivos que en GNS3 vienen predefinidos para su funcionamiento, como se muestra en la figura A1.20.

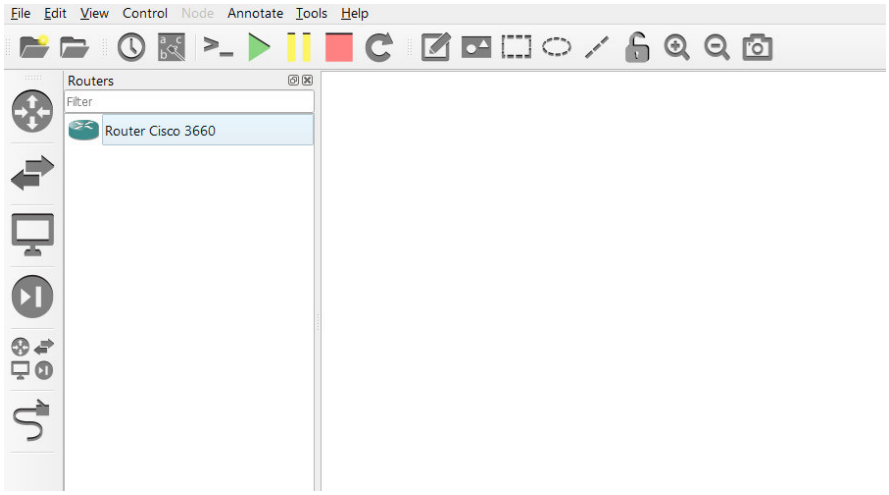


Figura A1.20 Finalización del proceso de instalación de un nuevo dispositivo

3.11. Para ejecutar el dispositivo de red, este se arrastra del menú de dispositivos al espacio de trabajo, se selecciona al mismo y en la barra de herramientas se dará clic en el reproductor de aplicación de color verde o dando clic derecho sobre el dispositivo y de igual manera se selecciona la opción de *start.* Para comprobar que el dispositivo se encuentra encendido al lado superior derecho se muestra el nombre del dispositivo por defecto y la señalización de color verde lo cual indica que el dispositivo se encuentra encendido y listo para ejecutarse., como se muestra en la figura A1.21.

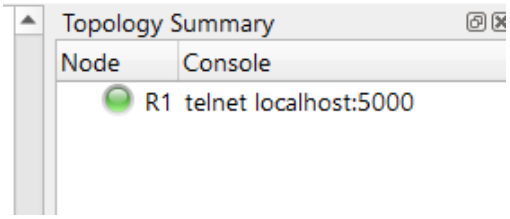


Figura A1.21 Comprobación de inicio de arranque del dispositivo

3.12. Para comenzar con la configuración del mismo se procede a dar clic derecho sobre el dispositivo y se selecciona la opción de consola con el objetivo de entrar a este modo y empezar a configurar el dispositivo, como se muestra en la figura A1.22.

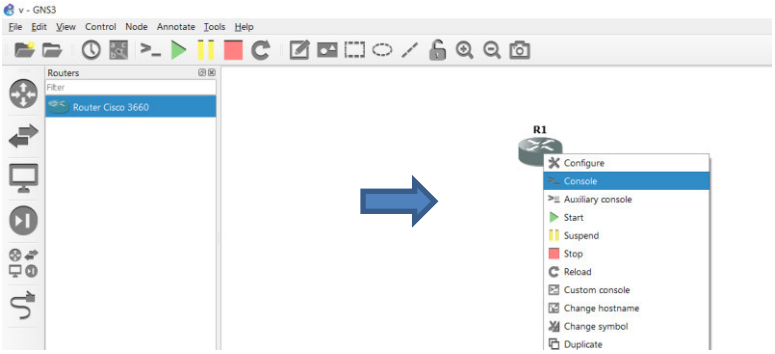


Figura A1.22 Ingreso de modo consola en el enrutador dentro de GNS3

3.13. Ahora, para relacionar al estudiante con la herramienta eNSP se procede a elaborar una topología de red básica para que el estudiante se familiarice con los diferentes dispositivos que este programa ofrece. Dentro de la ventana de trabajo de eNSP, se elabora la siguiente topología prevista para esta práctica con los siguientes parámetros, como se muestra en la figura A1.23

- *routers* AR3260 con 2 interfaces seriales.
- *switch* 3700
- PC

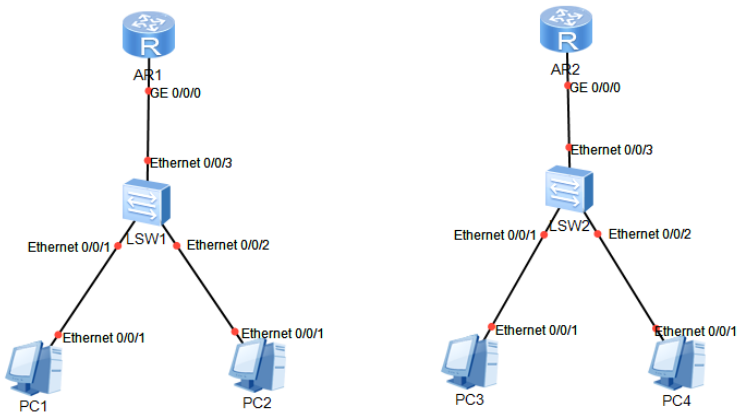


Figura A1.23 Topología de red en eNSP para la presente práctica

3.14. Para colocar las interfaces seriales en los enrutadores, seleccionar dicho dispositivo y sobre el mismo, clic derecho y seleccionar configuraciones, como se muestra en la figura A1.24.

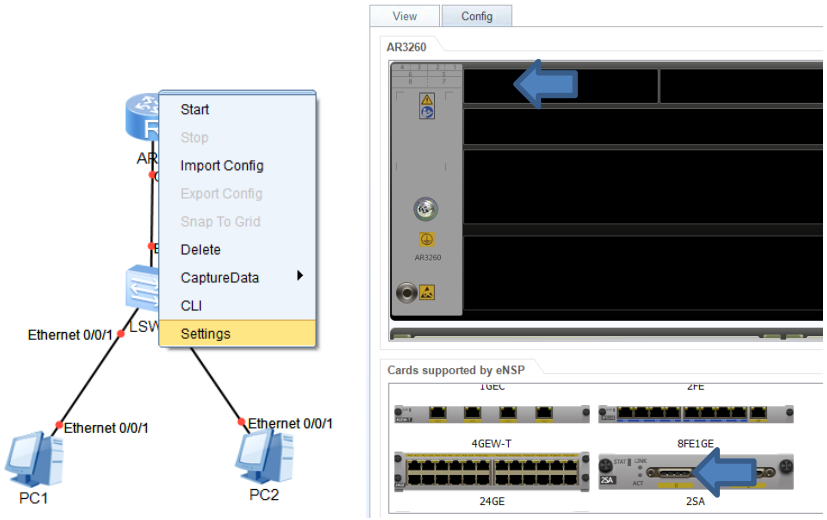


Figura A1.24 Agregación de módulo serial en el enrutador en eNSP

3.15. Al desplegarse una ventana de configuraciones, arrastrar el módulo 2SA el cual permite insertar interfaces seriales en los enrutadores hacia los *slots*. Y una vez colocadas dichas interfaces, interconectar los dispositivos, como se muestra en la figura A1.25.

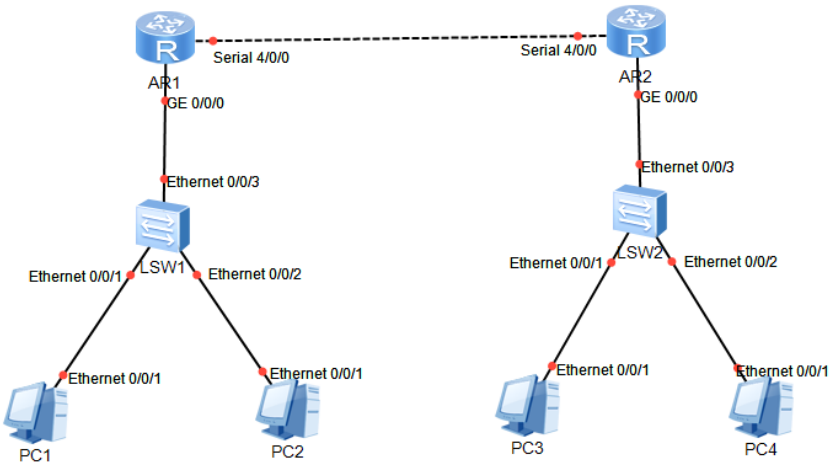


Figura A1.25 Conexión de enrutadores mediante enlaces seriales en eNSP

3.16. Una vez colocados e interconectados los dispositivos de red, se establece el direccionamiento IP para las diferentes redes a desarrollar, como se muestra en la figura A1.26.

- Primera red: 192.168.10.0/24
- Segunda red: 172.168.50.0/24
- Enlace serial: 10.10.10.0/30

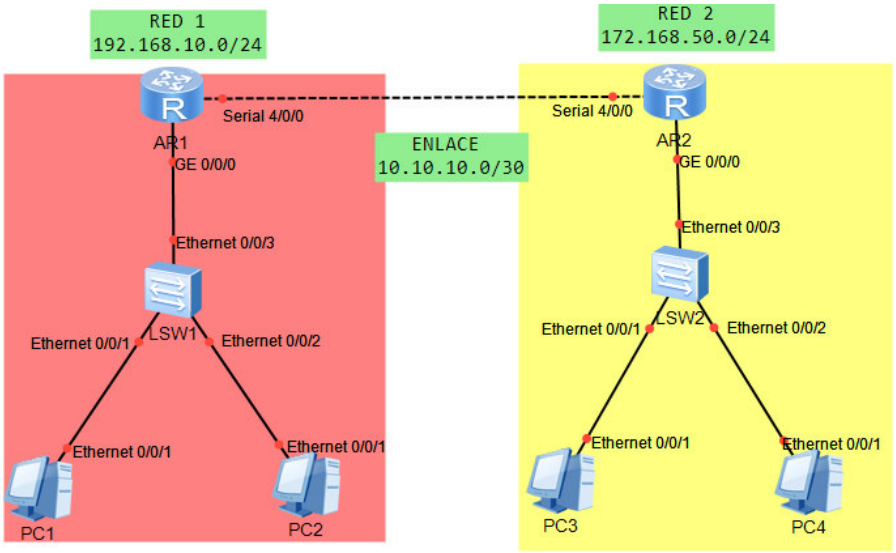


Figura A1.26 Conexión serial entre enrutadores en eNSP

3.17. Se comienza con la configuración de las diferentes redes que se interconectarán por medio de un protocolo de enrutamiento estático, como se muestra en las figuras A1.24, A1.28, A1.29, A1.30, A1.31. Cabe resaltar que se debe iniciar la ejecución de los dispositivos, para ello, en la barra de herramientas se encuentra el respectivo indicador de inicio de ejecución de dispositivos.

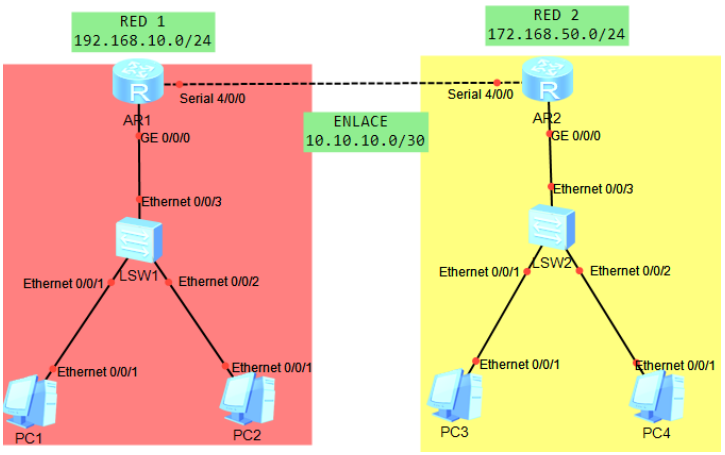


Figura A1.27 Inicio de dispositivos para la respectiva configuración en los mismos

RED 1

```
<Huawei>terminal monitor
Info: Current terminal monitor is on.
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1] interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0] ip address 192.168.10.1 255.255.255.0
Jul 5 2021 11:23:09-08:00 R1 %%01IFNET/4/LINK_STATE(1)[0]: The line protocol IP
on the interface GigabitEthernet0/0/0 has entered the UP state.
[R1-GigabitEthernet0/0/0] quit

[R1] interface Serial 4/0/0
[R1-Serial4/0/0] ip address 10.10.10.1 255.255.255.252
[R1-Serial4/0/0] return
<R1>save
  The current configuration will be written to the device.
  Are you sure to continue? (y/n) [n]: y
  It will take several minutes to save configuration file, please wait.......
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
```

Figura A1.28 Establecimiento de direccionamiento IP en interfaces del enrutador R1

RED 2

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2] interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0] IP address 172.168.50.1 255.255.255.0
Jul 5 2021 11:28:35-08:00 R2 %%01IFNET/4/LINK_STATE(l)[0]: The line
protocol IP on the interface GigabitEthernet0/0/0 has entered the UP
state.
[R2-GigabitEthernet0/0/0]quit

[R2]interface Serial 4/0/0
[R2-Serial4/0/0] ip address 10.10.10.2 255.255.255.252
[R2-Serial4/0/0]      Jul      5      2021      11:29:08-08:00      R2
%%01IFNET/4/LINK_STATE(l)[1]:  The  line  protocol  PPP  IPCP  on  the
interface Serial4/0/0 has entered the UP state.
[R2-Serial4/0/0] quit
[R2] return
<R2>save
```

Figura A1.29 Establecimiento de direccionamiento IP en interfaces del enrutador R2

Configuración de enrutamiento estático

RED 1

```
<R1> system-view
[R1] ip route-static 172.168.50.0 255.255.255.0 10.10.10.2
[R1] quit
<R1>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations: 12       Routes: 12

Destination/Mask    Proto   Pre-Cost      Flags NextHop         Interface

     10.10.10.0/30 Direct 0    0           D   10.10.10.1      Serial4/0/0
     10.10.10.1/32 Direct   0    0           D   127.0.0.1       Serial4/0/0
     10.10.10.2/32 Direct 0    0           D   10.10.10.2      Serial4/0/0
     10.10.10.3/32 Direct 0    0           D   127.0.0.1       Serial4/0/0
      127.0.0.0/8   Direct 0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32 Direct 0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32 Direct 0    0           D   127.0.0.1       InLoopBack0
   172.168.50.0/24 Static 60   0          RD   10.10.10.2      Serial4/0/0
   192.168.10.0/24 Direct 0    0           D   192.168.10.1    GigabitEthernet
0/0/0
   192.168.10.1/32 Direct 0    0           D   127.0.0.1       GigabitEthernet
0/0/0
 192.168.10.255/32 Direct 0    0           D   127.0.0.1       GigabitEthernet
0/0/0
255.255.255.255/32 Direct 0    0           D   127.0.0.1       InLoopBack0
```

Figura A1.30 Establecimiento de enrutamiento estático R1 a R2

RED 2

```
<R2> system-view
[R2] ip route-static 192.168.10.0 255.255.255.0 10.10.10.1
[R2] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations: 12       Routes: 12

Destination/Mask    Proto   Pre-Cost      Flags NextHop         Interface

     10.10.10.0/30 Direct 0    0           D   10.10.10.2      Serial4/0/0
     10.10.10.1/32 Direct 0    0           D   10.10.10.1      Serial4/0/0
     10.10.10.2/32 Direct 0    0           D   127.0.0.1       Serial4/0/0
     10.10.10.3/32 Direct 0    0           D   127.0.0.1       Serial4/0/0
      127.0.0.0/8   Direct 0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32 Direct 0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32 Direct 0    0           D   127.0.0.1       InLoopBack0
   172.168.50.0/24 Direct 0    0           D   172.168.50.1
   192.168.10.0/24 Static 60   0          RD   10.10.10.1      Serial4/0/0
255.255.255.255/32 Direct 0    0           D   127.0.0.1       InLoopBack0
```

Figura A1.31 Establecimiento de enrutamiento estático R2 a R1

4. CONCLUSIONES

4.1. En esta práctica se muestra cómo se lleva a cabo el proceso de instalación de los emuladores a utilizar, ilustrando algunos de sus procedimientos de forma gráfica para que el docente pueda tener un mejor entorno del programa y cómo utilizarlo.

4.2. El entorno de trabajo de eNSP permite tener una relación más directa con equipos de marca Huawei, en donde el estudiante logrará obtener una mejor visualización del sistema y la configuración del mismo.

5. RECOMENDACIONES

5.1. Al momento de descargar el instalador de eNSP como el de GNS3 es importante el registrase en dichas plataformas para obtener dichos programas.

5.2. Se sugiere que en el desarrollo de configuración de enrutamiento estático se compruebe si existe una correcta conexión entre ordenadores de las diferentes redes mediante el comando ***ping* + IP de la máquina,** que se ejecuta en la consola de las PC, que previamente deben estar establecidas con una dirección IP, puerta de enlace, máscara.

6. BIBLIOGRAFÍA.

[1] I. J. L. V. Zambrano, *Laboratorios virtuales para cursos de transmisión de datos,* Guayaquil, 2014. Available: https://n9.cl/6ea0w

[2] C. H. Enterprise, *Introducción al simulador de red de Huawei eNSP,* 2019. Available: https://n9.cl/fz9n7

[3] GNS3, "GNS3," 2021. [Online]. Available: https://www.gns3.com/software/download.

ESCUELA POLITÉCNICA NACIONAL
ESCUELA DE FORMACIÓN DE TECNÓLOGOS
Tecnología Superior en Redes y Telecomunicaciones
Redes de Computadoras
Hoja Guía Práctica 1 (Estudiante)

1. TEMA: Instalación de eNSP y GNS3

2. OBJETIVOS

2.1 Instalar los programas eNSP y GNS3 para las futuras prácticas de laboratorio.

2.2 Configurar GNS3 y eNSP para un correcto funcionamiento de dispositivos.

2.3 Establecer conexión de dispositivos mediante enrutamiento estático en eNSP.

3. TRABAJO PREPARATORIO

3.1. Investigar las principales diferencias entre un programa de emulación y uno de simulación.

3.2. Realizar un cuadro comparativo entre las principales diferencias entre eNSP y GNS3 (3 diferencias máximo).

3.3. Investigar sobre el enrutamiento estático y el comando respectivo para establecerlo dentro de una red con equipos Huawei.

3.4. Investigar ventajas y desventajas de usar GNS3.

3.5. Tener descargado en los ordenadores los instaladores respectivos de GNS3 y eNSP del siguiente *link*: https://n9.cl/p0u15.

4. DESCRIPCIÓN DE LA ACTIVIDAD

4.1. Ejecutar el programa instalador de eNSP.

4.2. En la parte superior izquierda, seleccionar la opción de nueva topología.

4.3. Elaborar la topología de red planteada por el instructor en base al *router* AR3260 en donde se establece el siguiente direccionamiento:

- Primera red: 192.168.10.0/24
- Segunda red: 172.168.50.0/24
- Enlace serial: 10.10.10.0/30

4.4. Establecer un enrutamiento estático en toda la red planteada para esta práctica.

4.5. Comprobar conectividad en la red.

4.6. Ejecutar el programa instalador de GNS3 y tener preparado la ISO de *router* Cisco 3660.

4.7. Una vez, ejecutado e instalado el programa GNS3, se procede a iniciar GNS3 y en la opción de editar-preferencias seleccionar la opción de *Dynamips* – IOS *routers.*

4.8. Seleccionar la opción de nuevo- nueva imagen y elegir la ISO correspondiente al *router* Cisco.

4.9. Continuar con las indicaciones del instructor para el establecimiento de un *router* en GNS3.

4.10. Ejecutar el *router* seleccionado la opción iniciar de la barra de herramientas de GNS3.

5. INFORME

5.1. Realizar la siguiente topología de red que se muestra en la figura A1.32 en base a un enrutamiento estático.

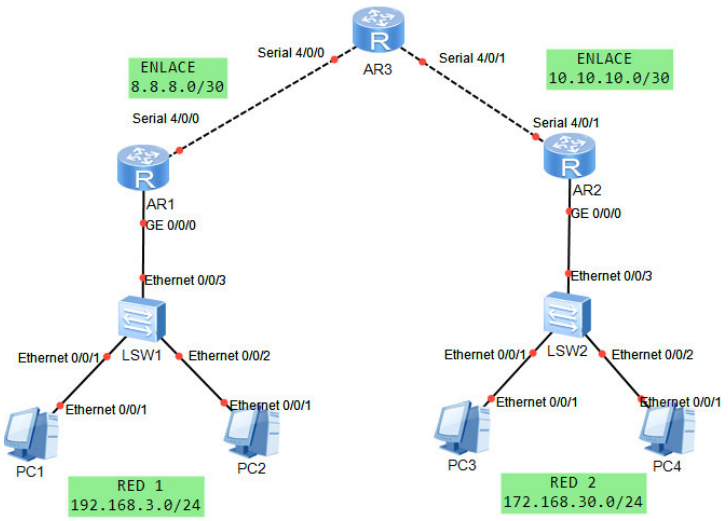


Figura A1.32 Topología de red propuesta para el informe

5.2. Evidenciar la conectividad entre dispositivos mediante el comando *ping*.

5.3. Conclusiones y Recomendaciones

6. BIBLIOGRAFÍA

[1] C. H. Enterprise, *Introducción al simulador de red de Huawei eNSP,* 2019. Available: https://n9.cl/fz9n7

[2] GNS3, "GNS3," 2021. [Online]. Available: https://www.gns3.com/software/download.

1. TEMA: Familiarización con eNSP

2. OBJETIVOS

2.1. Configurar en eNSP el establecimiento de protocolos de enrutamiento dinámicos.

2.2. Familiarizarse con los comandos de configuración para el levantamiento de interfaces, establecimiento de protocolos, configuración básica en el enrutador y redistribución de rutas.

3. DESARROLLO DE LA PRÁCTICA

3.1. Para la presente práctica se establece la siguiente topología de red a utilizar con base a las siguientes condiciones de direccionamiento que se muestran en la figura A1.33.

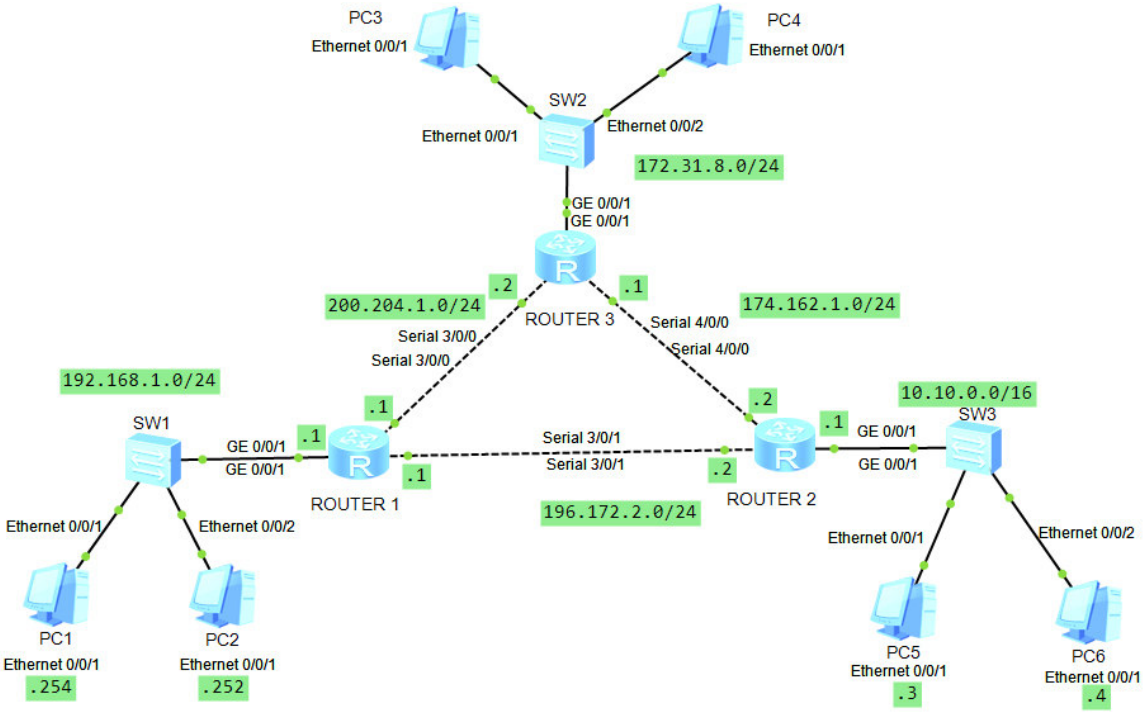


Figura A1.33 Topología de red propuesta para la presente práctica

3.2. Una vez establecida la topología a utilizar, se comienza con la respectiva configuración inicial en cada red iniciando con la configuración elemental:

- Cambio del nombre del *router* mediante el comando ***sysname* + "nuevo nombre".**

- Establecimiento de una cabecera de bienvenida mediante el comando ***header Shell information* "BIENVENIDO AL ROUTER X ".**

- Introducción de autenticación mediante el comando ***set autentication password*,** como se muestra en la figura A1.34.

```
<R1>terminal monitor
Info: Current terminal monitor is on.
<R1> system-view
[R1] sysname Router_1
[Router_1] header shell information "BIENVENIDO AL ROUTER_1"
[Router_1] user-interface console 0
[Router_1-ui-console0] authentication-mode password 123456
[Router_1] quit
<Router_1>save
  The current configuration will be written to the device.
  Are you sure to continue? (y/n) [n]: y
  It will take several minutes to save configuration file, please wait….
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
<Router_1>
```

Figura A1.34 Configuración de autenticación dentro del enrutador

NOTA: Al establecer un requerimiento de contraseña encriptada se añade el comando ***set autentication password cipher*,** como se muestra en la figura A1.35.

```
[Router_1-ui-console0] authentication-mode password cipher 123456
```

Figura A1.35 Configuración de autenticación encriptada

3.3. Una vez desarrollada la configuración elemental, se realiza el levantamiento respectivo de las diferentes interfaces de las tres redes con sus respectivos enlaces seriales, como se muestra en la figura A1.36.

Nota: El mismo proceso se repite en las diferentes redes planteadas.

```
<Router_1>terminal monitor
[Router_1] interface Serial 3/0/0
[Router_1-Serial3/0/0] ip address 4.4.0.1 255.255.255.252
[Router_1-Serial3/0/0] quit
[Router_1] interface Serial 3/0/1
[Router_1-Serial3/0/1] ip address 19.19.0.1 255.255.255.252
[Router_1-Serial3/0/1] quit
[Router_1] interface GigabitEthernet 0/0/1
[Router_1-GigabitEthernet0/0/1] ip address 192.168.1.1 255.255.255.0
[Router_1-GigabitEthernet0/0/1] quit
<Router_1>save
  The current configuration will be written to the device.
  Are you sure to continue? (y/n) [n]: y
  It will take several minutes to save configuration file, please wait..
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
```

Figura A1.36 Agregación de direccionamiento en cada enlace del enrutador

3.4. Ahora se procede a la configuración de protocolos de enrutamiento, como se muestran en las figuras A1.34, A1.38, A1.39.

RIP:

```
[Router_1] rip 1
[Router_1-rip-1] version 2
[Router_1-rip-1] network 192.168.1.0
[Router_1-rip-1] network 4.0.0.0
[Router_1-rip-1] network 19.0.0.0
[Router_1-rip-1] quit
```

Figura A1.37 Configuración del protocolo de enrutamiento RIP

OSPF:

```
[Router_2] ospf 1
[Router_2-ospf-1] area 0
[Router_2-ospf-1-area-0.0.0.0] network 19.19.0.2 0.0.0.3
[Router_2-ospf-1-area-0.0.0.0] network 8.8.0.2 0.0.0.3
[Router_2-ospf-1-area-0.0.0.0] network 10.10.0.1 0.0.0.255
[Router_2-ospf-1-area-0.0.0.0] quit
```

Figura A1.38 Configuración del protocolo de enrutamiento OSPF

IS-IS

```
[Router_3] isis 1
[Router_3-isis-1] network-entity 10.0001.0000.0000.1111.00
May  17  2021  03:53:30-08:00  ROUTER_&&01ISIS/4/START_ENABLE_ISIS  (1):
ISIS 256 enabled all ISIS modules
[Router_3-isis-1] quit
[Router_3] interface serial 4/0/0
[Router_3-Serial4/0/0] isis enable
[Router_3-Serial4/0/0] quit
[Router_3] interface serial 3/0/0
[Router_3-Serial3/0/0] isis enable
[Router_3-Serial3/0/0] quit
```

Figura A1.39 Configuración del protocolo de enrutamiento IS-IS

3.6. Realizar la redistribución de protocolos de enrutamiento mediante el comando ***import route***, como se muestra en la figura A1.40 con la siguiente sintaxis:

```
import-route:
   -  rip [ process-id-rip] [ cost cost | type type | tag tag | route-
      policy route-policy-name
   -  static [ cost cost | type type | tag tag | route-policy route-
      policy-name
   -  isis [ process-id-isis] [ cost cost | type type | tag tag |
      route-policy route-policy-name
   -  ospf [ process-id-ospf] [ cost cost | type type | tag tag |
      route-policy route-policy-name]}
```

Figura A1.40 Sintaxis del comando *import route* para diferentes protocolos de enrutamiento

3.7. Realizar la comprobación de funcionamiento con el comando ***display ip routing-table***, como se muestra en la figura A1.41.

```
<Router_1>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations: 18       Routes: 19

Destination/Mask    Proto   Pre-Cost      Flags NextHop         Interface

        4.4.0.0/30 Direct 0    0           D   4.4.0.1         Serial3/0/0
        4.4.0.1/32 Direct 0    0           D   127.0.0.1       Serial3/0/0
        4.4.0.2/32 Direct 0    0           D   4.4.0.2         Serial3/0/0
        4.4.0.3/32  Direct  0    0           D   127.0.0.1       Serial3/0/0
        8.8.0.0/30  OSPF    10   96          D   19.19.0.2       Serial3/0/1
                    OSPF    10   96          D   4.4.0.2         Serial3/0/0
      10.10.0.0/16  RIP     100  1           D   19.19.0.2       Serial3/0/1
      19.19.0.0/30  Direct  0    0           D   19.19.0.1       Serial3/0/1
      19.19.0.1/32  Direct  0    0           D   127.0.0.1       Serial3/0/1
      19.19.0.2/32  Direct  0    0           D   19.19.0.2       Serial3/0/1
      19.19.0.3/32  Direct  0    0           D   127.0.0.1       Serial3/0/1

<ROUTER_3>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 18       Routes : 19

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        4.4.0.0/30  Direct  0    0           D   4.4.0.2         Serial3/0/0
        4.4.0.1/32  Direct  0    0           D   4.4.0.1         Serial3/0/0
        8.8.0.0/30  Direct  0    0           D   8.8.0.1
Serial4/0/0
        8.8.0.2/32  Direct  0    0           D   8.8.0.2         Serial4/0/0
        8.8.0.3/32  Direct  0    0           D   127.0.0.1       Serial4/0/0
      10.10.0.0/16  RIP     100  1           D   8.8.0.2         Serial4/0/0
      19.19.0.0/30  OSPF    10   96          D   8.8.0.2         Serial4/0/0
                    OSPF    10   96          D   4.4.0.1         Serial3/0/0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
     172.31.8.0/24  Direct  0    0           D   172.31.8.1      GigabitEthernet
0/0/1
   172.31.8.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
    192.168.1.0/24  OSPF    10   49          D   4.4.0.1         Serial3/0/0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Figura A1.41 Tabla de enrutamiento de enrutadores

4. CONCLUSIONES

4.1. En esta práctica se mostró cómo se llevó a cabo el proceso de configuración de protocolos de enrutamiento dentro de eNSP cumpliendo todos los pasos a realizar para cumplir con los objetivos planteados para esta práctica.

4.2. El entorno de trabajo de eNSP permite tener una relación más directa con equipos de marca Huawei, en donde el estudiante logrará obtener una mejor visualización del sistema y la configuración del mismo.

5. RECOMENDACIONES

5.1. Al momento de establecer el enrutamiento respectivo de las diferentes interfaces, resaltando las interfaces seriales, tomar en cuenta el direccionamiento establecido para que no exista solapamiento en los mismos y para completar el comando utilizar la respectiva tecla de tabulador.

5.2. Se sugiere que en el desarrollo de configuración de enrutamiento tomar en cuenta que los enrutadores podrían demorarse en compartir sus tablas de enrutamiento y esto depende del procesamiento del ordenador. Además, al momento de configurar el comando de importación de ruta, tomar en cuenta que este puede variar en su funcionamiento dependiendo del modelo de enrutador Huawei que se esté utilizando.

5.3. Para comprobar el funcionamiento de conectividad en toda la red se recomienda realizar un *ping* extremo a extremo entre las diferentes máquinas pertenecientes a cada red.

6. BIBLIOGRAFÍA.

[1] C. H. Enterprise, « Huawei Enterprise,» 2021. [En línea]. Available: https://forum.Huawei.com/enterprise/es/forums.

[2] C. H. Enterprise, «Huawei Enterprise - eNSP,» 2021. [En línea]. Available: https://forum.Huawei.com/enterprise/es/eNSP/forum/100265.

1. TEMA: Familiarización con eNSP

2. OBJETIVOS

2.1. Configurar en eNSP el establecimiento de protocolos de enrutamiento dinámicos.

2.2. Familiarizarse con los comandos de configuración para el levantamiento de interfaces, establecimiento de protocolos, configuración básica en el enrutador y redistribución de rutas.

3. TRABAJO PREPARATORIO

3.1. Consultar sobre el programa de emulación eNSP y sus comandos básicos.

3.2. Elaborar una tabla de comparación de comandos usados en Cisco y su equivalencia en Huawei de los siguientes comandos:

Tabla A1.1 Comandos en Cisco

Comandos de Cisco
ping
traceroute
show
show interfaces
show ip route
show ip interface
show clock
exit
end
write terminal – running config
write erase
write mem - wr - copy run start
telnet
no shutdown
terminal monitor

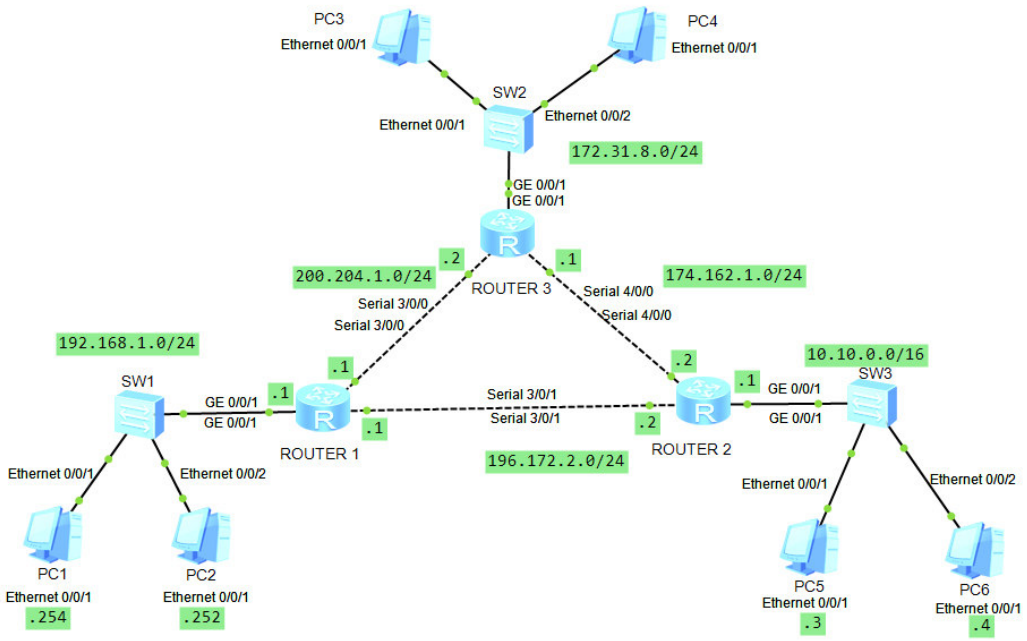
3.3. Consultar la configuración de establecimiento de contraseña en texto plano y encriptado para un *router* de marca Huawei.

3.4. Investigar sobre el comando *import route* y cómo configurar dependiendo del protocolo en eNSP.

3.5. Investigar la configuración para realizar enrutamiento mediante el protocolo RIP, OSPF y IS-IS. Además del comando respectivo para visualizar la tabla de enrutamiento.

4. DESCRIPCIÓN DE LA ACTIVIDAD

4.1. Construir la siguiente topología base de la figura A1.42 con el enrutador Huawei modelo 3260.



RED	Protocolo	*Gateway*
RED 1: 192.168.1.0/24	RIP	192.168.1.1 /24
RED 2: 172.31.8.0 /24	IS-IS	172.31.8.1 /24
RED 3: 10.10.0.0 /16	OSPF	10.10.0.1 /16
ENLACE 1: 8.8.0.0 /16		
ENLACE 2: 19.19.0.0 /16		
ENLACE 3: 4.4.0.0 /16		

Figura A1.42 Topología de red para informe

4.2. Establecer en los enrutadores los módulos de interfaces seriales.

4.3. Establecer el siguiente direccionamiento para las diferentes redes planteadas en la topología.

4.4. Utilizar el comando ***sysname*** para renombrar el nombre por defecto del enrutador.

4.5. Establecer una cabecera de bienvenida mediante el comando ***header Shell information.***

4.6. Configurar el método de autenticación encriptada mediante el comando ***set autentication password cipher*.**

4.7. Realizar el respectivo levantamiento de interfaces según el direccionamiento establecido en la tabla.

4.8. Configurar el protocolo de enrutamiento establecido para cada red.

4.9. Establecer la redistribución de rutas entre diferentes protocolos de enrutamiento con la utilización del comando ***import route.***

4.10. Configurar los dispositivos finales (ordenadores) con su respectiva dirección IP y *Gateway* para realizar la comprobación de conectividad entre las diferentes redes.

5. INFORME

5.1. Realizar la siguiente topología propuesta en la figura A1.43:

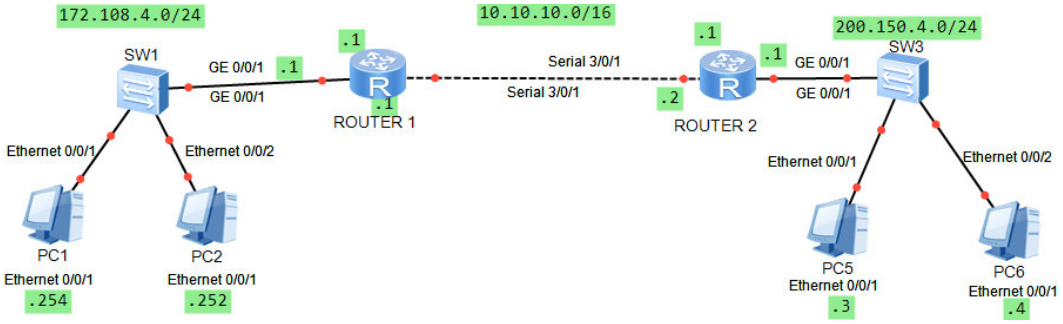


Figura A1.43 Topología de red propuesta para el informe

5.2. Realizar el enrutamiento RIP en la red 172.108.4.0/24 y para la red 200.150.4.0/24 OSPF.

5.3. Establecer conectividad total en toda la red mediante la redistribución de los protocolos RIP y OSPF, establecer las tablas de enrutamiento.

5.4. Evidenciar la conectividad total de la red realizando un *ping* entre ordenadores de las diferentes redes.

5.5. Conclusiones y Recomendaciones

6. BIBLIOGRAFÍA

[1] C. H. Enterprise, « Huawei Enterprise,» 2021. [En línea]. Available: https://forum.Huawei.com/enterprise/es/forums.

[2] C. H. Enterprise, «Huawei Enterprise - eNSP,» 2021. [En línea]. Available: https://forum.Huawei.com/enterprise/es/eNSP/forum/100265.

1. TEMA: Interconexión entre GNS3 y eNSP

2. OBJETIVOS

2.1. Establecer la interconexión entre un equipo Huawei y uno de la marca Cisco.

2.2. Interconectar los programas eNSP y GNS3 para realizar la vinculación entre los equipos de los diferentes proveedores.

3. DESARROLLO DE LA PRÁCTICA

3.1 En la figura A1.44 se presenta la conexión del equipo enrutador AR3260 de Huawei, el cual se conecta a la nube del eNSP y para ello, previamente se realiza una configuración en la misma para lograr conectarse con el equipo enrutador.

Figura A1.44 Topología de integración eNSP

3.2 A continuación, se puede visualizar la configuración respectiva de la nube para agregar el respectivo puerto Ethernet utilizando un puerto UDP. Y esto se consigue estableciendo los parámetros que se visualizan posteriormente, como se muestra en la figura A1.45.

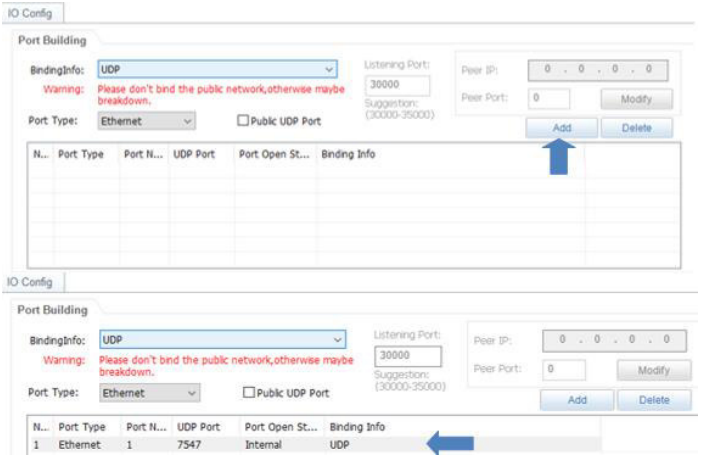


Figura A1.45 Configuración de nube para la interconexión con GNS3

3.3 Se procede a configurar el puerto de salida mediante una dirección *loopback* 127.0.0.1 y un número de puerto definido 30001 que será agregado y permitirá la interacción entre los puertos de los diferentes programas, como se muestra en la figura A1.46.

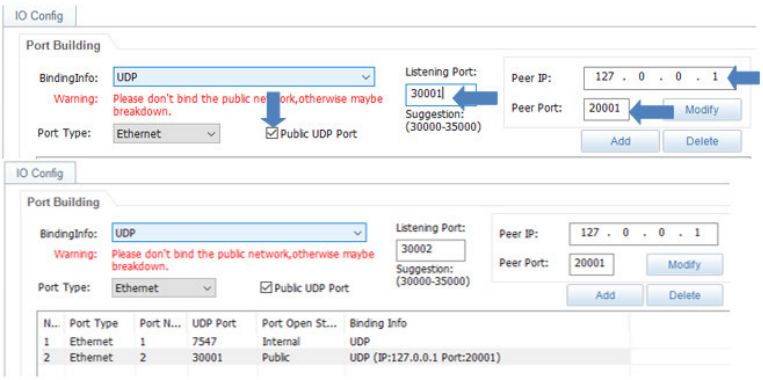


Figura A1.46 Agregación de puertos en la nube de eNSP

3.4 Al establecer los puertos de salida en la nube, se deberá añadir el número de puertos existentes a nivel local como remoto, para aquello, se solicita que en la parte inferior se configure lo que previamente se visualiza en las figuras A3.47 y A1.48.

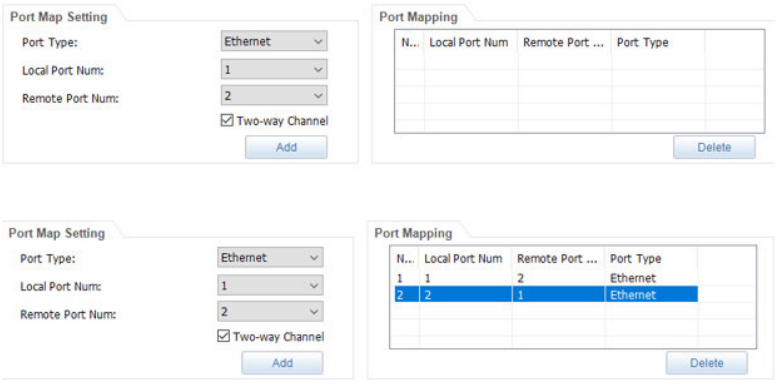


Figura A1.47 Agregación de número de puerto en la nube de eNSP

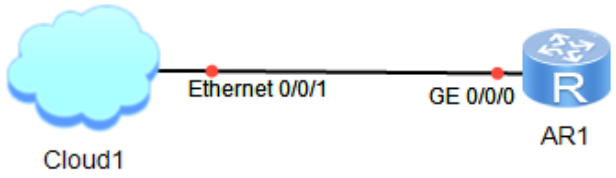


Figura A1.48 Conexión nube de eNSP con enrutador

3.5 En la figura A1.49 se presenta la conexión del equipo enrutador c3600 de Cisco, el cual se conecta a la nube GNS3 y para ello, previamente se realiza una configuración en la misma para lograr conectarse con el equipo enrutador.

Figura A1.49 Topología de integración en GNS3

3.6 A continuación, en la figura A1.50 se puede visualizar la configuración respectiva de la nube para agregar el respectivo puerto Ethernet utilizando un puerto UDP. Y esto se consigue estableciendo los parámetros que se visualizan en la figura A1.51.

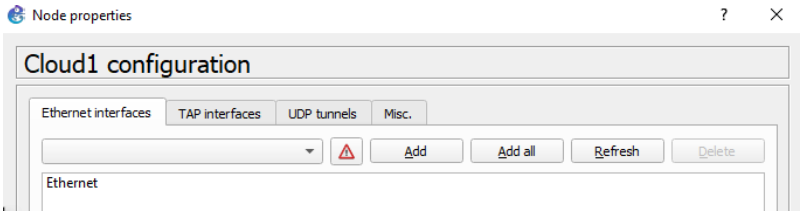


Figura A1.50 Colocación de UDP *tunnels* en GNS3

3.7 En las configuraciones de la nube, se seleccionará la pestaña de UDP *tunnels* en donde se configura los siguientes parámetros para iniciar con la conexión entre ambos programas, como se muestra en la figura A1.51.

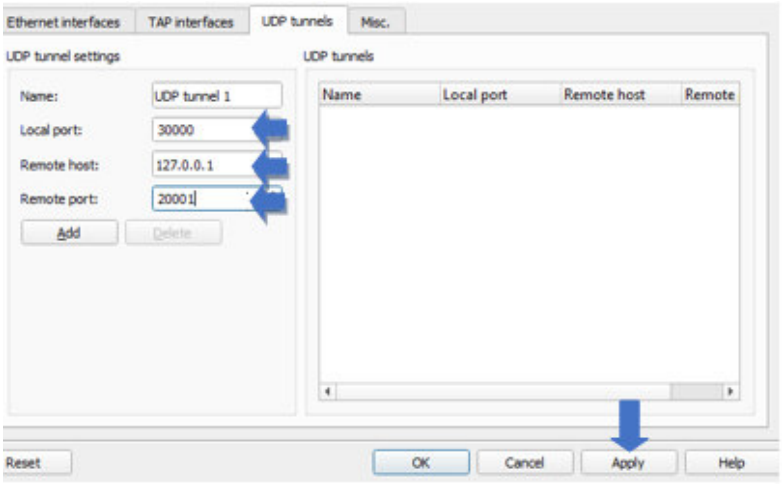


Figura A1.51 Configuración de puertos en la nube en GNS3

3.8 Una vez configurado el número de puerto tanto a nivel local como remoto se procede a conectar el dispositivo con la nube en el puerto UDP *tunnel* 1, como se muestra en la figura A1.52.

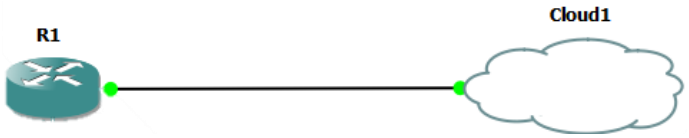
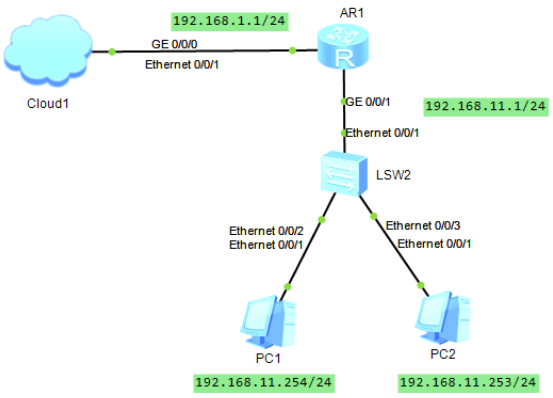


Figura A1.52 Conexión de equipo Cisco con la nube en GNS3

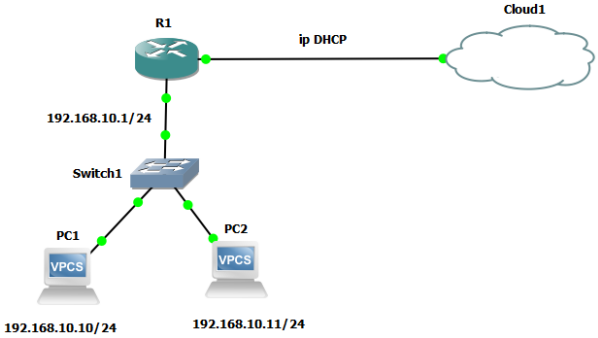
3.9 Ahora se establece el direccionamiento para enrutador, por lo tanto, se comienza con el enrutador en eNSP, en donde se configura el direccionamiento por DHCP a las interfaces hacia el dispositivo enrutador en GNS3 estableciendo la dirección como se muestra en la figura A1.53.




```
dhcp enable
#
ip pool 1
 gateway-list 192.168.1.1
 network 192.168.1.0 mask 255.255.255.0
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.1 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/1
 ip address 192.168.11.1 255.255.255.0
#
```

Figura A1.53 Configuración de DHCP en eNSP

3.10 Ahora se ingresa al equipo Cisco en GNS3 se configura la interfaz que conecta con la nube para un direccionamiento mediante DHCP, como se muestra en la figura A1.54.




```
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip address dhcp
R1(config-if)#no shutdown
R1(config-if)#exit
*Mar  1 00:00:37.191: %LINK-3-UPDOWN: Interface FastEthernet0/0,
changed state to up
*Mar  1 00:00:38.191: %LINEPROTO-5-UPDOWN: Line protocol on Interface
 FastEthernet0/0, changed state to up
Interface FastEthernet0/0 assigned DHCP address 192.168.1.254, mask
255.255.255.0
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status  Protocol
FastEthernet0/0            192.168.1.254   YES DHCP   up         up
```

Figura A1.54 Configuración de enlace en GNS3

3.11 Establecer la dirección del enlace de la red 192.168.10.0/24, como se muestra en la figura A1.55.

```
R1(config)#interface ethernet 1/1
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
*Mar  1 00:08:39.703: %LINK-3-UPDOWN: Interface Ethernet1/1,
changed state to up
*Mar  1 00:08:40.703: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet1/1, changed state to up
```

Figura A1.55 Establecimiento de direccionamiento en enlace

3.12 Ahora establecer como protocolo de enrutamiento predeterminado a RIP para la interconexión entre dispositivos de las diferentes marcas, como se muestra en la figura A1.56.

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 192.168.10.1
R1(config-router)#network 192.168.1.0

<Huawei>system-view
Enter system view, return user view
with Ctrl+Z.
[Huawei]rip
[Huawei-rip-1]version 2
[Huawei-rip-1]network 192.168.11.0
[Huawei-rip-1]network 192.168.1.0
```

Figura A1.56 Establecimiento del protocolo de enrutamiento RIP en eNSP

3.13 Realizar una prueba de conexión mediante el comando *ping* a los ordenadores de las diferentes redes compuestas por un equipo Huawei y Cisco, como se muestra en la figura A1.57.

```
PC1> ping 192.168.11.254
192.168.11.254 icmp_seq=1 timeout
84 bytes from 192.168.11.254 icmp_seq=2 ttl=126 time=64.957 ms
84 bytes from 192.168.11.254 icmp_seq=3 ttl=126 time=54.085 ms
84 bytes from 192.168.11.254 icmp_seq=4 ttl=126 time=55.107 ms
84 bytes from 192.168.11.254 icmp_seq=5 ttl=126 time=54.038 ms

PC>ping 192.168.10.10
Ping 192.168.10.10: 32 data bytes, Press Ctrl_C to break
From 192.168.10.10: bytes=32 seq=1 ttl=62 time=47 ms
From 192.168.10.10: bytes=32 seq=2 ttl=62 time=47 ms
From 192.168.10.10: bytes=32 seq=3 ttl=62 time=63 ms
From 192.168.10.10: bytes=32 seq=4 ttl=62 time=62 ms
From 192.168.10.10: bytes=32 seq=5 ttl=62 time=47 ms
```

Figura A1.57 Comprobación de conexión eNSP con GNS3

4 CONCLUSIONES

4.1. En esta práctica se mostró cómo se llevó a cabo el proceso de interconexión entre eNSP y GNS3 mediante la utilización de puertos UDP.

4.2. El entorno de trabajo, tanto de eNSP como GNS3, se permite tener una relación directa con equipos de marca Huawei y Cisco, por lo tanto, se puede conseguir que exista la correlación de funcionamiento entre dispositivos de diferentes marcas.

5 RECOMENDACIONES

5.1. Al momento de establecer el direccionamiento IP de los diferentes enlaces tomar en cuenta la activación del direccionamiento por DHCP.

5.2. Se sugiere que en el desarrollo de configuración de enrutamiento se tome en cuenta que los enrutadores podrían demorarse en compartir sus tablas de enrutamiento y esto depende del procesamiento del ordenador.

5.3. Para comprobar el funcionamiento de conectividad en toda la red se recomienda realizar un *ping* extremo a extremo entre las diferentes máquinas pertenecientes a cada red.

6 BIBLIOGRAFÍA.

[1] C. H. Enterprise, « Huawei Enterprise,» 2021. [En línea]. Available: https://forum.Huawei.com/enterprise/es/integraci%C3%B3n-entre-router-cisco-y-router-Huawei-con-gns3-y-ensp/thread/546567-100235

[2] M. Raio, «GNS3,» 24 07 25. [En línea]. Available: https://gns3.com/community/blog/connecting-Huawei-ensp-to-gns3.

ESCUELA POLITÉCNICA NACIONAL
ESCUELA DE FORMACIÓN DE TECNÓLOGOS
Tecnología Superior en Redes y Telecomunicaciones
Redes de Computadoras
Hoja Guía Práctica 3 (Estudiante)

1. TEMA: Interconexión entre GNS3 y eNSP

2. OBJETIVOS

2.1. Establecer la interconexión entre un equipo Huawei y uno de la marca Cisco.

2.2. Interconectar los programas eNSP y GNS3 para realizar la vinculación entre los equipos de los diferentes proveedores.

3. TRABAJO PREPARATORIO

3.1 Investigar el proceso de configuración de un equipo Huawei como Cisco para el funcionamiento de DHCP en ambos equipos

3.2 Investigar a qué hace referencia la dirección 127.0.0.1 y para qué es utilizada.

3.3 Elabore una tabla de comparación con las principales ventajas de los programas GNS3 y eNSP.

3.4 Descargar GNS3 al igual que instalar la ISO correspondiente del *router* Cisco 3660 del siguiente *link:* https://n9.cl/p0u15.

3.5 Investigar cómo configurar el puente de conexión entre GNS3 y eNSP.

4. DESCRIPCIÓN DE LA ACTIVIDAD

4.1 Conectar el equipo enrutador AR3260 de Huawei, conectar la nube del eNSP.

4.2 Realizar la configuración respectiva de la nube con la ayuda del docente para agregar el respectivo puerto Ethernet utilizando un puerto UDP.

4.3 Al establecer los puertos de salida en la nube, añadir el número de puertos existentes a nivel local como remoto.

4.4 En las configuraciones de la nube en GNS3, se seleccionará la pestaña de UDP *tunnels* en donde se configura los parámetros dictados por el docente.

4.5 Una vez configurado el número de puerto tanto a nivel local como remoto se procede a conectar el dispositivo con la nube en el puerto UDP *tunnel* 1.

4.6 Establecer el direccionamiento para enrutador por DHCP a las interfaces hacia el dispositivo enrutador en GNS3.

4.7 Ingresar al equipo Cisco en GNS3 y configurar la interfaz que conecta con la nube para un direccionamiento mediante DHCP.

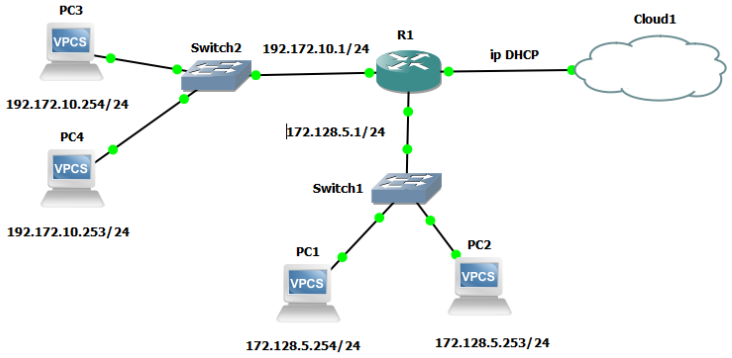
4.8 Establecer la dirección del enlace de la red 192.168.10.0/24.

4.9 Establecer como protocolo de enrutamiento predeterminado a RIP para la interconexión entre dispositivos de las diferentes marcas.

5. INFORME

5.1 Realizar la siguiente topología propuesta en la figura A1.58 en los distintos programas:

- En GNS3



- En eNSP

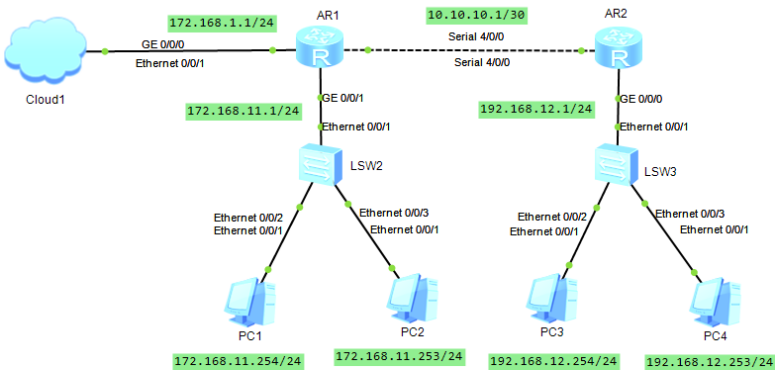


Figura A1.58 Topología de red propuesta para el informe

5.2 Establecer la interconexión respectiva GNS3 y eNSP.

5.3 Utilizar como protocolo de enrutamiento OSPF.

5.4 Evidenciar la conectividad total de la red realizando un *ping* entre ordenadores de las diferentes redes.

5.5 Conclusiones y Recomendaciones

6. BIBLIOGRAFÍA

[1] C. H. Enterprise, « Huawei Enterprise,» 2021. [En línea]. Available: https://forum.Huawei.com/enterprise/es/integraci%C3%B3n-entre-router-cisco-y-router-Huawei-con-gns3-y-ensp/thread/546567-100235

[2] M. Raio, «GNS3,» 24 07 25. [En línea]. Available: https://gns3.com/community/blog/connecting-Huawei-ensp-to-gns3.

1. TEMA: Protocolos de encapsulación, DHCP y *Firewall*.

2. OBJETIVOS

2.1. Establecer una topología y configuración básica en el programa eNSP, en donde se procederá al establecimiento de protocolos de encapsulación a nivel WAN, al igual que la implementación de servicios de DHCP y f*irewall* a nivel LAN.

2.2. Relacionar los comandos de configuración para el levantamiento de interfaces y el establecimiento de protocolos tanto de enrutamiento como de encapsulación.

3. DESARROLLO DE LA PRÁCTICA

3.1 Realizar la siguiente topología de red y asignar las respectivas direcciones IP de cada enlace mediante el comando *ip address* y asignar como protocolo de enrutamiento predeterminado RIPv2, como se muestra en las figuras A1.59, A1.60, A1.61.

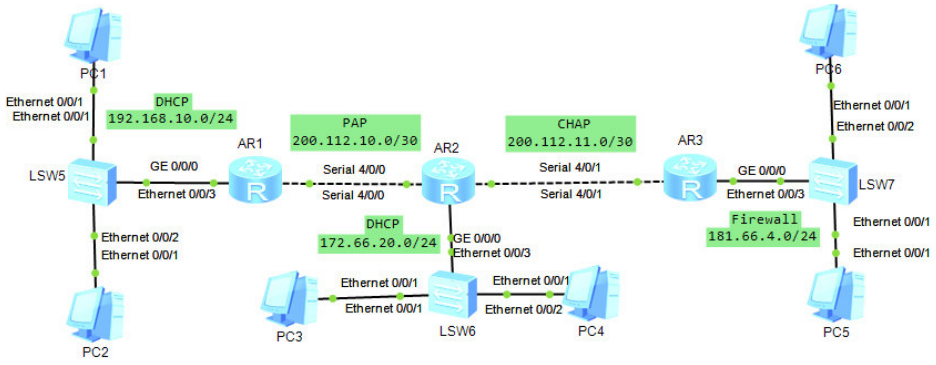


Figura A1.59 Topología de red propuesta para la presente práctica

```
<Huawei>system-view
[Huawei]sysname R1
[R1]interface Serial 4/0/0
[R1-Serial4/0/0]ip address 200.112.10.1 30
[R1-Serial4/0/0]quit
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]ip address 192.168.10.1 24
[R1-GigabitEthernet0/0/0]quit
```

```
<Huawei>system-view
[Huawei]sysname R2
[R2]interface Serial 4/0/0
[R2-Serial4/0/0]ip address 200.112.10.2 30
[R2-Serial4/0/0]quit
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]ip address 172.66.20.1 24
[R2-GigabitEthernet0/0/0]quit
[R2]interface Serial 4/0/1
[R2-Serial4/0/1]ip address 200.112.11.1 30
[R2-Serial4/0/1]quit
```

```
<Huawei>system-view
[Huawei]sysname R3
[R3]interface Serial 4/0/1
[R3-Serial4/0/1]ip address 200.112.11.2 30
[R3-Serial4/0/1]quit
[R3]interface GigabitEthernet 0/0/0
[R3-GigabitEthernet0/0/0]ip address 181.66.4.1 24
[R3-GigabitEthernet0/0/0]quit
```

Figura A1.60 Establecimiento de direccionamiento de enlaces

```
[R1]rip
[R1-rip-1]version 2
[R1-rip-1]network 200.112.10.0
[R1-rip-1]network 192.168.10.0
[R1-rip-1]quit
```

```
[R2]rip
[R2-rip-1]version 2
[R2-rip-1]network 200.112.10.0
[R2-rip-1]network 200.112.11.0
[R2-rip-1]network 172.66.0.0
[R2-rip-1]quit
```

```
[R3]rip
[R3-rip-1]version 2
[R3-rip-1]network 200.112.11.0
[R3-rip-1]network 181.66.0.0
[R3-rip-1]quit
```

Figura A1.61 Establecimiento de protocolo de enrutamiento RIP

3.2 Configurar cada enlace WAN mediante el protocolo de encapsulación HDLC el cual se configura en cada interfaz serial mediante el comando *link-protocol hdlc,* como se muestra en la figura A1.62.

```
<R1>system-view
[R1]interface Serial 4/0/0
[R1-Serial4/0/0]link-protocol hdlc
Warning: The encapsulation protocol of the link will be changed.
Continue? [Y/N]:y

<R2>system-view
[R2]interface Serial 4/0/0
[R2-Serial4/0/0]link-protocol hdlc
Warning: The encapsulation protocol of the link will be changed.
Continue? [Y/N]:y
[R2-Serial4/0/0]quit
[R2]interface Serial 4/0/1
[R2-Serial4/0/1]link-protocol hdlc
Warning: The encapsulation protocol of the link will be changed.
Continue? [Y/N]:y

<R3>system-view
[R3]interface Serial 4/0/1
[R3-Serial4/0/1]link-protocol hdlc
Warning: The encapsulation protocol of the link will be changed.
Continue? [Y/N]:y
```

Figura A1.62 Configuración de protocolo de encapsulación HDLC

3.3 Ahora mediante el comando *display interface* visualizar que dicho enlace se encuentra ya establecido con el protocolo de encapsulación HDLC, como se muestra en la figura A1.63

```
[R1]display interface Serial 4/0/0
Serial4/0/0 current state : UP
Line protocol current state : UP
Internet Address is 200.112.10.1/30
Link layer protocol is nonstandard HDLC

[R3]display interface Serial 4/0/1
Serial4/0/1 current state : UP
Line protocol current state : UP
Internet Address is 200.112.11.2/30
Link layer protocol is nonstandard HDLC
```

```
[R2]display interface Serial 4/0/0
Serial4/0/0 current state : UP
Line protocol current state : UP
Internet Address is 200.112.10.2/30
Link layer protocol is nonstandard HDLC
[R2]display interface Serial 4/0/1
Serial4/0/1 current state : UP
Line protocol current state : UP
Internet Address is 200.112.11.1/30
Link layer protocol is nonstandard HDL
```

Figura A1.63 Comprobación de encapsulamiento HDLC

3.4 Ahora proceder a configurar el protocolo de encapsulación PPP en las interfaces seriales mediante el comando *link-protocol PPP* y comprobar el establecimiento de dicho protocolo mediante el comando *display interface,* como se muestra en la figura A1.64.

```
[R1]interface Serial 4/0/0
[R1-Serial4/0/0]link-protocol ppp
Warning: The encapsulation protocol of the link will be changed.
Continue? [Y/N]:y
[R1-Serial4/0/0]quit
```

```
<R2>system-view
[R2]interface Serial 4/0/0
[R2-Serial4/0/0]link-protocol ppp
Warning: The encapsulation protocol of the link will be changed.
Continue? [Y/N]:y
[R2-Serial4/0/0]quit
[R2]interface Serial 4/0/1
[R2-Serial4/0/1]link-protocol ppp
Warning: The encapsulation protocol of the link will be changed.
Continue? [Y/N]:y
[R2-Serial4/0/1]quit

<R3>system-view
[R3]interface Serial 4/0/1
[R3-Serial4/0/1]link-protocol ppp
Warning: The encapsulation protocol of the link will be changed.
Continue? [Y/N]:y
[R3-Serial4/0/1]quit
```

Figura A1.64 Configuración de protocolo de encapsulamiento PPP

3.5 Proceder a configurar el protocolo de encapsulación PPP añadiendo la autenticación por PAP mediante el comando *ppp authentication-mode pap,* como se muestra en la figura A1.65.

```
[R1]interface Serial 4/0/0
[R1-Serial4/0/0]ppp authentication-mode pap
[R1-Serial4/0/0]quit

[R2]interface Serial 4/0/0
[R2-Serial4/0/0]ppp authentication-mode pap
[R2-Serial4/0/0]quit
[R2]interface Serial 4/0/1
[R2-Serial4/0/1]ppp authentication-mode pap
[R2-Serial4/0/1]quit

[R3]interface Serial 4/0/1
[R3-Serial4/0/1]ppp authentication-mode pap
[R3-Serial4/0/1]quit
```

Figura A1.65. Configuración de protocolo de encapsulación PPP por PAP

3.6 Establecer los respectivos parámetros de autenticación como es el usuario y contraseña, lo cual se lo realiza mediante el comando *aaa* y dentro del mismo establecer el comando *local-user* para la creación del respectivo usuario y a continuación *password cipher* para la creación de la respectiva contraseña. Además, configurar el tipo de servicio mediante el comando *local-user* (usuario creado*) service-type ppp***,** como se muestra en la figura A1.66.

Nota: Cabe resaltar que el servicio de autenticación PAP se establece conforme a un dispositivo autenticador (R1) y autenticado (R2).

```
[R1]aaa
[R1-aaa]local-user R1 password cipher PRACTICA
Info: Add a new user.
[R1-aaa]local-user R1 service-type ppp
[R1-aaa]quit

[R2]interface Serial 4/0/0
[R2-Serial4/0/0]ppp pap local-user R2 password cipher PRACTICA
[R2-Serial4/0/0]quit
```

Figura A1.66 Establecimiento de usuario y contraseña mediante el comando aaa

3.7 Proceder a configurar el protocolo de encapsulación PPP añadiendo la autenticación por CHAP mediante el comando *ppp authentication-mode chap* entre el enrutador R2(Autenticado) Y R3 (Autenticador) añadiendo la creación del respectivo parámetro de autenticación, como se muestra en la figura A1.67.

```
[R3]interface Serial 4/0/1
[R3-Serial4/0/1]ppp authentication-mode chap
[R3-Serial4/0/1]quit
[R3]aaa
[R3-aaa]local-user R3 password cipher PRACTICA
Info: Add a new user.
[R3-aaa]local-user R3 service-type ppp
[R3-aaa]quit


[R2]interface Serial 4/0/1
[R2-Serial4/0/1]ppp chap user R3
[R2-Serial4/0/1]ppp chap password cipher PRACTICA
[R2-Serial4/0/1]quit
```

Figura A1.67 Configuración de protocolo de encapsulación PPP por CHAP

3.8 Realizar la respectiva configuración del servicio de DHCP como se muestra en las figuras A1.68 y A1.69, además en los ordenadores habilitar el mencionado servicio.

```
[R1]ip pool DHCP-R1
[R1-ip-pool-DHCP-R1] gateway-list 192.168.10.1
[R1-ip-pool-DHCP-R1] network 192.168.10.0 mask 255.255.255.0
[R1-ip-pool-DHCP-R1] dns-list 8.8.4.4
[R1]dhcp enable
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]dhcp select global
[R1-GigabitEthernet0/0/0]quit

[R2]ip pool DHCP-R2
[R2-ip-pool-DHCP-R2] gateway-list 172.66.20.1
[R2-ip-pool-DHCP-R2] network 172.66.20.1 mask 255.255.255.0
[R2-ip-pool-DHCP-R2] dns-list 8.8.4.4
[R2]dhcp enable
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]dhcp select global
[R2-GigabitEthernet0/0/0]quit
```

Figura A1.68 Configuración de DHCP en los diferentes enrutadores

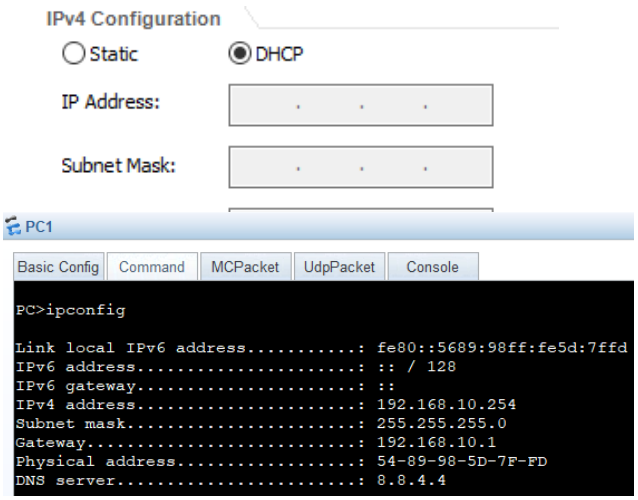


Figura A1.69 Comprobación del servicio DHCP

3.9 Para establecer un servicio de protección a nivel de red o *firewall* en un enrutador, se establece mediante el comando ***firewall* + (el servicio a prestar),** como se muestra en la figura A1.70.

```
[R3]firewall ?
black-white-list  Black-white-list
  blacklist         Blacklist
  defend            Firewall attack defend
  interzone         Enter interzone view
  log               Log information
  statistics        Traffic-statistics
  whitelist         Whitelist
  zone              Specify security zone configuration
```

Figura A1.70 Establecimiento de *Firewall* en eNSP

3.10 Para la práctica correspondiente establecer un servicio de denegación como mecanismo de control de acceso, como se muestra en la figura A1.71.

```
[R3] firewall blacklist 192.168.10.253
```

Figura A1.71 Comando de establecimiento básico de *Firewall*

4. CONCLUSIONES

4.1 En esta práctica se muestra cómo se lleva a cabo el proceso de configuración de protocolos de encapsulación dentro de eNSP en donde se establece todos los pasos a realizar para cumplir con los objetivos planteados para esta práctica.

4.2 En la topología de red prevista, se estableció un servicio de DHCP y *firewall* cumpliendo con el objetivo antes mencionado, con el cual el estudiante obtendrá un mayor conocimiento de configuración de estos servicios esenciales en una red.

5. RECOMENDACIONES

5.1 Al momento de establecer el enrutamiento respectivo de las diferentes interfaces, resaltando las interfaces seriales, tomar en cuenta el direccionamiento establecido para que no exista solapamiento en los mismos y para completar el comando utilizar la respectiva tecla de tabulador.

5.2 Se sugiere que, en el desarrollo de configuración del protocolo de encapsulación, tanto PAP como CHAP, identificar correctamente el enrutador autenticado y autenticador, al igual que no olvidarse de crear el respectivo usuario y contraseña que los enrutadores se compartirán.

5.3 Para comprobar el funcionamiento de conectividad en toda la red se recomienda realizar un *ping* extremo a extremo entre las diferentes máquinas pertenecientes a cada red.

6. BIBLIOGRAFÍA.

[1] C. H. Enterprise, « Huawei Enterprise,» 2021. [En línea]. Available: https://forum.Huawei.com/enterprise/es/forums.

[2] M. Lopez, «Steemit,» 2018. [En línea]. Available: https://steemit.com/spanish/@michelylopez/configuracion-de-enlaces-wan-con-ppp-hdlc-pap-y-chap-en-router-Huawei-ensp.

ESCUELA POLITÉCNICA NACIONAL
ESCUELA DE FORMACIÓN DE TECNÓLOGOS
Tecnología Superior en Redes y Telecomunicaciones
Redes de Computadoras
Hoja Guía Práctica 4 (Estudiante)

1. **TEMA: Protocolos de encapsulación, DHCP y *Firewall*.**

2. **OBJETIVOS**

2.1. Establecer una topología y configuración básica en el programa eNSP, en donde, se procederá al establecimiento de protocolos de encapsulación a nivel WAN, al igual que, la implementación de servicios de DHCP y *Firewall* a nivel LAN.

2.2. Relacionar con los comandos de configuración para el levantamiento de interfaces y el establecimiento de protocolos tanto de enrutamiento como de encapsulación.

3. **TRABAJO PREPARATORIO**

3.1 Realizar una tabla de comparación entre las principales características de los protocolos de encapsulación HDLC y PPP.

3.2 Investigar qué protocolo de autenticación es el más seguro entre PAP y CHAP y describir la respectiva justificación.

3.3 Investigar diferentes tipos de *firewall* que se pueden establecer dentro de una red a nivel LAN y los servicios que estos prestan y describir cada uno de ellos (mínimo 5 servicios).

3.4 Investigar mecanismos de seguridad orientados a proteger la información y detallar cada uno de ellos (mínimo 3 mecanismos).

3.5 Investigar los comandos básicos para la configuración del servicio de DHCP en eNSP.

3.6 Consultar cómo se utiliza el comando *debugging.*

4. DESCRIPCIÓN DE LA ACTIVIDAD

4.1 Realizar la topología de red propuesta por el docente y asignar las respectivas direcciones IP de cada enlace mediante el comando ***ip address*** y asignar como protocolo de enrutamiento predeterminado RIPv2.
4.2 Configurar cada enlace WAN mediante el protocolo de encapsulación HDLC el cual se configurar en cada interfaz serial mediante el comando ***link-protocol hdlc*.**

4.3 Ahora mediante el comando ***display interface*** visualizar que dicho enlace se encuentra ya establecido con el protocolo de encapsulación HDLC.

4.4 Ahora proceder a configurar el protocolo de encapsulación PPP en las interfaces seriales mediante el comando ***link-protocol PPP*** y comprobar el establecimiento de dicho protocolo mediante el comando ***display interface*.**

4.5 Proceder a configurar el protocolo de encapsulación PPP añadiendo la autenticación por PAP mediante el comando ***ppp authentication-mode pap*.**

4.6 Establecer los respectivos parámetros de autenticación como es el usuario y contraseña, para lo cual se lo realiza mediante el comando ***aaa*** y dentro del mismo establecer el comando ***local-user*** para la creación del respectivo usuario y a continuación ***password cipher*** para la creación de la respectiva contraseña. Además, configurar el tipo de servicio mediante el comando ***local-user* (usuario creado) service-*type ppp*.**

Nota: Cabe resaltar que el servicio de autenticación PAP se establece conforme a un dispositivo autenticador (R1) y autenticado (R2)

4.7 Proceder a configurar el protocolo de encapsulación PPP añadiendo la autenticación por CHAP mediante el comando ***ppp authentication-mode chap*** entre el enrutador R2(Autenticado) Y R3 (Autenticador) añadiendo la creación del respectivo parámetro de autenticación.

4.8 Realizar la respectiva configuración del servicio de DHCP y comprobar la asignación automática en cada ordenador.

4.9 Para establecer un servicio de protección a nivel de red o *firewall* en un enrutador, se establece mediante el comando ***firewall* + (el servicio a prestar).**

4.10 Para la práctica correspondiente establecer un servicio de denegación como mecanismo de control de acceso.

5. INFORME

5.1 Realizar la siguiente topología de red prevista en la figura A1.72.

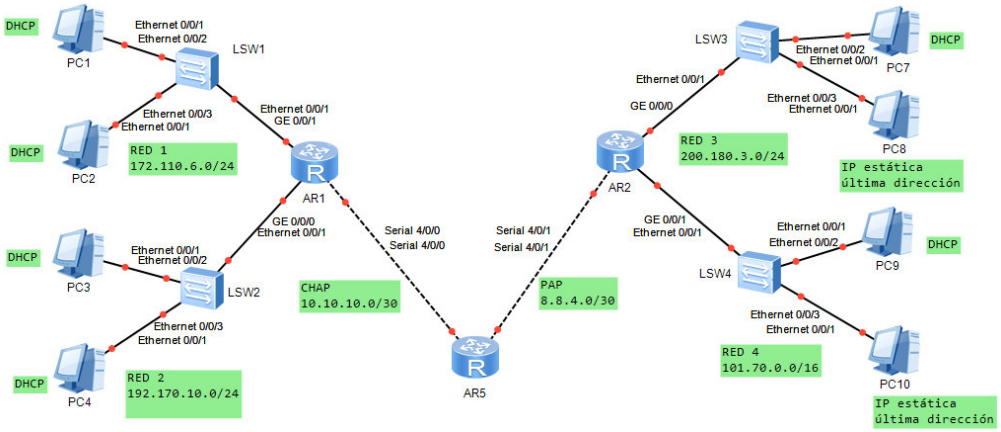


Figura A1.72 Topología de red propuesta para el informe

5.2 Establecer la interconexión respectiva entre todos los dispositivos.

5.3 Utilizar como protocolo de enrutamiento OSPF.

5.4 Evidenciar la conectividad total de la red realizando un ***ping*** entre ordenadores de las diferentes redes, al igual que, el funcionamiento del servicio DHCP.

5.5 Demostrar el establecimiento de CHAP y PAP mediante el comando de ***debugging*.**

5.6 Conclusiones y Recomendaciones.

6. BIBLIOGRAFÍA

[1] C. H. Enterprise, « Huawei Enterprise,» 2021. [En línea]. Available: https://forum.Huawei.com/enterprise/es/forums.

[2] M. Lopez, «Steemit,» 2018. [En línea]. Available: https://steemit.com/spanish/@michelylopez/configuracion-de-enlaces-wan-con-ppp-hdlc-pap-y-chap-en-router-Huawei-ensp.

1. TEMA: Establecimiento de VLANs en eNSP.

2. OBJETIVOS

2.1 Establecer una topología de red para la configuración básica de *switches* de capa 2 orientando al establecimiento de VLANs.

2.2 Desarrollar y configurar el enrutamiento entre VLANs.

3. DESARROLLO DE LA PRÁCTICA

3.1 Realizar la siguiente topología de red y asignar las respectivas direcciones IP de cada enlace del enrutador R1 y R2. Cabe resaltar que se establece un *gateway* para las diferentes VLANs mediante la creación de subinterfaces, como se muestra en la figura A1.73.

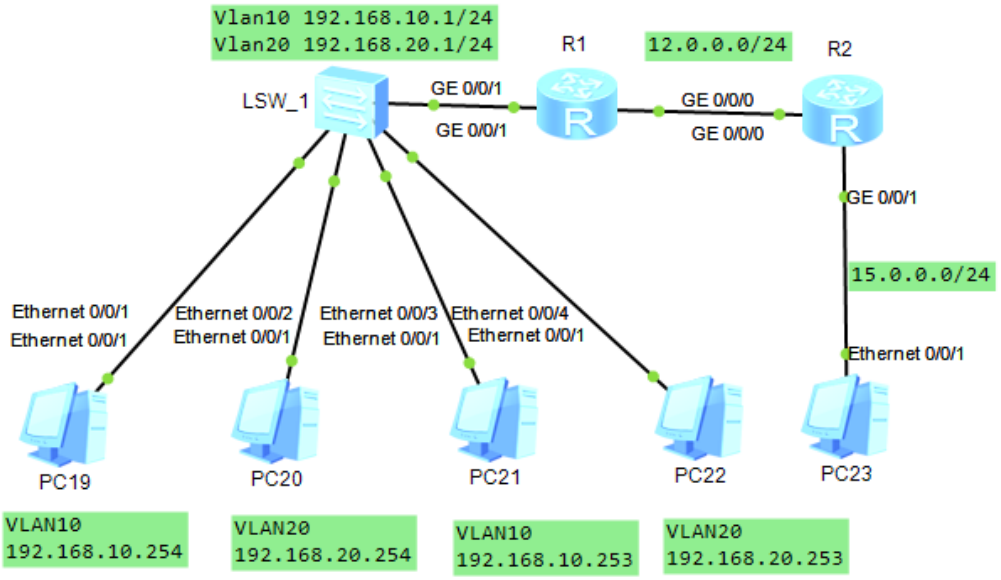


Figura A1.73 Topología base para la presente práctica

3.2 Dentro del CLI del enrutador “R1” definir las subinterfaces que pertenecen a la diferentes VLANs a desarrollarse. No obstante, se establece la VLAN que esa subinterfaz utilizará. Se recomienda utilizar el mismo número tanto para la subinterfaz como para la VLAN, como se muestra en la figura A1.74.

```
<R1>system-view
[R1] interface GigabitEthernet 0/0/0
[R1] ip address 12.0.0.1 255.255.255.0
[R1] quit
[R1]interface GigabitEthernet 0/0/0.10
[R1] ip address 192.168.10.1 255.255.255.0
[R1] quit
[R1]interface GigabitEthernet 0/0/0.20
[R1] ip address 192.168.20.1 255.255.255.0
[R1] quit
```

```
<R2>system-view
[R2] interface GigabitEthernet 0/0/0
[R2] ip address 12.0.0.2 255.255.255.0
[R2] quit
[R2]interface GigabitEthernet 0/0/1
[R2] ip address 15.0.0.1 255.255.255.0
[R2] quit
```

Figura A1.74 Agregación de direccionamiento IP en los diferentes enlaces

3.3 Dentro del CLI del *switch* “SW1” crear las VLANs que se van a desarrollar en la red mediante el comando ***vlan batch.***

3.4 Definir una interfaz del SW1 como un enlace troncal mediante el comando ***port link-type trunk*** con el objetivo de que por ese enlace se transporte todo el tráfico de las VLANs y para permitir que por ese enlace salgan las VLANs creadas, utilizar el comando ***port trunk allow-pass vlan*** + **(mencionar el número de VLANs creadas).**

3.5 En cada interfaz del SW1 que conecta a los ordenadores, se define como una interfaz de acceso mediante el comando ***port link-type Access.*** Además, con el comando ***port default*** establecer la VLAN que corresponderá a ese ordenador, como se muestra en la figura A1.75.

```
<SW1> system-view
[SW1] vlan batch 10 20
[SW1] interface GigabitEthernet0/0/1
[SW1] port link-type trunk
[SW1] port trunk allow-pass vlan 10 20
[SW1] quit
[SW1] interface Ethernet0/0/1
[SW1] port link-type access
[SW1] port default vlan 10
[SW1] quit
[SW1] interface Ethernet0/0/2
[SW1] port link-type access
[SW1] port default vlan 20
[SW1] quit
[SW1] interface Ethernet0/0/3
[SW1] port link-type access
[SW1] port default vlan 10
[SW1] quit
[SW1] interface Ethernet0/0/4
[SW1] port link-type access
[SW1] port default vlan 20
[SW1] quit
```

Figura A1.75 Agregación de VLANs, puertos troncales y de acceso

3.6 Dentro de las subinterfaces de las VLANs en R1 establecer el protocolo de encapsulación que corresponderá a la VLAN mediante el comando ***dotlq termination vid* (número de VLAN).** Y además habilitar la transmisión de las VLANs a través del comando ***arp broadcast enable*,** como se muestra en la figura A1.76.

```
[R1]interface GigabitEthernet 0/0/0.10
[R1] dotlq termination vid 10
[R1] arp broadcast enable.
[R1] quit
[R1]interface GigabitEthernet 0/0/0.20
[R1] dotlq termination vid 20
[R1] arp broadcast enable.
[R1] quit
```

Figura A1.76 Asignación y habilitación de VLANs

3.7 Establecer un enrutamiento estático mediante el comando ***ip route-static*** para la comunicación entre R1 y R2 y establecer un direccionamiento a los ordenadores mediante la dirección IP correspondiente a la VLAN a utilizar como se muestra en la figura A1.77.

```
[R1] ip route-static 0.0.0.0 0.0.0.0 12.0.0.2
[R2] ip route-static 192.168.10.0 255.255.255.0 12.0.0.1
[R2] ip route-static 192.168.20.0 255.255.255.0 12.0.0.1
```

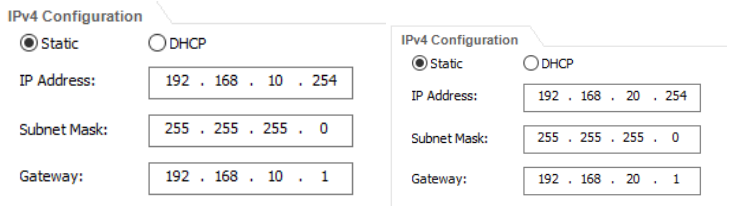


Figura A1.77 Establecimiento de enrutamiento estático y asignación de direccionamiento IP en ordenadores

4. CONCLUSIONES

4.1 Las VLANs utilizan un dominio de *broadcast* independiente para cada enlace, por lo tanto, elimina el riesgo de que un usuario que no pertenece al dominio, afecte a los enlaces de otras VLANs.

4.2 Al momento de establecer el enrutamiento respectivo de las diferentes interfaces, resaltando las interfaces seriales, se observó que si no se toma cuenta el direccionamiento adecuado acorde a las interfaces, puede existir solapamiento y no se podrá levantar el enlace.

5. RECOMENDACIONES

5.1 Se recomienda utilizar la misma numeración tanto para la subinterfaz como para la misma VLAN.

5.2 Al momento de iniciar con la configuración de VLANs, se recomienda crear y establecer las VLANs a utilizar mediante el comando ***vlan batch*.**

6. BIBLIOGRAFÍA.

[1] C. H. Enterprise, « Huawei Enterprise,» 2021. [En línea]. Available: https://forum.Huawei.com/enterprise/es/forums.

[2] L. Huawei Technologies Co., «HCNA Networking Study Guide,» China, Springer Science+Business Media Singapore, 2016, p. 119.

1. TEMA: Establecimiento de VLANs en eNSP.

2. OBJETIVOS

2.1 Establecer una topología de red para la configuración básica de *switches* de capa 2 orientando al establecimiento de VLANs.

2.2 Desarrollar y configurar el enrutamiento entre VLANs.

3. TRABAJO PREPARATORIO

3.1 Realiza un cuadro de comparación entra las ventajas y desventajas de utilizar VLANs dentro de una red.

3.2 Investigar para qué sirve el comando *dotlq termination vid* y *arp broadcast enable***.**

3.3 Investigar la diferencia entre la agregación de un enlace troncal y uno de acceso.

3.4 Investigar cómo establecer una subinterfaz dentro de un dispositivo enrutador.

4. DESCRIPCIÓN DE LA ACTIVIDAD

4.1 Realizar la topología de red propuesta por el docente y asignar las respectivas direcciones IP de cada enlace del enrutador R1 y R2. Cabe resaltar que se establece un *gateway* para las diferentes VLANs mediante la creación de subinterfaces.

4.2 Dentro del CLI del enrutador “R1” definir las subinterfaces que pertenecen a las diferentes VLANs a desarrollarse. **Nota:** Se recomienda utilizar el mismo número tanto para la subinterfaz como para la VLAN.

4.3 Dentro del CLI del *switch* “SW1” crear las VLANs que se van a desarrollar en la red.

4.4 Definir una interfaz del SW1 como un enlace troncal mediante el comando ***port link-type trunk***.

4.5 Permitir que por el enlace troncal salgan las VLANs usando el comando ***port trunk allow-pass vlan*** + **(mencionar el número de VLANs creadas).**

4.6 En cada interfaz del SW1 que conecta a los ordenadores, definirlos como una interfaz de acceso mediante el comando ***port link-type Access*****.**

4.7 Con el comando ***port default*** establecer la VLAN que corresponderá a ese

ordenador.

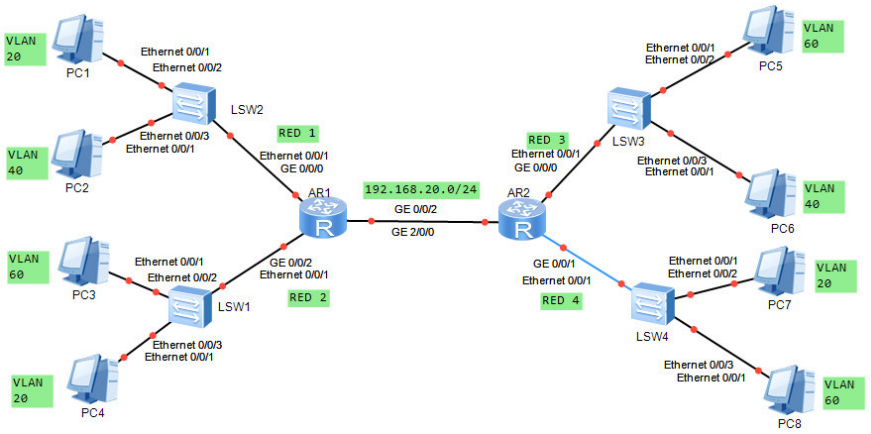
4.8 Dentro de las subinterfaces de las VLANs en R1 establecer el protocolo de encapsulación que corresponderá a la VLAN mediante el comando ***dotlq termination vid* (número de VLAN).**

4.9 Habilitar la transmisión de las VLANs a través del comando ***arp broadcast enable*.**

4.10 Establecer un enrutamiento estático para la comunicación entre R1 y R2 y establecer un direccionamiento a los ordenadores mediante la dirección IP correspondiente a la VLAN a utilizar.

5. INFORME

5.1 Realizar la siguiente topología de red prevista en la figura A1.78 y establecer el enrutamiento entre VLANs con base al siguiente direccionamiento:



RED 1	200.104.20.0/ 24
RED 2	172.168.10.0/24
RED 3	142.120.30.0/24
RED 4	192.172.40.0/24

Figura A1.78 Topología de red propuesta para el informe

5.3 Utilizar como protocolo de enrutamiento OSPF y evidenciar la conectividad total de la red realizando un ***ping*** entre ordenadores de las diferentes redes.

5.5 Conclusiones y Recomendaciones.

6. BIBLIOGRAFÍA

[1] C. H. Enterprise, « Huawei Enterprise,» 2021. [En línea]. Available: https://forum.Huawei.com/enterprise/es/forums.

[2] L. Huawei Technologies Co., «HCNA Networking Study Guide,» China, Springer Science+Business Media Singapore, 2016, p. 119.