



# POSGRADOS

## MAESTRÍA EN TELEMÁTICA

---

RPC-SO-01-NO.025-2021

OPCIÓN DE TITULACIÓN:

PROYECTO DE TITULACIÓN CON  
COMPONENTES DE INVESTIGACIÓN  
APLICADA Y/O DE DESARROLLO

TEMA:

ESTUDIO DE LA CONECTIVIDAD Y  
GESTIÓN DE LA INTERNET 2  
ECUATORIANA CEDIA MEDIANTE  
LA EMULACIÓN DE SU TOPOLOGÍA  
DE BACKBONE

AUTORA:

ZANDY SAMIRA ILLESCAS CARANGUI

DIRECTORA:

MÓNICA KAREL HUERTA

CUENCA – ECUADOR  
2023



*Autora:*



***Zandy Samira Illescas Carangui.***

Ingeniero en Sistemas.

Candidato a Magíster en Telemática por la Universidad  
Politécnica Salesiana - Sede Cuenca.

sami4\_3@hotmail.com

*Dirigido por:*



***Mónica Karel Huerta.***

Ingeniero Electrónico.

Maestría en Ingeniería Biomédica.

Doctora en Ingeniería Telemática.

mhuerta@ups.edu.ec

Todos los derechos reservados.

Queda prohibida, salvo excepción prevista en la Ley, cualquier forma de reproducción, distribución, comunicación pública y transformación de esta obra para fines comerciales, sin contar con autorización de los titulares de propiedad intelectual. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual. Se permite la libre difusión de este texto con fines académicos investigativos por cualquier medio, con la debida notificación a los autores.

DERECHOS RESERVADOS

©2023 Universidad Politécnica Salesiana.

CUENCA – ECUADOR – SUDAMÉRICA

ZANDY SAMIRA ILLESCAS CARANGUI

**Estudio de la conectividad y gestión de la internet 2 ecuatoriana  
cedia mediante la emulación de su topología de backbone**

# ÍNDICE

<b>INDICE GENERAL</b>	<b>III</b>
<b>LISTA DE TABLAS</b>	<b>VI</b>
<b>LISTA DE FIGURAS</b>	<b>VII</b>
<b>GLOSARIO</b>	<b>XI</b>
<b>ACRÓNIMOS</b>	<b>XII</b>
<b>RESUMEN</b>	<b>XVII</b>
<b>ABSTRACT</b>	<b>XIX</b>
<b>AGRADECIMIENTOS</b>	<b>XXI</b>
<b>DEDICATORIA</b>	<b>XXII</b>
<b>1. Introducción</b>	<b>1</b>
1.1. Antecedentes y Planteamiento . . . . .	1
1.2. Justificación . . . . .	4
1.3. Objetivo General . . . . .	5
1.4. Objetivos Específicos . . . . .	5
<b>2. Marco Teórico</b>	<b>6</b>
2.1. Antecedentes de la Internet . . . . .	6
2.2. Internet Comercial . . . . .	8
2.3. Internet en el Ecuador . . . . .	8
2.4. Antecedentes Redes Avanzadas . . . . .	9
2.4.1. Red Avanzada en América Latina . . . . .	11
2.4.2. Red Avanzada en el Ecuador . . . . .	12

2.5. Modelos de Protocolos . . . . .	14
2.5.1. Modelo TCP/IP . . . . .	14
2.5.2. Modelo Open System Interconnection . . . . .	14
2.6. RFC ( <i>REQUEST FOR COMMENTS</i> ) . . . . .	15
2.7. Protocolos . . . . .	16
2.7.1. Protocolos de Red . . . . .	16
2.7.2. Protocolos de Enrutamiento . . . . .	17
2.7.3. Protocolos de Estado de Enlace . . . . .	18
2.7.4. Protocolos de Gestión de Red . . . . .	20
<b>3. Materiales y Metodología</b>	<b>24</b>
3.1. Topología del Backbone CEDIA . . . . .	25
3.2. Diseño de Topología . . . . .	25
3.3. Especificación Técnica de Hardware . . . . .	26
3.4. Especificación Técnica de Software . . . . .	27
3.5. Configuración para la simulación - Packet Tracer(PKT) . . . . .	27
3.5.1. Asignación de direcciones para el enrutamiento en IPv4 . . . . .	28
3.5.2. Asignación de direcciones para el enrutamiento en IPv6 . . . . .	30
3.5.3. Configuración de routers - PKT . . . . .	32
3.5.4. Configuración de enrutamiento OSPF . . . . .	34
3.5.5. Configuración del protocolo de Gestión SNMP . . . . .	42
3.6. Configuración para la emulación - GNS3 . . . . .	43
3.6.1. Tablas de enrutamiento - IPv4 . . . . .	44
3.6.2. Configuración de routers de backbone y MV . . . . .	48
3.6.3. Configuración Protocolo OSPF . . . . .	51
3.6.4. Verificación del enrutamiento OSPF . . . . .	51
3.6.5. Configuración protocolo de gestión SNMP . . . . .	59
3.6.6. Configuración de los NMS en las máquinas virtuales: IPv4 . . . . .	61
3.6.7. Configuración de los NMS en las MV: IPv6 . . . . .	64
<b>4. Resultados</b>	<b>67</b>
4.1. Simulación en Packet Tracer - PKT . . . . .	67
4.1.1. Pruebas de conectividad -PKT . . . . .	67
4.1.2. Análisis de trafico de los mensajes del Protocolo OSPF . . . . .	70
4.1.3. Pruebas de gestión -PKT . . . . .	73
4.2. Emulación en <i>Graphic Network Simulator-3</i> . . . . .	80
4.2.1. Pruebas de conectividad - GNS3 . . . . .	82
4.2.2. Captura de paquetes OSPF - Wireshark . . . . .	85
4.2.3. Resultados de la Latencia para simulación y emulación . . . . .	95

## ÍNDICE

v

4.2.4. Resultados del flujo de datos con Wireshark - IPv4 . . .	99
4.2.5. Resultados de flujo de datos con Wireshark - IPv6 . . .	101
4.2.6. Desempeño de la Simulación y Emulación en la Máquina Real . . . . .	104
4.2.7. Pruebas de gestión - GNS3 . . . . .	105
4.2.8. Diferencia entre SNMPv2 y SNMPv3 . . . . .	110
<b>5. Conclusiones</b>	<b>112</b>
<b>BIBLIOGRAFÍA</b>	<b>116</b>

# LISTA DE TABLAS

2.1. Proveedores ISP, disponibles en el año 2022 . . . . .	9
2.2. Descripción RFC y sus Respectivos Protocolos . . . . .	16
2.3. Diferentes Protocolos de Red TCP/IP - OSI . . . . .	17
2.4. Comparación entre OSPFv2 y OSPFv3 . . . . .	20
2.5. Comparación SNMP . . . . .	21
3.1. Características de Hardware . . . . .	26
3.2. Direcciones de Enrutamiento Routers IPV4 . . . . .	29
3.3. Direcciones de Enrutamiento PCs IPV4 . . . . .	30
3.4. Direcciones de Enrutamiento - Routers IPv6 . . . . .	31
3.5. Direcciones de Enrutamiento PCs IPV6 . . . . .	32
3.6. Direccionamiento para Routers IPV4 - GNS3 . . . . .	45
3.7. Direccionamiento para los NMS bajo IPV4 - GNS3 . . . . .	46
3.8. Direcciones de enrutamiento IPv6 - GNS3 . . . . .	47
3.9. Direccionamiento los NMS bajo IPv6 - GNS3 . . . . .	47
4.1. Comparación de latencia entre IPv4 vs IPv6 . . . . .	99
4.2. Desempeño de la máquina real . . . . .	105

# LISTA DE FIGURAS

2.1. Nodos ARPANET 1969. . . . .	7
2.2. Logos de las Redes Avanzadas a Nivel Mundial. . . . .	10
2.3. Mapa de distribución de las Redes Avanzadas a Nivel Mundial. . . . .	10
2.4. Topología RedCLARA para el año 2021 . . . . .	11
2.5. Servicios RED CEDIA. . . . .	13
2.6. Capas del Modelo TCP/IP. . . . .	14
2.7. Capas de Modelo OSI. . . . .	15
2.8. División Protocolos de Enrutamiento. . . . .	18
2.9. Representación Multiárea OSPF v2 . . . . .	19
2.10. Estructura de Árbol MIB. . . . .	22
2.11. Intercambio de Mensajes. . . . .	23
3.1. Topología de la Red Avanzada CEDIA Ecuador. . . . .	25
3.2. Topología Propuesta. . . . .	26
3.3. Topología Lógica IPv4 - Packet Tracer. . . . .	28
3.4. Topología Lógica IPv6 - Packet Tracer. . . . .	30
3.5. Asignación de Módulos a Routers Cisco. . . . .	32
3.6. Configuración de Interfaces IPv4 del Router Guayaquil. . . . .	33
3.7. Configuración de Interfaces IPv6 del Router Quito. . . . .	33
3.8. Verificación de conectividad IPv4 desde PC Tulcan hacia router Tulcan. . . . .	34
3.9. Verificación de conectividad IPv6 desde PC Tulcan hacia router Tulcan. . . . .	34
3.10. Configuración del Protocolo OSPF-IPv4 en el router Cuenca. . . . .	35
3.11. Configuración del protocolo OSPF-IPv6 en el router Quito. . . . .	35
3.12. Verificación de tablas de enrutamiento - IPv4. . . . .	36
3.13. Verificación de tablas de enrutamiento - IPv6. . . . .	37
3.14. Verificación de protocolos - IPv4. . . . .	38
3.15. Verificación de protocolos - IPv6. . . . .	38

3.16. Verificación de vecinos vía OSPF-IPv4. . . . .	39
3.17. Verificación de vecinos vía OSPF -IPv6. . . . .	39
3.18. Verificación de interfaces configuradas bajo OSPF-IPv4 . . . .	40
3.19. Verificación de interfaces configuradas bajo OSFF-IPv6 . . . .	40
3.20. Verificación de tablas de enrutamiento - IPV4 . . . . .	41
3.21. Verificación de tablas de enrutamiento - IPv6 . . . . .	42
3.22. Configuración SNMPv2 para IPv4 e IPv6. . . . .	42
3.23. Topología Lógica IPv4 - GNS3. . . . .	43
3.24. Topología Lógica IPv6 - GNS3. . . . .	44
3.25. Configuración Routers GNS3. . . . .	48
3.26. Configuración Interfaz Router Tulcan IPv4 - GNS3 . . . . .	48
3.27. Configuración Interfaz Router Tulcan IPv6 - GNS3 . . . . .	49
3.28. Configuración de la Máquina Virtual Quito - IPv4 . . . . .	49
3.29. Configuración Máquina Virtual Sistema Linux Cuenca y Windows Tulcan- IPv6 . . . . .	50
3.30. Configuración OSPFv2 - IPv4 . . . . .	51
3.31. Configuración OSPFv3 - IPv6 . . . . .	51
3.32. Verificación de la tabla de enrutamiento - router Quito - IPv4	52
3.33. Verificación de la tabla de enrutamiento - router Quito - IPv6	53
3.34. Resultado Comando show ip protocols - router Quito - IPv4 .	54
3.35. Resultado Comando show ipv6 protocols - router Quito - IPv6	55
3.36. Resultado Comando show ip ospf neighbor - router Quito - IPv4	55
3.37. Resultado Comando show ipv6 neighbor - router Quito - IPv6	56
3.38. Resultado Comando show IP ospf interface brief - router Quito	56
3.39. Resultado Comando show IPv6 ospf interface brief - router Quito . . . . .	57
3.40. Resultado Comando show IPv4 route OSPF - router Quito . .	58
3.41. Resultado Comando show IPv6 route OSPF - router Quito . .	59
3.42. Configuración de SNMP V2 - router Quito - IPv4 . . . . .	60
3.43. Configuración de SNMP V3 - IPv6 . . . . .	60
3.44. Verificación de la configuración SNMP - IPv4 . . . . .	60
3.45. Verificación de la configuración SNMP - IPv6 . . . . .	61
3.46. Configuración del agente SNMPv2 y gestión de OID's desde la MV de Tulcán hacia el router de Quevedo . . . . .	62
3.47. Captura de paquetes mediante el uso de Wireshark SNMP v2 -IPv4 . . . . .	63
3.48. Soporte de Versiones IREASONING . . . . .	64
3.49. Configuración de Versión SNMP v3 - IPv6 . . . . .	65
3.50. Autenticación del Usuario SNMP v3 - IPv6 . . . . .	65



4.1. Conectividad entre la PC Guayaquil a la PC Quito . . . . .	68
4.2. Conectividad entre Routers IPv4. . . . .	68
4.3. Conectividad entre Routers IPv6. . . . .	69
4.4. Encabezado OSPF IPv4. . . . .	70
4.5. Paquete Hello OSPFv3. . . . .	71
4.6. Resultado de Paquete Link State Update IPv4 e IPv6. . . . .	72
4.7. Obtención de paquetes OSPFv3 - Simulador . . . . .	72
4.8. Visualización de la Obtención de Objetos OID. . . . .	74
4.9. Captura de Paquetes SNMP. . . . .	75
4.10. Nombre del router solicitado vía el MIB Browser . . . . .	76
4.11. Gestión remota de la localización física del router Cuenca . . . . .	77
4.12. Tabla de interfaces, indicando las 7 disponibles . . . . .	77
4.13. Uso de recursos para la simulación en Packet Tracer . . . . .	78
4.14. Topología IPv4 con los 15 routers apagados - GNS3 . . . . .	80
4.15. Topología IPv6 con los 15 routers apagados -GNS3 . . . . .	81
4.16. Topología IPv4 con los 15 routers y las 4 VM funcionando -GNS3 . . . . .	81
4.17. Topología IPv6 con los 15 routers y las 4 VM funcionando -GNS3 . . . . .	82
4.18. Tabla de enrutamiento del router Quito - IPv6 . . . . .	83
4.19. Tabla de enrutamiento del router Tulcan - IPv6 . . . . .	84
4.20. Detalles de los paquetes OSPF bajo IPv4 - Wireshark . . . . .	85
4.21. Detalles de los paquetes OSPF bajo IPv6 - Wireshark . . . . .	86
4.22. Visualización Wireshark - Paquetes OSPF . . . . .	87
4.23. Paquete Hello Ospf2 IPv4 . . . . .	88
4.24. Paquete Hello OSPFv3 IPv6 . . . . .	89
4.25. Paquete DB Description IPv4 . . . . .	90
4.26. Paquete DB Description IPv6 . . . . .	90
4.27. Paquete Link State Request IPv4 . . . . .	91
4.28. Paquete Link State Request IPv6 . . . . .	91
4.29. Paquete Link-State Update IPv4 . . . . .	92
4.30. Paquete Link-State Update IPv6 . . . . .	93
4.31. Paquete LS Acknowledge OSPF IPv4 . . . . .	94
4.32. Paquete LS Acknowledge OSPF IPv6 . . . . .	94
4.33. Latencia en la prueba de Ping - IPv4 . . . . .	95
4.34. Pruebas de conectividad desde la MV Quito a la MV Guayaquil- IPv4 . . . . .	95
4.35. Resultados de la prueba Ping desde la VM Guayaquil a la VM Cuenca - IPv6 . . . . .	96

4.36. Resultados de la prueba Ping entre la VM desde Ubuntu hacia el router Cuenca - IPv6 . . . . .	97
4.37. Resultados de la conectividad desde la VM Guayaquil a la VM Cuenca . . . . .	97
4.38. Conectividad entre las MV Quito, Tulcan, Guayaquil y Cuenca	98
4.39. Flujo de datos Ping MV Quito – MV Guayaquil . . . . .	100
4.40. Flujo de datos para paquetes OSPFv2 para el router Ibarra . . . . .	101
4.41. Flujo de datos SNMPv2 desde MV Quito a Router Ibarra . . . . .	101
4.42. Gráfica de flujo de datos Conectividad IPv6 de Router Cuenca a Router Ibarra . . . . .	102
4.43. Flujo de datos OSPFv3 entre Router Quevedo y Manta . . . . .	103
4.44. Flujo de datos SNMPv3 - IPv6 desde MV Quito hacia Router Ibarra . . . . .	104
4.45. Obtención de localización para el router Cuenca utilizando la herramienta ManageEngine MibBrowser - IPv4 . . . . .	106
4.46. Obtención de localización para el router Cuenca utilizando la herramienta ManageEngine MibBrowser - IPv6 . . . . .	107
4.47. Monitoreo de la tabla de interfaces usando SNMP v3 - IPv6 . . . . .	108
4.48. Monitoreo del nombre del router en SNMP v3 - IPv6 . . . . .	109
4.49. Análisis de paquetes SNMPv3 - Wireshark . . . . .	110
4.50. Comparación de paquetes SNMPv2 vs SNMPv3 . . . . .	111

# Glosario

**Backbone** principal conexión troncal.

**Conmutación de paquetes** divide los datos(mensaje) en mas pequeños, denominados paquetes, para transferencia por el medio.

**Emulador** hardware que simula el funcionamiento de otro dispositivo de hardware.

**Gestión de red** actividades de configuración, monitoreo, resolución de problemas y actualización de una red.

**Herramientas de monitoreo** sistemas de telecomunicaciones que detectan problemas , permitiendo buscar soluciones.

**Interconectividad** comunicación entre 2 o más redes, permitiendo compartir recursos.

**Redes académicas** medio de intercambio de información entre instituciones, establecimientos o personas que comparten un interés en común en el área académica o científica.

**Repositorio de Información** almacenamiento digital centralizado, que permite organizar y compartir información digital.

**Seguridad de la Información** incluye cumplimiento de la confidencialidad, disponibilidad e integridad de la información.

**Simulador** software que imita el comportamiento de un sistema real en tiempo y espacio.

**Topología de Red** diagrama de las comunicaciones de una red, ya sea representada en forma física o lógica.

# Acrónimos

**ADVNETLAB** *Advanced Networking Laboratory*

**ALICE** *América Latina Interconectada con Europa*

**APAN** *Red Avanzada Asia Pacífico*

**ARPA** *Agencia de Proyectos de Investigación Avanzada*

**ARPANET** *Advanced Research Projects Agency Network*

**ARCOTEL** *Agencia de Regulación y Control de las Telecomunicaciones*

**CANARIE** *Canada's Advanced Research and Innovation Network*

**CLARA** *Consortio Latinoamericano de Redes Avanzadas*

**CEDIA** *Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia*

**CIDR** *Enrutamiento entre Dominios sin Clase*

**CUDI** *Corporación Universitaria para el Desarrollo de Internet*

**CEPRA** Concurso Ecuatoriano de Proyectos en Redes Avanzadas

**CNU** Consejo Nacional de Universidades

**DBD** *Database Description*

**GEANT** *Gigabit European Advanced network*

**GNS3** *Graphic Network Simulation*

**HTTP** *Hypertext Transfer Protocol*

**ICMP** *Internet Control Message Protocol*

**IES** Instituciones de Educación Superior

**IETF** *Internet Engineering Task Force*

**ISP** Proveedoras de Servicio de Internet

**IPV4** *Internet Protocol Version 4*

**IPV6** *Internet Protocol Version 6*

**IES** Instituciones de Educación Superior

**LAN** Red de Área Local

**LSAck** *Link-State Acknowledgement*

**LSR** *Link-State Request*

**LSU** *Link-State Update*

**MPLS** *Commutación de Etiquetas Multiprotocolo*

**MIB** *Management Information Base*

**NCP** *Network Control Protocol*

**NREN** *National Research and Education Networks*

**OSI** *Open System Interconnection*

**OID** *Object Identifier*

**OSPF** *Open Shortest Path First*

**RAGIE** *Red Avanzada Guatemalteca para la Investigación y Educación*

**RAAP** *Red Avanzada Peruana*

**RAU** *Red Académica Uruguay*

**RedCONARE** *Red del Consejo Nacional de Rectores*

**RedNESAH** *Red Nacional de Educación Superior Avanzada de Honduras*

**RedRUNBA** *Red Universitaria Nicaragüense de banda ancha*

**RENATA** Red Nacional Académica de Tecnología Avanzada

**RFC** *Request for Comments*

**RNP** Red Nacional de Enseñanza e Investigación

**REUNA** Red Universitaria Avanzada

**RNIE** Red Nacional de Investigación y Educación Ecuatoriana

**Syslog** *System Logging*

**SNMP** *Simple Network Management Protocol*

**Syslog** *System Logging*

**SPF** *Shortest Path First*

**TCP** Protocolo de Control de Transmisión

**IP** Internet Protocol

**UACM** Universidad Autónoma de la Ciudad de México

**UDP** *User Data Protocol*

**UNIVAC** *UNIVersAl Computer*

**UIT** Unión Internacional de Telecomunicaciones

**UNIVAC** *UNI*Ver*sAl* Computer

**VLSM** Máscara de Subred de Longitud Variable

**WACREN** *West and Central African Research and Education Network*

**WAN** Red de Área Extensa

**WMI** *Windows Management Instrumentation*

**WWW** *World Wide Web*



# Resumen

En la actualidad, Internet ha evolucionado de ser un repositorio de información a convertirse en una herramienta fundamental que garantiza el acceso a la educación, el empleo, la socialización y la medicina, entre otras áreas. El crecimiento exponencial de Internet comercial ha dado lugar a la creación de redes exclusivas para universidades y centros de investigación, conocidas como Internet 2. Estas redes avanzadas han permitido el desarrollo de colaboraciones científicas y académicas con amplio ancho de banda y alta disponibilidad. A nivel mundial, se han establecido redes avanzadas en diferentes regiones, como Canadá, Europa, África, América Latina y Asia. El Consorcio Latinoamericano de Redes Avanzadas (CLARA) en América Latina, interconecta las redes académicas avanzadas de varios países. En Ecuador, la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia (CEDIA) encontrándose adherido a CLARA, proporcionando servicios de redes avanzadas a varias universidades. En este contexto, la Universidad Autónoma de la Ciudad de México (UACM) ha llevado a cabo investigaciones sobre las topologías y protocolos de redes avanzadas en diferentes países. Sin embargo, no se ha realizado un estudio específico sobre la red avanzada de CEDIA en Ecuador. Por lo tanto, se propone realizar la emulación de la topología de backbone de la red CEDIA para estudiar su conectividad y gestión. Esto permitirá obtener una aproximación a la red real y proponer mejoras para brindar un mejor servicio en latencia y ancho de banda. Por lo antes expuesto, en este trabajo se estudió la conectividad y gestión del backbone de CEDIA mediante la emulación de su topología. Para lograr esto, la topología física estudiada en este proyecto se actualizó en 2021 y se mantuvo vigente hasta principios de 2023, con presencia de CEDIA en 15 provincias del Ecuador. Se llevaron a cabo simulaciones y emulaciones de topologías físicas utilizando tanto direccionamiento IPv4 como IPv6. Además, se implementó el protocolo de enrutamiento Open Shortest Path First utilizando OSPF versión 2 para direccionamiento IPv4 y OSPF versión 3 para direccionamiento IPv6. Durante la simulación de la topología, se

utilizó un equipo con 4 GB de RAM y un procesador Intel Core i7 de undécima generación, sin experimentar problemas en la configuración de la topología y los protocolos. Sin embargo, al realizar la emulación, fue necesario ampliar la memoria RAM de 4 GB a 20 GB debido a los mayores recursos requeridos. Se emplearon dos herramientas: el simulador Packet Tracer y el emulador GNS3. Este último permitió crear topologías de red más realistas al incluir equipos backbone y trabajar con protocolos en sus últimas versiones. A diferencia de Packet Tracer, GNS3 no presenta limitaciones en términos de funcionalidad y configuración, lo que lo convierte en una opción más versátil para este tipo de emulaciones. Los resultados indican que la emulación en GNS3 consume más recursos en términos de CPU y memoria en comparación con la simulación en Packet Tracer. Además, los tiempos de encendido son un factor importante para considerar al simular topologías de redes complejas utilizando emuladores.

*Palabras clave:* CEDIA, GNS3, IPv6, OSPFv3, SNMPv3, Advanced Networks.

# Abstract

Today, the Internet has evolved from being an information repository to becoming a fundamental tool that guarantees access to education, employment, socialization and medicine, among other areas. The exponential growth of the commercial Internet has given rise to the creation of exclusive networks for universities and research centers, known as Internet 2. These advanced networks have allowed the development of scientific and academic collaborations with high bandwidth and high availability. Globally, advanced networks have been established in different regions such as Canada, Europe, Africa, Latin America and Asia. The Latin American Consortium of Advanced Networks (CLARA) in Latin America interconnects the advanced academic networks of various countries. In Ecuador, the Ecuadorian Corporation for the Development of Research and Academia (CEDIA) is joining CLARA, providing advanced network services to several universities. In this context, the Autonomous University of Mexico City (UACM) has carried out research on the topologies and protocols of advanced networks in different countries. However, a specific study on the advanced network of CEDIA in Ecuador has not been carried out. Therefore, it is proposed to emulate the backbone topology of the CEDIA network to study its connectivity and management. This will allow to obtain an approximation to the real network and propose improvements to provide a better service in latency and bandwidth. Due to the above, in this work the connectivity and management of the CEDIA backbone was studied by emulating its topology. To achieve this, the physical topology studied in this project was updated in 2021 and remained in force until the beginning of 2023, with CEDIA present in 15 provinces of Ecuador. Simulations and emulations of physical topologies were carried out using both IPv4 and IPv6 addressing. In addition, the Open Shortest Path First routing protocol has been implemented using OSPF version 2 for IPv4 addressing and OSPF version 3 for IPv6 addressing. During the simulation of the topology, a computer with 4 GB of RAM and an eleventh generation Intel Core i7 processor was used,

without experiencing problems in the configuration of the topology and protocols. However, when emulating, it was necessary to expand the RAM from 4 GB to 20 GB due to the higher resources required. Two tools were used: the Packet Tracer simulator and the GNS3 emulator. The latter made it possible to create more realistic network topologies by including backbone equipment and working with protocols in their latest versions. Unlike Packet Tracer, GNS3 has no limitations in terms of functionality and configuration, making it a more versatile option for these types of emulations. The results indicate that GNS3 emulation consumes more resources in terms of CPU and memory compared to Packet Tracer simulation. Also, power-up times are an important factor to consider when simulating complex network topologies using emulators.

*Keywords:* CEDIA, GNS3, IPv6, OSPFv3, SNMPv3, Advanced Networks.

# Agradecimientos

Primeramente, agradeciendo a Dios por continuar y alcanzar otro logro más en mi vida. A mis tutores Dr. José Ignacio Castillo Velázquez y Dra. Mónica Karel Huerta, no solo por su dirección en la tesis sino por su paciencia, orientación y por transmitirme su experiencia a lo largo de la elaboración del presente trabajo. De igual manera a mis padres, esposo e hijos y toda mi familia, que con su amor incondicional y respaldo me ayudan a alcanzar mis objetivos. A mis compañeros de maestría y futuros colegas que me ayudaron con su buena voluntad y de manera desinteresada a través del curso y en la terminación de mi tesis.

# Dedicatoria

Todo este trabajo y esfuerzo va dedicado a mi familia por su paciencia, amor y apoyo no solo en este proyecto sino en todo momento.

A mis hijos y esposo, que son el mejor regalo que Dios me ha dado y son los que me recargan de energía para levantarme ante cualquier dificultad.

A mis padres y hermana, por siempre estar a mi lado con su soporte incondicional. Y para los que se convirtieron en mis angelitos en el cielo mis abuelitos, que siempre los llevo en mi corazón y pensamientos.

Samira

# Capítulo 1

## Introducción

### 1.1. Antecedentes y Planteamiento

Hoy en día, con la aparición de la pandemia y la conexión de más dispositivos, Internet dejó de ser un [Repositorio de Información](#), convirtiéndose en una herramienta para el acceso a educación y al empleo. Lo que permitió eliminar barreras, pasando así de la era industrial a la era de las redes.

Uno de los pioneros de la Internet Michel Elie, pertenecía a un selecto grupo de profesionales de la computación que realizaron la interconexión entre cuatro universidades, denominándose a esa red Advanced Research Projects Agency Network ([ARPANET](#)) en 1969, [Sain \[2015\]](#). El objetivo era mantener en contacto cuando detone la guerra, además de pasar a ser una ventaja competitiva en investigación y desarrollo no comercial. Se realizó bajo el direccionamiento IPv4, mientras que para el año de 1995 se da paso a la “Internet Comercial”. En el año 2021, un estudio de la Unión Internacional de Telecomunicaciones ([UIT](#)) reveló un incremento del uso de la Internet a nivel mundial con un número estimado de 4.900 millones de usuarios conectados, [ITU](#).

El gran despliegue de la “Internet comercial” en la década de los 80 y su liberación administrativa en 1995, se produjo por su crecimiento exponencial global, por esta razón, se hizo necesario crear una “Internet 2” exclusiva para que universidades y centros de investigación continuaran experimentando y generando los protocolos necesarios para mejorar la Internet. El nacimiento de redes avanzadas o Internet 2 ha contribuido con el desarrollo de “redes de datos” con un alto desempeño logrado que la red de [Backbone](#), que conforma la “columna vertebral” de la Internet

en regiones o países, sea insosteniblemente costosa, sólo asequibles para las grandes compañías Proveedoras de Servicio de Internet (ISP), [Bakardjieva \[2005\]](#).

Internet 2 nació en 1996 en los EEUU como una red independiente de la Internet comercial, con fines específicos para la academia, participando 34 Universidades donde se desarrollaron protocolos como: IPv6 [Hinden \[1998\]](#), [Coltun et al. \[1999, 2008\]](#), [Group et al. \[1999\]](#), IPv6 con calidad de Servicio [Padilla et al. \[2005\]](#), Multicast [Deering \[1989\]](#), redes Conmutación de Etiquetas Multiprotocolo (MPLS), [Rosen et al. \[2001\]](#), [Huerta et al. \[2004\]](#), entre otros. Estos desarrollos han permitido un aumento de usuarios a la Internet comercial y se empezó a conocer como REDES AVANZADAS que tienen un entorno de colaboración e intercambio de información de carácter científico, de investigación y académico, con un gran ancho de banda y disponibilidad, posee ventajas desde la utilización de bibliotecas digitales multimedia, calidad y nitidez en la utilización de videoconferencias en tiempo real hasta el acceso a bases de datos con un gran volumen de información.

En general, a las redes de “*Internet 2*” son conocidas como *National Research and Education Networks* (NREN) en castellano Redes nacionales de investigación y educación. En las redes avanzadas se presentan en diferentes áreas investigaciones como lo son: en medicina, física de partículas, astronomía, por citar algunos [Gaudet et al. \[2010\]](#).

En 1993, para Canadá surgió la Red Avanzada *Canada’s Advanced Research and Innovation Network* (CANARIE), mientras que *Gigabit European Advanced network* (GEANT) fue creada para Europa, [Clark \[1998 Ed Int\]](#), [CANARIE](#), [GÉANT](#).

Por otro lado, los africanos vieron la necesidad de tener una red de alta velocidad la cual llamaron AfricaConnect, esta misma necesidad hizo que emergiera la red APAN para Asia y el Pacífico [AfricaConnect2](#), [AsiaPacific](#).

Para el caso de Latinoamérica, mediante el proyecto América Latina Interconectada con Europa (ALICE), se formó el Consorcio Latinoamericano de Redes Avanzadas (CLARA), [Red\\_Clara \[a\]](#). La red CLARA esta conformada por las redes avanzadas de 15 países en América Latina. En sus inicios interconecta las [Redes académicas](#) avanzadas nacionales de Argentina, El Salvador, Brasil, Chile, Costa Rica, Panamá, Guatemala, México, Perú, Uruguay, Venezuela con Europa y el mundo, con una capacidad aproximada de 10 Gbits/seg. Luego se incorpora la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia (CEDIA) en Ecuador, [CEDIA \[a\]](#).

En la actualidad, algunas Universidades del Ecuador tienen a CEDIA como su proveedor de servicio de Redes Avanzadas. Estas han creado



proyectos en donde se integran varias Universidades como es el caso en donde se diseñaron soluciones escalables para infraestructura de red, servicios multimedia basados en IP en la red CEDIA con el objetivo de brindar mayor interacción entre la comunidad virtual de científicos del consorcio. También se presentó un sistema de Entrenamiento Virtual para Medicina, su objetivo es crear modelos tridimensionales para el acceso a los usuarios mediante herramientas de navegación virtual, [CEDIA \[a\]](#)

En la literatura científica son pocos los trabajos académicos relacionados con las topologías de las redes avanzadas ya que por lo general pertenecen al dominio de las algunas compañías de telecomunicaciones que en cada país proveen Internet 2. Por ejemplo, México tiene 10 grandes compañías de telecomunicaciones que proveen Internet comercial fijo a empresas y hogares. Sin embargo, sólo dos de ellas proveen Internet 2 a centros de investigación, universidades y empresas, que dispongan de los recursos suficientes para contratar la Internet comercial de uso general e Internet 2, el cual es estrictamente de uso no comercial como ya se ha mencionado [Velázquez \[2016\]](#).

Una de las universidades que ha apostado al estudio de las redes avanzadas es la Universidad Autónoma de la Ciudad de México (UACM). Desde el año 2013 el *Advanced Networking Laboratory* ([ADVNETLAB](#)) de la carrera de Ingeniería en Sistemas Electrónicos y de Telecomunicaciones viene estudiando las distintas topologías de las redes avanzadas en el mundo y su evolución, así como la aplicación de protocolos de enrutamiento y gestión de las redes [Castillo and Galicia \[2016\]](#), [Castillo-Velazquez and Sanchez-Trejo \[2016\]](#), [Castillo-Velazquez et al. \[2017\]](#), [Castillo-Velázquez and Revilla-Melo \[2020\]](#). Este laboratorio ha detectado que no se han realizado estudios de la red avanzada de CEDIA en Ecuador. Por esta razón se procedió a realizar la emulación de la topología de backbone de la red avanzada en el Ecuador, bajo el modelo CEDIA, con direccionamiento IPv6, que nos permite aplicar [Herramientas de monitoreo y gestión](#), y comparar resultados de otros proyectos que realizan simulaciones similares. Varios estudios se han enfocados a estudiar las topologías de redes avanzadas a nivel mundial. En [Castillo-Velázquez et al. \[2018\]](#), se estudio la topología de la Red Universitaria Avanzada (REUNA) de Chile, demostrando las limitaciones y capacidades del emulador frente a una infraestructura de backbone real. Por otro lado, en [Ramírez Díaz \[2019\]](#), se realizó la evaluación de los protocolos *System Logging* (Syslog) y *Simple Network Management Protocol* (SNMP); en configuración para encontrar la mejor alternativa se diseñó una topología de Red Avanzada del Perú Red Avanzada Peruana (RAAP) con router C7200 y con 4 escenarios donde se realizaron pruebas. Adicionalmente, se han

estudiado la arquitectura backbone, funcionamiento e integración de las redes avanzadas CANARIE, INTERNET y CLARA de América, Canada y USA emulando la conectividad y gestión con un CPU Xeon, con direccionamiento *Internet Protocol Version 4 (IPV4)*, obteniendo una sola red integrada AMERONET, en GNS3, [Jose-Ignacio et al. \[2019\]](#), [Castillo-Velázquez et al. \[2023\]](#).

En el trabajo presentado en [Castillo-Velázquez and Revilla-Melo \[2020\]](#) se emuló la integración de las tres redes de AFRICACONNECT, que están conectadas por medio de GEANT al mundo, la red avanzada de Europa, utilizando el emulador *Graphic Network Simulation (GNS3)*. Se usó direccionamiento *Internet Protocol Version 6 (IPV6)* y durante el proceso, los recursos del computador llegaron al 99% de sus capacidades y la RAM al 94%. La emulación de toda la red integrada se completó en aproximadamente 45 minutos.

En el trabajo presentado en [Castillo-Velazquez and Velazquez-Cruz \[2022\]](#), se llevó a cabo una comparación entre de la topología backbone de la red CANARIE versión 2022 con la versión del año 2020. Los resultados indicaron que durante la comparación se utilizó el 90,2% de la memoria RAM y el 30,4% de la capacidad del CPU. Esto demostró que la actualización no presentó cambios importantes en comparación con el estudio anterior.

Tras consultar y revisar la literatura científica, se puede evidenciar que aún no se han realizado estudios relacionados con la conectividad y gestión de la red Internet 2 ecuatoriana CEDIA mediante la emulación de su topología de backbone. Dicha emulación permitiría obtener la máxima aproximación a la red real que se encuentra en la industria de telecomunicaciones.

## 1.2. Justificación

Por las razones indicadas en los antecedentes, la colaboración internacional entre la UACM y la Universidad Politécnica Salesiana permite abordar temas relacionados con el estudio de la topología de backbone de la red avanzada en Ecuador. La cual permitirá dar un soporte óptimo a las universidades. Estudiar la topología de la red troncal avanzada de CEDIA y generar propuestas para mejorar la topología con el fin de brindar mejores servicios de ancho de banda y latencia para la futura expansión y escalabilidad de la red de Ecuador.

### **1.3. Objetivo General**

Estudiar la conectividad y gestión del backbone de CEDIA, la Internet 2 ecuatoriana, mediante la emulación de su topología para obtener la máxima aproximación a la red real soportada por el proveedor de servicios de internet.

### **1.4. Objetivos Específicos**

1. Realizar la revisión bibliográfica acerca de las redes avanzadas en el mundo.
2. Analizar los softwares que permitan crear y administrar máquinas virtuales y redes.
3. Configurar y monitorear routers de backbone bajo los protocolos para enrutamiento y gestión tanto para IPv4 como para IPv6.
4. Emular la gestión y conectividad del backbone de la red CEDIA.

## Capítulo 2

# Marco Teórico

Las topologías de las Redes Avanzadas pertenecen al dominio de algunas instituciones como tenemos REUNA en Chile, CEDIA en Ecuador, y así en cada país que tienen acceso a las mismas, por lo cual, en el país no se han realizado estudios sobre la red avanzada y con direccionamiento IPv6, mediante la colaboración internacional que existe entre la UACM y la Universidad Politécnica Salesiana resultó realizar el presente estudio de la conectividad y administración de la topología del backbone CEDIA red avanzada del Ecuador, con el objetivo de obtener la máxima aproximación a la red. En este capítulo se analizarán los antecedentes de Internet, así como, el de las redes avanzadas y los diferentes modelos y protocolos de redes.

### 2.1. Antecedentes de la Internet

Como primera red de telecomunicaciones comercial, tenemos la telegrafía desarrollada por Cooke y Wheatstone en Inglaterra y patentado en 1837, funcionaba emitiendo señales eléctricas mediante cables conectados desde el emisor al receptor y se interpretaba la información utilizando código Morse. Como la segunda red de telecomunicaciones en 1877 nace la telefonía comercial, con su primera línea telefónica en Boston Somerville.

El nacimiento de las computadoras se da en 1940, con grandes máquinas que se usaban exclusivamente con fines científicos o gubernamentales que realizaban cálculos y almacenaban información.

En 1950 tenemos la evolución de las primeras computadoras comerciales iniciando con *UNIVersAl Computer* (UNIVAC), que además de leer cintas magnéticas en su memoria central tenía más de mil palabras.

Gracias a las iniciativas antes mencionadas, aparecen las primeras redes

computacionales denominada Red de Área Local (**LAN**), que permiten conectar dos computadores dentro de una habitación entre 10 m y 1 km mediante un módem de 56 kbps, así las empresas empezaron a organizar redes independientes para cada departamento, luego aparecieron la Red de Área Extensa (**WAN**), permitiendo conectar dos computadoras dentro de un país o continente entre 100 Km a 1000 Km, las dos tecnologías no eran compatibles ni permitían compartir información.

Para 1958 el Departamento de Defensa de los Estados Unidos fundaron la Agencia de Proyectos de Investigación Avanzada (**ARPA**) con unos 200 científicos de alto nivel, desarrollando nuevas tecnologías con fines defensivos y militares, además establecieron redes interconectadas vía satélite utilizando las tecnologías creadas LAN y WAN. En 1965 Licklider y su equipo logran la comunicación de una computadora situada al este de Estados Unidos, Estado Massachusetts, con otra situada en California mediante los protocolos de **Commutación de paquetes** desarrollado por Donald Watts Davies de Reino Unido, y se crea ARPANET, como podemos observar en la figura 2.1, donde se gráfica los 4 nodos con los que se inicio la comunicación, además se generan los primeros documentos denominados *Request for Comments* (**RFC**), que describen la implementación, estandarización, protocolos, procedimientos de las redes de computadoras, etc.

En 1969 se creó la primera red informática que logra la interconexión entre las redes WAN y LAN conectando a varias universidades norteamericanas, esta conexión de interredes se denomina la INTERNET [Kleinrock \[2010\]](#).

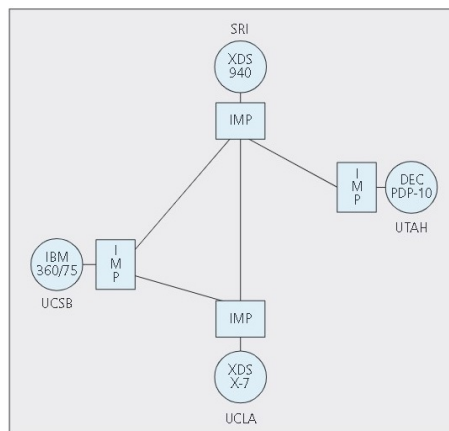


Figura 2.1: Nodos ARPANET 1969.

Fuente:([Kleinrock \[2010\]](#))

## 2.2. Internet Comercial

Desde 1990 con el cierre de ARPANET se desarrollan varias aplicaciones como el navegador web conocido como *World Wide Web* ([WWW](#)) con el protocolo *Hypertext Transfer Protocol* ([HTTP](#)) y anunciado públicamente en 1991, en 1993 aparece el primer navegador web NCSA Mosaic. Además, en 1994 nació Yahoo, ya para 1995 se tenía alrededor de 200 servidores web en todo el mundo y NSFNET ya no es el backbone de la Internet pasando al sector privado naciendo la “Internet Comercial”.

El acceso a la Internet evolucionó gracias a los ISP, que permitieron el incremento de conexiones y accesibilidad a la red.

Se debe tomar en cuenta que, en la actualidad, lo que comenzó con 4 ordenadores centrales conectados para el 2023 se alcanzado con unos 5,160 billones personas conectadas representando un 64,4 % de la población en el mundo, [Kemp \[2023\]](#).

## 2.3. Internet en el Ecuador

La Agencia de Regulación y Control de las Telecomunicaciones ([ARCOTEL](#)), en su Boletín N°6, en el Ecuador EcuaneX estableció el primer nodo en 1991 y en 1992 EcuaneX, el segundo nodo por medio de la Corporación de la Información del Ecuador administrada por el Banco del Pacífico, universidades públicas y privadas, su uso es exclusivo para empresas y universidades. A partir del año 2000 se impulsaron proyectos para el acceso a nivel del público en general como café internet, hogares, etc. [de Regulación y Control de las Telecomunicaciones \[2023\]](#)

El mayor prestador de Internet fijo en Ecuador en el primer trimestre del 2022 a nivel nacional es MEGADATOS S.A. con la participación en el mercado del 26.1 % seguida de Corporación Nacional de Telecomunicaciones CNTEP con el 23.7 % y CONECEL S.A con el 12.6 %, SETEL con el 9.5 % y el resto el 28 %. En Internet móvil por prestador tenemos a CONECEL S.A con el 55.3 %, seguido por OTECEL S.A con el 32.2 % y CNT EP con el 12.5%. [est \[2022\]](#).

La tabla [2.1](#) detalla los proveedores ISP, disponibles en el año 2022.

Cuadro 2.1: Proveedores ISP, disponibles en el año 2022

Fuente: (est [2022])

ISP DISPONIBLES (2022)				
PROVEEDOR	PÁGINA WEB	FUNDADA	MATRIZ	CIUDAD
Megadatos S.A.	<a href="https://www.netlife.ec">https://www.netlife.ec</a>	2010	Calle Inaquito, lote 2 y Corea, Edif. Platinum, locales 1 y 2.	Quito
Corporación Nacional de Telecomunicaciones CNT EP	<a href="https://www.cnt.com.ec">https://www.cnt.com.ec</a>	2008	Av. Amazonas N36-49 y Corea	Quito
Servicio de Telecomunicaciones SETEL S.A.	<a href="http://setel.ec">http://setel.ec</a>	1986 Km	Eloy Alfaro N44-406 y de las Higueras	Quito
Punto Net S.A.	<a href="https://www.puntonet.ec">https://www.puntonet.ec</a>	1997	Av. Amazonas 4545 y Pereira, Edif. Cento Financiero, of 401	Quito
Etapa EP	<a href="https://www.etapa.net.ec">https://www.etapa.net.ec</a>	1948	Tarqui 9-76	Cuenca
Telconet S.A.	<a href="https://www.telconet.net">https://www.telconet.net</a>	1995	Av. Kennedy Norte Mz 109 S. 21	Guayaquil
Pacheco Saguay Luis Eduardo	<a href="https://www.cbvision.net.ec">https://www.cbvision.net.ec</a>	1998	Paute	Paute
In. Planet S.A.	<a href="https://hey.ec">https://hey.ec</a>	2002	Malecon 312, entre Sucre y Federico Proaño	Milagro
Necusoft Cia.Ltda.	<a href="https://www.nettplus.net">https://www.nettplus.net</a>	2004	Sucre 209-23, Edif Chamba Buele, Piso 2	Loja

## 2.4. Antecedentes Redes Avanzadas

El auge de la “Internet Comercial” y su uso para la comunidad científica y educativa se volvió no accesible por la información delicada que se manejaba como fotos, vídeos y audios. Pero, lo más importante era transmitir en tiempo real las conferencias o garantizar comunicación sincrónica, lo cual se volvió tedioso, no solo por la demora en la conexión sino por la [Seguridad de la Información](#) que se intercambiaba.

En Estados Unidos, en 1996, se establecieron redes académicas con el fin de brindar servicios de investigación y desarrollo a través de ISP o proveedores de servicios de conexión a Internet. Sus conexiones de alta velocidad, independientes de la Internet comercial, van desde los 2 Mbps hasta los 500 Gbps. La mayoría de las conexiones utilizan fibra óptica con topología en estrella extendida y admiten soporte para el protocolo IPv6.

Actualmente, la Internet es considerada una gran red de redes, distribuida por todo el mundo entre las cuales se tiene **GEANT** que interconecta las NREN de Europa, en África Central y Occidental tenemos la *West and Central African Research and Education Network* (**WACREN**), en Asia y Pacífico la Red Avanzada Asia Pacífico (**APAN**), **CAREN** en Asia Central, **UbuntuNet Alliance** en África del Este y del Sur, red **CANARIE** en Canadá, **Internet2** en los Estados Unidos, y en América Latina **Red CLARA**.

La figura 2.2, muestra los logos de las Redes Avanzadas, y la figura 2.3 como están distribuidos a Nivel Mundial.



Figura 2.2: Logos de las Redes Avanzadas a Nivel Mundial.

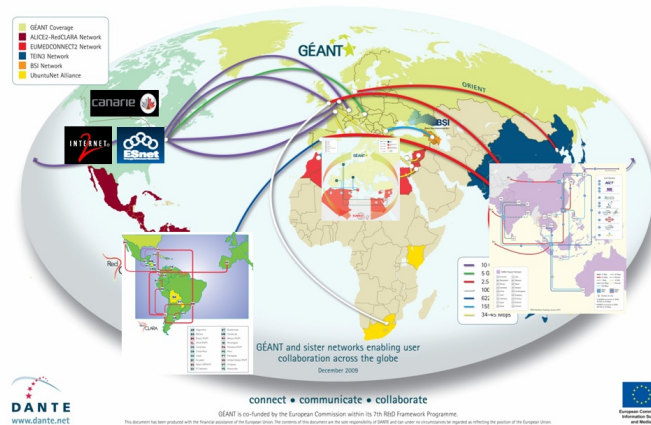


Figura 2.3: Mapa de distribución de las Redes Avanzadas a Nivel Mundial.  
Fuente:([GEANT](#))



### 2.4.1. Red Avanzada en América Latina

Desde 2004, Red CLARA promueve el desarrollo de la educación, la ciencia, la cultura y la innovación en América Latina, utilizando las redes avanzadas de manera efectiva, siendo la base de su misión, y como visión convertirse en actor clave para fortalecer la ciencia y la tecnología en América Latina. Como socios activos se tiene 80 % de países en América Latina, y 60 % de usuarios finales que pertenecen a las RNIE, mismos que utilizan las plataformas y aplicaciones colaborativas de RedCLARA, [Red\\_Clara](#) [b]. La figura 2.4 muestra la topología de Red Clara para el año 2021.

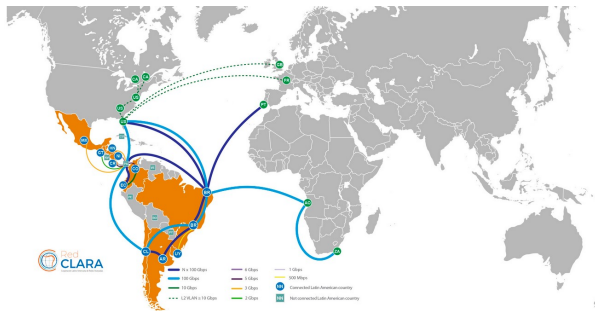


Figura 2.4: Topología RedCLARA para el año 2021  
Fuente:([RedCLARA](#))

Desde el año 2018 y mediante su enlace a la red avanzada del antiguo continente tiene como miembros a:

- Brasil con Red Nacional de Enseñanza e Investigación ([RNP](#)), que conecta a más de 250 instituciones brasileñas.
- Colombia se conecta con Red Nacional Académica de Tecnología Avanzada ([RENATA](#)), con aproximadamente 120 conexiones.
- Costa Rica se conecta con Red del Consejo Nacional de Rectores ([RedCONARE](#)), que conectan 6 universidades.
- Chile con REUNA conecta más de 40.000 instituciones.
- Guatemala con Red Avanzada Guatemalteca para la Investigación y Educación ([RAGIE](#)), para la Investigación y Educación) con 5 miembros.

- Honduras con Red Nacional de Educación Superior Avanzada de Honduras ([RedNESAH](#)), con la participación de 20 universidades entre públicas y privadas.
- México con la Corporación Universitaria para el Desarrollo de Internet ([CUDI](#)), quien está conformada por 16 comunidades para áreas de investigación especializada.
- Nicaragua con Red Universitaria Nicaragüense de banda ancha ([RedRUNBA](#)), que articula e integra las universidades del Consejo Nacional de Universidades ([CNU](#)).
- Red Académica Uruguaya ([RAU](#)), que funciona desde 1988 y es promovida por la Universidad de la República.

#### 2.4.2. Red Avanzada en el Ecuador

En Ecuador, el Consorcio Ecuatoriano de Investigación y Desarrollo CEDIA establecido el 25 de marzo de 2002, inicia con el objetivo principal de facilitar la [Interconectividad](#) entre universidades, centros de investigación y desarrollo, en el mismo año el 17 de septiembre en presencia del Vicepresidente de la República del Ecuador y el Secretario Nacional de Ciencia y Tecnología se oficializa.

El 9 de junio de 2003 pasó a formar parte de RedCLARA a través del cable submarino conectado al hub de Santiago de Chile con un enlace de 10 Mbit/s. En la actualidad, su conexión se da mediante un anillo de fibra óptica avanzado con capacidad inicial de 100 Gbps, siendo hasta el momento el canal académico en el Ecuador.

En 2017, CEDIA implementó su propia red IP/MPLS con conexión a Estados Unidos tanto para tráfico de red avanzada como Internet comercial, con el objetivo de proveer conexión nacional e internacional a las Instituciones de Educación Superior ([IES](#)) miembros y ofrecer servicios relacionados a las tecnologías de la información enfocadas al desarrollo científico, tecnológico, innovador y educativo. Conformando la Red Nacional de Investigación y Educación Ecuatoriana ([RNIE](#)) con escuelas politécnicas, centros de investigación, organismos públicos y privados, creando 142 proyectos de investigación y desarrollo. Desde 2009, CEDIA ha creado una de sus iniciativas más innovadoras, el Concurso Ecuatoriano de Proyectos en Redes Avanzadas ([CEPRA](#)). Este esfuerzo generó resultados impactantes como infraestructuras de datos espaciales y establecer un grupo ecuatoriano para estudios experimentales y teóricos de nanosistemas.

Además, se firma un acuerdo en el 2020 de cooperación técnica y científica con las Redes de América Latina y la RedClara para la expansión de las prácticas de salud digital en la región.

La ventaja como miembro de CEDIA entre las más importantes se tiene acceso a redes avanzadas de educación e investigación, donde permiten generar aplicaciones relacionadas con la tecnología, mediante recursos de computación avanzada y redes de alta velocidad, acceso a publicaciones, a bibliotecas digitales y la interconexión nacional e internacional, en la figura 2.5 se puede observar algunos de los servicios que ofrece CEDIA.



Figura 2.5: Servicios RED CEDIA.

Fuente:(CEDIA [c])

Para 2021, los servicios de red avanzada de CEDIA cubren 15 ciudades del país con 370 sedes, 74 de las cuales brindan servicios a través de la red propia de CEDIA, permitiendo la transmisión de alta velocidad a través de canales de fibra óptica con una capacidad de 100 Gbps CEDIA [b].

## 2.5. Modelos de Protocolos

### 2.5.1. Modelo TCP/IP

Entre 1969 y 1973 se conectaron cientos de computadoras entre sí, estableciendo Network Control Protocol (NCP), protocolo de control, que permitía la comunicación y desarrollo de algunas aplicaciones con dispositivos conectados a la ARPANET, y en 1971 se creó el correo electrónico.

Con el crecimiento de las conexiones se desarrolló en 1974 el protocolo TCP/IP, que son el Protocolo de Control de Transmisión (TCP), que proporciona una transferencia de datos fiable, y el Internet Protocol (IP) que transporta los datos a otras dispositivos de red, creado por Robert Kahn y Vinton Cerf el mismo que es aplicado por ARPANET en 1983 y adoptado como protocolo estándar de la Internet y acceso a los servidores de la web.

TCP/IP actualmente es un conjunto de protocolos que permiten enviar y recibir comunicación entre todos los dispositivos, independientemente de la marca, hardware, software, tipo de conexión o sistema operativo, consta de 5 capas como se muestra en la figura 2.6.

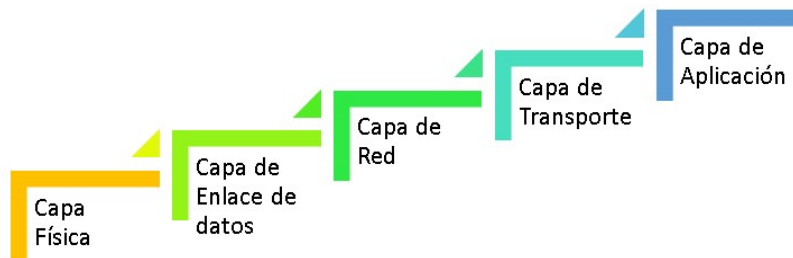


Figura 2.6: Capas del Modelo TCP/IP.

### 2.5.2. Modelo Open System Interconnection

Con el objetivo de estandarizar un modelo de referencia para la comunicación, la Organización Internacional para la Estandarización lanzó el modelo *Open System Interconnection* (OSI), en español Interconexión de Sistemas Abiertos, que consta de 7 capas, pasando a ser el lenguaje universal para la conexión, como se describe en la figura 2.7.

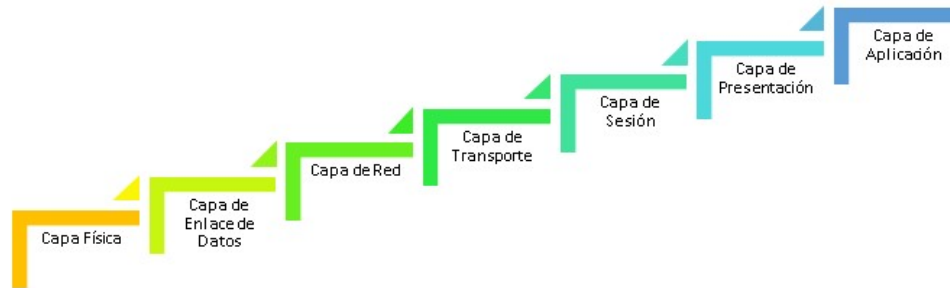


Figura 2.7: Capas de Modelo OSI.

## 2.6. RFC (*REQUEST FOR COMMENTS*)

Los RFC son documentos públicos numerados, creado por Steve Crocker en 1969, el primer registro RFC1, son las notas no oficiales sobre ARPANET, siendo en la actualidad en donde se definen protocolos de comunicación, conceptos, métodos y programas que tienen referencia con lo que conocemos como la Internet, su gestión la realiza *Internet Engineering Task Force* (IETF). Después de 54 años se tienen más de 8,500 documentos, los mismos que se pueden visualizar desde [rfc-es.org](http://rfc-es.org).

La tabla 2.2 muestra los RFC y protocolos importantes para el presente proyecto.

Cuadro 2.2: Descripción RFC y sus Respectivos Protocolos

PROTOCOLOS Y RFC		
PROTOCOLO	NOMBRE	RFC
IP	Protocolo de Internet	791
TCP	Protocolo de Control de Transmisión	793
TCP/IP	Conjunto TCP/IP	1180
ICMP	Protocolo de Mensajes de Control de Internet	792
UDP	Protocolo de Datagrama de Usuario	768
FTP	Protocolo de Transferencia de Ficheros	959
SNMP	Protocolo Sencillo de Administración de Redes	3416
SNMPv2	Protocolo Sencillo de Administración de Redes v2	2273
SNMPv3	Protocolo Sencillo de Administración de Redes v3	791
MIB-I	Base de Información de Administración	3418
MIB-II	Base de Información de Administración II	1213
OSI	Modelo de interconexión de sistemas abiertos	1574
OSPF2	Protocolo de Direccionamiento de tipo Enlace - Estado v2	2328
OSPF3	Protocolo de Direccionamiento de tipo Enlace - Estado v3	5340
IPV4	Protocolo de Internet v4	791
IPV6	Nueva Versión del Protocolo de Internet	2460

## 2.7. Protocolos

### 2.7.1. Protocolos de Red

Para realizar una comunicación es necesario saber el origen, destino y el medio por donde se va a transmitir la información, para que el sistema tenga un mismo idioma y la comunicación fluya sin problemas, por lo cual, los protocolos son estándares de comunicaciones que rigen todas las características de la misma. En la tabla 2.3 se detallan los protocolos

utilizados en las capas tanto para el modelo OSI como para TCP/IP.

Cuadro 2.3: Diferentes Protocolos de Red TCP/IP - OSI  
(Velázquez [2019], Acevedo [2006])

NIVEL	TCP/IP PROTOCOLOS		OSI
1.- APLICACIÓN	FTP, DNS, HTTP, SSH, SSL, Telnet, SMTP, NFS, RIP...		1.- APLICACION 2.- PRESENTACIÓN 3.- SESIÓN
2.- TRANSPORTE	TCP	UDP	4.- TRANSPORTE
3.- INTERNET	IP	ICMP IGMP ARP, RARP	5.- RED
4.- ACCESO A LA RED	Ethernet, 802.11, MAC/LLC, VALN, HDP, Fibre Channel, CSMA, Token-ring, ATM, PPP, Q. 921...		6.- ENLACE
5.- FISICO	RJ45, RS-232, V.34, 100BASE-TX, SDH, DSL, 802.11...		7.- FISICO

### 2.7.2. Protocolos de Enrutamiento

Funcionan en capa de red, pasando a ser el conjunto de reglas que especifican la gestión de los enrutadores, además del enrutamiento, el envío de los datos en toda la red. Se dividen en enrutamiento interno o externo. Enrutamiento Interno funcionan en redes autónomas y van desde redes de tamaño medio a grande, mientras que el Enrutamiento Externo diseñado para múltiples redes autónomas.

En la figura 2.8 se detallan los protocolos respectivos de enrutamiento.

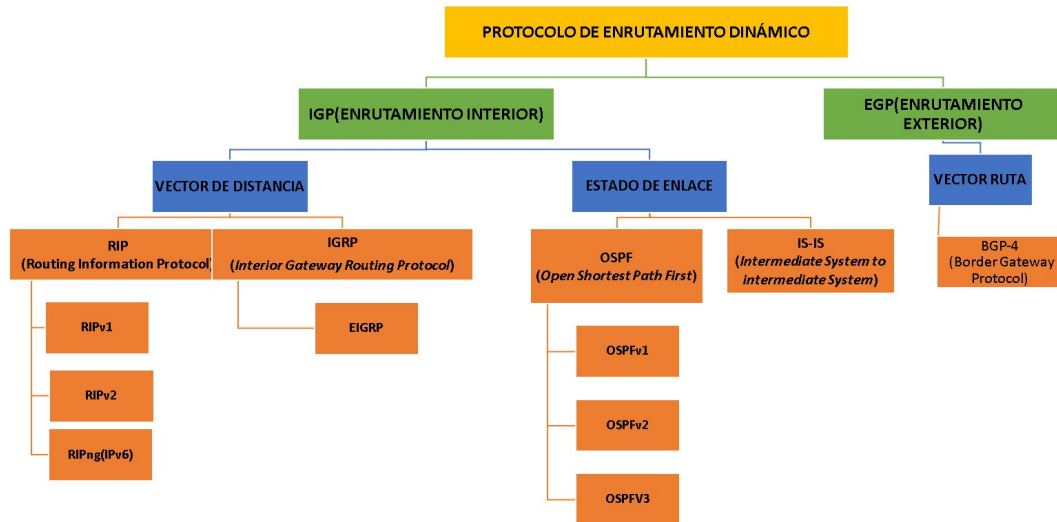


Figura 2.8: División Protocolos de Enrutamiento.

### 2.7.3. Protocolos de Estado de Enlace

Protocolos de enrutamiento que calculan independiente de su forma, la mejor ruta hacia su destino, aparte que toda la información se recopila de los enrutadores y se envían mensajes para conocer los cambios en la [Topología de Red](#). Entre ellos está el protocolo *Open Shortest Path First (OSPF)*, como muestra la figura 2.8.

#### Protocolos OSPF

Desarrollado en 1987, por IETF, reemplazando a Routing Information Protocol, su primera RFC fue en el 1989 naciendo el OSPFv1 experimental que finalmente no fue implementado. En la actualidad se tienen dos versiones implementadas: **OSPFv2** y **OSPFv3**.

OSPFv2 actualizado en el RFC 2328, que acepta Máscara de Subred de Longitud Variable ([VLSM](#)) y Enrutamiento entre Dominios sin Clase ([CIDR](#)), además de ser escalable para topologías grandes y pequeñas, con direccionamiento IPv4. Funciona de la siguiente manera:

1. Primero, los routers se reconocen entre sí, con los paquetes HELLO para establecer adyacencias con los vecinos.



2. Intercambian paquetes de estado del enlace, con información de su estado y costo.
3. Después, se crea con la información de los estados de enlace proporcionada la base de datos, permitiendo crear la topología del área.
4. Con la topología se ejecuta el algoritmo *Shortest Path First (SPF)* que crea el árbol.
5. Finalmente se selecciona la ruta más corta tomando en consideración toda la información que contiene en sus bases.

OSPFv2 al ser un protocolo que permite escalabilidad, se implementa de dos formas:

- **OSPF de área única.**- routers en una sola área, preferiblemente cero.
- **Multiarea OSPF.**- se divide en diferentes áreas, donde la principal es el área 0, como muestra la figura 2.9.

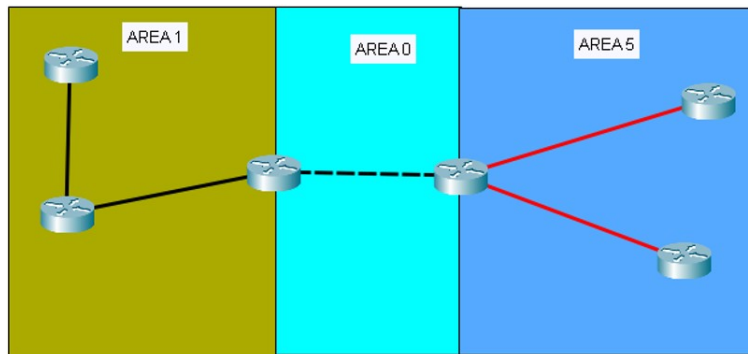


Figura 2.9: Representación Multiárea OSPF v2

OSPFv3, funciona en la capa de red, igual que OSPFv2, pero sobre direccionamiento IPv6, se debe considerar que la estructura de datos en las dos versiones es la misma. La tabla 2.4 muestra una comparación de las especificaciones OSPFv2 y OSPFv3.

Cuadro 2.4: Comparación entre OSPFv2 y OSPFv3

Fuente: (Jain and Payal [2019])

COMPARACIONES		
ESPECIFICACIONES	OSPFv2	OSPFv3
IP	Protocolo de Internet	791
Protocolo IP Versión	IPv4	IPv6
Tamaño del Encabezado	24 Bytes	16 Bytes
Router y Area ID	32 bits	32 bits
Protocolo de Procesamiento	Subred de IP	Por enlace
Autenticación	Texto no cifrado y MD5	Autenticación por IP
Descubrimiento de Vecinos	Utiliza el enrutador ID y la Dirección de Interfaz	Usa solamente el Router ID
Dirección IP Multicast	224.0.0.5	FF02::5
Dirección IP de Multidifusión del DR/BDR	224.0.0.6	FF02::6
Dirección IP Unicast	No disponible	Por defecto

#### 2.7.4. Protocolos de Gestión de Red

Los protocolos de **Gestión de red** permiten administrar una red, es decir supervisar, comprobar, monitorear y controlar mediante herramientas la infraestructura de la red. Entre ellos tenemos los que permiten detectar fallos y un esquema como *Internet Control Message Protocol (ICMP)*, en español protocolo de mensajería de control de Internet; otros que analizan el comportamiento como SNMP sin importar sistema operativo o fabricante y por último los que corren en un sistema operativo en específico como *Windows Management Instrumentation (WMI)*, que permite administrar un dispositivo ya sea local o remoto con sistema Windows.

##### Protocolo SNMP (*Simple Network Management Protocol*)

Protocolo de capa de aplicación, que permite administrar una red ya sea local o remotamente, definido en la RFC 1157, siendo parte de los protocolos de Internet TCP/IP, permitiendo administrar una red de las más sencilla a la más compleja o de otra forma desde una red LAN a una red WAN y a cualquier dispositivo de red que tenga una IP y un agente SNMP.

SNMP utiliza el número de puerto 161 predeterminado para consulta y el 162 puerto de excepción, de igual manera esta predeterminado el *User Data Protocol (UDP)*, que forma parte de los protocolos de transporte.

### Componentes SNMP

El componente principal de SNMP es el Administrador de SNMP, que envía una solicitud al Agente de SNMP y las reenvía a los Dispositivos Administrados.

### Versiones SNMP

Actualmente se han determinado tres versiones de SNMP tenemos SNMPv1 definidos en el RFC 1155 y 1157, el SNMPv2 en RFC 1901, RFC 1905 y RFC 1906, basada en la comunidad y por último la versión más segura SNMPv3 definida en RFC 1905, RFC 1906, RFC 2571, RFC 2572, RFC 2574 y RFC 2575.

La tabla 2.5, muestra las características principales entre las versiones de SNMP.

Cuadro 2.5: Comparación SNMP

Fuente:(SNM)

Versión	Descripción	Tipos Paquetes	Autenticación	Direccionamiento	Seguridad
SNMPv1	Protocolo Simple de Administración de Red, fácil de configurar.	Get-Request,Get-Next-Request,Set Request,Get Response	Cadena de Comunidad	Solo IPv4	Coincidencia de cadena .
SNMPv2c	Idéntica a la versión 1	Get-Request,Get-Bulk-Request, Get-Next-Request,Set Request, Inform-Response, SNMP v2 Trap	Cadena de Comunidad	IPv4 e Ipv6	Coincidencia de cadena .
SNMPv3	Configuración más compleja, se tiene dos niveles de seguridad	Tiene los mismo de v1 y v2. Nuevo formato de mensaje SNMP.	Nombre de Usuario y dos algoritmos MD5 y HASH.	IPv4 e Ipv6	Coincidencia de nombre de usuario, encriptación convencional con DES y autenticación con MD5.

### SNMP OID

*Object Identifier (OID)*, son los identificadores de objeto que reúnen información en un dispositivo con SNMP, su nivel de acceso es de lectura

y escritura, se obtiene mucha información como interfaz, localización, descripción del dispositivo entre otros.

Los OIDS están definidos en Management Information Base (MIB), base de datos de objetos y valores jerárquicos, con un conjunto de preguntas para el agente que el administrador puede realizarlas. Se tienen dos tipos, estándar como RFC y las Personalizadas/Privadas.

La figura 2.10 muestra una parte de la organización del árbol de MIB donde se puede obtener información como la interface o cualquier objeto referenciado por un identificador, por ejemplo, el objeto MIB-2 se referenciaría por 1.3.6.1.1.1 forma numérica. De igual manera se tienen buscadores en donde podemos ingresar la referencia numérica y se obtiene el objeto a cual hace referencia.

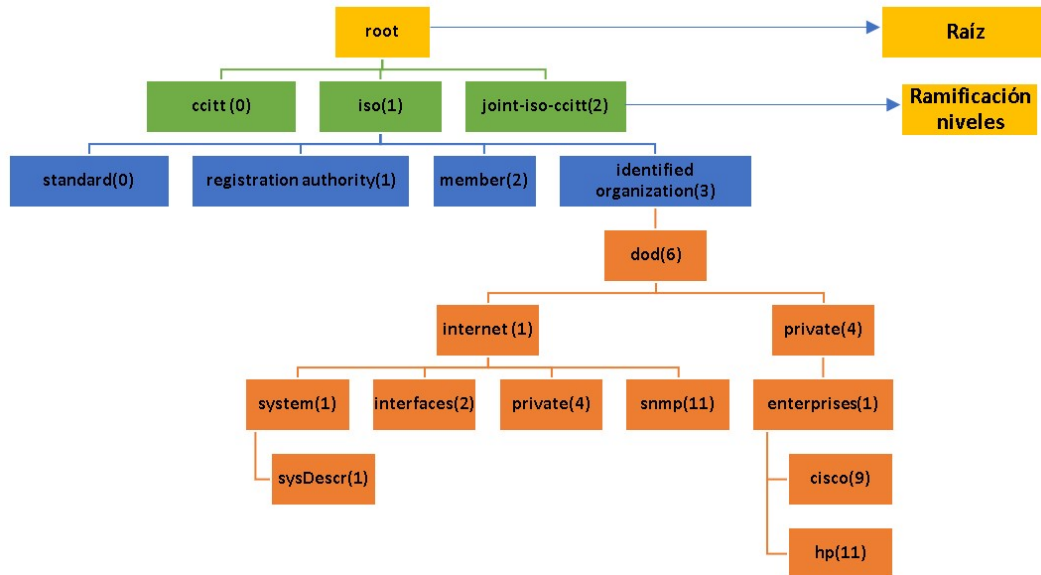


Figura 2.10: Estructura de Árbol MIB.

Fuente:(Rodríguez and Javier [2009])

La figura 2.11 permite observar los comandos que se utilizan con el protocolo SNMP, entre el administrador y el agente MIB, la descripción que realiza cada comando es la siguiente:

- **Get.-** obtiene el valor de la solicitud enviada por el administrador.

- **Get Next.**- obtiene en el árbol MIB el valor siguiente del OID.
- **Get Bulk.**- obtiene el valor de una tabla.
- **Set.**- permite modificar o asignar un valor.

**SNMP Comandos**

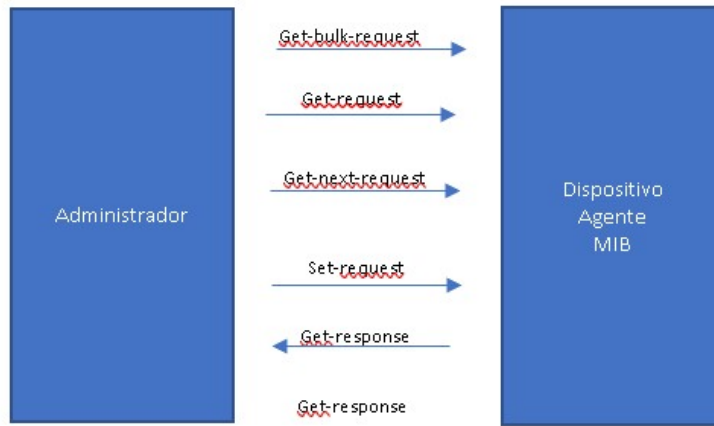


Figura 2.11: Intercambio de Mensajes.

## Capítulo 3

# Materiales y Metodología

En el trabajo que se detalla a continuación se aplicó investigación bibliográfica, recopilando información desde revistas, informes, libros, estadísticas, boletines y tesis relacionadas con el estudio a desarrollar, lo que permitió adquirir conocimiento sobre redes avanzadas, herramientas de monitoreo y gestión desde lo más básico hasta lo fundamental para un administrador de redes WAN.

La investigación se desarrolló en cuatro fases, las mismas que nos permitieron cumplir con las metas planteadas.

La fase primera se recopiló información con el inicio de la Internet en el mundo y en Ecuador, además los antecedentes de redes avanzadas, red CEDIA, protocolos de enrutamiento como protocolos de gestión usados por los backbone de CEDIA, para saber por qué y cómo se va a implementar la topología respectiva.

En la segunda fase comenzamos desde lo más sencillo simulando en la herramienta packet tracer, redes sencillas y luego topologías más complejas hasta simular la red CEDIA con direccionamiento tanto en IPv4 como en IPv6, además se realizaron pruebas de funcionamiento del backbone en el emulador GNS3, carga del sistema operativo de los routers c7200 y la creación de máquinas virtuales.

En la tercera fase se implementó la topología de los routers backbone con las máquinas virtuales en ambos direccionamientos y protocolos de enrutamiento y administración se configuraron.

En la cuarta fase se realizó la emulación de CEDIA red avanzada del Ecuador con direccionamiento IPv6 y emulando la gestión de los diferentes routers backbone.

### 3.1. Topología del Backbone CEDIA

CEDIA brinda el internet académico de alta conectividad y velocidad conocido como Redes Avanzadas a las Instituciones de Educación Superior en gran parte del Ecuador. La figura 3.1 es el modelo emulado y simulado basado en la topología backbone de la Internet 2 Ecuatoriana de CEDIA de su última actualización de 2021, en donde a cada ciudad conectada se le asigna un router, implementando un total de 15 routers de backbone.

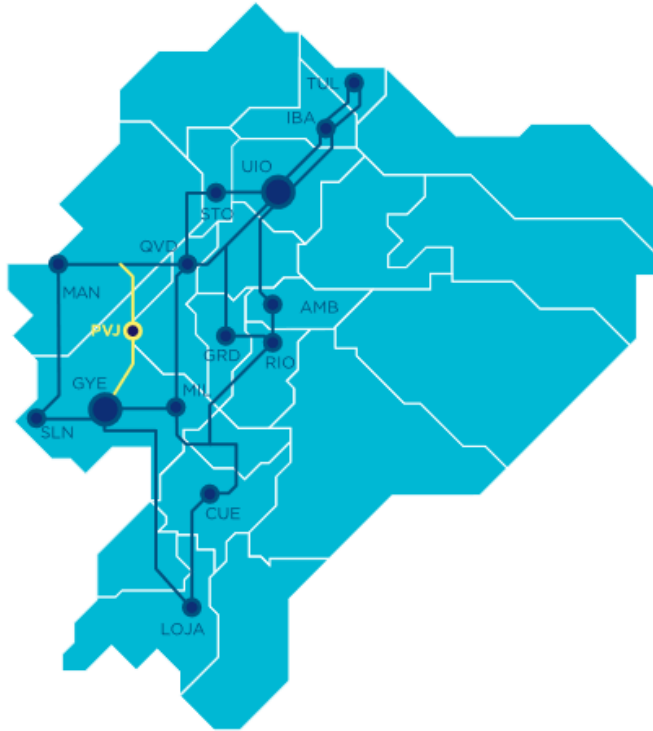


Figura 3.1: Topología de la Red Avanzada CEDIA Ecuador.  
Fuente:([CEDIA \[b\]](#))

### 3.2. Diseño de Topología

En la figura 3.2, se presenta el diseño de la topología propuesta para la simulación y emulación de la red CEDIA.

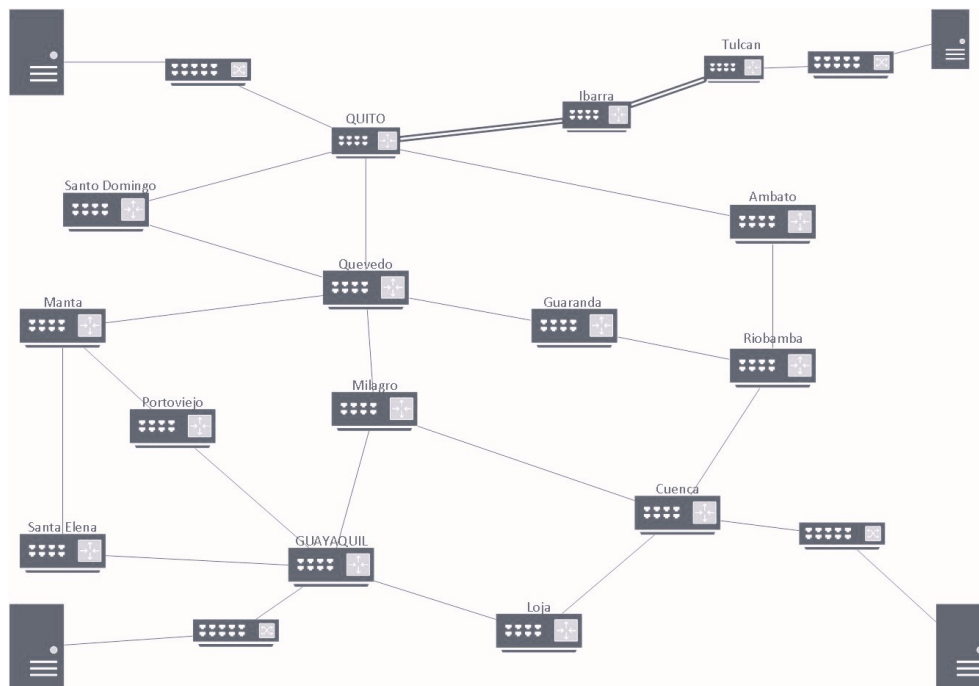


Figura 3.2: Topología Propuesta.

### 3.3. Especificación Técnica de Hardware

En este trabajo se utilizó una portátil para llevar a cabo tanto la simulación como la emulación. Las características técnicas de la portátil se detallan en la tabla 3.1.

Cuadro 3.1: Características de Hardware

PORTÁTIL	
DESCRIPCIÓN	CARACTERÍSTICAS
Sistema Operativo:	Windows 11
Procesador:	11th Gen Intel(R) Core(TM) i7-1195G7 @ 2.90GHz 2.92 GHz
RAM instalada:	8 GB
Tipo de Sistema:	64 bits

Dado que el proceso de emulación presentaban problemas, es decir, no era posible ejecutar la emulación de CEDIA con los recursos de hardware



originales de la portátil, se decidió aumentar la memoria RAM a 20,0 GB (19,7 GB utilizable) para llevar a cabo este estudio. El aumento de memoria permitió cargar y ejecutar con éxito el software de emulación, lo que permitió obtener los resultados deseados y realizar el análisis correspondiente.

### 3.4. Especificación Técnica de Software

Antes de explicar cómo se realizó la simulación y emulación, es importante destacar las herramientas y conceptos que se utilizaron en el estudio.

1. **Packet Tracer v8.2.1(2023)**, una herramienta desarrollada por Cisco para la simulación de redes.
2. **GNS3 v2.2**, permite la emulación de dispositivos como routers y switches con conexiones a máquinas virtuales.
3. **Virtual Box v7.0.6(2023)**, una herramienta de virtualización que permite la instalación de un sistema operativo dentro de otro, utilizando los recursos del mismo.
4. **ManageEngine MIB Browser v1.0**, una herramienta de gestión con una interfaz intuitiva que permite el empleo del protocolo SNMPv2 y SNMPv3.
5. **Wireshark v4.0.3**, herramienta que analiza paquetes de red mediante la captura de la información correspondiente a través de una conexión.

### 3.5. Configuración para la simulación - Packet Tracer(PKT)

#### Topología lógica bajo IPv4

Dado que el [Simulador](#) Cisco Packet Tracer no cuenta con routers de tipo backbone o core, solamente tiene routers de acceso y distribución, se utilizó un router genérico “Router-PT-Empty”. Para realizar la simulación con direccionamiento IPV4, se utilizaron 15 routers, tal que a cada uno se le añadieron las interfaces de Giga Ethernet y Fast Ethernet, para simular los routers de backbone, así como se agregaron 4 “Switches 2960”. Para la conexión de 4 PC distribuidas en las ciudades de Tulcán, Quito, Guayaquil y Cuenca. La figura [3.3](#) presenta la topología lógica de IPv4.

### 3.5. CONFIGURACIÓN PARA LA SIMULACIÓN - PACKET TRACER(PKT)28

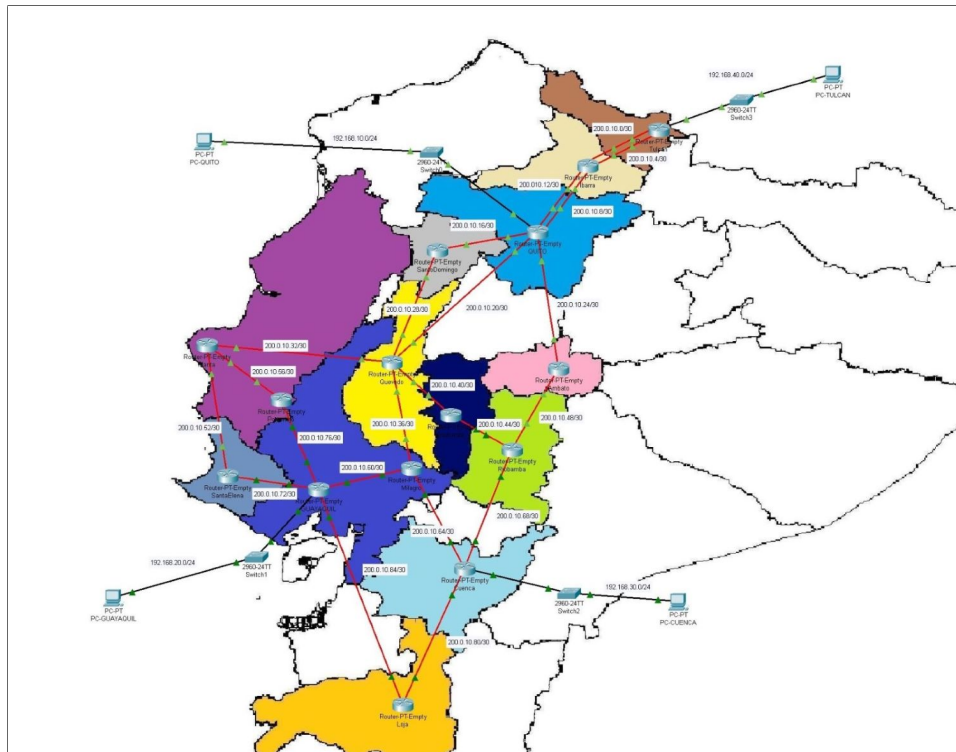


Figura 3.3: Topología Lógica IPv4 - Packet Tracer.

#### 3.5.1. Asignación de direcciones para el enrutamiento en IPv4

En el direccionamiento de IPv4, se utilizaron direcciones de clase C, como se detalla en la tabla 3.2 en donde se indica el nombre de cada Router, la dirección de red con su respectiva máscara, la interfaz a la que pertenece con su respectiva IP.

### 3.5. CONFIGURACIÓN PARA LA SIMULACIÓN - PACKET TRACER(PKT)29

Cuadro 3.2: Direcciones de Enrutamiento Routers IPV4

N°	ROUTER	RED	MASCARA	INTERFAZ	IP
1	Tulcán	200.0.10.0	255.255.255.252	Gig0/0	200.0.10.1
		200.0.10.4	255.255.255.252	Gig1/0	200.0.10.5
		192.168.0.0	255.255.255.0	Fa3/0	192.168.0.1
2	Ibarra	200.0.10.0	255.255.255.252	Gig0/0	200.0.10.2
		200.0.10.4	255.255.255.252	Gig1/0	200.0.10.6
		200.0.10.12	255.255.255.252	Gig2/0	200.0.10.13
		200.0.10.8	255.255.255.252	Gig3/0	200.0.10.9
3	Quito	200.0.10.12	255.255.255.252	Gig0/0	200.0.10.14
		200.0.10.8	255.255.255.252	Gig1/0	200.0.10.10
		200.0.10.16	255.255.255.252	Gig2/0	200.0.10.17
		200.0.10.24	255.255.255.252	Gig3/0	200.0.10.25
		200.0.10.20	255.255.255.252	Gig4/0	200.0.10.21
4	Santo Domingo	192.168.10.0	255.255.255.0	Fa6/0	192.168.10.1
		200.0.10.16	255.255.255.252	Gig0/0	200.0.10.18
5	Ambato	200.0.10.28	255.255.255.252	Gig1/0	200.0.10.29
		200.0.10.24	255.255.255.252	Gig0/0	200.0.10.26
6	Quevedo	200.0.10.48	255.255.255.252	Gig1/0	200.0.10.49
		200.0.10.20	255.255.255.252	Gig0/0	200.0.10.22
		200.0.10.28	255.255.255.252	Gig1/0	200.0.10.30
		200.0.10.40	255.255.255.252	Gig2/0	200.0.10.41
		200.0.10.32	255.255.255.252	Gig3/0	200.0.10.33
7	Guaranda	200.0.10.36	255.255.255.252	Gig4/0	200.0.10.37
		200.0.10.40	255.255.255.252	Gig0/0	200.0.10.42
		200.0.10.44	255.255.255.252	Gig1/0	200.0.10.45
8	Riobamba	200.0.10.48	255.255.255.252	Gig0/0	200.0.10.50
		200.0.10.44	255.255.255.252	Gig1/0	200.0.10.46
		200.0.10.68	255.255.255.252	Gig2/0	200.0.10.69
9	Manta	200.0.10.32	255.255.255.252	Gig0/0	200.0.10.34
		200.0.10.52	255.255.255.252	Gig1/0	200.0.10.53
		200.0.10.56	255.255.255.252	Gig2/0	200.0.10.57
10	Portoviejo	200.0.10.56	255.255.255.252	Gig0/0	200.0.10.58
		200.0.10.76	255.255.255.252	Gig1/0	200.0.10.77
11	SantaElena	200.0.10.52	255.255.255.252	Gig0/0	200.0.10.54
		200.0.10.72	255.255.255.252	Gig1/0	200.0.10.73
12	Milagro	200.0.10.36	255.255.255.252	Gig0/0	200.0.10.38
		200.0.10.64	255.255.255.252	Gig1/0	200.0.10.65
		200.0.10.60	255.255.255.252	Gig2/0	200.0.10.61
13	Cuenca	200.0.10.68	255.255.255.252	Gig0/0	200.0.10.70
		200.0.10.64	255.255.255.252	Gig1/0	200.0.10.66
		200.0.10.80	255.255.255.252	Gig2/0	200.0.10.81
		192.168.30.0	255.255.255.0	Fa4/0	192.168.30.1
14	Loja	200.0.10.80	255.255.255.252	Gig0/0	200.0.10.82
		200.0.10.84	255.255.255.252	Gig1/0	200.0.10.86
15	Guayaquil	200.0.10.76	255.255.255.252	Gig0/0	200.0.10.78
		200.0.10.72	255.255.255.252	Gig1/0	200.0.10.74
		200.0.10.60	255.255.255.252	Gig2/0	200.0.10.62
		200.0.10.84	255.255.255.252	Gig3/0	200.0.10.85
		192.168.20.0	255.255.255.0	Fa6/0	192.168.20.1

### 3.5. CONFIGURACIÓN PARA LA SIMULACIÓN - PACKET TRACER(PKT)30

Para las PCs se asigna el direccionamiento con nombre del dispositivo, red con máscara y respectiva interfaz, puerta de enlace con su IP, como detalla la tabla 3.3.

Cuadro 3.3: Direcciones de Enrutamiento PCs IPV4

N°	DISPOSITIVO	RED	MASCARA	INTERFAZ	IP	GATEWAY
1	PC-QUITO	192.168.10.0	255.255.255.0	F0	192.168.10.2	192.168.10.1
2	PC-GUAYAQUIL	192.168.20.0	255.255.255.0	F0	192.168.20.2	192.168.20.1
3	PC-CUENCA	192.168.30.0	255.255.255.0	F0	192.168.30.2	192.168.30.1
4	PC-TULCAN	192.168.40.0	255.255.255.0	F0	192.168.40.2	192.168.40.1

#### 3.5.2. Asignación de direcciones para el enrutamiento en IPv6

En la simulación con direccionamiento IPV6, se utilizaron 15 Routers “Cisco 2811”, que soportaban direccionamiento IPV6 y pasaron a ser los routers de backbone. También, se agregaron interfaces para la conexión y se utilizaron 4 “switches 2960” para la conexión de 4 PCs. La figura 3.4 visualiza la topología final elaborada con la herramienta Packet Tracer con direccionamiento IPv6. En el direccionamiento de IPv6, se utiliza el prefijo 2001:DB8:ABCD como se detalla en la tabla 3.4.

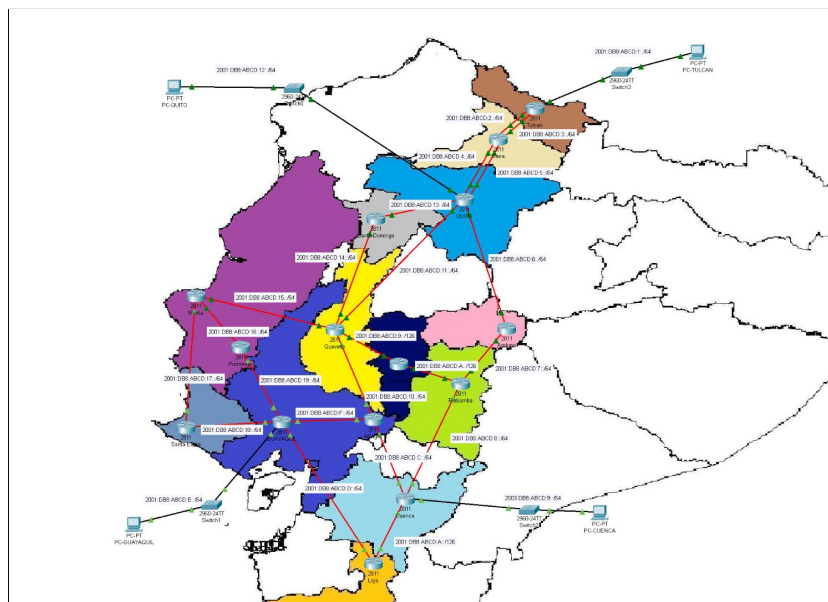


Figura 3.4: Topología Lógica IPv6 - Packet Tracer.

### 3.5. CONFIGURACIÓN PARA LA SIMULACIÓN - PACKET TRACER(PKT)31

Cuadro 3.4: Direcciones de Enrutamiento - Routers IPv6

N°	ROUTER	RED-MASCARA	INTERFAZ	IP	LINK-LOCAL	ID-ROUTER
1	Tulcan	2001:DB8:ABCD:1::/64	Gig0/0	2001:DB8:ABCD:1::1	FE80::1	1.1.1.1
		2001:DB8:ABCD:2::/64	Gig1/0	2001:DB8:ABCD:2::1		
		2001:DB8:ABCD:3::/64	Gig2/0	2001:DB8:ABCD:3::1		
2	Ibarra	2001:DB8:ABCD:2::/64	Gig0/0	2001:DB8:ABCD:2::2	FE80::2	2.2.2.2
		2001:DB8:ABCD:3::/64	Gig1/0	2001:DB8:ABCD:3::2		
		2001:DB8:ABCD:4::/64	Gig2/0	2001:DB8:ABCD:4::1		
		2001:DB8:ABCD:5::/64	Gig3/0	2001:DB8:ABCD:5::1		
3	QUITO	2001:DB8:ABCD:4::/64	Gig0/0	2001:DB8:ABCD:4::2	FE80::3	3.3.3.3
		2001:DB8:ABCD:5::/64	Gig1/0	2001:DB8:ABCD:5::2		
		2001:DB8:ABCD:6::/64	Gig2/0	2001:DB8:ABCD:6::2		
		2001:DB8:ABCD:11::/64	Gig3/0	2001:DB8:ABCD:11::2		
		2001:DB8:ABCD:12::/64	Gig4/0	2001:DB8:ABCD:12::1		
4	Santo-Domingo	2001:DB8:ABCD:13::/64	Gig5/0	2001:DB8:ABCD:13::2	FE80::4	4.4.4.4
		2001:DB8:ABCD:14::/64	Gig0/0	2001:DB8:ABCD:14::1		
5	Quevedo	2001:DB8:ABCD:14::/64	Gig1/0	2001:DB8:ABCD:14::2	FE80::5	5.5.5.5
		2001:DB8:ABCD:11::/64	Gig0/0	2001:DB8:ABCD:11::1		
		2001:DB8:ABCD:1A::/64	Gig1/0	2001:DB8:ABCD:1A::2		
		2001:DB8:ABCD:10::/64	Gig2/0	2001:DB8:ABCD:10::2		
6	Guaranda	2001:DB8:ABCD:14::/64	Gig3/0	2001:DB8:ABCD:14::1	FE80::6	6.6.6.6
		2001:DB8:ABCD:15::/64	Gig4/0	2001:DB8:ABCD:15::2		
7	Riobamba	2001:DB8:ABCD:B::/64	Gig0/0	2001:DB8:ABCD:B::1	FE80::7	7.7.7.7
		2001:DB8:ABCD:1A::/64	Gig1/0	2001:DB8:ABCD:1A::1		
		2001:DB8:ABCD:7::/64	Gig0/0	2001:DB8:ABCD:7::2		
8	Ambato	2001:DB8:ABCD:8::/64	Gig1/0	2001:DB8:ABCD:8::2	FE80::8	8.8.8.8
		2001:DB8:ABCD:B::/64	Gig2/0	2001:DB8:ABCD:B::2		
9	Manta	2001:DB8:ABCD:6::/64	Gig0/0	2001:DB8:ABCD:6::1	FE80::9	9.9.9.9
		2001:DB8:ABCD:7::/64	Gig1/0	2001:DB8:ABCD:7::1		
		2001:DB8:ABCD:15::/64	Gig0/0	2001:DB8:ABCD:15::1		
10	SantaElena	2001:DB8:ABCD:16::/64	Gig1/0	2001:DB8:ABCD:16::1	FE80::A	10.10.10.10
		2001:DB8:ABCD:17::/64	Gig2/0	2001:DB8:ABCD:17::1		
11	Portoviejo	2001:DB8:ABCD:17::/64	Gig0/0	2001:DB8:ABCD:17::2	FE80::B	11.11.11.11
		2001:DB8:ABCD:18::/64	Gig1/0	2001:DB8:ABCD:18::2		
12	Milagro	2001:DB8:ABCD:16::/64	Gig0/0	2001:DB8:ABCD:16::2	FE80::C	12.12.12.12
		2001:DB8:ABCD:19::/64	Gig1/0	2001:DB8:ABCD:19::2		
		2001:DB8:ABCD:C::/64	Gig2/0	2001:DB8:ABCD:10::1		
13	Cuenca	2001:DB8:ABCD:10::/64	Gig0/0	2001:DB8:ABCD:10::1	FE80::D	13.13.13.13
		2001:DB8:ABCD:8::/64	Gig1/0	2001:DB8:ABCD:8::1		
		2001:DB8:ABCD:9::/64	Gig0/0	2001:DB8:ABCD:9::1		
		2001:DB8:ABCD:A::/64	Gig2/0	2001:DB8:ABCD:A::1		
14	Loja	2001:DB8:ABCD:A::/64	Gig3/0	2001:DB8:ABCD:C::1	FE80::E	14.14.14.14
		2001:DB8:ABCD:C::/64	Gig0/0	2001:DB8:ABCD:A::2		
15	GUAYAQUIL	2001:DB8:ABCD:D::/64	Gig1/0	2001:DB8:ABCD:D::2	FE80::F	15.15.15.15
		2001:DB8:ABCD:D::/64	Gig0/0	2001:DB8:ABCD:D::1		
		2001:DB8:ABCD:F::/64	Gig1/0	2001:DB8:ABCD:F::1		
		2001:DB8:ABCD:19::/64	Gig2/0	2001:DB8:ABCD:19::1		
		2001:DB8:ABCD:18::/64	Gig3/0	2001:DB8:ABCD:18::1		
		2001:DB8:ABCD:E::/64	Gig4/0	2001:DB8:ABCD:E::1		

En la tabla 3.4 tenemos los siguientes elementos:

- **Router:** nombre del router que se determinó a cada equipo de backbone.
- **Interfaz:** interfaz a la que se le asignó la IP.
- **Red/Máscara:** la red y máscara a la que se le asignó.

### 3.5. CONFIGURACIÓN PARA LA SIMULACIÓN - PACKET TRACER(PKT)32

- **Link-Local:** se le asigna manualmente una dirección local con prefijo FE80.
- **ID-Router:** dirección utilizada para configuración OSPF.

A las Pcs se les asigna el direccionamiento IPv6, como se detalla en la tabla 3.5.

Cuadro 3.5: Direcciones de Enrutamiento PCs IPV6

Dispositivo	RED/MASCARA	INTERFAZ	IP	GATEWAY
PC-QUITO	2001:DB8:ABCD::12::/64	F0	2001:DB8:ABCD::12::2	2001:DB8:ABCD::12::1
PC-GUAYAQUIL	2001:DB8:ABCD::E::/64	F0	2001:DB8:ABCD::E::2	2001:DB8:ABCD::E::1
PC-CUENCA	2001:DB8:ABCD::9::/64	F0	2001:DB8:ABCD::9::2	2001:DB8:ABCD::9::1
PC-TULCAN	2001:DB8:ABCD::1::/64	F0	2001:DB8:ABCD::1::2	2001:DB8:ABCD::1::1

#### 3.5.3. Configuración de routers - PKT

En cada router, tanto para IPv4 como IPv6, a cada uno de ellos se le asignó varios módulos tanto Giga Ethernet dependiendo de la cantidad de routers a interconectar, como módulos Fast Ethernet como se indica en la figura 3.5. Las interfaces Fast Ethernet se usaron para realizar las respectivas pruebas de conectividad y monitoreo con PCs.

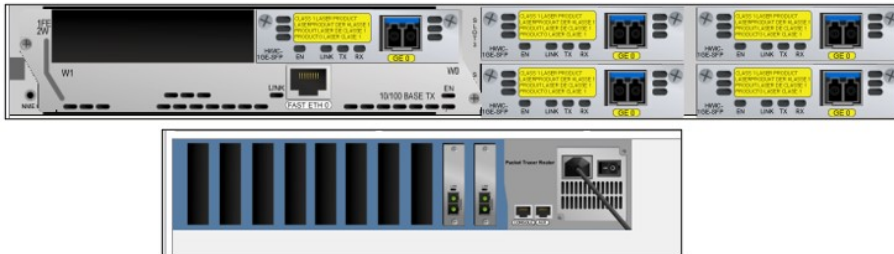


Figura 3.5: Asignación de Módulos a Routers Cisco.

**Configuración de Interfaces Routers:** A cada router, en sus respectivas interfaces se le asignó una dirección IP y máscara tanto en direccionamiento IPv4 e IPv6. La figura 3.6 es un ejemplo del Router Guayaquil con su configuración y direccionamiento **IPv4**.

### 3.5. CONFIGURACIÓN PARA LA SIMULACIÓN - PACKET TRACER(PKT)33

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host
Router(config)#hostname GUAYAQUIL
GUAYAQUIL(config)#int gigabitEthernet 0/0
GUAYAQUIL(config-if)#ip address 200.0.10.73 255.255.255.252
GUAYAQUIL(config-if)#no shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to down
GUAYAQUIL(config-if)#exit
```

Figura 3.6: Configuración de Interfaces IPv4 del Router Guayaquil.

La figura 3.7 muestra un ejemplo de configuración del Router Quito con direccionamiento **IPv6**.

```
QUITO#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
QUITO(config)#int g0/0/0
QUITO(config-if)#ipv6 address 2001:DB8:ABCD:4::2/64
QUITO(config-if)#ipv6 address FE80::3 link-local
QUITO(config-if)#no shutdown
QUITO(config-if)#
QUITO(config-if)#
```

Figura 3.7: Configuración de Interfaces IPv6 del Router Quito.

#### **Configuración de Interfaces PCs**

En modo gráfico se asignó a cada Pc su dirección y desde COMAND PROMPT, se le realizaron las pruebas de conectividad con su respectivo router. En direccionamiento IPv4 e IPv6, se realizó un ping desde PC Tulcan hacia el router Tulcan como se observa en las figuras 3.8 y 3.9 respectivamente.

### 3.5. CONFIGURACIÓN PARA LA SIMULACIÓN - PACKET TRACER(PKT)34

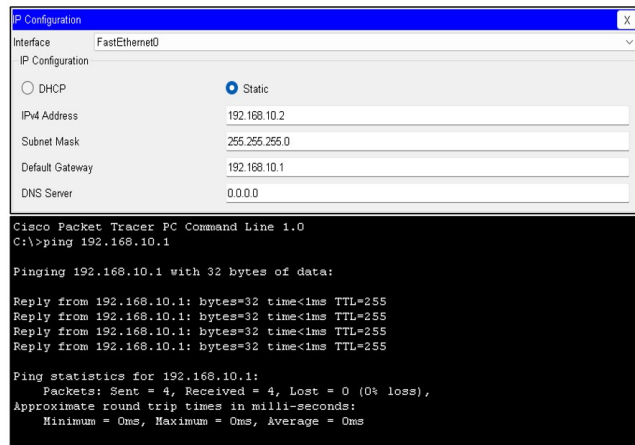


Figura 3.8: Verificación de conectividad IPv4 desde PC Tulcan hacia router Tulcan.

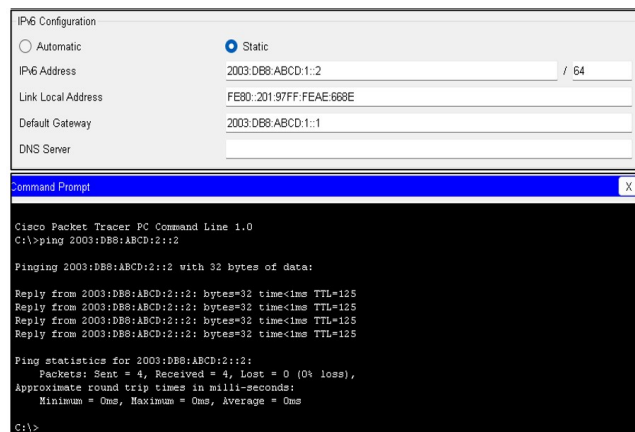


Figura 3.9: Verificación de conectividad IPv6 desde PC Tulcan hacia router Tulcan.

#### 3.5.4. Configuración de enrutamiento OSPF

Se configuró Open Shortest Path First- OSPF, protocolo de enrutamiento, que construye el mapa completo de la topología, además analiza la velocidad, el costo, congestión y de esta manera calcula el trayecto óptimo.



### 3.5. CONFIGURACIÓN PARA LA SIMULACIÓN - PACKET TRACER(PKT)35

#### IPV4

En todos los routers backbone de la red se configura OSPF, versión 2 asignada para Redes IPv4, como se puede observar en la figura 3.10. Se configuró en el Router Cuenca la id del proceso en este caso es OSPF 1, como se muestra en el círculo amarillo (1), además se agrega la dirección IPv4, de los routers vecinos con su wildcard que es la inversa a la máscara de subred de la interfaz, y se asignó el área 0, como se muestra en el círculo amarillo (2), aquí se habilita de manera predeterminada el routing de unidifusión, como muestra la figura 3.10.

```
(config-router)#router ospf 1
(config-router)#network 200.0.10.80 0.0.0.3 area 0
(config-router)#network 200.0.10.64 0.0.0.3 area 0
(config-router)#network 200.0.10.68 0.0.0.3 area 0
(config-router)#exit
```

Figura 3.10: Configuración del Protocolo OSPF-IPv4 en el router Cuenca.

#### IPV6

En direccionamiento IPv6 se establece OSPFv3, versión 3 para prefijos IPv6, en donde el comando global de configuración se configura, como se muestra con el círculo amarillo (1), la id del proceso en este caso es OSPF 1, como se muestra con el círculo amarillo (2), y si OSPFv3 lo solicita, se le asigna el id del router, número de 32 bits, como se muestra con el círculo amarillo (3), de igual manera a cada interfaz del router se le ingresa el id del proceso y del área cero, como se muestra con el círculo amarillo (4), la figura 3.11, muestra el procedimiento del router Quito.

```
Quito(config)#ipv6 unicast-routing
Quito(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id, please configure manually
Quito(config-rtr)#router-id 3.3.3.3
Quito(config-rtr)#exit
Quito(config)#
Quito(config)#interface g0/0/0
Quito(config-if)#ipv6 ospf 1 area 0
Quito(config-if)#exit
```

Figura 3.11: Configuración del protocolo OSPF-IPv6 en el router Quito.

Se debe tomar en cuenta que en cada Router con direccionamiento IPv4 se configuran las redes vecinas del mismo, en cambio en direccionamiento

### 3.5. CONFIGURACIÓN PARA LA SIMULACIÓN - PACKET TRACER(PKT)36

IPv6 se configura en cada interfaz y se debe habilitar IPv6 en el router.

#### Validación de tablas de enrutamiento

Para verificación del protocolo de enrutamiento OSPF e información de routing se realizó con el router backbone CUENCA, tanto para direccionamiento IPv4 e IPv6.

En las figuras 3.12 y 3.13 Se muestra el resultado de los comandos de direccionamiento IPv4, 'show ip route', y de direccionamiento IPv6, 'show ipv6 route', respectivamente. Estos comandos proporcionan detalles sobre la tabla de rutas, incluyendo las rutas conocidas (rutas conectadas directamente), las rutas estáticas (configuradas manualmente), las rutas predeterminadas (rutas determinadas) y las métricas asociadas a cada ruta, así como el siguiente salto. Se llevó a cabo la validación de rutas en cada router para comprobar la conectividad en ambos direccionamientos.

```
Cuenca#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O 192.168.10.0/24 [110/4] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
O 192.168.20.0/24 [110/3] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
O 192.168.30.0/24 [110/3] via 200.0.10.82, 06:15:09, GigabitEthernet2/0
C 192.168.30.0/24 is directly connected, FastEthernet4/0
O 192.168.40.0/24 [110/6] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
200.0.10.0/30 is subnetted, 22 subnets
O 200.0.10.0 [110/5] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
O 200.0.10.4 [110/3] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
O 200.0.10.8 [110/4] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
O 200.0.10.12 [110/4] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
O 200.0.10.16 [110/4] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
O 200.0.10.20 [110/3] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
O 200.0.10.24 [110/4] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
O 200.0.10.28 [110/3] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
O 200.0.10.32 [110/3] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
O 200.0.10.36 [110/2] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
O 200.0.10.40 [110/3] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
O 200.0.10.44 [110/4] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
O 200.0.10.48 [110/5] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
O 200.0.10.52 [110/4] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
O 200.0.10.56 [110/4] via 200.0.10.82, 06:15:09, GigabitEthernet2/0
O 200.0.10.60 [110/2] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
C 200.0.10.64 is directly connected, GigabitEthernet1/0
C 200.0.10.68 is directly connected, GigabitEthernet0/0
O 200.0.10.72 [110/3] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
O 200.0.10.76 [110/3] via 200.0.10.82, 06:15:09, GigabitEthernet2/0
O 200.0.10.80 [110/3] via 200.0.10.65, 06:15:09, GigabitEthernet1/0
C 200.0.10.84 [110/3] via 200.0.10.82, 06:15:09, GigabitEthernet2/0
O 200.0.10.88 is directly connected, GigabitEthernet2/0
O 200.0.10.92 [110/2] via 200.0.10.82, 06:15:09, GigabitEthernet2/0
```

Figura 3.12: Verificación de tablas de enrutamiento - IPv4.

### 3.5. CONFIGURACIÓN PARA LA SIMULACIÓN - PACKET TRACER(PKT)37

```
Cuenca#show ipv6 route
IPv6 Routing Table - 18 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDR - Redirect
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
O 2001:DB8:ABCD:1::/126 [110/5]
  via FE80::8, GigabitEthernet0/2/0
  via FE80::C, GigabitEthernet0/1/0
O 2001:DB8:ABCD:2::/126 [110/5]
  via FE80::8, GigabitEthernet0/2/0
  via FE80::C, GigabitEthernet0/1/0
O 2001:DB8:ABCD:6::/126 [110/3]
  via FE80::C, GigabitEthernet0/1/0
O 2001:DB8:ABCD:9::/126 [110/3]
  via FE80::8, GigabitEthernet0/2/0
  via FE80::C, GigabitEthernet0/1/0
O 2001:DB8:ABCD:E::/126 [110/4]
  via FE80::C, GigabitEthernet0/1/0
  via FE80::E, GigabitEthernet0/0/0
O 2001:DB8:ABCD:11::/126 [110/3]
  via FE80::C, GigabitEthernet0/1/0
  via FE80::E, GigabitEthernet0/0/0
C 2001:DB8:ABCD:13::/126 [0/0]
  via GigabitEthernet0/1/0, directly connected
L 2001:DB8:ABCD:13:2/128 [0/0]
  via GigabitEthernet0/1/0, receive
C 2001:DB8:ABCD:14::/126 [0/0]
  via GigabitEthernet0/2/0, directly connected
L 2001:DB8:ABCD:14:2/128 [0/0]
  via GigabitEthernet0/2/0, receive
C 2001:DB8:ABCD:15::/126 [0/0]
  via GigabitEthernet0/0/0, directly connected
L 2001:DB8:ABCD:15:1/128 [0/0]
  via GigabitEthernet0/0/0, receive
O 2003:DB8:ABCD:1::/64 [110/6]
  via FE80::8, GigabitEthernet0/2/0
  via FE80::C, GigabitEthernet0/1/0
O 2003:DB8:ABCD:2::/64 [110/4]
  via FE80::8, GigabitEthernet0/2/0
  via FE80::C, GigabitEthernet0/1/0
O 2003:DB8:ABCD:3::/64 [110/3]
  via FE80::C, GigabitEthernet0/1/0
  via FE80::E, GigabitEthernet0/0/0
C 2003:DB8:ABCD:4::/64 [0/0]
  via FastEthernet0/0, directly connected
L 2003:DB8:ABCD:4:1/128 [0/0]
```

Figura 3.13: Verificación de tablas de enrutamiento - IPv6.

#### Verificar información de la configuración de OSPF

La figura 3.14 muestra el resultado del comando **ip protocols**, en donde se detalla el ID del proceso (marcados con círculos amarillos) OSPF 1 (1), ID del router, los vecinos del router (2) y la distancia administrativa establecida es 110 para OSPF(3).

### 3.5. CONFIGURACIÓN PARA LA SIMULACIÓN - PACKET TRACER(PKT)38

```
Cuenca#show ip protocols
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 200.0.10.81
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
 200.0.10.64 0.0.0.3 area 0
 200.0.10.68 0.0.0.3 area 0
 200.0.10.80 0.0.0.3 area 0
192.168.30.0 0.0.0.255 area 0
Routing Information Sources:
Gateway          Distance      Last Update
200.0.10.5       110           00:16:22
200.0.10.13      110           00:16:13
200.0.10.25      110           00:16:15
200.0.10.29      110           00:16:15
200.0.10.41      110           00:16:14
200.0.10.45      110           00:16:20
200.0.10.49      110           00:16:23
200.0.10.57      110           00:16:14
200.0.10.65      110           00:16:21
200.0.10.69      110           00:16:19
200.0.10.73      110           00:16:21
200.0.10.77      110           00:16:14
200.0.10.81      110           00:16:21
200.0.10.85      110           00:16:19
200.0.10.86      110           00:16:21
Distance: (default is 110)
```

Figura 3.14: Verificación de protocolos - IPv4.

La figura 3.15, muestra resultado del comando **ipv6 protocols**, para direccionamiento IPv6 que nos detalla las interfaces habilitadas para OSPF, en qué área se encuentran y el ID del proceso OSPF 1.

```
Cuenca#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 0)
    GigabitEthernet0/2/0
    GigabitEthernet0/1/0
    GigabitEthernet0/0/0
    FastEthernet0/0
  Redistribution:
    None
```

Figura 3.15: Verificación de protocolos - IPv6.

Utilizando el comando "protocols", se puede verificar configuración del protocolo de enrutamiento para todos los enrutadores, lo que permite validar la configuración del enrutamiento OSPF establecida correctamente.

#### Validar Adyacencia

**Ip ospf neighbor**, valida la adyacencia entre enrutadores vecinos con ospf como se puede observar en la figura 3.16, con direccionamiento IPv4.

### 3.5. CONFIGURACIÓN PARA LA SIMULACIÓN - PACKET TRACER(PKT)39

```
Cuenca#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
200.0.10.65	1	FULL/BDR	00:00:37	200.0.10.65	GigabitEthernet1/0
200.0.10.86	1	FULL/DR	00:00:37	200.0.10.82	GigabitEthernet2/0

Figura 3.16: Verificación de vecinos vía OSPF-IPv4.

Se describen los siguientes parámetros:

**Neighbor ID:** ID de enrutador vecino.

**Pri:** prioridad que tiene el enrutador vecino.

**State:** el estado del enrutador vecino.

**Dead Time:** Tiempo de espera para recibir un paquete Hello OSPF, antes de exponer que el enrutador está inactivo.

**Address:** es la dirección IP de interfaz del vecino conectada.

**Interface:** Interfaz del vecino OSPF.

Para el direccionamiento IPv6 con el comando **ipv6 ospf neighbor**, se tiene un resultado similar al de IPv4, como se observa en la figura 3.17, pero con la diferencia que se detalla la ID de interfaz y los mismos requisitos para formar una adyacencia vecina por lo cual en ambos casos si tenemos un STATE FULL, se valida la formación de la adyacencia.

```
Cuenca#show ipv6 ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
14.14.14.14	1	FULL/DR	00:00:38	3	GigabitEthernet0/0/0
8.8.8.8	1	FULL/BDR	00:00:36	5	GigabitEthernet0/2/0
12.12.12.12	1	FULL/BDR	00:00:36	4	GigabitEthernet0/1/0

Figura 3.17: Verificación de vecinos vía OSPF -IPv6.

#### Validar Interfaces Configuradas

Para tener una lista de interfaces habilitadas y que utilizan OSPF, se utilizó **ip ospf interface brief** para IPv4 y **ipv6 ospf interface brief**, como se puede observar en las figuras 3.18 y 3.19.

### 3.5. CONFIGURACIÓN PARA LA SIMULACIÓN - PACKET TRACER(PKT)40

```
Cuenca#show ip ospf interface brief
```

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs F/C
Gig0/0	1	0	200.0.10.70/255.255.255.252	1	DR	0/0
Gig1/0	1	0	200.0.10.66/255.255.255.252	1	DR	0/0
Gig2/0	1	0	200.0.10.81/255.255.255.252	1	BDR	0/0
Fa4/0	1	0	192.168.30.1/255.255.255.0	1	DR	0/0

Figura 3.18: Verificación de interfaces configuradas bajo OSPF-IPv4

```
Cuenca#show ipv6 ospf interface brief
```

Interface	PID	Area	Intf ID	Cost	State	Nbrs F/C
Gig0/2/0	1	0	5	1	DR	0/0
Gig0/1/0	1	0	4	1	DR	0/0
Gig0/0/0	1	0	3	1	BDR	0/0
Fa0/0	1	0	1	1	DR	0/0

Interfaz del router	ID del Proceso	Área	Número de secuencia de estado de enlace	Costo	Estado del Link, DR y BDR establecen adyacencias.
---------------------	----------------	------	---	-------	---

Figura 3.19: Verificación de interfaces configuradas bajo OSFF-IPv6

#### Visualización Tablas

Con direccionamiento IPv4 el comando “Show ip route osp” y en en direccionamiento IPv6 “show ipv6 route osp” visualiza tabla de enrutamiento sobre las rutas OSPF, como se puede observar en las figuras 3.20 y 3.21.

### 3.5. CONFIGURACIÓN PARA LA SIMULACIÓN - PACKET TRACER(PKT)41

```
Cuenca(config)#do show ip route ospf
0   192.168.10.0 [110/4] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
0   192.168.20.0 [110/3] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
    [110/3] via 200.0.10.82, 06:41:39, GigabitEthernet2/0
0   192.168.40.0 [110/6] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
    200.0.10.0/30 is subnetted, 22 subnets
0     200.0.10.0 [110/5] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
0     200.0.10.4 [110/5] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
0     200.0.10.8 [110/4] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
0     200.0.10.12 [110/4] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
0     200.0.10.16 [110/4] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
0     200.0.10.20 [110/3] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
0     200.0.10.24 [110/4] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
0     200.0.10.28 [110/3] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
0     200.0.10.32 [110/3] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
0     200.0.10.36 [110/2] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
0     200.0.10.40 [110/3] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
0     200.0.10.44 [110/4] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
0     200.0.10.48 [110/5] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
0     200.0.10.52 [110/4] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
    [110/4] via 200.0.10.82, 06:41:39, GigabitEthernet2/0
0     200.0.10.56 [110/4] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
    [110/4] via 200.0.10.82, 06:41:39, GigabitEthernet2/0
0     200.0.10.60 [110/2] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
0     200.0.10.72 [110/3] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
    [110/3] via 200.0.10.82, 06:41:39, GigabitEthernet2/0
0     200.0.10.76 [110/3] via 200.0.10.65, 06:41:39, GigabitEthernet1/0
    [110/3] via 200.0.10.82, 06:41:39, GigabitEthernet2/0
0     200.0.10.84 [110/2] via 200.0.10.82, 06:41:39, GigabitEthernet2/0
```

Figura 3.20: Verificación de tablas de enrutamiento - IPV4

### 3.5. CONFIGURACIÓN PARA LA SIMULACIÓN - PACKET TRACER(PKT)42

```
Cuenca#show ipv6 route ospf
IPv6 Routing Table - 19 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
O 2001:DB8:ABCD:1::/126 [110/5]
  via FE80::8, GigabitEthernet0/2/0
  via FE80::C, GigabitEthernet0/1/0
O 2001:DB8:ABCD:2::/126 [110/5]
  via FE80::8, GigabitEthernet0/2/0
  via FE80::C, GigabitEthernet0/1/0
O 2001:DB8:ABCD:6::/126 [110/3]
  via FE80::C, GigabitEthernet0/1/0
O 2001:DB8:ABCD:9::/126 [110/3]
  via FE80::8, GigabitEthernet0/2/0
  via FE80::C, GigabitEthernet0/1/0
O 2001:DB8:ABCD:D::/126 [110/2]
  via FE80::C, GigabitEthernet0/1/0
O 2001:DB8:ABCD:E::/126 [110/4]
  via FE80::C, GigabitEthernet0/1/0
  via FE80::E, GigabitEthernet0/0/0
O 2001:DB8:ABCD:11::/126 [110/3]
  via FE80::C, GigabitEthernet0/1/0
  via FE80::E, GigabitEthernet0/0/0
O 2003:DB8:ABCD:1::/64 [110/6]
  via FE80::8, GigabitEthernet0/2/0
  via FE80::C, GigabitEthernet0/1/0
O 2003:DB8:ABCD:2::/64 [110/4]
  via FE80::8, GigabitEthernet0/2/0
  via FE80::C, GigabitEthernet0/1/0
O 2003:DB8:ABCD:3::/64 [110/3]
  via FE80::C, GigabitEthernet0/1/0
  via FE80::E, GigabitEthernet0/0/0
```

Figura 3.21: Verificación de tablas de enrutamiento - IPv6

#### 3.5.5. Configuración del protocolo de Gestión SNMP

Para habilitar al agente de la gestión de red del protocolo SNMP, en cada router se realizó la configuración mostrada en la figura 3.22, que es SNMPv2, tanto para direccionamiento IPv4 como IPv6, en donde se establece la “comunidad” de sólo lectura (ro) y también se tiene la de lectura y escritura (rw) para poder ingresar al router y realizar la respectiva gestión mediante los objetos OID.

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#snmp-server community cedia ro
%SNMP-5-WARMSTART: SNMP agent on host Router is undergoing a warm start
Router(config)#snmp-server community cedia rw
```

Figura 3.22: Configuración SNMPv2 para IPv4 e IPv6.



### 3.6. Configuración para la emulación - GNS3

#### Topología Lógica - IPv4

En GNS3, para realizar la emulación con direccionamiento IPV4 se utilizaron 15 routers “Cisco 7200”. Se añadieron módulos para emular los routers backbone y 4 “Switch” para la conexión de 4 PC’s distribuidas en las ciudades Quito, Tulcan, Cuenca y Guayaquil. Se utilizaron los sistemas operativos Windows 10, Windows Server, Ubuntu y Windows 7 para pruebas, figura 3.23 muestra la topología lógica.

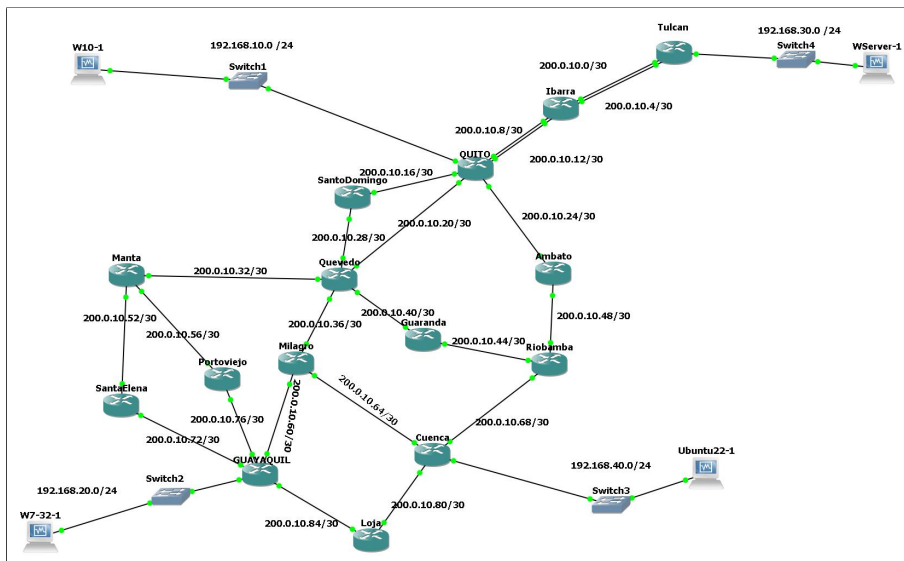


Figura 3.23: Topología Lógica IPv4 - GNS3.

#### Topología lógica - IPv6

Para la emulación con direccionamiento IPv6, se utilizaron 15 routers “Cisco 7200”. Se añadieron módulos, para emular los routers backbone y 4 “Switch”, para la conexión de 4 PC distribuidas en las ciudades de Guayaquil, Quito, Tulcan y Cuenca. Se utilizaron los sistemas operativos Windows 10, Windows 8, Ubuntu 22 y Windows Server para pruebas de uso de recursos, de modo que las 4 máquinas virtuales, hacen las veces de los Network Management Systems (NMS), como se observa en la figura 3.24.

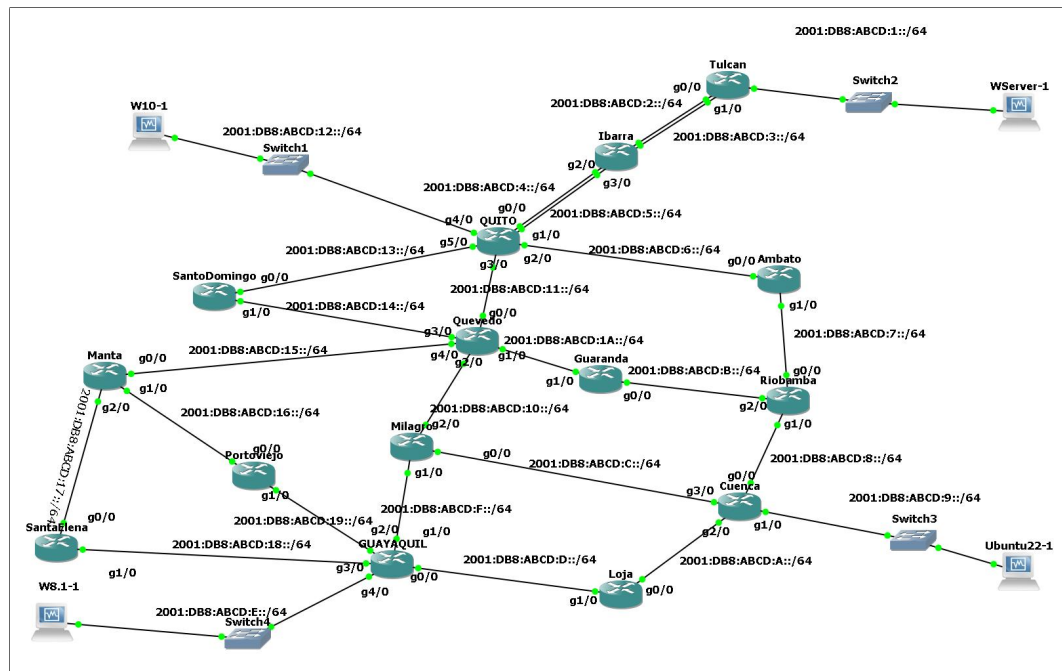


Figura 3.24: Topología Lógica IPv6 - GNS3.

### 3.6.1. Tablas de enrutamiento - IPv4

Para IPv4, se utilizaron direcciones de clase C, como se detalla en la tabla 3.6 en donde se indica el nombre de cada router, la dirección de red con su respectiva máscara, la interfaz a la que pertenece con su respectiva IP.

Cuadro 3.6: Direccionamiento para Routers IPV4 - GNS3

N°	ROUTER	RED	MASCARA	INTERFAZ	IP
1	Tulcan	200.0.10.0	255.255.255.252	G0/0	200.0.10.1
		200.0.10.5	255.255.255.252	G1/0	200.0.10.5
		192.168.20.0	255.255.255.0	G2/0	192.168.20.1
2	Ibarra	200.0.10.0	255.255.255.252	G0/0	200.0.10.2
		200.0.10.4	255.255.255.252	G1/0	200.0.10.6
		200.0.10.8	255.255.255.252	G2/0	200.0.10.9
		200.0.10.12	255.255.255.252	G3/0	200.0.10.13
3	QUITO	200.0.10.8	255.255.255.252	G0/0	200.0.10.10
		200.0.10.12	255.255.255.252	G1/0	200.0.10.14
		192.168.10.0	255.255.255.0	G2/0	192.168.10.1
		200.0.10.16	255.255.255.252	G3/0	200.0.10.17
		200.0.10.20	255.255.255.252	G4/0	200.0.10.21
		200.0.10.24	255.255.255.252	G5/0	200.0.10.25
4	SantoDomingo	200.0.10.16	255.255.255.252	G0/0	200.0.10.18
		200.0.10.28	255.255.255.252	G1/0	200.0.10.29
5	Ambato	200.0.10.24	255.255.255.252	G0/0	200.0.10.26
		200.0.10.48	255.255.255.252	G1/0	200.0.10.49
6	Quevedo	200.0.10.20	255.255.255.252	G0/0	200.0.10.22
		200.0.10.28	255.255.255.252	G1/0	200.0.10.30
		200.0.10.32	255.255.255.252	G2/0	200.0.10.33
		200.0.10.36	255.255.255.252	G3/0	200.0.10.37
		200.0.10.40	255.255.255.252	G4/0	200.0.10.41
7	Guaranda	200.0.10.40	255.255.255.252	G0/0	200.0.10.42
		200.0.10.44	255.255.255.252	G1/0	200.0.10.45
8	Riobamba	200.0.10.44	255.255.255.252	G0/0	200.0.10.46
		200.0.10.48	255.255.255.252	G1/0	200.0.10.50
		200.0.10.68	255.255.255.252	G2/0	200.0.10.69
9	Manta	200.0.10.32	255.255.255.252	G0/0	200.0.10.34
		200.0.10.52	255.255.255.252	G1/0	200.0.10.53
		200.0.10.56	255.255.255.252	G2/0	200.0.10.57
10	Portoviejo	200.0.10.56	255.255.255.252	G0/0	200.0.10.58
		200.0.10.76	255.255.255.252	G1/0	200.0.10.77
11	SantaElena	200.0.10.52	255.255.255.252	G0/0	200.0.10.54
		200.0.10.72	255.255.255.252	G1/0	200.0.10.73
12	Milagro	200.0.10.36	255.255.255.252	G0/0	200.0.10.38
		200.0.10.60	255.255.255.252	G1/0	200.0.10.65
		200.0.10.64	255.255.255.252	G2/0	200.0.10.61
13	Cuenca	200.0.10.64	255.255.255.252	G0/0	200.0.10.70
		200.0.10.68	255.255.255.252	G1/0	200.0.10.66
		200.0.10.80	255.255.255.252	G2/0	200.0.10.81
		192.168.40.0	255.255.255.0	G3/0	192.168.40.1
14	Loja	200.0.10.80	255.255.255.252	G0/0	200.0.10.82
		200.0.10.84	255.255.255.252	G1/0	200.0.10.86
15	GUAYAQUIL	200.0.10.72	255.255.255.252	G0/0	200.0.10.74
		200.0.10.76	255.255.255.252	G1/0	200.0.10.78
		200.0.10.60	255.255.255.252	G2/0	200.0.10.62
		200.0.10.84	255.255.255.252	G3/0	200.0.10.85
		192.168.20.0	255.255.255.0	G4/0	192.168.20.1

En el [Emulador](#) se asignan máquinas virtuales con el direccionamiento indicado en la tabla [3.7](#), que se configura manualmente a la interfaz de red de cada máquina.

Cuadro 3.7: Direccionamiento para los NMS bajo IPV4 - GNS3

Dispositivo	RED	MÁSCARA	INTERFAZ	IP	GATEWAY
W10-1	192.168.10.0	255.255.255.0	F0	192.168.10.2	192.168.10.1
W7-32-1	192.168.20.0	255.255.255.0	F0	192.168.20.2	192.168.20.1
WServer1	192.168.30.0	255.255.255.0	F0	192.168.30.2	192.168.30.1
Ubuntu	192.168.40.0	255.255.255.0	F0	192.168.40.2	192.168.40.1

### IPV6

Para IPv6, se utilizó el prefijo **2001:DB8:ABCD**, para link local la dirección **FE80**, también se les asignó el id de router desde la 1.1.1.1 hasta la 15.15.15.15, que son valores de 32 bits, se detalla en la tabla [3.8](#).

Cuadro 3.8: Direcciones de enrutamiento IPv6 - GNS3

N°	ROUTER	RED/MASCARA	INTERFAZ	IP	LINK-LOCAL	ID-ROUTER
1	Tulcan	2001:DB8:ABCD:1::/64	Gig0/0	2001:DB8:ABCD:1::1	FE80::1	1.1.1.1
		2001:DB8:ABCD:2::/64	Gig1/0	2001:DB8:ABCD:2::1		
		2001:DB8:ABCD:3::/64	Gig2/0	2001:DB8:ABCD:3::1		
2	Ibarra	2001:DB8:ABCD:2::/64	Gig0/0	2001:DB8:ABCD:2::2	FE80::2	2.2.2.2
		2001:DB8:ABCD:3::/64	Gig1/0	2001:DB8:ABCD:3::2		
		2001:DB8:ABCD:4::/64	Gig2/0	2001:DB8:ABCD:4::1		
3	QUITO	2001:DB8:ABCD:4::/64	Gig0/0	2001:DB8:ABCD:4::2	FE80::3	3.3.3.3
		2001:DB8:ABCD:5::/64	Gig1/0	2001:DB8:ABCD:5::2		
		2001:DB8:ABCD:6::/64	Gig2/0	2001:DB8:ABCD:6::2		
		2001:DB8:ABCD:11::/64	Gig3/0	2001:DB8:ABCD:11::2		
		2001:DB8:ABCD:12::/64	Gig4/0	2001:DB8:ABCD:12::1		
4	Santo-Domingo	2001:DB8:ABCD:13::/64	Gig5/0	2001:DB8:ABCD:13::2	FE80::4	4.4.4.4
		2001:DB8:ABCD:14::/64	Gig0/0	2001:DB8:ABCD:14::1		
5	Quevedo	2001:DB8:ABCD:11::/64	Gig1/0	2001:DB8:ABCD:11::1	FE80::5	5.5.5.5
		2001:DB8:ABCD:1A::/64	Gig2/0	2001:DB8:ABCD:1A::2		
		2001:DB8:ABCD:10::/64	Gig3/0	2001:DB8:ABCD:10::1		
		2001:DB8:ABCD:14::/64	Gig4/0	2001:DB8:ABCD:14::2		
6	Guaranda	2001:DB8:ABCD:15::/64	Gig0/0	2001:DB8:ABCD:15::2	FE80::6	6.6.6.6
		2001:DB8:ABCD:1A::/64	Gig1/0	2001:DB8:ABCD:1A::1		
7	Riobamba	2001:DB8:ABCD:7::/64	Gig0/0	2001:DB8:ABCD:7::2	FE80::7	7.7.7.7
		2001:DB8:ABCD:8::/64	Gig1/0	2001:DB8:ABCD:8::2		
8	Ambato	2001:DB8:ABCD:8::/64	Gig2/0	2001:DB8:ABCD:8::2	FE80::8	8.8.8.8
		2001:DB8:ABCD:6::/64	Gig3/0	2001:DB8:ABCD:6::1		
9	Manta	2001:DB8:ABCD:7::/64	Gig0/0	2001:DB8:ABCD:7::1	FE80::9	9.9.9.9
		2001:DB8:ABCD:15::/64	Gig1/0	2001:DB8:ABCD:15::1		
10	Santa Elena	2001:DB8:ABCD:16::/64	Gig2/0	2001:DB8:ABCD:16::1	FE80::A	10.10.10.10
		2001:DB8:ABCD:17::/64	Gig0/0	2001:DB8:ABCD:17::2		
		2001:DB8:ABCD:18::/64	Gig1/0	2001:DB8:ABCD:18::2		
11	Portoviejo	2001:DB8:ABCD:17::/64	Gig0/0	2001:DB8:ABCD:17::2	FE80::B	11.11.11.11
		2001:DB8:ABCD:16::/64	Gig1/0	2001:DB8:ABCD:16::2		
12	Milagro	2001:DB8:ABCD:19::/64	Gig0/0	2001:DB8:ABCD:19::2	FE80::C	12.12.12.12
		2001:DB8:ABCD:C::/64	Gig1/0	2001:DB8:ABCD:C::2		
		2001:DB8:ABCD:F::/64	Gig2/0	2001:DB8:ABCD:F::2		
13	Cuenca	2001:DB8:ABCD:10::/64	Gig0/0	2001:DB8:ABCD:10::1	FE80::D	13.13.13.13
		2001:DB8:ABCD:8::/64	Gig1/0	2001:DB8:ABCD:8::1		
		2001:DB8:ABCD:9::/64	Gig2/0	2001:DB8:ABCD:9::1		
		2001:DB8:ABCD:A::/64	Gig3/0	2001:DB8:ABCD:A::1		
14	Loja	2001:DB8:ABCD:C::/64	Gig0/0	2001:DB8:ABCD:C::1	FE80::E	14.14.14.14
		2001:DB8:ABCD:A::/64	Gig1/0	2001:DB8:ABCD:A::2		
15	GUAYAQUIL	2001:DB8:ABCD:D::/64	Gig0/0	2001:DB8:ABCD:D::2	FE80::F	15.15.15.15
		2001:DB8:ABCD:D::/64	Gig1/0	2001:DB8:ABCD:D::1		
		2001:DB8:ABCD:F::/64	Gig2/0	2001:DB8:ABCD:F::1		
		2001:DB8:ABCD:19::/64	Gig3/0	2001:DB8:ABCD:19::1		
		2001:DB8:ABCD:18::/64	Gig4/0	2001:DB8:ABCD:18::1		

Para las máquinas virtuales se le asignó el mismo prefijo, como se detalla en la tabla 3.9.

Cuadro 3.9: Direccionamiento los NMS bajo IPv6 - GNS3

Dispositivo	RED/MASCARA	INTERFAZ	IP	GATEWAY
Wserver-1	2001:DB8:ABCD::1::/64	F0	2001:DB8:ABCD::1::2	2001:DB8:ABCD::1::1
W10	2001:DB8:ABCD::12::/64	F0	2001:DB8:ABCD::12::2	2001:DB8:ABCD::12::1
WS.1-1	2001:DB8:ABCD::E::/64	F0	2001:DB8:ABCD::E::2	2001:DB8:ABCD::3::1
Ubuntu22	2001:DB8:ABCD::9::/64	F0	2001:DB8:ABCD::9::2	2001:DB8:ABCD::4::1

### 3.6.2. Configuración de routers de backbone y MV

Para la configuración en los enrutadores, GNS3 permite agregar más módulos en los slots como se puede observar en la figura 3.25, por lo cual a cada router backbone se le asignaron los módulos necesarios para las topologías.

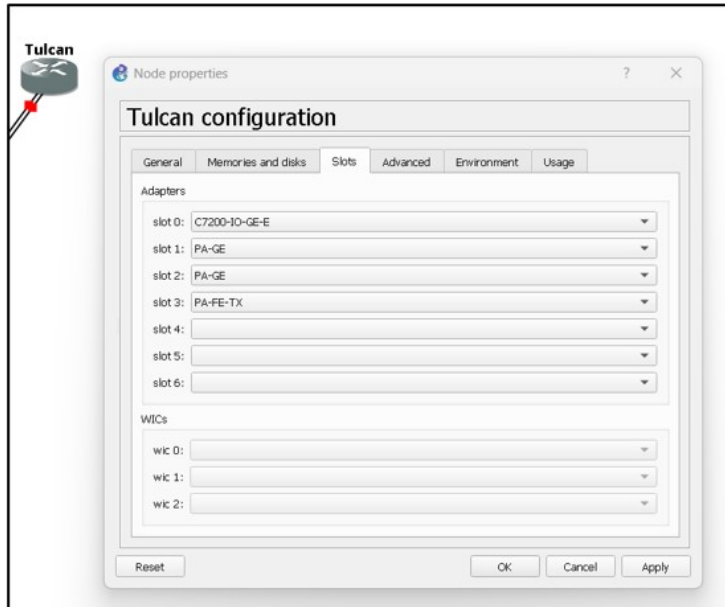


Figura 3.25: Configuración Routers GNS3.

En el modo privilegiado a cada router y en las máquinas virtuales en sus tarjetas de red en sus respectivas interfaces se le asignó una dirección IP y máscara tanto en direccionamiento IPv4 e IPv6. La figura 3.26 muestra la Interfaz del Router Tulcan IPv4 - GNS3 configurada.

La figura 3.27 permite observar la Interfaz del Router Tulcan IPv6 - GNS3 configurada.

```
Tulcan(config)#interfacegi
Tulcan(config)#interface gi
Tulcan(config)#interface gigabitEthernet 0/0
Tulcan(config-if)#ip address 200.0.10.1 255.255.255.252
Tulcan(config-if)#no shutdown
Tulcan(config-if)#
```

Figura 3.26: Configuración Interfaz Router Tulcan IPv4 - GNS3

```
Tulcan(config)#interface g0/0
Tulcan(config-if)#ipv6 address 2001:DB8:ABCD:1::1/64
Tulcan(config-if)#no shutdown
Tulcan(config-if)#exit
Tulcan(config)#
```

Figura 3.27: Configuración Interfaz Router Tulcan IPv6 - GNS3

La figura 3.28, muestra la Máquina Virtual Quito con IPv4 configurada, y en la figura 3.29 muestra la Máquina Virtual del Sistema Linux Cuenca y Windows Quito- IPv6, configurada.

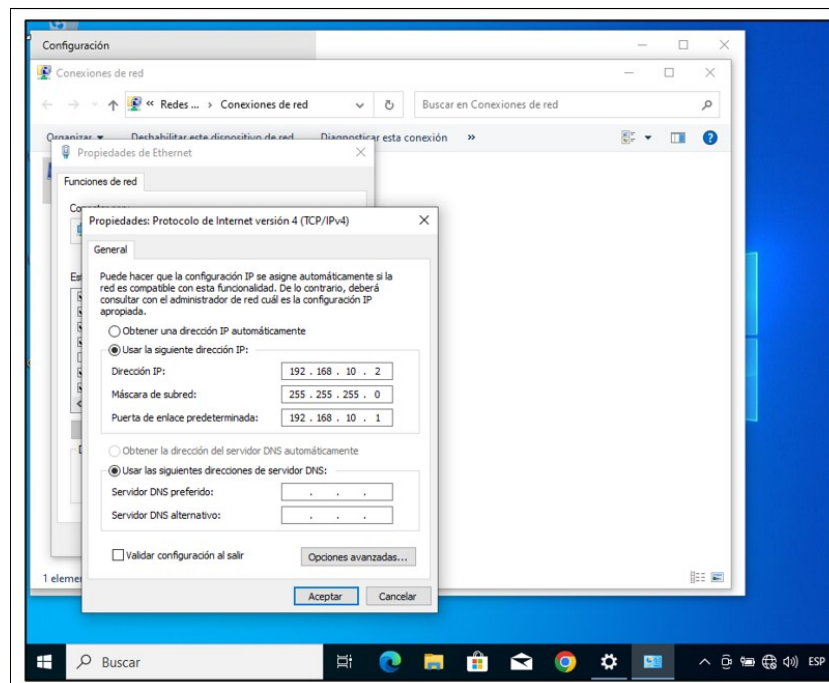


Figura 3.28: Configuración de la Máquina Virtual Quito - IPv4



Figura 3.29: Configuración Máquina Virtual Sistema Linux Cuenca y Windows Tulcan- IPv6



### 3.6.3. Configuración Protocolo OSPF

#### IPV4

Cada router se configura el protocolo OPSFv2, como muestra la figura 3.30 para el router Tulcan, se estableció OSPF en cada interfaz.

```
Tulcan(config)#router ospf 1
Tulcan(config-router)#network 200.0.10.0 0.0.0.3 area 0
Tulcan(config-router)#network 200.0.10.4 0.0.0.3 area 0
Tulcan(config-router)#exit
Tulcan(config)#
```

Figura 3.30: Configuración OSPFv2 - IPv4

#### IPV6

Para el caso del direccionamiento IPv6, se debe configurar OPSFv3 en las interfaces con su respectivo ID y área asignada como se describe en la figura 3.31 para el caso del router Tulcan.

```
Tulcan(config)#ipv6 unicast-routing
Tulcan(config)#ipv6 router ospf 1
Tulcan(config-rtr)#

Tulcan(config-rtr)#router-id 1.1.1.1
Tulcan(config-rtr)#exit

Tulcan(config)#interface g0/0
Tulcan(config-if)#ipv6 ospf 1 area 0
Tulcan(config-if)#exit
Tulcan(config)#interface g1/0
Tulcan(config-if)#ipv6 ospf 1 area 0
Tulcan(config-if)#exit
Tulcan(config)#
```

Figura 3.31: Configuración OSPFv3 - IPv6

### 3.6.4. Verificación del enrutamiento OSPF

Para validar una conexión exitosa, es necesario realizar un ping de extremo a extremo en la topología. Además, existen comandos y palabras clave específicas que permiten validar enrutamiento. Por ejemplo, comando ‘show ip ospf’ se utiliza para confirmar interfaces activas y tenemos ‘show ip interface brief’ que permite validar interfaces operativas.

Para asegurar que se hayan creado correctamente las tablas de enrutamiento completas, se debe verificar la presencia de rutas locales (indicadas con ‘L’) y las rutas obtenidas a través de OSPF (indicadas con ‘O’). En el caso del direccionamiento IPv4, se puede utilizar ‘show ip route’,

cuyo resultado muestra la figura 3.32 para el enrutador Quito. Para el direccionamiento IPv6, 'show ipv6 route', cuyo resultado presenta la figura 3.33, también para el enrutador Quito.

```

QUITO#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet2/0
L       192.168.10.1/32 is directly connected, GigabitEthernet2/0
O       192.168.20.0/24 [110/4] via 200.0.10.22, 00:10:34, GigabitEthernet4/0
200.0.10.0/24 is variably subnetted, 27 subnets, 2 masks
O       200.0.10.0/30 [110/2] via 200.0.10.13, 00:10:54, GigabitEthernet1/0
        [110/2] via 200.0.10.9, 00:10:54, GigabitEthernet0/0
O       200.0.10.4/30 [110/2] via 200.0.10.13, 00:10:54, GigabitEthernet1/0
        [110/2] via 200.0.10.9, 00:10:54, GigabitEthernet0/0
C       200.0.10.8/30 is directly connected, GigabitEthernet0/0
L       200.0.10.10/32 is directly connected, GigabitEthernet0/0
C       200.0.10.12/30 is directly connected, GigabitEthernet1/0
L       200.0.10.14/32 is directly connected, GigabitEthernet1/0
C       200.0.10.16/30 is directly connected, GigabitEthernet3/0
L       200.0.10.17/32 is directly connected, GigabitEthernet3/0
C       200.0.10.20/30 is directly connected, GigabitEthernet4/0
L       200.0.10.21/32 is directly connected, GigabitEthernet4/0
C       200.0.10.24/30 is directly connected, GigabitEthernet5/0
L       200.0.10.25/32 is directly connected, GigabitEthernet5/0
O       200.0.10.28/30 [110/2] via 200.0.10.22, 00:10:54, GigabitEthernet4/0
        [110/2] via 200.0.10.18, 00:10:54, GigabitEthernet3/0
O       200.0.10.32/30 [110/2] via 200.0.10.22, 00:10:54, GigabitEthernet4/0
O       200.0.10.36/30 [110/2] via 200.0.10.22, 00:10:44, GigabitEthernet4/0
O       200.0.10.40/30 [110/2] via 200.0.10.22, 00:10:54, GigabitEthernet4/0
O       200.0.10.44/30 [110/3] via 200.0.10.26, 00:10:54, GigabitEthernet5/0
        [110/3] via 200.0.10.22, 00:10:54, GigabitEthernet4/0
O       200.0.10.48/30 [110/2] via 200.0.10.26, 00:10:54, GigabitEthernet5/0
O       200.0.10.52/30 [110/3] via 200.0.10.22, 00:10:44, GigabitEthernet4/0
O       200.0.10.56/30 [110/3] via 200.0.10.22, 00:10:44, GigabitEthernet4/0
O       200.0.10.60/30 [110/3] via 200.0.10.22, 00:10:34, GigabitEthernet4/0
O       200.0.10.64/30 [110/3] via 200.0.10.22, 00:10:34, GigabitEthernet4/0
O       200.0.10.68/30 [110/3] via 200.0.10.26, 00:10:44, GigabitEthernet5/0
O       200.0.10.72/30 [110/4] via 200.0.10.22, 00:10:34, GigabitEthernet4/0
O       200.0.10.76/30 [110/4] via 200.0.10.22, 00:10:34, GigabitEthernet4/0
O       200.0.10.80/30 [110/4] via 200.0.10.26, 00:10:44, GigabitEthernet5/0
        [110/4] via 200.0.10.22, 00:10:34, GigabitEthernet4/0
O       200.0.10.84/30 [110/4] via 200.0.10.22, 00:10:34, GigabitEthernet4/0

```

Figura 3.32: Verificación de la tabla de enrutamiento - router Quito - IPv4

```

QUITO#show ipv6 route
IPv6 Routing Table - default - 33 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDR - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, I - LISP
O 2001:DB8:ABCD:1::/64 [110/3]
  via FE80::2, GigabitEthernet1/0
  via FE80::2, GigabitEthernet0/0
O 2001:DB8:ABCD:2::/64 [110/2]
  via FE80::2, GigabitEthernet0/0
  via FE80::2, GigabitEthernet1/0
O 2001:DB8:ABCD:3::/64 [110/2]
  via FE80::2, GigabitEthernet0/0
  via FE80::2, GigabitEthernet1/0
C 2001:DB8:ABCD:4::/64 [0/0]
  via GigabitEthernet0/0, directly connected
L 2001:DB8:ABCD:4::2/128 [0/0]
  via GigabitEthernet0/0, receive
C 2001:DB8:ABCD:5::/64 [0/0]
  via GigabitEthernet1/0, directly connected
L 2001:DB8:ABCD:5::2/128 [0/0]
  via GigabitEthernet1/0, receive
C 2001:DB8:ABCD:6::/64 [0/0]
  via GigabitEthernet2/0, directly connected
L 2001:DB8:ABCD:6::2/128 [0/0]
  via GigabitEthernet2/0, receive
O 2001:DB8:ABCD:7::/64 [110/2]
  via FE80::8, GigabitEthernet2/0
O 2001:DB8:ABCD:8::/64 [110/3]
  via FE80::8, GigabitEthernet2/0
  via FE80::5, GigabitEthernet3/0
O 2001:DB8:ABCD:9::/64 [110/4]
  via FE80::8, GigabitEthernet2/0
  via FE80::5, GigabitEthernet3/0
O 2001:DB8:ABCD:A::/64 [110/4]
  via FE80::8, GigabitEthernet2/0
  via FE80::5, GigabitEthernet3/0
O 2001:DB8:ABCD:B::/64 [110/3]
  via FE80::8, GigabitEthernet2/0
  via FE80::5, GigabitEthernet3/0
O 2001:DB8:ABCD:C::/64 [110/3]
  via FE80::5, GigabitEthernet3/0
O 2001:DB8:ABCD:D::/64 [110/4]
  via FE80::5, GigabitEthernet3/0
O 2001:DB8:ABCD:E::/64 [110/4]
  via FE80::5, GigabitEthernet3/0
O 2001:DB8:ABCD:F::/64 [110/3]
  via FE80::5, GigabitEthernet3/0
O 2001:DB8:ABCD:10::/64 [110/2]
  via FE80::5, GigabitEthernet3/0
C 2001:DB8:ABCD:11::/64 [0/0]
  via GigabitEthernet3/0, directly connected
L 2001:DB8:ABCD:11::2/128 [0/0]
  via GigabitEthernet3/0, receive
C 2001:DB8:ABCD:12::/64 [0/0]
  via GigabitEthernet4/0, directly connected
L 2001:DB8:ABCD:12::1/128 [0/0]
--More--

```

Figura 3.33: Verificación de la tabla de enrutamiento - router Quito - IPv6

**Verificación de protocolos.-** Para obtener detalles y parámetros e información de los protocolos configurados en el router, como su ID, número de área, interfaces con su área respectiva se tiene “show ip protocols” con direccionamiento IPv4 y “show ipv6 protocols” con direccionamiento IPv6 como se indica en las figuras 3.34, y 3.35 para el caso del router Quito.

```
QUITO#show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 200.0.10.25
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.10.0 0.0.0.255 area 0
    200.0.10.8 0.0.0.3 area 0
    200.0.10.12 0.0.0.3 area 0
    200.0.10.16 0.0.0.3 area 0
    200.0.10.20 0.0.0.3 area 0
    200.0.10.24 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    200.0.10.65      110          00:15:20
    200.0.10.69      110          00:15:30
    200.0.10.73      110          00:15:20
    200.0.10.77      110          00:15:20
    200.0.10.81      110          00:15:10
    200.0.10.86      110          00:15:10
    200.0.10.85      110          00:15:10
    200.0.10.13      110          00:15:30
    200.0.10.41      110          00:15:30
    200.0.10.45      110          00:15:30
    200.0.10.49      110          00:15:41
    200.0.10.57      110          00:15:30
  Distance: (default is 110)
```

Figura 3.34: Resultado Comando show ip protocols - router Quito - IPv4

```

QUITO#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
  Router ID 3.3.3.3
  Number of areas: 1 normal, 0 stub, 0 nssa
  Interfaces (Area 0):
    GigabitEthernet5/0
    GigabitEthernet4/0
    GigabitEthernet3/0
    GigabitEthernet2/0
    GigabitEthernet1/0
    GigabitEthernet0/0
  Redistribution:
    None

```

Figura 3.35: Resultado Comando show ipv6 protocols - router Quito - IPv6

**Verificación de vecinos.** Para obtener datos de la estructura del router vecino con OSPF, su estado, su interfaz, su ID y prioridad se utiliza show ip ospf neighbor.

#### IPv4

La figura 3.36 muestra el resultado de 'show ip ospf neighbor' con direccionamiento IPv4, realizado en el router Quito, donde se tiene información de los routers vecinos, con estado FULL, indicando conectividad sin problema.

```

QUITO#show ip ospf neighbor
Neighbor ID    Pri  State           Dead Time   Address        Interface
200.0.10.49    1    FULL/DR         00:00:34   200.0.10.26   GigabitEthernet5/0
200.0.10.41    1    FULL/DR         00:00:38   200.0.10.22   GigabitEthernet4/0
200.0.10.29    1    FULL/DR         00:00:31   200.0.10.18   GigabitEthernet3/0
200.0.10.13    1    FULL/BDR        00:00:37   200.0.10.13   GigabitEthernet1/0
200.0.10.13    1    FULL/BDR        00:00:36   200.0.10.9    GigabitEthernet0/0

```

Figura 3.36: Resultado Comando show ip ospf neighbor - router Quito - IPv4

#### IPv6

En el router Quito con IPv6, "show ipv6 neighbor" detalla los routers vecinos y se muestra en la figura 3.37, la versión OSPFv3, el ID del router y del proceso, de igual manera tenemos estado FULL conectividad.

```

QUITO#show ipv6 ospf neighbor

      OSPFv3 Router with ID (3.3.3.3) (Process ID 1)

Neighbor ID    Pri  State           Dead Time   Interface ID  Interface
8.8.8.8        1   FULL/DR         00:00:36   3             GigabitEthernet5/0
5.5.5.5        1   FULL/DR         00:00:37   4             GigabitEthernet4/0
4.4.4.4        1   FULL/DR         00:00:35   3             GigabitEthernet3/0
2.2.2.2        1   FULL/BDR        00:00:33   6             GigabitEthernet1/0
2.2.2.2        1   FULL/BDR        00:00:39   5             GigabitEthernet0/0
QUITO#

```

Figura 3.37: Resultado Comando show ipv6 neighbor - router Quito - IPv6

**Resumen del estado de las interfaces.** Para obtener información sobre el direccionamiento IP relacionado con OSPF y sus interfaces, se utilizan diferentes comandos según el protocolo de Internet utilizado.

En el caso del direccionamiento IPv4, el comando utilizado es ‘show ip ospf interface brief’, la figura 3.38 muestra resultado. Este comando proporciona los parámetros OSPF configurados en las interfaces del router Quito.

Para el direccionamiento IPv6, se utiliza show ipv6 ospf interface brief’, cuyo resultado muestra la figura 3.39. Este comando permite obtener información similar, pero específica para el protocolo IPv6.

Estos comandos y figuras brindan una visión detallada de los parámetros OSPF configurados en las interfaces del router Quito, tanto para IPv4 como para IPv6.

```

QUITO#show ip ospf interface brief
Interface      PID  Area          IP Address/Mask  Cost  State Nbrs F/C
Gi5/0         1    0             200.0.10.25/30   1     BDR   1/1
Gi4/0         1    0             200.0.10.21/30   1     BDR   1/1
Gi3/0         1    0             200.0.10.17/30   1     BDR   1/1
Gi1/0         1    0             200.0.10.14/30   1     DR    1/1
Gi0/0         1    0             200.0.10.10/30   1     DR    1/1
Gi2/0         1    0             192.168.10.1/24  1     DR    0/0
QUITO#

```

Figura 3.38: Resultado Comando show IP ospf interface brief - router Quito

```
QUITO#show ipv6 ospf interface brief
Interface    PID  Area    Intf ID  Cost  State Nbrs F/C
Gi5/0        1    0       8        1    BDR   1/1
Gi4/0        1    0       7        1    BDR   1/1
Gi3/0        1    0       6        1    BDR   1/1
Gi2/0        1    0       5        1    DR    0/0
Gi1/0        1    0       4        1    DR    1/1
Gi0/0        1    0       3        1    DR    1/1
QUITO#
```

Figura 3.39: Resultado Comando show IPv6 ospf interface brief - router Quito

**Rutas OSPF descubiertas.** Para visualizar únicamente las rutas descubiertas por OSPF, se utilizan comandos específicos en cada protocolo de Internet.

En el caso del direccionamiento IPv4, se utiliza ‘show ip route ospf’, cuyo resultado muestra la figura 3.40. Este comando permite obtener las rutas obtenidas a través de OSPF en el router Quito.

Por otro lado, para el direccionamiento IPv6, ‘show ipv6 route ospf’, como muestra la figura 3.41. Siendo posible de esta manera obtener las rutas descubiertas por OSPF específicamente para IPv6 en el router Quito.

Ambas validaciones se llevan a cabo en el router Quito y proporcionan información de rutas obtenidas mediante el protocolo OSPF en cada protocolo de la Internet.

```

QUITC#show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O 192.168.20.0/24 [110/4] via 200.0.10.22, 00:22:50, GigabitEthernet4/0
   200.0.10.0/24 is variably subnetted, 27 subnets, 2 masks
O   200.0.10.0/30 [110/2] via 200.0.10.13, 00:23:10, GigabitEthernet1/0
     [110/2] via 200.0.10.9, 00:23:10, GigabitEthernet0/0
O   200.0.10.4/30 [110/2] via 200.0.10.13, 00:23:10, GigabitEthernet1/0
     [110/2] via 200.0.10.9, 00:23:10, GigabitEthernet0/0
O   200.0.10.28/30 [110/2] via 200.0.10.22, 00:23:10, GigabitEthernet4/0
     [110/2] via 200.0.10.18, 00:23:10, GigabitEthernet3/0
O   200.0.10.32/30 [110/2] via 200.0.10.22, 00:23:10, GigabitEthernet4/0
O   200.0.10.36/30 [110/2] via 200.0.10.22, 00:23:00, GigabitEthernet4/0
O   200.0.10.40/30 [110/2] via 200.0.10.22, 00:23:10, GigabitEthernet4/0
O   200.0.10.44/30 [110/3] via 200.0.10.26, 00:23:10, GigabitEthernet5/0
     [110/3] via 200.0.10.22, 00:23:10, GigabitEthernet4/0
O   200.0.10.48/30 [110/2] via 200.0.10.26, 00:23:10, GigabitEthernet5/0
O   200.0.10.52/30 [110/3] via 200.0.10.22, 00:23:00, GigabitEthernet4/0
O   200.0.10.56/30 [110/3] via 200.0.10.22, 00:23:00, GigabitEthernet4/0
O   200.0.10.60/30 [110/3] via 200.0.10.22, 00:22:50, GigabitEthernet4/0
O   200.0.10.64/30 [110/3] via 200.0.10.22, 00:22:50, GigabitEthernet4/0
O   200.0.10.68/30 [110/3] via 200.0.10.26, 00:23:00, GigabitEthernet5/0
O   200.0.10.72/30 [110/4] via 200.0.10.22, 00:22:50, GigabitEthernet4/0
O   200.0.10.76/30 [110/4] via 200.0.10.22, 00:22:50, GigabitEthernet4/0
O   200.0.10.80/30 [110/4] via 200.0.10.26, 00:23:00, GigabitEthernet5/0
     [110/4] via 200.0.10.22, 00:22:50, GigabitEthernet4/0
O   200.0.10.84/30 [110/4] via 200.0.10.22, 00:22:50, GigabitEthernet4/0

```

Figura 3.40: Resultado Comando show IPv4 route OSPF - router Quito



```

QUITO#show ipv6 route ospf
IPv6 Routing Table - default - 33 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
        B - OSP, R - RIP, M - NHRP, I1 - ISIS L1
        I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
        EX - EIGRP external, ND - ND Default, NDP - ND Prefix, DCE - Destination
        NDR - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
        OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, I - IISP
O 2001:DB8:ABCD:1::/126 [110/2]
  via FE80::2, GigabitEthernet0/0
  via FE80::2, GigabitEthernet1/0
O 2001:DB8:ABCD:2::/126 [110/2]
  via FE80::2, GigabitEthernet0/0
  via FE80::2, GigabitEthernet1/0
O 2001:DB8:ABCD:6::/126 [110/2]
  via FE80::4, GigabitEthernet3/0
  via FE80::5, GigabitEthernet4/0
O 2001:DB8:ABCD:9::/126 [110/2]
  via FE80::5, GigabitEthernet4/0
O 2001:DB8:ABCD:A::/126 [110/3]
  via FE80::5, GigabitEthernet4/0
  via FE80::8, GigabitEthernet5/0
O 2001:DB8:ABCD:B::/126 [110/2]
  via FE80::8, GigabitEthernet5/0
O 2001:DB8:ABCD:C::/126 [110/2]
  via FE80::5, GigabitEthernet4/0
O 2001:DB8:ABCD:D::/126 [110/2]
  via FE80::5, GigabitEthernet4/0
O 2001:DB8:ABCD:E::/126 [110/3]
  via FE80::5, GigabitEthernet4/0
O 2001:DB8:ABCD:F::/126 [110/3]
  via FE80::5, GigabitEthernet4/0
O 2001:DB8:ABCD:10::/126 [110/4]
  via FE80::5, GigabitEthernet4/0
O 2001:DB8:ABCD:11::/126 [110/4]
  via FE80::5, GigabitEthernet4/0
O 2001:DB8:ABCD:12::/126 [110/3]
  via FE80::5, GigabitEthernet4/0
O 2001:DB8:ABCD:13::/126 [110/3]
  via FE80::5, GigabitEthernet4/0
O 2001:DB8:ABCD:14::/126 [110/3]
  via FE80::8, GigabitEthernet5/0
O 2001:DB8:ABCD:15::/126 [110/4]
  via FE80::5, GigabitEthernet4/0
  via FE80::8, GigabitEthernet5/0
O 2001:DB8:ABCD:16::/126 [110/4]
  via FE80::5, GigabitEthernet4/0
O 2003:DB8:ABCD:1::/64 [110/3]
  via FE80::2, GigabitEthernet1/0
  via FE80::2, GigabitEthernet0/0
O 2003:DB8:ABCD:3::/64 [110/4]
  via FE80::5, GigabitEthernet4/0
O 2003:DB8:ABCD:4::/64 [110/4]
  via FE80::8, GigabitEthernet5/0
  via FE80::5, GigabitEthernet4/0

```

Figura 3.41: Resultado Comando show IPv6 route OSPF - router Quito

### 3.6.5. Configuración protocolo de gestión SNMP

#### IPv4

Para direccionamiento IPv4, se utiliza SNMPv2 para acceder y configurar los routers de la topología. Esto se logra mediante la configuración de una comunidad de escritura y una comunidad de lectura. La figura 3.42 muestra

cómo se configuran estas comunidades para permitir el acceso respectivo a cada router de la topología utilizando SNMPv2.

```
QUITO#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
QUITO(config)#snmp-server community cedia RW
QUITO(config)#snmp-server community cedia1 R0
QUITO(config)#EXIT
QUITO#
```

Figura 3.42: Configuración de SNMP V2 - router Quito - IPv4

### IPv6

En este caso para configurar SNMPv3 se realizan además de la configuración básica, las configuraciones de seguridad como contraseña y usuario para ingreso, detallado en figura 3.43.

```
Milagro(config)#!snmp-configuracion
Milagro(config)# user sami tesis v3 auth sha 0301235040 priv des 03012350
Milagro(config)#snmp-server contact Samira
Milagro(config)#snmp-server location LMilagro
Milagro(config)#exit
Milagro#
*Apr 15 14:25:50.903: %SYS-5-CONFIG_I: Configured from console by console
Milagro#
```

Figura 3.43: Configuración de SNMP V3 - IPv6

### Comprobación de Protocolo SNMP

En cada router, con el comando `show snmp user`, se puede mostrar a las configuraciones de SNMP ingresadas, en la figura 3.44 con direccionamiento IPv4 y en la figura 3.45 con direccionamiento IPv6. En ellas se detalla usuario, protocolo de autenticación, protocolo de privacidad y grupo.

```
snmp-server group tesis v3 priv
snmp-server location LMilagro
snmp-server contact Samira
```

Figura 3.44: Verificación de la configuración SNMP - IPv4

```
Milagro#show snmp user
User name: sami
Engine ID: 800000090300CA0C8C6C0006
storage-type: nonvolatile      active
Authentication Protocol: SHA
Privacy Protocol: DES
Group-name: tesis
```

Figura 3.45: Verificación de la configuración SNMP - IPv6

### 3.6.6. Configuración de los NMS en las máquinas virtuales: IPv4

En cada máquina virtual, se instaló IReasoning y se utilizó SNMPv2 para realizar el monitoreo. En la figura 3.46, con direccionamiento IPv4, se muestra el monitoreo realizado desde la máquina virtual de Tulcán hacia el router de Quevedo. Durante el monitoreo, se gestionaron varios OIDs para obtener información específica del router. Además, en la figura 3.47 se presentan los paquetes capturados mediante el uso de Wireshark. Estos paquetes reflejan intercambio de información y la comunicación ocurrida durante el monitoreo utilizando SNMPv2 con direccionamiento IPv4.

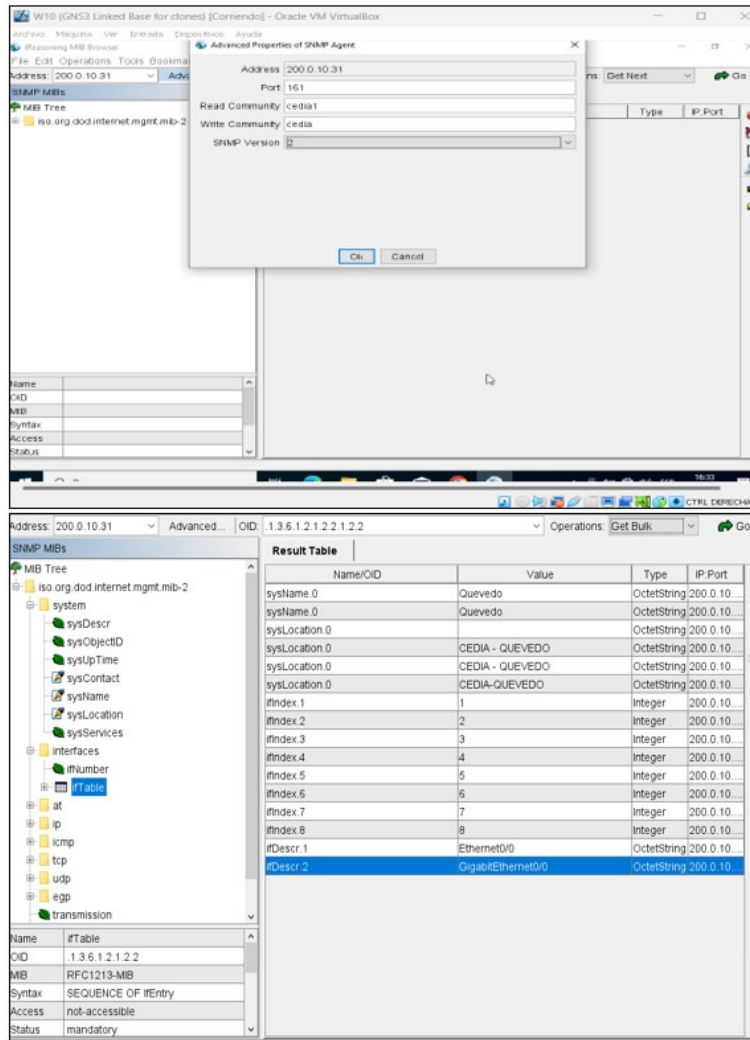


Figura 3.46: Configuración del agente SNMPv2 y gestión de OID's desde la MV de Tulcán hacia el router de Quevedo

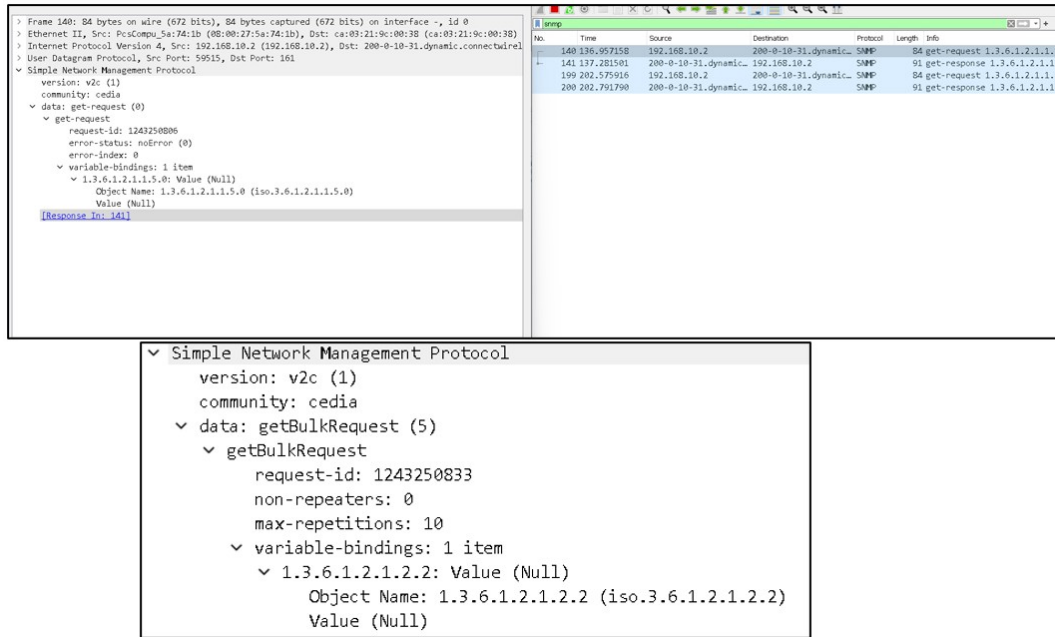


Figura 3.47: Captura de paquetes mediante el uso de Wireshark SNMP v2 -IPv4

Es importante destacar que IReasoning solo admite SNMPv2 y no SNMPv3, como se puede observar en la figura 3.48. Debido a esta limitación, fue necesario instalar otro navegador (o herramienta) para aprovechar todo el potencial del protocolo SNMP en el contexto de IPv6. Con esta nueva herramienta, se logró realizar el monitoreo y gestión de dispositivos utilizando SNMPv3 y direccionamiento IPv6, permitiendo una mayor funcionalidad y seguridad en la administración de las redes.

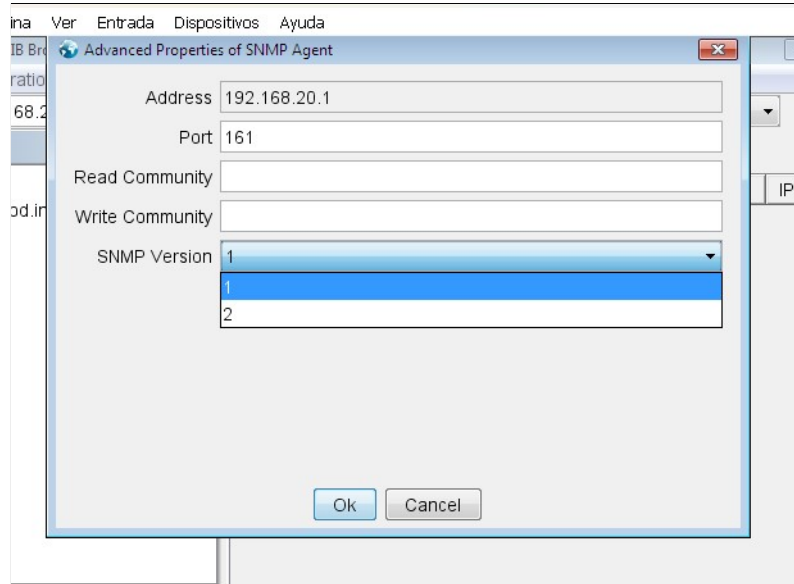


Figura 3.48: Soporte de Versiones IREASONING

### 3.6.7. Configuración de los NMS en las MV: IPv6

Se utilizó el ManageEngine MibBrowser Free, una herramienta que brinda soporte para SNMPv3. Esta elección permitió seleccionar la versión SNMPv3 en las máquinas virtuales, como muestra la figura 3.49. Además, el ManageEngine MibBrowser Free facilita la configuración de usuarios, contraseñas y parámetros de autenticación, detallado en la figura 3.50.

Estas características, permitió aprovechar todas las capacidades de SNMPv3, incluyendo mejoras en seguridad y autenticación, en las operaciones de gestión y monitoreo de los dispositivos conectados, tanto en el contexto de direccionamiento IPv4 como en IPv6.

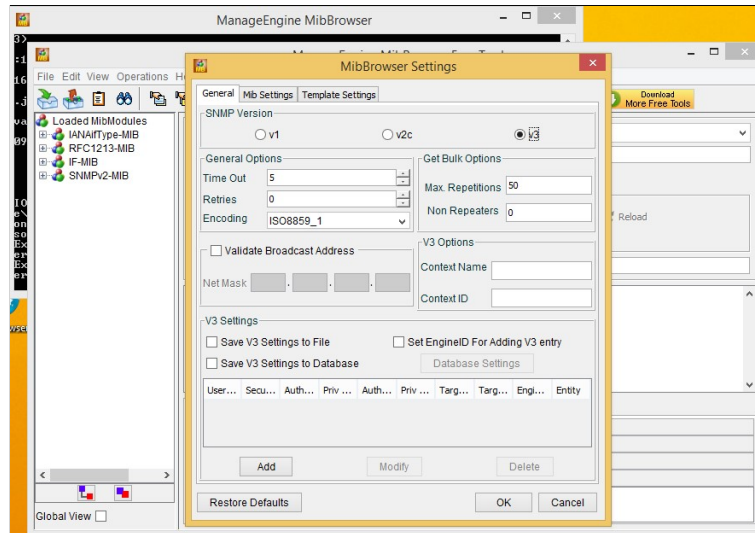


Figura 3.49: Configuración de Versión SNMP v3 - IPv6

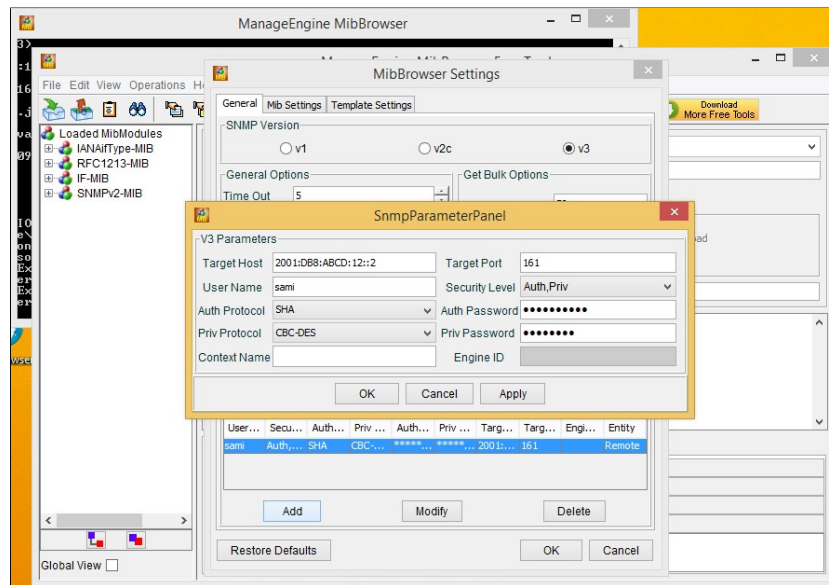


Figura 3.50: Autenticación del Usuario SNMP v3 - IPv6

En este capítulo de trabajo de titulación se sentaron las bases teóricas y prácticas necesarias para comprender y desarrollar una red avanzada como la

de CEDIA Ecuador. A través de la investigación, simulaciones y emulaciones, se ha logrado adquirir conocimientos y habilidades valiosas en el ámbito de las redes WAN, sentando así las bases para para lograr los resultados del Capítulo 4.



## Capítulo 4

# Resultados

A continuación se detallan los resultados con su respectivo análisis de los escenarios desarrollados con la metodología. Primero se detallan los resultados obtenidos en las simulaciones con Packet Tracer. Luego se presentan los resultados de la emulación en GNS3.

### 4.1. Simulación en Packet Tracer - PKT

Luego de creada la topología y realizar todas las configuraciones con direccionamiento IPv4 e IPv6 en las herramientas explicadas en el capítulo 3, se realizaron las pruebas de conectividad, el envío de paquetes de los mensajes del Protocolo OSPF y las Pruebas de gestión -PKT.

#### 4.1.1. Pruebas de conectividad -PKT

Se realizó una prueba de conectividad utilizando el comando ping desde el PC Guayaquil, que corresponde al router de Guayaquil, hacia el PC Quito, que corresponde al router de Quito, bajo el direccionamiento IPv6. La figura [4.1](#) muestra los resultados obtenidos.

```

Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 2003:DB8:ABCD:2::2

Pinging 2003:DB8:ABCD:2::2 with 32 bytes of data:

Reply from 2003:DB8:ABCD:2::2: bytes=32 time<1ms TTL=125
Reply from 2003:DB8:ABCD:2::2: bytes=32 time<1ms TTL=125
Reply from 2003:DB8:ABCD:2::2: bytes=32 time<1ms TTL=125
Reply from 2003:DB8:ABCD:2::2: bytes=32 time<1ms TTL=125

Ping statistics for 2003:DB8:ABCD:2::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

```

Figura 4.1: Conectividad entre la PC Guayaquil a la PC Quito

Luego de validar las tablas de enrutamiento y el direccionamiento en todas las interfaces se comprueba la conectividad entre todos los routers y pruebas de ping entre PCs, para IPv4 como muestra la figura 4.2 y para IPv6 la figura 4.3.

The screenshot displays the Packet Tracer simulation environment. On the left, a geographical map of Ecuador is shown with various regions color-coded (purple, yellow, blue, green, pink). A network topology is overlaid on the map, with routers and PCs connected by lines. On the right, the 'Simulation Panel' is visible, featuring an 'Event List' table and 'Play Controls'.

Vis	Time(sec)	Last Device	All Device	Type
Visible	0:00:00	Cuenca	Laja	OSPF
Visible	0:00:00	-	Santa Elena	OSPF
Visible	0:00:00	Santa Elena	GUARAOUIL	OSPF
Visible	0:00:00	-	Laja	OSPF
Visible	0:00:00	Milagro	GUARAOUIL	OSPF
Visible	0:00:00	-	GUARAOUIL	OSPF
Visible	0:00:00	-	GUARAOUIL	OSPF
Visible	0:00:00	-	GUARAOUIL	OSPF
Visible	0:00:00	Morona	GUARAOUIL	OSPF
Visible	0:00:00	-	GUARAOUIL	OSPF
Visible	0:00:00	Putumayo	Morona	OSPF
Visible	0:00:00	Putumayo	Morona	OSPF
Visible	0:00:00	Putumayo	Santa Elena	OSPF
Visible	0:00:00	-	Putumayo	OSPF
Visible	0:00:00	Tulcan	Baños	OSPF
Visible	0:00:00	-	GUARAOUIL	OSPF
Visible	0:00:00	Morona	Ovando	OSPF
Visible	0:00:00	-	Baños	OSPF

Below the table, the 'Simulation Panel' includes 'Play Controls' (Start, Stop, Reset buttons) and 'Event List Filters - Visible Events' (OSPF) with 'Edit Filters' and 'Show All/None' buttons.

Figura 4.2: Conectividad entre Routers IPv4.

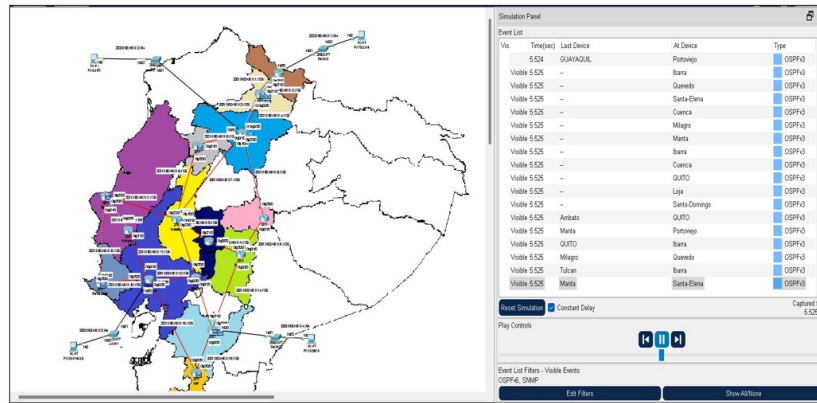


Figura 4.3: Conectividad entre Routers IPv6.

### 4.1.2. Análisis de tráfico de los mensajes del Protocolo OSPF

#### Paquete Tipo 1: Hello

La figura 4.4, muestra el contenido del paquete saludo (Hello), sus detalles corresponden a lo indicado en el apartado teórico en el que se describieron los 5 tipos de paquetes OSPF.

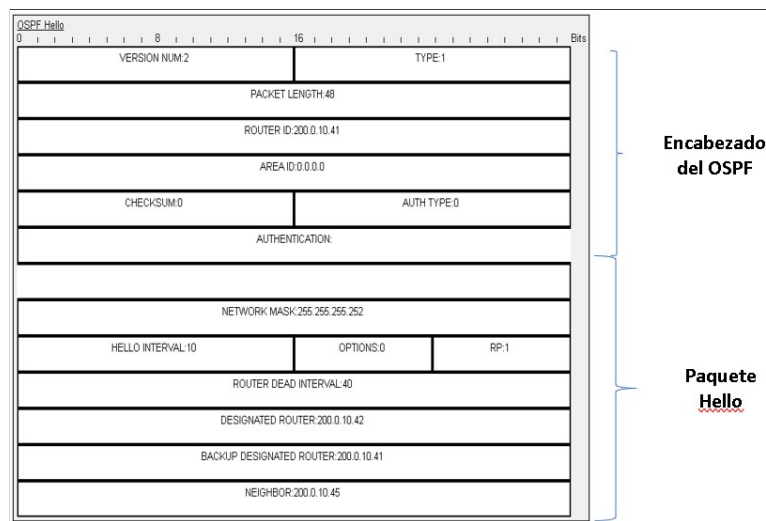


Figura 4.4: Encabezado OSPF IPv4.

En la figura 4.5, se detalla el contenido del paquete hello con direccionamiento IPv6, en el cual se distingue el protocolo de la versión. Para IPv6, se utiliza OSPFv3. Además, se encuentra el campo Network Mask, el cual incluye la Interface ID que permite identificar la interfaz de origen del router.

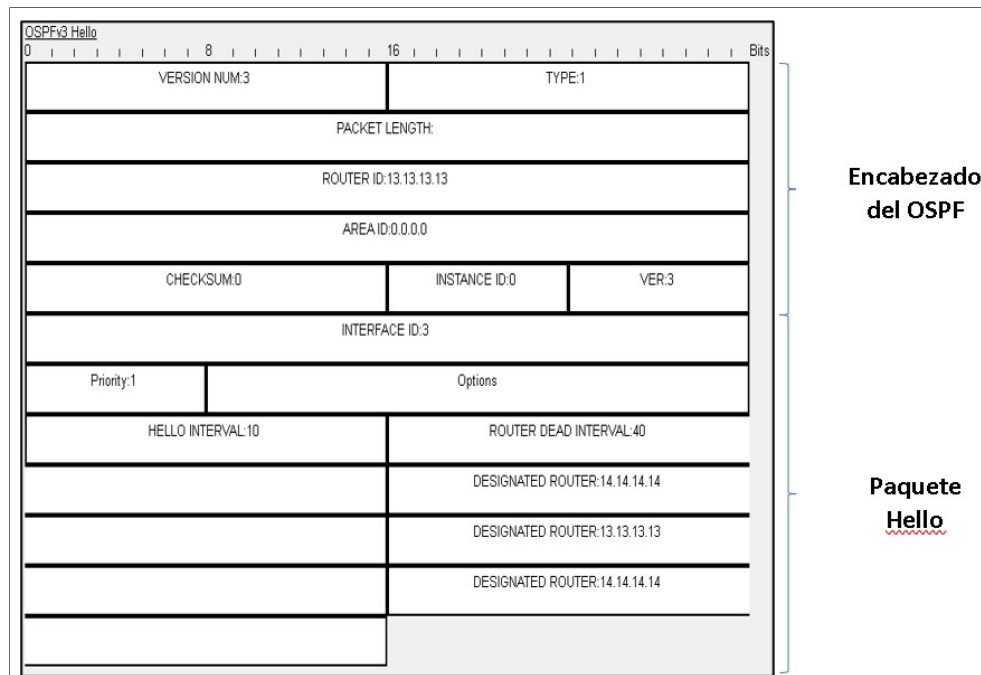


Figura 4.5: Paquete Hello OSPFv3.

### Paquete tipo 2: Link State Update

Son la actualización de los estados de enlaces, tanto en IPv4 como en IPv6, se utilizan los mismos campos de versión, tipo, tamaño de paquete, ID de área, checksum, tipo y autenticación. Además, ambos protocolos emplean paquetes LSA (Link State Advertisement) para intercambiar información sobre la topología de la red. La figura. 4.6, permite mostrar esta información.

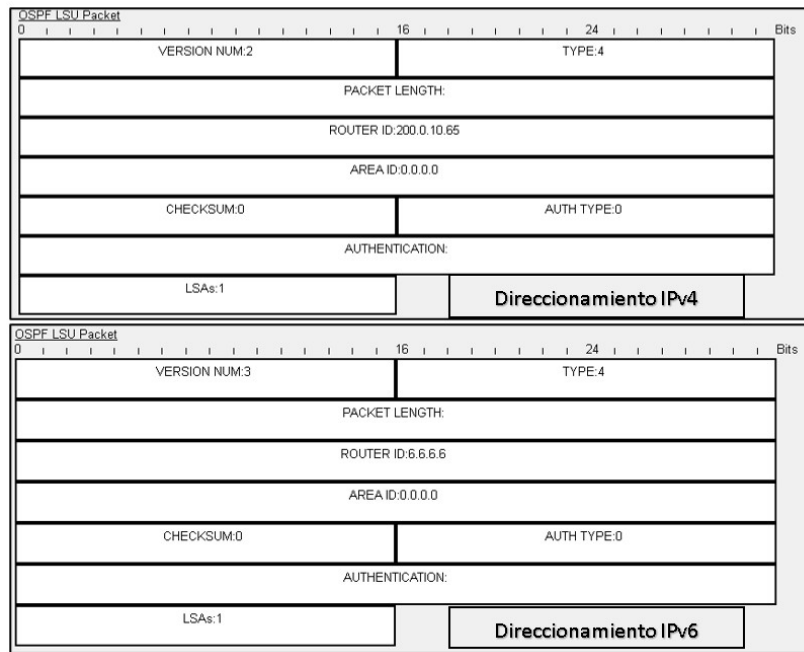


Figura 4.6: Resultado de Paquete Link State Update IPv4 e IPv6.

Siguiendo el mismo procedimiento, con el simulador, la figura 4.7, muestra como se puede obtener la captura de paquetes e ir verificando como va trasportándose el paquete capa por capa, con OSPFv3.

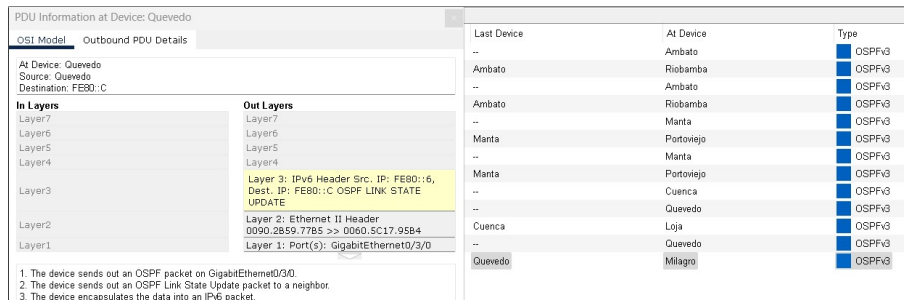


Figura 4.7: Obtención de paquetes OSPFv3 - Simulador

### 4.1.3. Pruebas de gestión -PKT

#### Verificación de Protocolo SNMP

Para monitorear el Router Tulcán desde el PC que está conectado a él en Packet Tracer, se utiliza el programa MIB Browser. Si el router Guayaquil no tiene un nombre asignado, se puede hacer esto ingresando al árbol de MIBS. Durante la simulación, se pueden visualizar los paquetes que se generan. Es importante destacar que en este caso, debido a las limitaciones del simulador, sólo es posible utilizar la versión 2 del protocolo SNMP.

#### Obtención de nombre

La figura 4.8 muestra el proceso de obtener nombre del router que representa a la Provincia de Guayas con la operación GET (1), marcado con círculo amarillo, el cual se encuentra como "Route", antes del cambio. Este se configura indicando la ip address ya sea ipv4 o ipv6 en el apartado *avanzado*, e ingresamos los datos que configuramos en cada router y escogemos la versión 2, (ya que en Packet Tracer, la v3 no funciona).

#### Cambio de nombre

Para cambiarla ejecutamos la operación SET (2), marcado con círculo amarillo, donde ingresamos el valor que es un OcteString y le cambiamos por GUAYAQUIL y finalmente tenemos cambiado el valor del nombre del router (3), marcado con círculo amarillo.

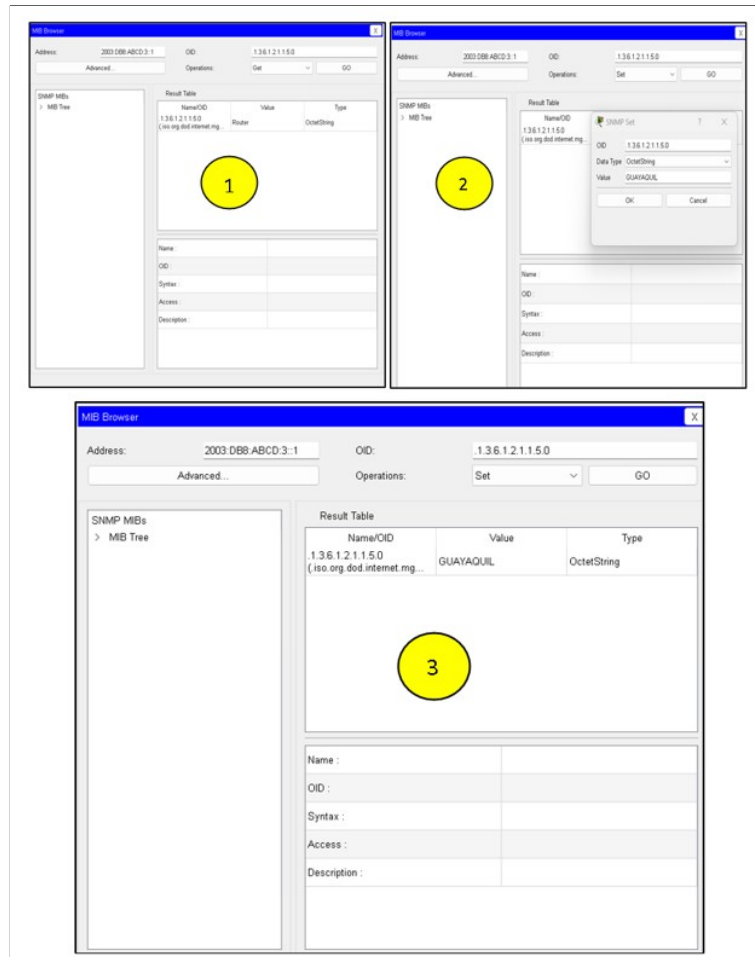


Figura 4.8: Visualización de la Obtención de Objetos OID.

La figura 4.9, muestra los paquetes SNMP generados cuando se monitorea un router, en este caso cambio de nombre de Router Guayaquil.



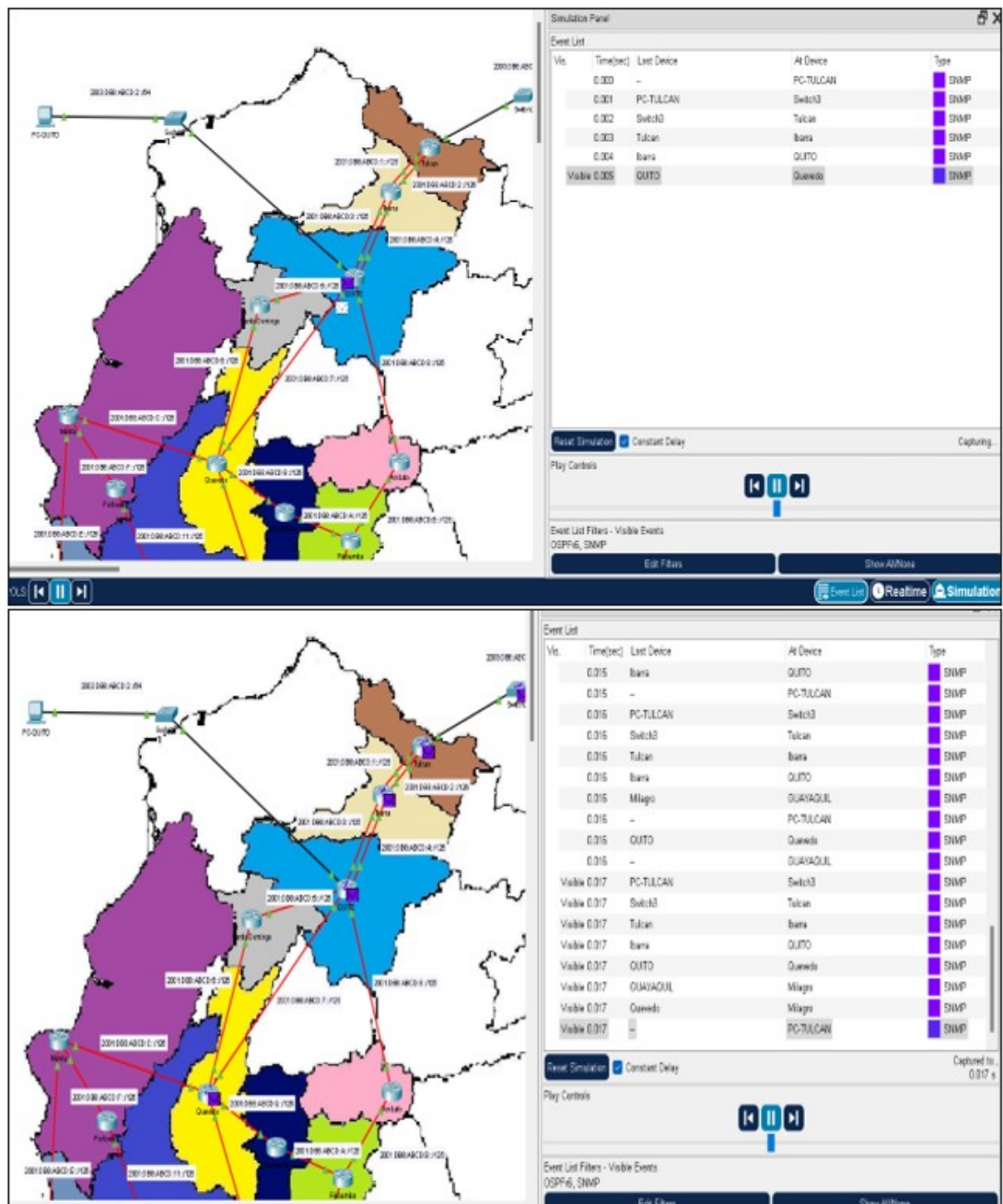


Figura 4.9: Captura de Paquetes SNMP.

La gestión del router Cuenca, se realizó desde el PC de Quito (NMS). Para lo cual se seleccionaron variables a solicitar o cambiar. Por ejemplo, para el caso de requerir **SOLICITAR EL NOMBRE** del router vía remota (MIB), se usa la operación **Get** y el OID "**sysName 1.3.6.1.2.1.1.5.0**". Estos detalles muestra la figura 4.10.

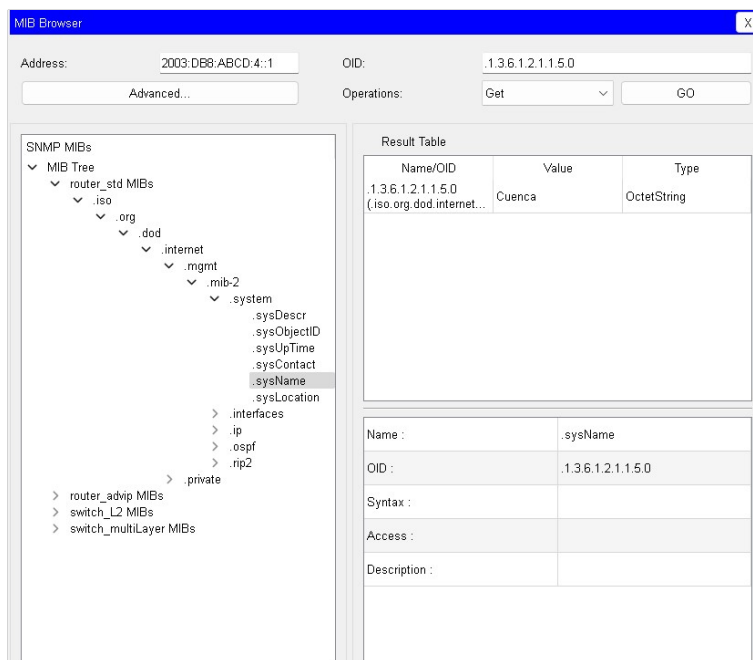


Figura 4.10: Nombre del router solicitado vía el MIB Browser

Para el caso de querer **ASIGNAR LA LOCALIZACIÓN** del router vía remota, se usa la operación **Set** y el OID "**SysLocation 1.3.6.1.2.1.1.6.**" para colocar datos de la ubicación física de un router como indica la figura 4.11, donde se detalla la gestión remota de localización física del router Cuenca.

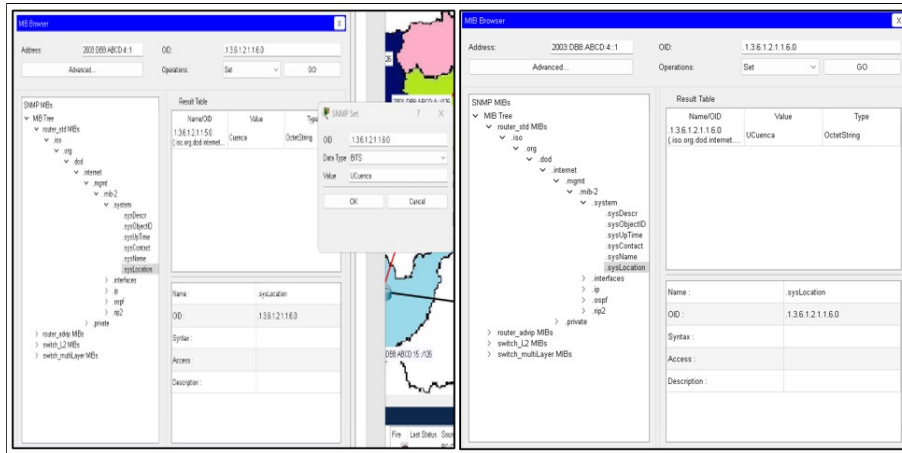


Figura 4.11: Gestión remota de la localización física del router Cuenca

Para obtener la **TABLA DE INTERFACES** del router vía remota, se usa la operación **Get Bulk** y el OID **ifTable 1.3.6.1.2.1.2.2**, como se muestra en la figura 4.12.

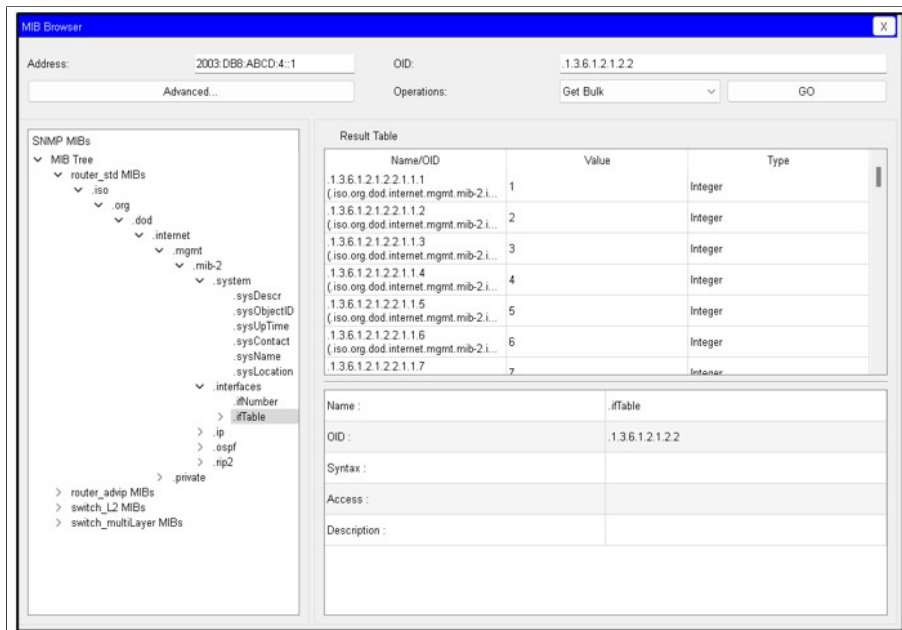


Figura 4.12: Tabla de interfaces, indicando las 7 disponibles

Durante las simulaciones de conectividad y gestión, Cisco Packet Tracer consume pocos recursos de la máquina real, aproximadamente un 26 % de la capacidad de la CPU y un 56 % de la memoria RAM total, como muestra la figura 4.13.

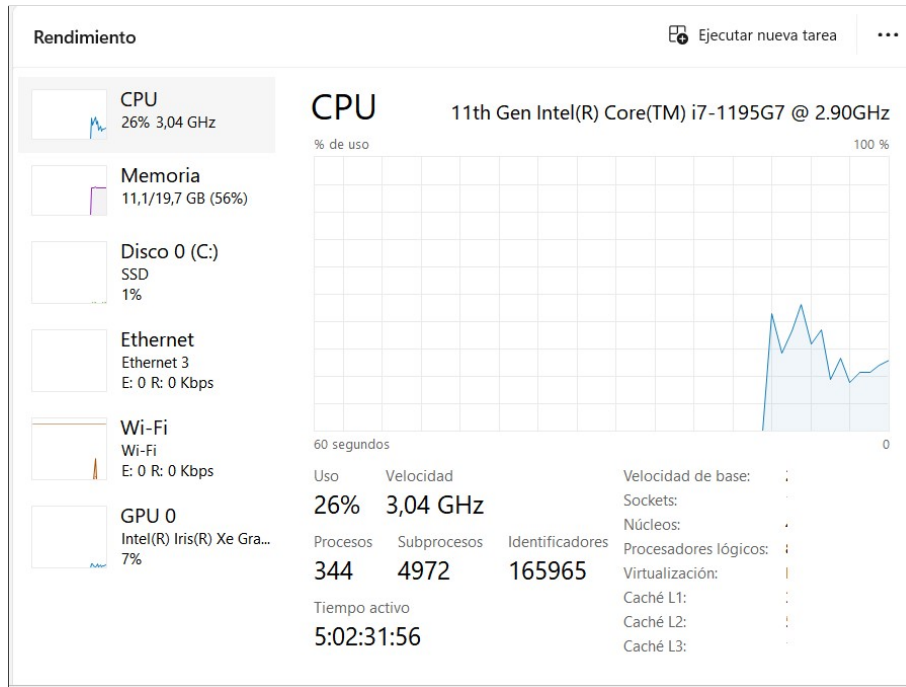


Figura 4.13: Uso de recursos para la simulación en Packet Tracer

Con el simulador Cisco Packet Tracer se realizaron pruebas de conectividad y gestión en la red avanzada CEDIA, tanto en IPv4 como en IPv6. No obstante, existen dos limitaciones principales. En primer lugar, el simulador no dispone de routers de backbone específicos, por lo que fue necesario utilizar routers genéricos, lo cual impide una réplica exacta de la infraestructura de red de CEDIA, que es nuestro objetivo principal.

Además, no es posible replicar las características de seguridad proporcionadas por SNMPv3, ya que el simulador no es compatible con esta versión del protocolo. Por lo tanto, este proyecto se llevó a cabo utilizando SNMPv2. Es importante mencionar que se realizaron pruebas adicionales de gestión, como la obtención de las tablas de enrutamiento de los enrutadores mediante cualquier NMS, así como obtener detalles de cada interfaz, entre otros. Sin embargo, debido a la extensión de las pruebas, se

omiten en este informe.

Las pruebas presentadas para gestionar el router Cuenca también se realizaron para gestionar a cada uno de los 15 routers que conforman CEDIA, y la gestión se puede realizar desde cualquiera de los NMS.

## 4.2. Emulación en *Graphic Network Simulator-3*

Para la emulación en *Graphic Network Simulator-3*, se utilizó una topología física con IPv4, tal como muestra la figura 3.23. En el escenario donde todos los routers se encuentran apagados, la emulación consume aproximadamente un 1.3% de la capacidad de la CPU y un 75.5% de la memoria RAM total de la máquina real, como muestra la figura 4.14.

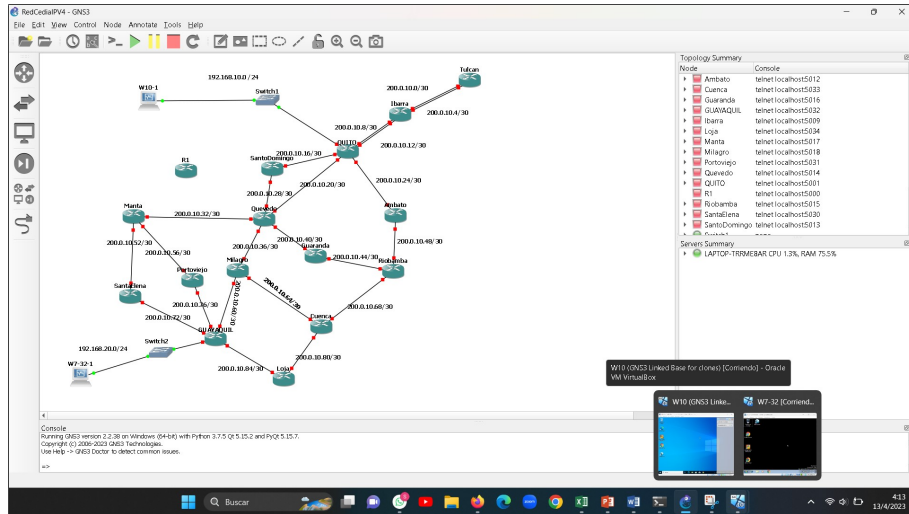


Figura 4.14: Topología IPv4 con los 15 routers apagados - GNS3

Para la topología basada en IPv6, se utilizó la figura 3.24. Durante el escenario en el que los routers están apagados, se observó un consumo de recursos de aproximadamente un 5.3% de la capacidad de la CPU y un 73.6% de la memoria RAM total, la figura 4.15 lo indica.

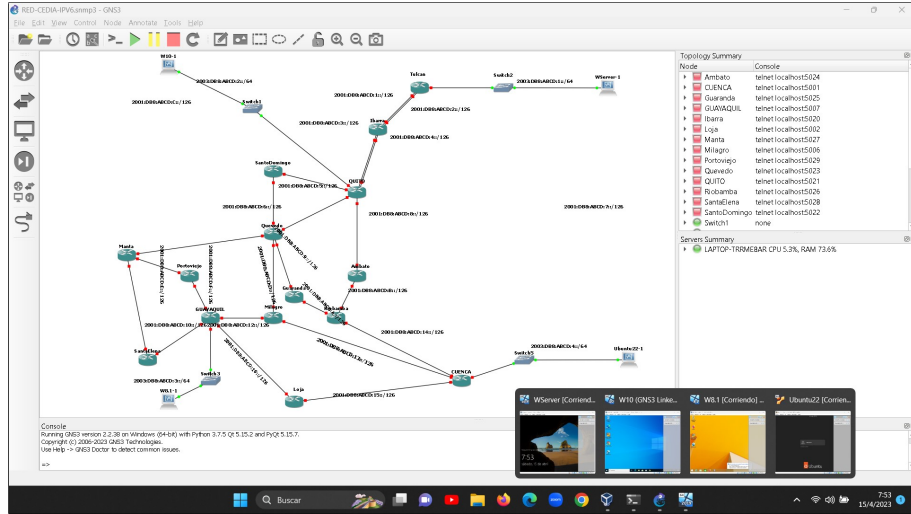


Figura 4.15: Topología IPv6 con los 15 routers apagados -GNS3

Bajo la topología IPv4, cuando los routers y las máquinas virtuales (VM) están encendidos y en funcionamiento, se observa un consumo de recursos del 100% de la capacidad de la CPU y del 93.9% de la memoria RAM total, como muestra la figura 4.16.

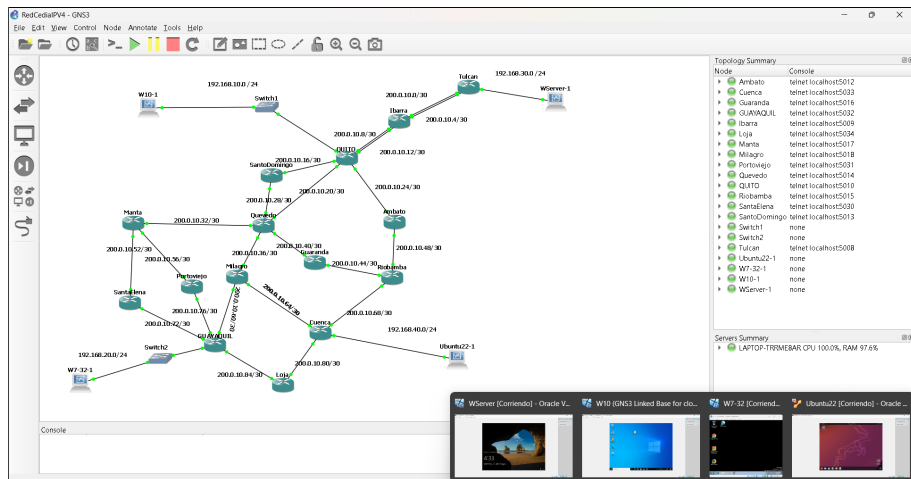


Figura 4.16: Topología IPv4 con los 15 routers y las 4 VM funcionando -GNS3

Bajo la topología IPv6, cuando los routers y VM están encendidos y en funcionamiento, se observa un consumo de recursos del 100 % de la capacidad de la CPU y del 97.3 % de la memoria RAM total, la figura 4.17 lo demuestra.

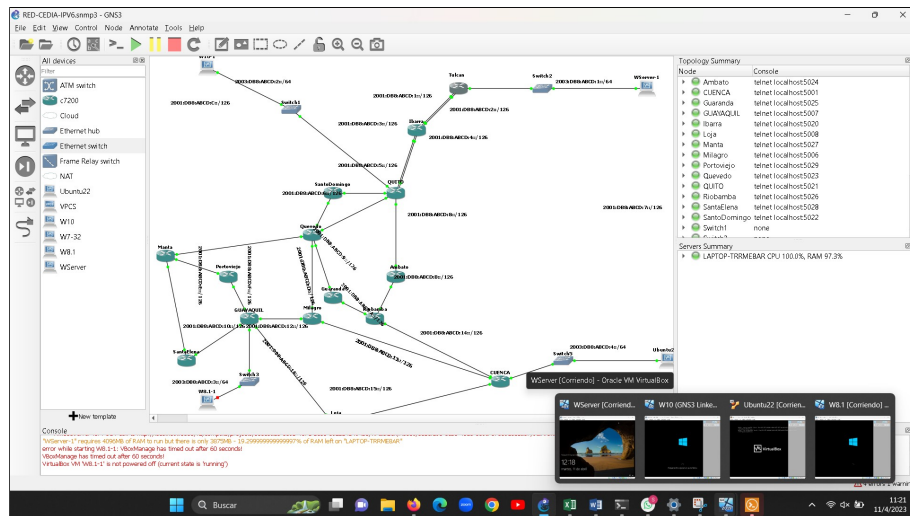


Figura 4.17: Topología IPv6 con los 15 routers y las 4 VM funcionando -GNS3

#### 4.2.1. Pruebas de conectividad - GNS3

Durante las pruebas realizadas, se pudo comprobar el correcto funcionamiento del enrutamiento OSPFv3, obteniendo para verificar la tabla de enrutamiento con la presencia de todas las redes de CEDIA. Para ello, se utilizó `show ipv6 route` en el enrutador Quito, como detalla la figura 4.18. El comando "`show ipv6 route`" permite verificar el enrutamiento en el router de Tulcán, como detalla la figura 4.19.



```

QUITO#show ipv6 route
IPv6 Routing Table - default - 13 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
R - RIP, R - RIPv6, M - OSPF, H - ISIS
I1 - ISIS L1, I4 - ISIS Interarea, I5 - ISIS summary, O - OSPF
EX - OSPF external, ND - ND Default, ND - ND Prefix, OCE - Destination
Nbr - neighbor, O - OSPF Intra, OI - OSPF Inter, OEI - OSPF ext 1
OEO - OSPF ext 2, ONO - OSPF NGA ext 1, ONO - OSPF NGA ext 2, I - ISIS
0/0:0001:0001:ARCD:0::/126 [110/2]
  via FE80::1, GigabitEthernet0/0
  via FE80::1, GigabitEthernet1/0
0/0:0001:0001:ARCD:0::/126 [110/1]
  via FE80::1, GigabitEthernet0/0
  via FE80::1, GigabitEthernet1/0
0/0:0001:0001:ARCD:0::/126 [0/0]
  via GigabitEthernet0/0, directly connected
0/0:0001:0001:ARCD:0::/126 [0/0]
  via GigabitEthernet1/0, receive
0/0:0001:0001:ARCD:0::/126 [0/0]
  via GigabitEthernet1/0, directly connected
0/0:0001:0001:ARCD:0::/126 [0/0]
  via GigabitEthernet1/0, receive
0/0:0001:0001:ARCD:0::/126 [0/0]
  via GigabitEthernet1/0, receive
0/0:0001:0001:ARCD:0::/126 [0/0]
  via GigabitEthernet1/0, directly connected
0/0:0001:0001:ARCD:0::/126 [0/0]
  via GigabitEthernet1/0, receive
0/0:0001:0001:ARCD:0::/126 [110/1]
  via FE80::1, GigabitEthernet0/0
  via FE80::1, GigabitEthernet1/0
0/0:0001:0001:ARCD:0::/126 [0/0]
  via GigabitEthernet0/0, directly connected
0/0:0001:ARCD:0::/126 [0/0]
  via GigabitEthernet0/0, receive
0/0:0001:ARCD:0::/126 [0/0]
  via GigabitEthernet1/0, directly connected
0/0:0001:ARCD:0::/126 [0/0]
  via GigabitEthernet1/0, receive
0/0:0001:ARCD:0::/126 [110/1]
  via FE80::1, GigabitEthernet0/0
  via FE80::1, GigabitEthernet1/0
0/0:0001:ARCD:0::/126 [110/1]
  via FE80::1, GigabitEthernet0/0
  via FE80::1, GigabitEthernet1/0
0/0:0001:ARCD:0::/126 [110/1]
  via FE80::1, GigabitEthernet0/0
  via FE80::1, GigabitEthernet1/0
0/0:0001:ARCD:0::/126 [110/1]
  via FE80::1, GigabitEthernet0/0
  via FE80::1, GigabitEthernet1/0
0/0:0001:ARCD:0::/126 [110/3]
  via FE80::1, GigabitEthernet0/0
0/0:0001:ARCD:0::/126 [110/3]
  via FE80::1, GigabitEthernet0/0
  -More-

```

Figura 4.18: Tabla de enrutamiento del router Quito - IPv6

```

Tulcan#show ipv6 route
IPv6 Routing Table - 24 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       ND - ND Default, NDP - ND Prefix, DCE - Destination, NDR - Redirect
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C 2001:DB8:ABCD:1::/126 [0/0]
   via GigabitEthernet0/0/0, directly connected
L 2001:DB8:ABCD:1::1/128 [0/0]
   via GigabitEthernet0/0/0, receive
C 2001:DB8:ABCD:2::/126 [0/0]
   via GigabitEthernet0/1/0, directly connected
L 2001:DB8:ABCD:2::1/128 [0/0]
   via GigabitEthernet0/1/0, receive
O 2001:DB8:ABCD:3::/126 [110/2]
   via FE80::2, GigabitEthernet0/0/0
O 2001:DB8:ABCD:4::/126 [110/2]
   via FE80::2, GigabitEthernet0/0/0
O 2001:DB8:ABCD:5::/126 [110/3]
   via FE80::2, GigabitEthernet0/0/0
O 2001:DB8:ABCD:6::/126 [110/4]
   via FE80::2, GigabitEthernet0/0/0
O 2001:DB8:ABCD:8::/126 [110/3]
   via FE80::2, GigabitEthernet0/0/0
O 2001:DB8:ABCD:9::/126 [110/4]
   via FE80::2, GigabitEthernet0/0/0
O 2001:DB8:ABCD:A::/126 [110/5]
   via FE80::2, GigabitEthernet0/0/0
O 2001:DB8:ABCD:C::/126 [110/4]
   via FE80::2, GigabitEthernet0/0/0
O 2001:DB8:ABCD:D::/126 [110/4]
   via FE80::2, GigabitEthernet0/0/0
O 2001:DB8:ABCD:E::/126 [110/5]
   via FE80::2, GigabitEthernet0/0/0
O 2001:DB8:ABCD:F::/126 [110/5]
   via FE80::2, GigabitEthernet0/0/0
O 2001:DB8:ABCD:14::/126 [110/5]
   via FE80::2, GigabitEthernet0/0/0
O 2001:DB8:ABCD:15::/126 [110/6]
   via FE80::2, GigabitEthernet0/0/0
O 2001:DB8:ABCD:16::/126 [110/6]
   via FE80::2, GigabitEthernet0/0/0
C 2003:DB8:ABCD:1::/64 [0/0]
   via FastEthernet0/0, directly connected
L 2003:DB8:ABCD:1::1/128 [0/0]
   via FastEthernet0/0, receive
O 2003:DB8:ABCD:2::/64 [110/3]

```

Figura 4.19: Tabla de enrutamiento del router Tulcan - IPv6

### 4.2.2. Captura de paquetes OSPF - Wireshark

Se realizó con la herramienta Wireshark el análisis de paquetes OSPF. La figura 4.20 detalla cada paquete OSPF capturado durante la emulación en IPv4, mientras que la figura 4.21 con direccionamiento IPv6 muestra paquetes OSPF capturados durante la emulación.

```

Frame 28: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface -, id 0
Ethernet II, Src: ca:02:04:7c:00:08 (ca:02:04:7c:00:08), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
Internet Protocol Version 4, Src: 200-0-10-2.dynamic.connectwireless.net.br (200.0.10.2), Dst: ospf-all.mcast.net (224.0.0.5)
Open Shortest Path First
  OSPF Header
    Version: 2
    Message Type: Hello Packet (1)
    Packet Length: 48
    Source OSPF Router: 200-0-10-13.dynamic.connectwireless.net.br (200.0.10.13)
    Area ID: 0.0.0.0 (0.0.0.0) (Backbone)
    Checksum: 0xa386 [correct]
    Auth Type: Null (0)
    Auth Data (none): 0000000000000000
  OSPF Hello Packet
    Network Mask: 255.255.255.252
    Hello Interval [sec]: 10
    Options: 0x12, (L) LLS Data block, (E) External Routing
    0... .. = DN: Not set
    .0... .. = D: Not set
    ..0... .. = (DC) Demand Circuits: Not supported
    ...1... .. = (L) LLS Data block: Present
    ....0... .. = (N) NSSA: Not supported
    ....0... .. = (MC) Multicast: Not capable
    ....1... .. = (E) External Routing: Capable
    ....0... .. = (MT) Multi-Topology Routing: No
    Router Priority: 1
    Router Dead Interval [sec]: 40
    Designated Router: 200-0-10-2.dynamic.connectwireless.net.br (200.0.10.2)
    Backup Designated Router: 200-0-10-1.dynamic.connectwireless.net.br (200.0.10.1)
    Active Neighbor: 200-0-10-5.dynamic.connectwireless.net.br (200.0.10.5)
  OSPF LLS Data Block
    Checksum: 0xffff6
    LLS Data Length: 12 bytes
    > Extended options TLV
  
```

Figura 4.20: Detalles de los paquetes OSPF bajo IPv4 - Wireshark

```
> Frame 24: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface -, id 0
> Ethernet II, Src: ca:02:32:34:00:08 (ca:02:32:34:00:08), Dst: IPv6mcast_05 (33:33:00:00:00:05)
> Internet Protocol Version 6, Src: fe80::2 (fe80::2), Dst: ff02::5 (ff02::5)
▼ Open Shortest Path First
  ▼ OSPF Header
    Version: 3
    Message Type: Hello Packet (1)
    Packet Length: 40
    Source OSPF Router: 2.2.2.2 (2.2.2.2)
    Area ID: 0.0.0.0 (0.0.0.0) (Backbone)
    Checksum: 0xf176 [correct]
    Instance ID: IPv6 unicast AF (0)
    Reserved: 00
  ▼ OSPF Hello Packet
    Interface ID: 3
    Router Priority: 1
  > Options: 0x000013, R, E, V6
    Hello Interval [sec]: 10
    Router Dead Interval [sec]: 40
    Designated Router: 2.2.2.2 (2.2.2.2)
    Backup Designated Router: one.one.one.one (1.1.1.1)
    Active Neighbor: one.one.one.one (1.1.1.1)
```

Figura 4.21: Detalles de los paquetes OSPF bajo IPv6 - Wireshark

En el emulador GNS3, es posible visualizar una mayor cantidad de paquetes en comparación con Packet Tracer, debido a que se trabaja en un entorno con máquinas virtuales y se utiliza la herramienta Wireshark, como se detalla en la figura [4.22](#).

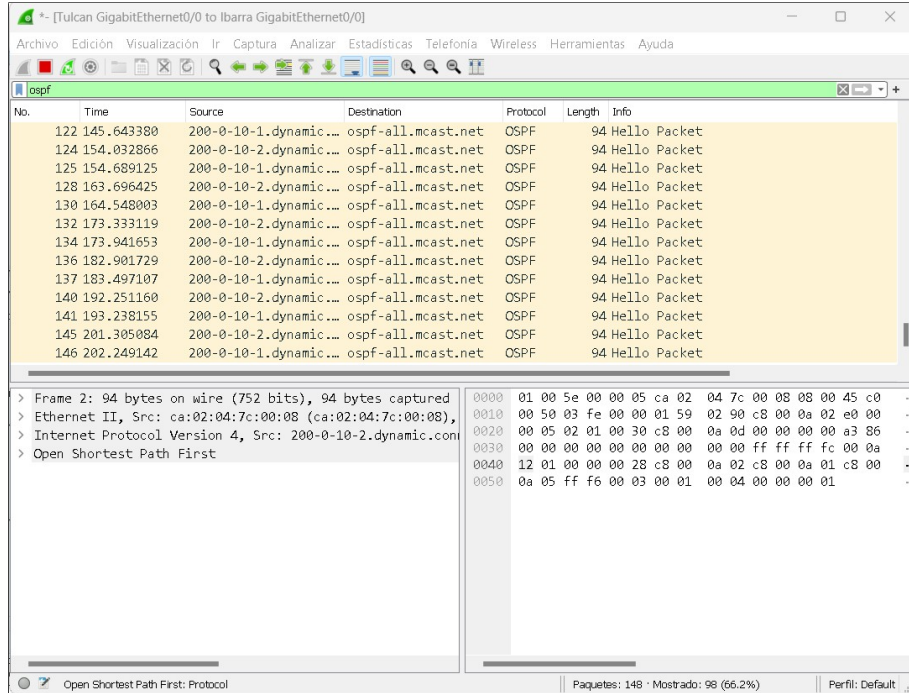


Figura 4.22: Visualización Wireshark - Paquetes OSPF

Wireshark permite monitorear y visualizar los tipos de paquetes OSPF que tenemos:

Tipo 1: Hello

Tipo 2: *Database Description (DBD)*

Tipo 3: *Link-State Request (LSR)*

Tipo 4: *Link-State Update (LSU)*

Tipo 5: *Link-State Acknowledgement (LSAck)*

A continuación, se describen los cinco tipos de paquetes OSPF en el emulador GNS3.

### Paquete tipo 1: Hello - IPv4

En la figura 4.23, resaltada en un círculo amarillo, se muestra la cabecera OSPF Header (1), que indica la versión del protocolo. Para nuestro caso, se indica que es la segunda versión debido al uso de direccionamiento IPv4. Además, se visualiza el tamaño del paquete, tipo de mensaje y el ID de

Área. Dentro del Paquete Hello OSPF (2), se pueden identificar diferentes elementos, como la máscara de red, el intervalo de los paquetes Hello, la prioridad y el Bloque de Datos LLS OSPF (3). Estos componentes son parte integral del paquete Hello y contribuyen a la comunicación y configuración del protocolo OSPF.

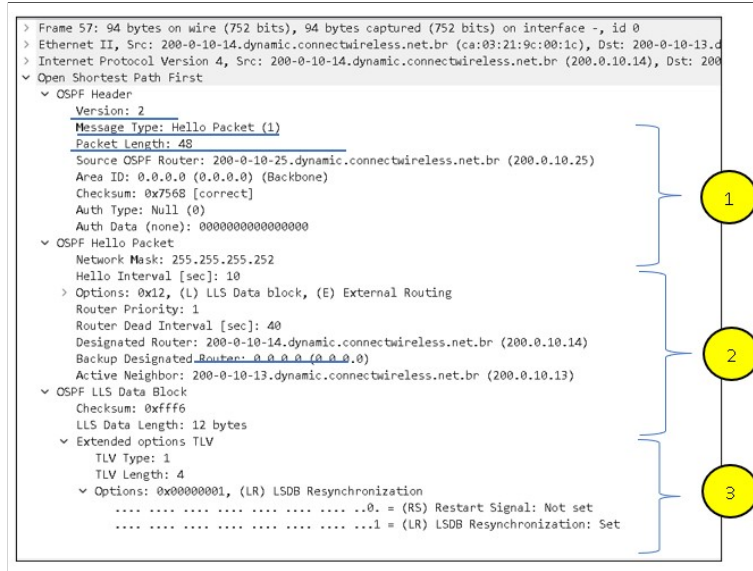


Figura 4.23: Paquete Hello OspfV2 IPv4

### Paquete tipo 1: Hello - IPv6

En el direccionamiento IPv6, el paquete Hello también juega un papel importante en el protocolo OSPF. La figura 4.24 proporciona una descripción detallada de este paquete en particular. El paquete Hello en IPv6 contiene información esencial, como el intervalo de los paquetes Hello, la prioridad y la máscara de red. Estos elementos son fundamentales para el funcionamiento correcto y configuración de OSPF en un entorno IPv6. La figura 4.24 ofrece una representación visual de los componentes y detalles específicos del paquete Hello en el contexto del direccionamiento IPv6.

```

Open Shortest Path First
├── OSPF Header
│   ├── Version: 3
│   ├── Message Type: Hello Packet (1)
│   ├── Packet Length: 40
│   ├── Source OSPF Router: 2.2.2.2 (2.2.2.2)
│   ├── Area ID: 0.0.0.0 (0.0.0.0) (Backbone)
│   ├── Checksum: 0xe96c [correct]
│   ├── Instance ID: IPv6 unicast AF (0)
│   └── Reserved: 00
├── OSPF Hello Packet
│   ├── Interface ID: 5
│   ├── Router Priority: 1
│   └── Options: 0x000013, R, E, V6
│       ├── .....0.. ..... = AT: Not set
│       ├── .....0. .... = L: Not set
│       ├── .....0 ..... = AF: Not set
│       ├── .....0. .... = DC: Not set
│       ├── .....1 ..... = R: Set
│       ├── .....0... = N: Not set
│       ├── .....0.. = MC: Not set
│       ├── .....1. .... = E: Set
│       └── .....1 = V6: Set
└── Hello Interval [sec]: 10
    Router Dead Interval [sec]: 40
    Designated Router: 3.3.3.3 (3.3.3.3)
    Backup Designated Router: 2.2.2.2 (2.2.2.2)
    Active Neighbor: 3.3.3.3 (3.3.3.3)

```

Figura 4.24: Paquete Hello OSPFv3 IPv6

### Paquete tipo 2: DB Description - IPv4 e IPv6

El paquete DB Descripción en OSPF transporta información crítica del router y las cabeceras de los LSA (Link State Advertisement). En este paquete, se lleva a cabo la validación tanto para los direccionamientos IPv4 como IPv6. En la figura 4.25, resaltada en un círculo amarillo, se puede observar la descripción del paquete *DB description* en el contexto del direccionamiento IPv4. En dicha figura, se detallan los bits Init, More y MS Master, que tienen funciones específicas dentro del protocolo OSPF. Además, se proporciona información relevante sobre los routers involucrados.

Por otro lado, la figura 4.26, visualiza la descripción del paquete *DB description* en el contexto del direccionamiento IPv6. En esta figura, también se presentan los bits Init, More y MS Master, junto con información adicional sobre los routers.

Estas figuras brindan una representación visual detallada de los paquetes *DB description* y sus componentes específicos para los direccionamientos IPv4 e IPv6.

```

  ▾ OSPF Header
    Version: 2
    Message Type: DB Description (2)
    Packet Length: 32
    Source OSPF Router: 200.0.10.13.dynamic.connectwireless.net.br (200.0.10.13)
    Area ID: 0.0.0.0 (0.0.0.0) (Backbone)
    Checksum: 0xbe6a [correct]
    Auth Type: Null (0)
    Auth Data (none): 0000000000000000
  ▾ OSPF DB Description
    Interface MTU: 1500
    > Options: 0x52, O, (L) LLS Data block, (E) External Routing
    > DB Description: 0x07, (I) Init, (M) More, (MS) Master
    DD Sequence: 5506
  ▾ OSPF LLS Data Block
    Checksum: 0xffff
    LLS Data Length: 12 bytes
  ▾ Extended options TLV
    TLV Type: 1
    TLV Length: 4
  ▾ Options: 0x00000001, (LR) LSOB Resynchronization
    .... = (RS) Restart Signal: Not set
    .... = (LR) LSOB Resynchronization: Set
  
```




Figura 4.25: Paquete DB Description IPv4

```

  ▾ OSPF Header
    Version: 3
    Message Type: DB Description (2)
    Packet Length: 28
    Source OSPF Router: 3.3.3.3 (3.3.3.3)
    Area ID: 0.0.0.0 (0.0.0.0) (Backbone)
    Checksum: 0x2edb [correct]
    Instance ID: IPv6 unicast AF (0)
    Reserved: 00
  ▾ OSPF DB Description
    Reserved: 00
  ▾ Options: 0x000013, R, E, V6
    .... = AT: Not set
    .... = L: Not set
    .... = AF: Not set
    .... = DC: Not set
    .... = R: Set
    .... = N: Not set
    .... = MC: Not set
    .... = E: Set
    .... = V6: Set
    Interface MTU: 1500
    Reserved: 00
  ▾ DB Description: 0x07, (I) Init, (M) More, (MS) Master
    .... = (R) OOBResync: Not set
    .... = (I) Init: Set
    .... = (M) More: Set
    .... = (MS) Master: Yes
    DD Sequence: 274052153
  
```

Figura 4.26: Paquete DB Description IPv6



### Paquete tipo 3: Link State Request IPv4 e IPv6

La figura 4.27 muestra la actualización de la base de datos de los vecinos, para direccionamiento IPv4 y la figura 4.28 para direccionamiento IPv6.

```

▼ Open Shortest Path First
  ▼ OSPF Header
    Version: 2
    Message Type: LS Request (3)
    Packet Length: 36
    Source OSPF Router: 200-0-10-13.dynamic.connectwireless.net.br (200.0.10.13)
    Area ID: 0.0.0.0 (0.0.0.0) (Backbone)
    Checksum: 0x8796 [correct]
    Auth Type: Null (0)
    Auth Data (none): 0000000000000000
  ▼ Link State Request
    LS Type: Router-LSA (1)
    Link State ID: 200-0-10-25.dynamic.connectwireless.net.br (200.0.10.25)
    Advertising Router: 200-0-10-25.dynamic.connectwireless.net.br (200.0.10.25)

```

Figura 4.27: Paquete Link State Request IPv4

```

▼ OSPF Header
  Version: 3
  Message Type: LS Request (3)
  Packet Length: 748
  Source OSPF Router: 2.2.2.2 (2.2.2.2)
  Area ID: 0.0.0.0 (0.0.0.0) (Backbone)
  Checksum: 0x4618 [correct]
  Instance ID: IPv6 unicast AF (0)
  Reserved: 00
  ▼ Link State Request
    Reserved: 0000
    ▼ LS Type: 0x2001
      0... .. = LSA Handling: Store and flood the LSA as if the type is understood
      .01. .... = Flooding Scope: Area Scoping - Flooded only in originating area (0x1)
      ...0 0000 0000 0001 = Function Code: Router-LSA (1)
      Link State ID: 0.0.0.0 (0.0.0.0)
      Advertising Router: one.one.one.one (1.1.1.1)
    ▼ Link State Request
      Reserved: 0000
      ▼ LS Type: 0x2001
        0... .. = LSA Handling: Store and flood the LSA as if the type is understood
        .01. .... = Flooding Scope: Area Scoping - Flooded only in originating area (0x1)
        ...0 0000 0000 0001 = Function Code: Router-LSA (1)
        Link State ID: 0.0.0.0 (0.0.0.0)
        Advertising Router: 2.2.2.2 (2.2.2.2)
    > Link State Request
    > Link State Request
    > Link State Request
    > Link State Request
    > Link State Request
    > Link State Request
    > Link State Request
    > Link State Request
    > Link State Request
    > Link State Request

```

Figura 4.28: Paquete Link State Request IPv6

### Paquete tipo 4: Link-State Update IPv4 e IPv6

Paquetes de información que describen el estado de enlace conteniendo varios LSAs (Link State Advertisements) de tipos diferentes. Pueden incluir información tanto para IPv4 como para IPv6, como se muestra en las figuras 4.29 para el direccionamiento IPv4 y 4.30 para el direccionamiento IPv6.

```

Open Shortest Path First
  OSPF Header
    Version: 2
    Message Type: LS Update (4)
    Packet Length: 124
    Source OSPF Router: 200.0.10.25.dynamic.connectwireless.net.br (200.0.10.25)
    Area ID: 0.0.0.0 (0.0.0.0) (Backbone)
    Checksum: 0x97f7 [correct]
    Auth Type: Null (0)
    Auth Data (none): 0000000000000000
  LS Update Packet
    Number of LSAs: 1
    LSA Type 1 (Router-LSA), len=96
      .000 0000 0000 0001 = LS Age (seconds): 1
      0... .. = Do Not Age Flag: 0
    Options: 0x22, (DC) Demand Circuits, (E) External Routing
      0... .. = DN: Not set
      .0... .. = O: Not set
      ..1... .. = (DC) Demand Circuits: Supported
      ...0... .. = (L) LLS Data block: Not Present
      .... 0... = (N) NSSA: Not supported
      .... .0... = (MC) Multicast: Not capable
      .... ..1... = (E) External Routing: Capable
      .... ...0 = (MT) Multi-Topology Routing: No
    LS Type: Router-LSA (1)
    Link State ID: 200.0.10.25.dynamic.connectwireless.net.br (200.0.10.25)
    Advertising Router: 200.0.10.25.dynamic.connectwireless.net.br (200.0.10.25)
    Sequence Number: 0x8000000a
    Checksum: 0x126e
    Length: 96
    > Flags: 0x00
    Number of Links: 6
    > Type: Transit ID: 200.0.10.26 Data: 200.0.10.25 Metric: 1
    > Type: Transit ID: 200.0.10.22 Data: 200.0.10.21 Metric: 1
    > Type: Transit ID: 200.0.10.18 Data: 200.0.10.17 Metric: 1
    > Type: Transit ID: 200.0.10.14 Data: 200.0.10.14 Metric: 1
    > Type: Stub ID: 200.0.10.8 Data: 255.255.255.252 Metric: 1
    > Type: Stub ID: 192.168.10.0 Data: 255.255.255.0 Metric: 1
  
```

Figura 4.29: Paquete Link-State Update IPv4

```

v Open Shortest Path First
  v OSPF Header
    Version: 3
    Message Type: LS Acknowledge (5)
    Packet Length: 36
    Source OSPF Router: 2.2.2.2 (2.2.2.2)
    Area ID: 0.0.0.0 (0.0.0.0) (Backbone)
    Checksum: 0xab52 [correct]
    Instance ID: IPv6 unicast AF (0)
    Reserved: 00
  v LSA-type 1 (Router-LSA), len 88
    .000 0000 0000 0001 = LS Age (seconds): 1
    0... .. = Do Not Age: False
  v LS Type: 0x2001
    0... .. = LSA Handling: Store and flood the LSA as if the type is understood
    .01. .... = Flooding Scope: Area Scoping - Flooded only in originating area (0x1)
    ...0 0000 0000 0001 = Function Code: Router-LSA (1)
    Link State ID: 0.0.0.0 (0.0.0.0)
    Advertising Router: 3.3.3.3 (3.3.3.3)
    Sequence Number: 0x00000009
    Checksum: 0xa992
    Length: 88

```

Figura 4.30: Paquete Link-State Update IPv6

#### Paquete tipo 5: LS Acknowledge IPv4 e IPv6

El paquete tipo 5, conocido como LS Acknowledge (LSAck), se utiliza para confirmar la recepción de cada paquete DD (Database Description), Link State Request o Link State Update en el protocolo OSPF. La figura 4.31, muestra un ejemplo del paquete LS Acknowledge del direccionamiento IPv4. Este paquete contiene información relevante sobre los paquetes LSA (Link State Advertisement) tipo 1, que indican los routers directamente conectados. De manera similar, en la figura 4.32, también resaltada en un círculo amarillo, se presenta el paquete LS Acknowledge en el contexto del direccionamiento IPv6. Este paquete confirma la recepción de los paquetes LSA tipo 1 y proporciona información correspondiente a los routers directamente conectados. Ambas figuras muestran información necesaria que aseguran la correcta recepción de los paquetes LSA y garantizan entre los routers la sincronización de la base de datos .

```

  ▾ OSPF Header
    Version: 2
    Message Type: LS Acknowledge (5)
    Packet Length: 44
    Source OSPF Router: 200-0-10-13.dynamic.connectwireless.net.br (200.0.10.13)
    Area ID: 0.0.0.0 (0.0.0.0) (Backbone)
    Checksum: 0xid15 [correct]
    Auth Type: Null (0)
    Auth Data (none): 0000000000000000
  ▾ LSA-type 1 (Router-LSA), len 60
    .000 0000 0000 0100 = LS Age (seconds): 4
    0... .. = Do Not Age Flag: 0
  ▾ Options: 0x22, (DC) Demand Circuits, (E) External Routing
    0... .. = DN: Not set
    .0.. .. = O: Not set
    ..1. .... = (DC) Demand Circuits: Supported
    ...0 .... = (L) LLS Data block: Not Present
    .... 0... = (N) NSSA: Not supported
    .... .0.. = (MC) Multicast: Not capable
    .... .1. = (E) External Routing: Capable
    .... ..0 = (MT) Multi-Topology Routing: No
  LS Type: Router-LSA (1)
  Link State ID: 200-0-10-69.dynamic.connectwireless.net.br (200.0.10.69)
  Advertising Router: 200-0-10-69.dynamic.connectwireless.net.br (200.0.10.69)
  Sequence Number: 0x80000008
  Checksum: 0xc7d6
  Length: 60

```

Figura 4.31: Paquete LS Acknowledge OSPF IPv4

```

  ▾ Open Shortest Path First
  ▾ OSPF Header
    Version: 3
    Message Type: LS Acknowledge (5)
    Packet Length: 36
    Source OSPF Router: 2.2.2.2 (2.2.2.2)
    Area ID: 0.0.0.0 (0.0.0.0) (Backbone)
    Checksum: 0xab52 [correct]
    Instance ID: IPv6 unicast AF (0)
    Reserved: 00
  ▾ LSA-type 1 (Router-LSA), len 88
    .000 0000 0000 0001 = LS Age (seconds): 1
    0... .. = Do Not Age: False
  ▾ LS Type: 0x2001
    0... .. = LSA Handling: Store and flood the LSA as if the type is understood
    .01. .... = Flooding Scope: Area Scoping - Flooded only in originating area (0x1)
    ...0 0000 0000 0001 = Function Code: Router-LSA (1)
  Link State ID: 0.0.0.0 (0.0.0.0)
  Advertising Router: 3.3.3.3 (3.3.3.3)
  Sequence Number: 0x00000009
  Checksum: 0xa992
  Length: 88

```

Figura 4.32: Paquete LS Acknowledge OSPF IPv6

### 4.2.3. Resultados de la Latencia para simulación y emulación

Los resultados de la latencia para la simulación y emulación se obtuvieron al realizar el comando Ping entre las máquinas virtuales Guayaquil y Quito en la topología de IPv4. La figura 4.33 muestra los resultados.

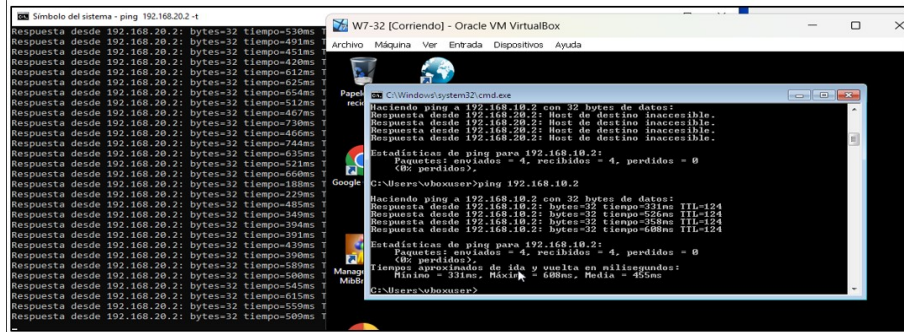


Figura 4.33: Latencia en la prueba de Ping - IPv4

La prueba de conectividad con el comando PING y métrica de enrutamiento “tracert” realizado desde la MV de Quito hacia la MV de Guayaquil utilizando direccionamiento IPv4 se muestra en la figura 4.34. En la misma se puede observar la ruta que toma el paquete y se verifica que no existe pérdida de paquetes durante la comunicación.

```
C:\Users\GNS3-W10>tracert 192.168.20.1

Traza a 192.168.20.1 sobre caminos de 30 saltos como máximo.

  1  106 ms  139 ms  30 ms  192.168.10.1
  2  350 ms  239 ms  221 ms  200.0.10.22
  3  409 ms  316 ms  419 ms  200.0.10.38
  4  693 ms  726 ms  718 ms  192.168.20.1

Traza completa.

C:\Users\GNS3-W10>ping 192.168.20.1

Haciendo ping a 192.168.20.1 con 32 bytes de datos:
Respuesta desde 192.168.20.1: bytes=32 tiempo=732ms TTL=252
Respuesta desde 192.168.20.1: bytes=32 tiempo=613ms TTL=252
Respuesta desde 192.168.20.1: bytes=32 tiempo=886ms TTL=252
Respuesta desde 192.168.20.1: bytes=32 tiempo=624ms TTL=252

Estadísticas de ping para 192.168.20.1:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 613ms, Máximo = 886ms, Media = 713ms
```

Figura 4.34: Pruebas de conectividad desde la MV Quito a la MV Guayaquil-IPv4

Los resultados de las pruebas de conectividad y latencia se muestran en las figuras 4.35, 4.36 y 4.37, que permiten verificar la configuración y conectividad entre las máquinas virtuales y routers de la topología. Los resultados muestran los comandos Ping ejecutados entre las máquinas virtuales de Quito, Guayaquil, Cuenca y Tulcan utilizando direccionamiento IPv6. Estos resultados permiten observar la conectividad exitosa entre las diferentes máquinas virtuales y la latencia asociada a cada conexión.

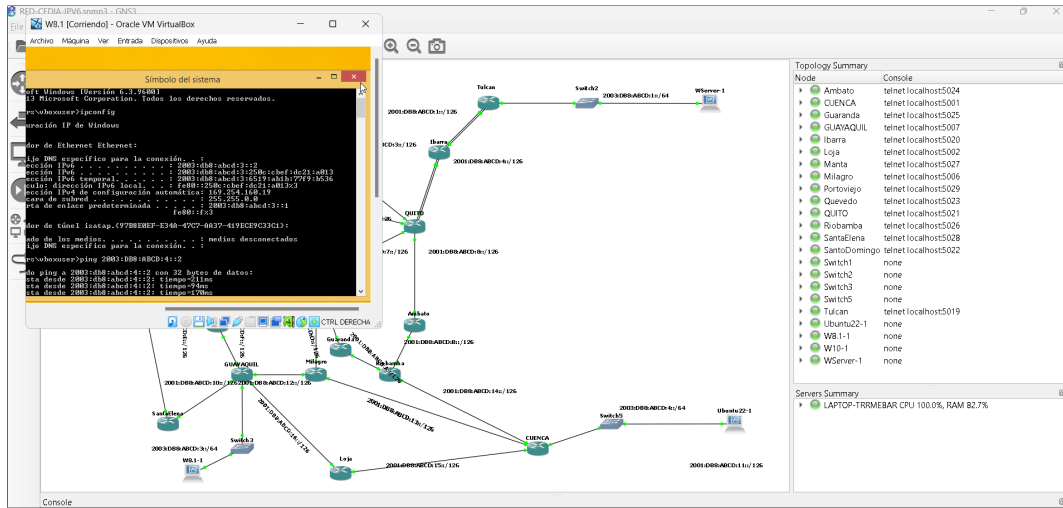


Figura 4.35: Resultados de la prueba Ping desde la VM Guayaquil a la VM Cuenca - IPv6

```

ubuntu@ubuntu-VirtualBox: ~
64 bytes from 2003:db8:abcd:4::1: icmp_seq=4 ttl=64 time=61.9 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=5 ttl=64 time=83.3 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=6 ttl=64 time=28.8 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=7 ttl=64 time=117 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=8 ttl=64 time=30.0 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=9 ttl=64 time=10.4 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=10 ttl=64 time=9.13 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=11 ttl=64 time=9.80 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=12 ttl=64 time=10.8 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=13 ttl=64 time=77.6 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=14 ttl=64 time=87.0 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=15 ttl=64 time=115 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=16 ttl=64 time=178 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=17 ttl=64 time=46.6 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=18 ttl=64 time=87.6 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=19 ttl=64 time=80.3 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=20 ttl=64 time=222 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=21 ttl=64 time=130 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=22 ttl=64 time=92.3 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=23 ttl=64 time=74.0 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=24 ttl=64 time=55.2 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=25 ttl=64 time=89.0 ms
64 bytes from 2003:db8:abcd:4::1: icmp_seq=26 ttl=64 time=56.5 ms
  
```

Figura 4.36: Resultados de la prueba Ping entre la VM desde Ubuntu hacia el router Cuenca - IPv6

```

64 bytes from 2003:db8:abcd:2::2: icmp_seq=111 ttl=60 time=256 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=112 ttl=60 time=298 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=113 ttl=60 time=284 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=114 ttl=60 time=286 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=115 ttl=60 time=332 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=116 ttl=60 time=372 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=117 ttl=60 time=372 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=118 ttl=60 time=476 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=119 ttl=60 time=468 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=120 ttl=60 time=346 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=121 ttl=60 time=348 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=122 ttl=60 time=384 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=123 ttl=60 time=329 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=124 ttl=60 time=352 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=125 ttl=60 time=433 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=126 ttl=60 time=844 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=127 ttl=60 time=593 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=128 ttl=60 time=531 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=129 ttl=60 time=529 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=130 ttl=60 time=377 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=131 ttl=60 time=445 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=132 ttl=60 time=395 ms
64 bytes from 2003:db8:abcd:2::2: icmp_seq=133 ttl=60 time=354 ms
  
```

Figura 4.37: Resultados de la conectividad desde la VM Guayaquil a la VM Cuenca

En la figura 4.38, podemos observar un mosaico de las pruebas de conectividad entre varios sistemas con direccionamiento IPv6.

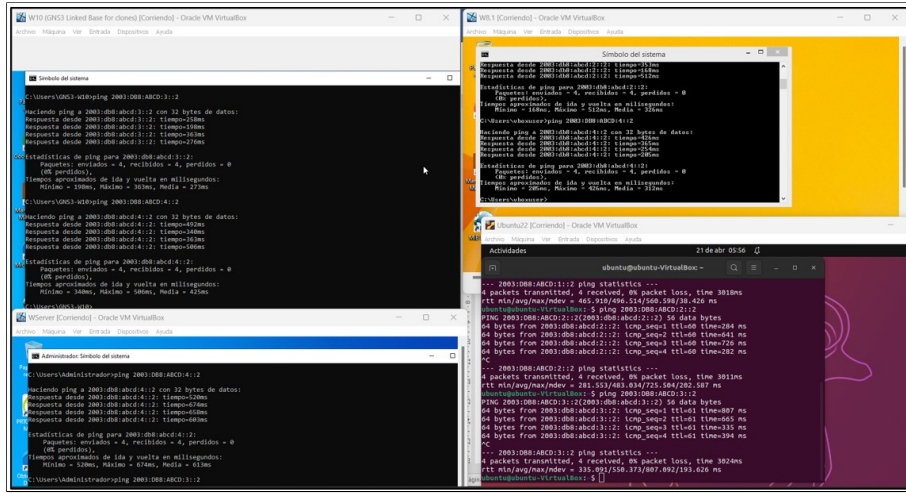


Figura 4.38: Conectividad entre las MV Quito, Tulcan, Guayaquil y Cuenca

En todas las pruebas de conectividad realizadas, tanto para IPv4 como IPv6, se verificó que todos los dispositivos estuvieran conectados correctamente con sus vecinos. La tabla 4.1 detalla comparación de la latencia entre el direccionamiento IPv4 e IPv6.

Los resultados muestran una reducción significativa en la latencia al utilizar el direccionamiento IPv6 en comparación con IPv4. Esto indica que el protocolo IPv6 puede ofrecer una mayor eficiencia y menor tiempo de respuesta en las comunicaciones de red.



Cuadro 4.1: Comparación de latencia entre IPv4 vs IPv6

Origen - Destino	Latencia desde IPv4	Latencia desde IPv6
Quito a Guayaquil	728ms	650ms
Quito a Cuenca	732ms	621ms
Quito a Tulcan	411ms	382ms
Guayaquil a Quito	645ms	579ms
Guayaquil a Cuenca	405ms	201ms
Guayaquil a Tulcan	981ms	887ms
Cuenca a Quito	632ms	540ms
Cuenca a Guayaquil	434ms	193ms
Cuenca a Tulcan	908ms	739ms
Tulcan a Quito	361ms	199ms
Tulcan a Guayaquil	958ms	528ms
Tulcan a Cuenca	986ms	432ms

#### 4.2.4. Resultados del flujo de datos con Wireshark - IPv4

Como resultado del análisis realizado en Wireshark, se generaron los gráficos de flujo de datos capturados durante la prueba de conectividad entre la máquina virtual de Quito y Guayaquil. Estos resultados, representados en la figura 4.39, proporcionan una visión detallada del flujo de datos registrado durante la prueba, mostrando información precisa sobre los paquetes intercambiados entre ambas máquinas virtuales.

El análisis de estos gráficos de flujo de datos resulta invaluable para comprender y evaluar el rendimiento de la conexión entre las máquinas virtuales. Proporciona información sobre la cantidad de paquetes enviados y recibidos, así como detalles específicos sobre los protocolos utilizados, los tamaños de los paquetes y otros datos relevantes.

Estos resultados son útiles para determinar eficiencia de transmisión de datos y calidad de conexión entre máquinas virtuales, de modo que se puedan tomar mejores decisiones para optimizar el rendimiento de la red.

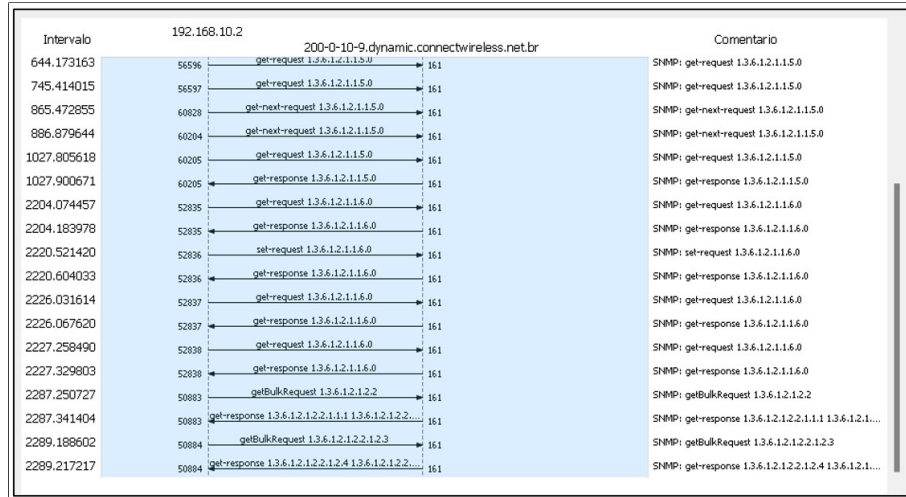


Figura 4.39: Flujo de datos Ping MV Quito – MV Guayaquil

La figura 4.40 muestra el flujo de datos que corresponden a los paquetes OSPFv2 con el direccionamiento IPv4 para el router Ibarra. Esta representación gráfica proporciona una visión detallada del intercambio de paquetes OSPFv2 que ocurre en el entorno de red del router Ibarra, permitiendo analizar la comunicación y el enrutamiento en esta configuración específica. Por otro lado, la gráfica del flujo de datos relacionada con el uso de SNMPv2 se detalla en la figura 4.41, desde la máquina virtual de Quito hacia el router Ibarra. Esta visualización brinda información valiosa sobre la transferencia de datos y las interacciones entre la máquina virtual y el router mediante el protocolo SNMPv2.

Estas figuras de flujo de datos son herramientas esenciales para comprender y analizar el comportamiento de los protocolos OSPFv2 y SNMPv2 en el entorno de red. Proporcionan una representación visual de las transmisiones de datos y permiten identificar posibles problemas o mejora de áreas en el enrutamiento y la administración de la red. El análisis detallado de estos flujos de datos contribuye a la optimización y mejora del rendimiento de la red, así como a una administración más eficiente de los dispositivos y protocolos involucrados en el entorno de red considerado.

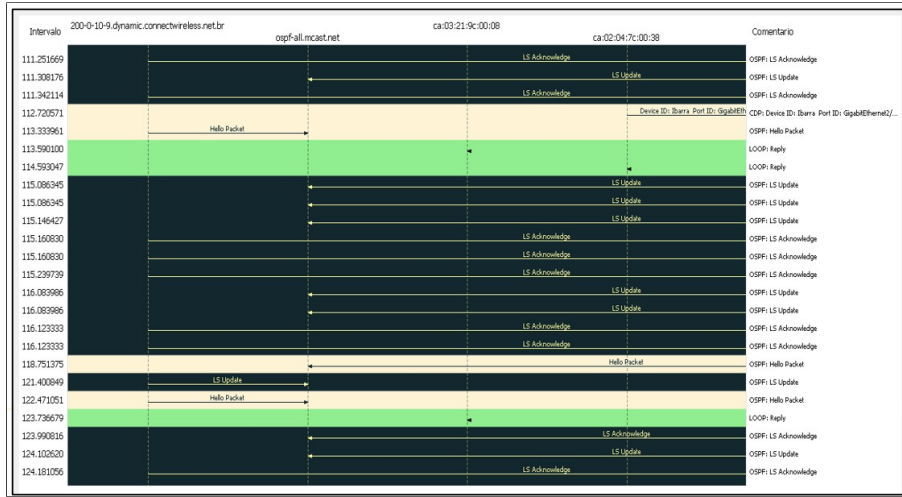


Figura 4.40: Flujo de datos para paquetes OSPFv2 para el router Ibarra

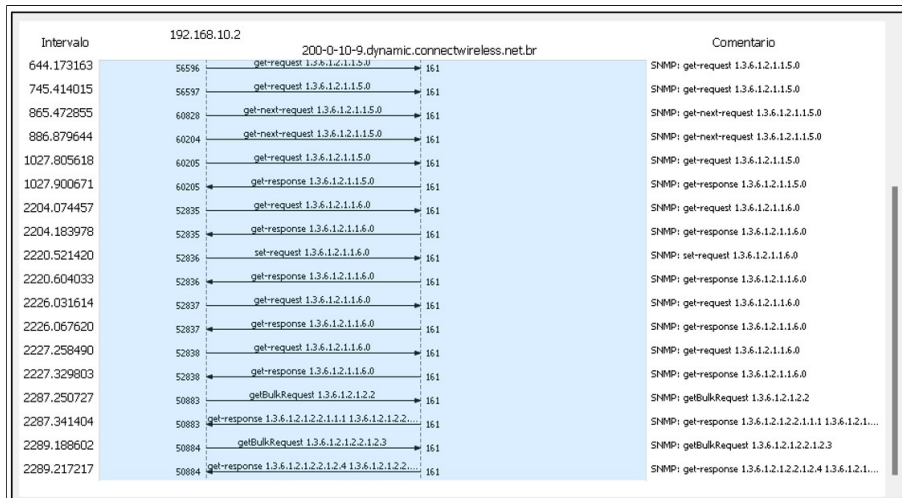


Figura 4.41: Flujo de datos SNMPv2 desde MV Quito a Router Ibarra

### 4.2.5. Resultados de flujo de datos con Wireshark - IPv6

Utilizando la herramienta Wireshark, también se realizó el análisis de flujo de datos en el contexto del direccionamiento IPv6. Como resultado, se obtuvieron gráficos de flujo de datos que proporcionan información detallada sobre el intercambio de paquetes durante la prueba de conectividad entre el

Router Cuenca y el Router Ibarra. Estos resultados se muestran en la figura 4.42, visualizando los datos capturados durante la prueba de conectividad, brindando una visión detallada de los paquetes intercambiados entre los routers Cuenca e Ibarra en un entorno IPv6. Este análisis permite evaluar la calidad de la conexión y verificar el correcto funcionamiento del enrutamiento en el contexto del direccionamiento IPv6.

Con base en estos resultados, se pueden identificar posibles problemas de conectividad, optimizar la configuración de la red y mejorar el rendimiento y la eficiencia del enrutamiento con decisiones informadas en un entorno IPv6.

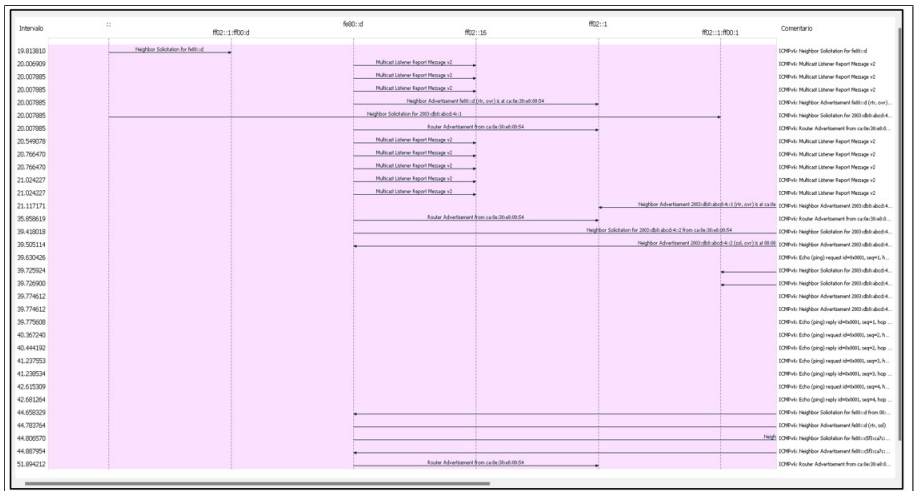


Figura 4.42: Gráfica de flujo de datos Conectividad IPv6 de Router Cuenca a Router Ibarra

La figura 4.43 muestra el resultado del enrutamiento OSPFv3 del flujo de datos entre el Router Quevedo y el Router Manta. Esta figura muestra los paquetes capturados que validan la conectividad exitosa entre ambos routers en un entorno de direccionamiento IPv6. El análisis del flujo de datos en esta figura proporciona información del intercambio de paquetes OSPFv3 entre los enrutadores Quevedo y Manta. Además, validar la correcta configuración y funcionamiento del enrutamiento OSPFv3 en un entorno IPv6, así como validar la conectividad exitosa entre ambos dispositivos.

La visualización detallada de los paquetes capturados en el gráfico del flujo de datos ayuda a identificar cualquier problema o irregularidad en la comunicación entre los routers. Esto permite realizar ajustes necesarios en la configuración de OSPFv3 y asegurar un enrutamiento eficiente y confiable en la red.

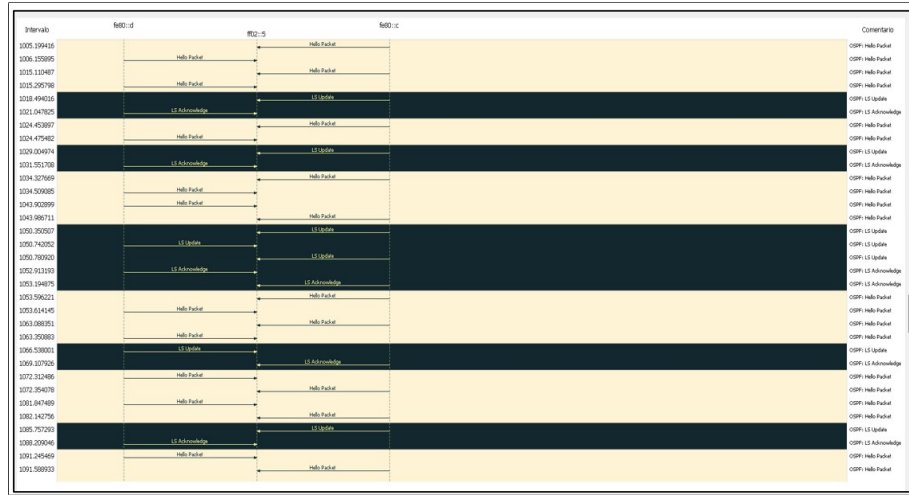


Figura 4.43: Flujo de datos OSPFv3 entre Router Quevedo y Manta

### Resultados del flujo de SNMPv3

En la figura 4.44 se visualiza los resultados de los paquetes del protocolo SNMPv3 desde el NMS (Sistema de Gestión de Red) de Quito hacia el router Ibarra. Esta representación gráfica del flujo de paquetes permite validar la configuración del protocolo de gestión SNMPv3 en el entorno considerado.

El análisis del flujo de paquetes en esta figura proporciona información detallada sobre la interacción entre el NMS de Quito y el router Ibarra a través del protocolo SNMPv3. Permite validar el correcto funcionamiento y configuración de SNMPv3, así como la comunicación exitosa entre el NMS y el router en el entorno IPv6.

La visualización de los paquetes capturados en el gráfico del flujo de datos del protocolo SNMPv3 es esencial para garantizar una gestión efectiva de la red. Permite controlar dispositivos de red y su respectivo monitoreo, recopilar información y realizar configuraciones remotas de manera segura y eficiente.

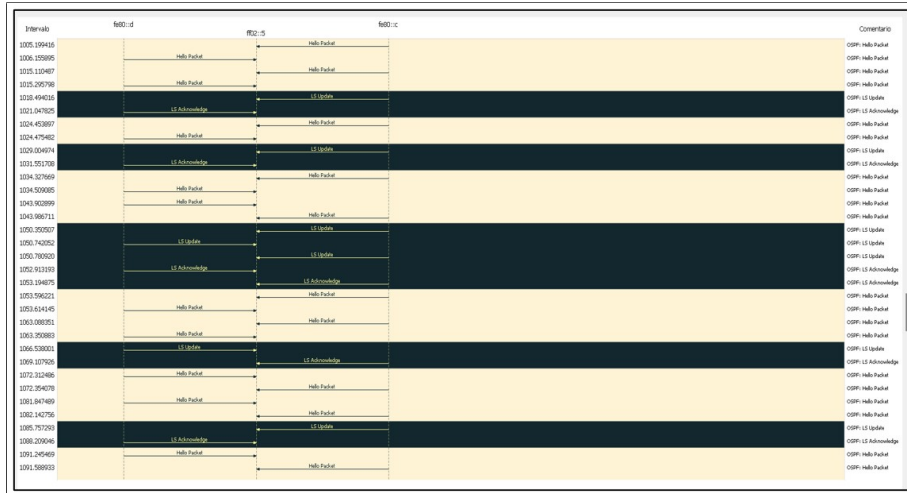


Figura 4.44: Flujo de datos SNMPv3 - IPv6 desde MV Quito hacia Router Ibarra

#### 4.2.6. Desempeño de la Simulación y Emulación en la Máquina Real

En la tabla 4.2, se presenta un detalle del uso de recursos para cada tipo de direccionamiento, resaltando las diferencias entre Packet Tracer y GNS3. Como simulador, Packet Tracer tiene ciertas limitaciones en cuanto a la configuración de topologías backbone más complejas. Por otro lado, GNS3 permite la emulación y configuración de dispositivos como máquinas virtuales y software de enrutamiento de routers reales, lo cual implica un mayor consumo de recursos en comparación con un simulador convencional.

En términos de recursos, Packet Tracer generalmente requiere menos capacidad de procesamiento y memoria, lo que lo hace más ligero y fácil de usar en configuraciones básicas. Sin embargo, debido a sus limitaciones, puede resultar insuficiente para escenarios de redes avanzadas y topologías más complejas.

Por otro lado, GNS3 proporciona un entorno más completo y flexible, permitiendo la emulación de dispositivos y la configuración de routers reales con sus sistemas operativos correspondientes. Esto brinda mayor realismo en la simulación, pero también implica un mayor consumo de recursos, ya que los dispositivos emulados requieren más capacidad de procesamiento y memoria para funcionar adecuadamente.

Cuadro 4.2: Desempeño de la máquina real

Direccionamiento	Uso de UPC%	RAM%	Estado Máquinas Virtuales	Estado de Routers
IPv4	100 %	93.9 %	ON	ON
IPv6	100 %	97.3 %	ON	ON
IPv4	1.3 %	75.5 %	ON	OFF
IPv6	5.3 %	73.6 %	ON	OFF

#### 4.2.7. Pruebas de gestión - GNS3

En las pruebas de gestión en la topología con direccionamiento IPv6, se implementó la herramienta Manage Engine MibBrowser en las cuatro máquinas virtuales. Esta herramienta es compatible tanto con SNMPv2 como con SNMPv3, lo que permitió realizar operaciones de gestión en el entorno IPv6. En el caso del direccionamiento IPv4, se utilizó la operación GET para solicitar nombres de forma remota y la operación SET para realizar asignaciones en la gestión de los dispositivos de red. Un ejemplo concreto de esta operación se observa en la conexión entre la máquina virtual de Quito y el enrutador de Guayaquil, donde se realizó la gestión de parámetros específicos. Para el análisis y visualización de los paquetes durante el transporte, se utilizó la herramienta Wireshark. Esta herramienta permitió capturar y examinar los paquetes en tiempo real, brindando información valiosa sobre la comunicación entre los dispositivos de red. La figura 4.45 muestra un ejemplo de cómo se utilizó Wireshark para analizar los paquetes en el entorno IPv4.

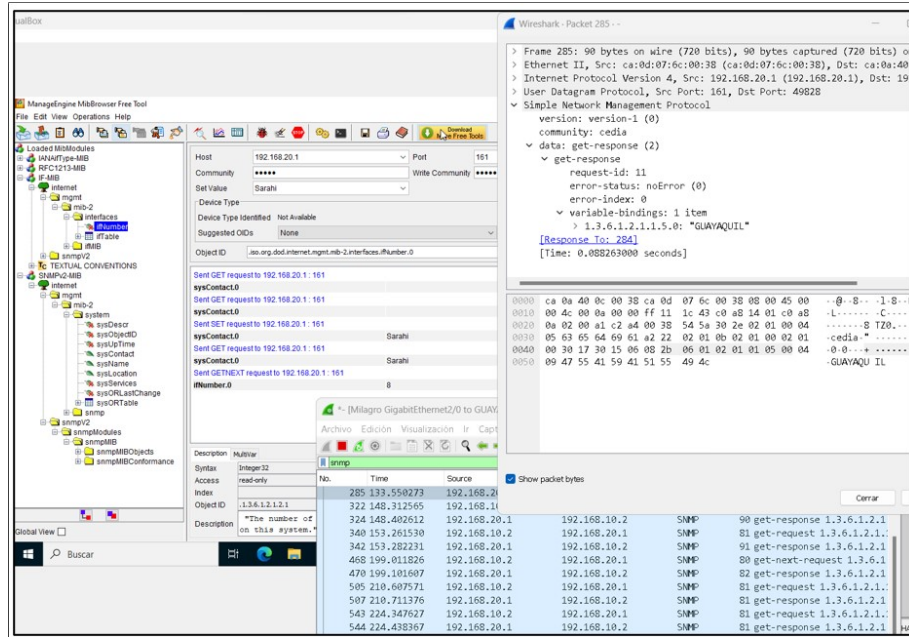


Figura 4.45: Obtención de localización para el router Cuenca utilizando la herramienta ManageEngine MibBrowser - IPv4

Para la gestión de IPv6, se llevó a cabo la administración remota desde la máquina virtual de Quito hacia el router Cuenca. Durante este proceso, se obtuvieron los OID correspondientes para diferentes parámetros, como la localización del dispositivo (`sysLocation`), el nombre del router (`sysName`), el nombre del contacto (`sysContact`), así como las tablas de interfaces (`IFtable`) y las tablas de enrutamiento (`RouteTable`).

Estos OID permitieron acceder y extraer información relevante del router Cuenca mediante el protocolo SNMP. La figura 4.46 muestra un ejemplo específico de la gestión realizada, donde se obtienen y visualizan los valores correspondientes a los OID mencionados. Con esta información, se logró tener un control y supervisión efectiva del router Cuenca desde la máquina virtual de Quito, lo que facilitó la administración y monitoreo de los parámetros y configuraciones relacionados con IPv6 en el entorno de la red.



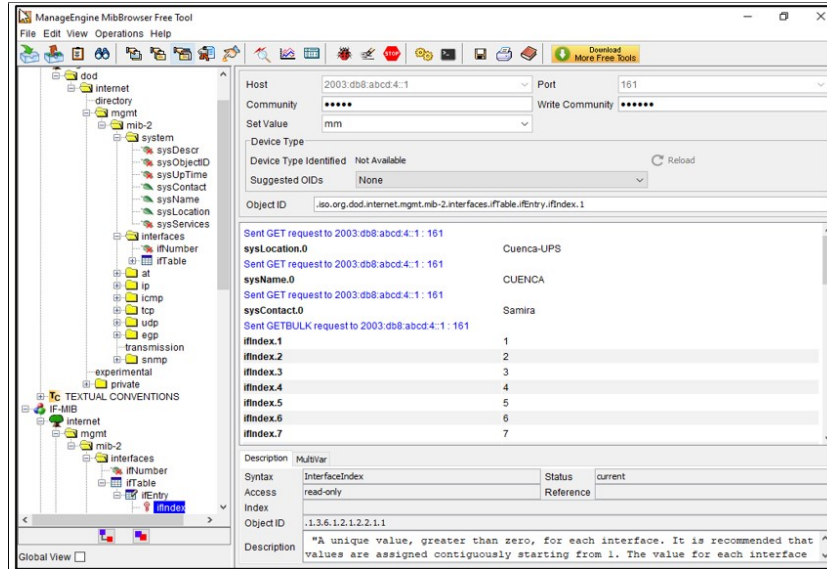


Figura 4.46: Obtención de localización para el router Cuenca utilizando la herramienta ManageEngine MibBrowser - IPv6

La figura 4.47, muestra la validación de ingreso de los MIB del Router Milagro, donde se obtienen los valores específicos de la tabla de las interfaces, usando SNMP v3 - IPv6.

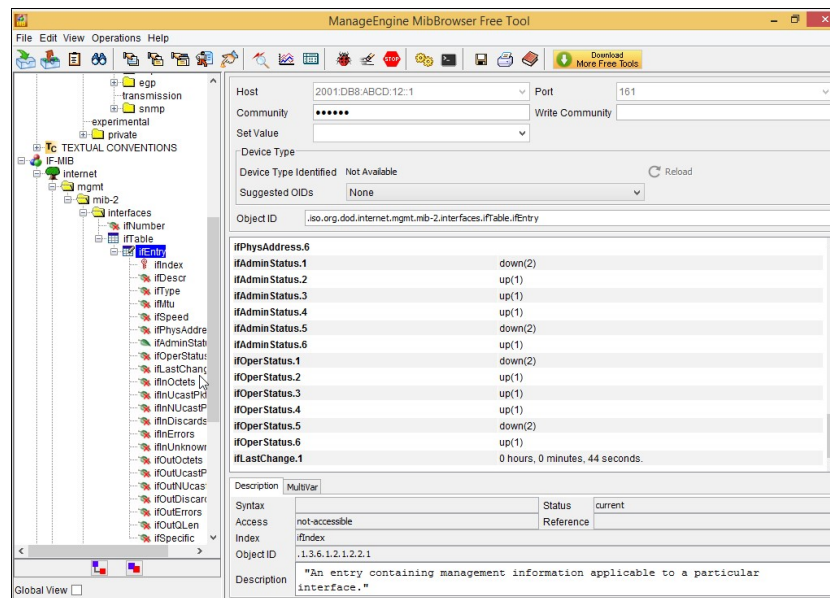


Figura 4.47: Monitoreo de la tabla de interfaces usando SNMP v3 - IPv6

La figura 4.48 se obtiene desde el NMS, el nombre del router, que se esta monitoreando en esta caso el resultado es Milagro, permitiendo validar, las operaciones de gestión.

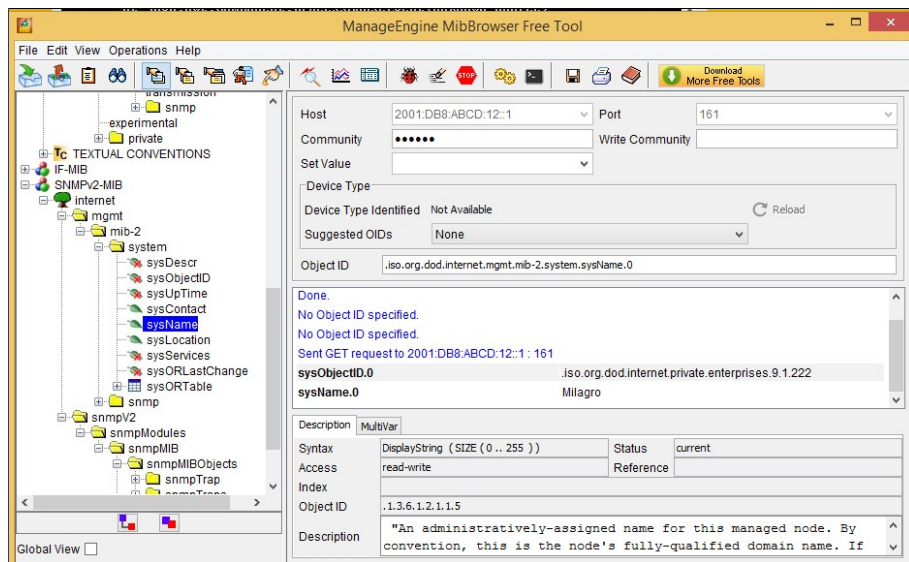


Figura 4.48: Monitoreo del nombre del router en SNMP v3 - IPv6

Mientras tanto, con Wireshark se capturan los paquetes SNMP y se transmiten al ejecutar las operaciones de gestión solicitadas, como muestra la figura 4.49.

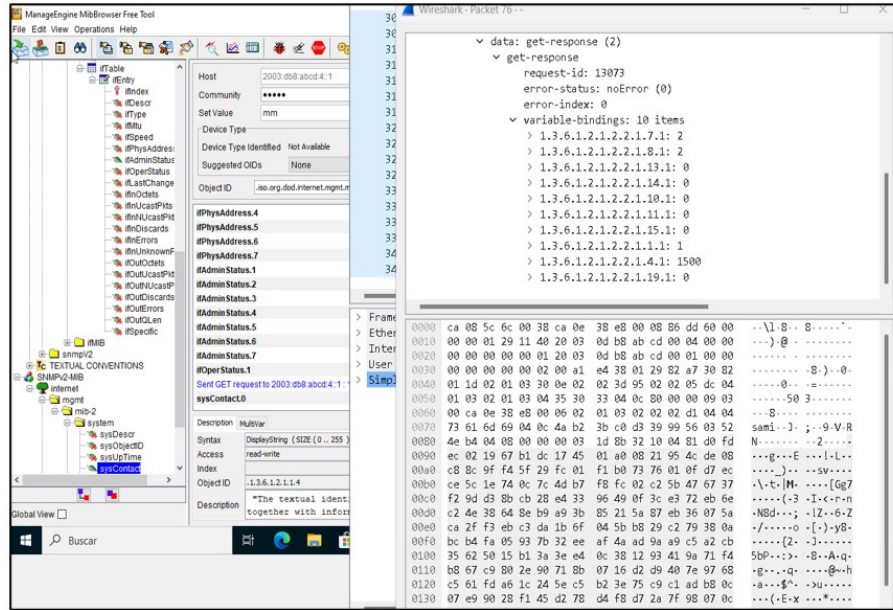


Figura 4.49: Análisis de paquetes SNMPv3 - Wireshark

#### 4.2.8. Diferencia entre SNMPv2 y SNMPv3

Como se puede apreciar en la figura 4.50 la captura de Wireshark evidencia una diferencia significativa entre SNMPv2 y SNMPv3. En particular, se destaca que SNMPv3 ofrece la capacidad de encriptar los datos transmitidos, lo cual es un aspecto crucial para acercarnos a la realidad de la topología física de CEDIA.

La encriptación de datos proporcionada por SNMPv3 garantiza confidencialidad e integridad en la información transmitida, lo que resulta fundamental en entornos de redes avanzadas. Esta característica adicional de seguridad en SNMPv3 se alinea con los estándares actuales y es una mejora significativa en comparación con SNMPv2. Al tener la capacidad de encriptar los datos, SNMPv3 brinda una capa adicional de protección contra posibles ataques y asegura que la información sensible esté protegida durante la transmisión. Esto es especialmente importante en entornos donde la privacidad y seguridad de los datos son aspectos críticos.

Como se puede observar en la captura de Wireshark en la figura 4.50, se puede notar que a diferencia de SNMPv2, SNMPv3 ofrece encriptación de

datos, lo que nos acerca más a la realidad de la topología física de CEDIA.

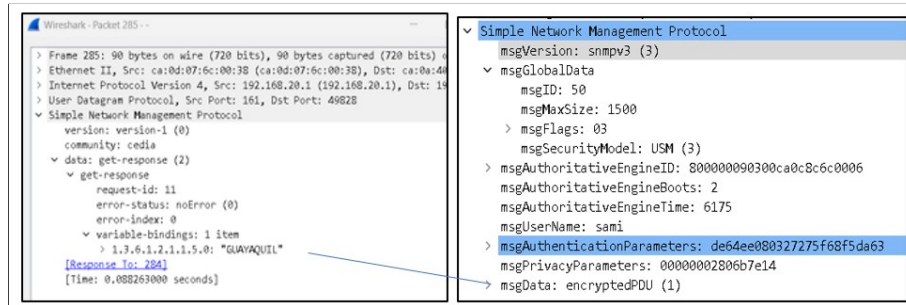


Figura 4.50: Comparación de paquetes SNMPv2 vs SNMPv3

## Capítulo 5

# Conclusiones

En este proyecto, se hizo un estudio de la gestión y conectividad del backbone CEDIA, Internet 2 ecuatoriana, mediante la emulación de su topología para obtener una aproximación máxima a la red real respaldada por el proveedor de servicios de Internet. Las redes avanzadas cumplen un papel importante en la investigación y educación en la actualidad, ya que permiten la colaboración entre diferentes entidades educativas para resolver problemas y aportar en temas específicos.

Ecuador forma parte de esta red de redes a través de CEDIA y la Red Nacional de Investigación y Educación, que vincula a instituciones académicas y de investigación en el país. CEDIA cuenta con una conexión de 10 Mbps a través del cable submarino que va hacia el nodo de la Red CLARA de Santiago de Chile. Esta red ofrece no solo colaboración a nivel nacional e internacional, sino también una conexión con un ancho de banda superior al de la Internet comercial, con un enfoque en la seguridad de la información transmitida.

La topología física estudiada en este proyecto se actualizó en 2021 y se mantuvo vigente hasta principios de 2023, con presencia de CEDIA en 15 provincias del país. Esto nos permitió emular el backbone de CEDIA, utilizando un total de 15 routers conectados usando las herramientas de simulación y emulación. La simulación brindó una primera aproximación sin utilizar routers de backbone reales, mientras que la emulación nos acercó más al funcionamiento de equipos reales y permitió trabajar en un entorno de configuración y pruebas más realista. Durante el estudio, se pudieron apreciar los protocolos utilizados para el enrutamiento, como OSPF, y para

la gestión de la red, como SNMP.

Se simuló y emuló la topología física utilizando tanto direccionamiento IPv4 como IPv6. Esto se hizo para hacer frente al crecimiento de Internet y a la necesidad de implementar equipos con direccionamiento IPv6 por agotamiento de direcciones IPv4.

Open Shortest Path First protocolo de enrutamiento se configuró en cada router de backbone de la topología de CEDIA, OSPFv2 con direccionamiento IPv4 y OSPFv3 con direccionamiento IPv6. OSPF es un protocolo que envía paquetes para mantener actualizadas las tablas de enrutamiento, lo que permite detectar cambios dentro de la red CEDIA. Los 5 tipos de paquetes OSPF se detectaron con Wireshark en el emulador Graphic Network Simulator-3.

SNMP protocolo de gestión, se configuró en cada router de backbone de CEDIA, bajo su versión SNMPV2. Mientras que las actividades de gestión se realizaron desde cada NMS instalado en cada máquina virtual, que en un principio fue el Ireasoning. Sin embargo, para acercarse mas a la gestión real de CEDIA se configuró a cada routers de CEDIA con la versión SNMPv3 para poder incluir una mayor privacidad y seguridad a la gestión. Sin embargo Ireasoning como NMS, no permitía manejar la versión 3 de SNMP, por lo cual fue necesario cambiar de software de gestión. Por lo anterior se instaló ManageEngine Mib Browser en cada máquina virtual y se realizaron las actividades de gestión correspondientes. Todos los paquetes SNMPv2 y SNMPv3 se analizaron mediante Wireshark en GNS3. Las actividades de gestión consistieron en cambiar el nombre los routers, dar de alta o cambiar la localización del mismo, solicitar número de interfaces, tablas de interfaces, tablas de enrutamiento de un router o incluso solicitar detalles de las tablas.

La simulación en Packet Tracer de la topología CEDIA se realizó en un equipo con 4 GB de RAM y un procesador Intel Core i7 de undécima generación, no se experimentaron problemas con la configuración de la topología, los protocolos la simulación y las actividades de gestión. Sin embargo, al intentar realizar la emulación en GNS3, se requirió ampliar la memoria RAM de 4 GB a 20 GB para poder inicializar los routers y las máquinas virtuales necesarias para reproducir la topología de CEDIA. Esto indica que, para estudiar redes avanzadas y trabajar con topologías complejas, se recomienda contar con un equipo que tenga un procesador igual o superior a Intel Core i7 de última generación o al menos 16 GB de

RAM. Estos recursos adicionales son necesarios para crear topologías más realistas y garantizar un rendimiento adecuado.

En cuanto al sistema operativo, no se experimentaron problemas a pesar de utilizar la última actualización disponible. Tanto el simulador como el emulador se ejecutaron correctamente, lo que indica que son compatibles con el sistema operativo utilizado en el proyecto.

Los beneficios del emulador GNS3 son significativos, ya que permite crear topologías de red realistas al incluir equipos backbone y trabajar con protocolos en sus últimas versiones. A diferencia de herramientas como Packet Tracer, GNS3 no tiene limitaciones en términos de funcionalidad y configuración, lo que nos brinda una experiencia más cercana a la realidad de las redes LAN y WAN. Al utilizar GNS3, podemos adquirir habilidades más avanzadas en el manejo de redes, ya que permite explorar y experimentar con una variedad de configuraciones de red. Esto incluye trabajar con protocolos de enrutamiento, configuración de dispositivos de red y realizar solución y pruebas de problemas en ambientes simulados. Además, GNS3 tiene una amplia comunidad de usuarios y recursos disponibles en línea, lo que facilita el aprendizaje y la colaboración con otros profesionales de redes. En general, GNS3 es una herramienta valiosa para aquellos que desean practicar y profundizar en redes, proporcionando una plataforma flexible y poderosa para la simulación y emulación de topologías de red. Quizás la limitación de GNS3 al usar equipos de backbone de cisco 7200 es que su máximo ancho de banda otorgado es 1 Gbps.

Los siguientes son los resultados mas importantes obtenidos:

1. Uso de recursos: Con Packet Tracer se realizó la simulación en donde se pudo observar un uso máximo de la RAM del 56 % y del CPU del 26 % con todos los equipos encendidos. Por otro lado, en la emulación con GNS3, utilizando direccionamiento IPv4 y teniendo todos los equipos encendidos, se alcanzó un uso de la RAM del 93.9 % y del CPU del 100 %. En el caso de la emulación con direccionamiento IPv6 y cuatro máquinas virtuales encendidas, se registró un uso del CPU del 100 % y de la memoria del 97.3 % en la mayoría de la emulación. Estos resultados indican que la emulación en GNS3 requiere más recursos en comparación con la simulación en Packet Tracer.

2. Tiempo de encendido: En cuanto al tiempo requerido para encender los dispositivos, se observó que en promedio tomó entre 3 y 5 minutos para encender todos los dispositivos en la topología. A nivel de máquinas virtuales,



el tiempo de encendido fue de aproximadamente 2 a 3 minutos por máquina. Estos tiempos son relevantes para tener en cuenta al trabajar con emuladores y simular topologías de redes complejas.

# Bibliografía

A guide to understanding SNMP - tech tip | SolarWinds.

Agencia de regulación y control de las telecomunicaciones, 2022. URL <http://www.arcotel.gob.ec/servicio-de-acceso-a-internet-sai2/>.

E. R. C. Acevedo. Transition plan of network protocol ipv4 to ipv6 in universidad industrial de santander. <https://docplayer.es/10068407-Plan-de-transicion-del-protocolo-de-red-ipv4-a-ipv6.html>, 2006. Accessed: Feb, 2023.

AfricaConnect2. AfricaConnect2. <https://archive.geant.org/projects/africconnect/ac2/Pages/Welcome%20to%20AfricaConnect2.html>. Accessed: Nov, 2022.

AsiaPacific. Asia Pacific Advanced Network. <https://apan.net>. Accessed: Nov, 2022.

M. Bakardjieva. *Internet society: The Internet in everyday life*. Sage, 2005.

CANARIE. Hikvision. <https://www.canarie.ca/scientific-research/>. Accessed: Nov, 2022.

J. I. Castillo and N. Galicia. Routing algorithms applied to an advanced academic network know as cuci. *IEEE Latin America Transactions*, 14 (6):2974–2979, 2016.

J.-I. Castillo-Velázquez and L.-C. Revilla-Melo. Management emulation of advanced network backbones in africa: 2019 topology. In *2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 1–4. IEEE, 2020.

J.-I. Castillo-Velazquez and J.-J. Sanchez-Trejo. Emulation for clara’s operation, the advanced network for latin america. In *2016 IEEE ANDESCON*, pages 1–4. IEEE, 2016.

- J.-I. Castillo-Velazquez and N.-G. Velazquez-Cruz. Emulation of the updated canarie backbone network topology under ipv6 up to 2022. *Proceedings of CECNet*, page 465, 2022.
- J.-I. Castillo-Velazquez, D.-J. Serrano-Martinez, and A. Morales. Emulation of backbone's connectivity and management for the advanced network in latin america: 2016's topology. In *2017 Sensors Networks Smart and Emerging Technologies (SENSET)*, pages 1–4. IEEE, 2017.
- J.-I. Castillo-Velázquez, V. R. C. Panduro, and W. R. M. Niño. Ipv6 connectivity and management emulation for reuna, the chilean advanced network. In *2018 IEEE XXV International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*, pages 1–4. IEEE, 2018.
- J.-I. Castillo-Velázquez, I. Varela-Sánchez, Y. Buendia-Gomez, and M.-K. Huerta. The pacific wave advanced network backbone: An emulation approach under ipv6. In *2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA)*, pages 37–43. IEEE, 2023.
- CEDIA. Red CEDIA Ecuador. <https://cedia.edu.ec>, a. Accessed: Mar, 2023.
- CEDIA. Publicaciones. <https://cedia.edu.ec/publicaciones/>, b. Accessed: Mar, 2023.
- CEDIA. Servicios. <https://cedia.edu.ec/folletos/>, c. Accessed: Mar, 2023.
- H. C. Clark. Formal knowledge networks: A syudy of candian experiences,. *Inst. for Sust. Dev*, pages 60–61, 1998 Ed Int.
- R. Coltun, D. Ferguson, and J. Moy. Rfc2740: Ospf for ipv6, 1999.
- R. Coltun, D. Ferguson, J. Moy, and A. Lindem. Rfc5340: Ospf for ipv6. Technical report, 2008.
- A. de Regulación y Control de las Telecomunicaciones. Internet: Boletín estadístico del sector de telecomunicaciones, 2023. URL <https://www.arcotel.gob.ec/internet-boletin-estadistico-del-sector-de-telecomunicaciones/>.
- S. E. Deering. Rfc1112: Host extensions for ip multicasting, 1989.

- S. Gaudet, N. Hill, P. Armstrong, N. Ball, J. Burke, B. Chapel, E. Chapin, A. Damian, P. Dowler, I. Gable, et al. Canfar: the canadian advanced network for astronomical research. In *Software and Cyberinfrastructure for Astronomy*, volume 7740, pages 577–586. SPIE, 2010.
- GEANT. GÉANT Global Connectivity Map. <https://geant3plus.archive.geant.net/Pages/Network/Global-Connectivity.html>. Accessed: Feb, 2023.
- N. W. Group et al. Rfc 2570-introduction to version 3 of the internet-standard network management framework. *The Internet Engineering Task Force*, 1999.
- GÉANT. GÉANT pan-European network Europe’s essential terabit-ready network is the most advanced and well-connected research and education network in the world. [www.geant.org/](http://www.geant.org/). Accessed: Nov, 2022.
- R. Hinden. Internet protocol, version 6 (ipv6) specification. *Request for Comments 2460*, 1998.
- M. Huerta, O. Calderon, and X. Hesselbach. Model for flows allocation and cost minimization in mpls networks. In *Proceedings of the Fifth IEEE International Caracas Conference on Devices, Circuits and Systems, 2004.*, volume 1, pages 244–248. IEEE, 2004.
- ITU. Global Connectivity Report 2022 - International Telecommunication Union Development Sector. <https://www.itu.int/hub/publication/d-ind-global-01-2022/>. Accessed: Mar, 2023.
- N. Jain and A. Payal. Comparison between IPv4 and IPv6 using OSPF and OSPFv3 on riverbed modeler. In *2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. IEEE, Dec. 2019. doi: 10.1109/ants47819.2019.9118101. URL <https://doi.org/10.1109/ants47819.2019.9118101>.
- C.-V. Jose-Ignacio, D.-J. Serrano-Martinez, and H. Monica. Management emulation for advanced networks interconnection in all america: 2019 topology. In *2019 IEEE 39th Central America and Panama Convention (CONCAPAN XXXIX)*, pages 1–6. IEEE, 2019.
- S. Kemp. Datareportal, 2023. URL <https://datareportal.com/reports/digital-2023-global-overview-report/>.

- L. Kleinrock. An early history of the internet [history of communications]. *IEEE Communications Magazine*, 48(8):26–36, 2010. doi: <http://doi.org/10.1109/mcom.2010.5534584>.
- J. Padilla, M. Huerta, J. Paradells, and X. Hesselbach. Intserv6: an approach to support qos over ipv6 networks. In *10th IEEE Symposium on Computers and Communications (ISCC'05)*, pages 77–82. IEEE, 2005.
- E. Y. Ramírez Díaz. Alternativas de configuración con el uso de los protocolos syslog y snmp para la gestión de red de redes avanzadas. 2019.
- Red\_Clara. Red CLARA. <https://redclara.net/index.php/es/>, a. Accessed: Mar, 2023.
- Red\_Clara. Red CLARA. <https://https://www.redclara.net/index.php/es/somos/redclara-la-organizacion/mision-vision-y-estatutos>, b. Accessed: Mar, 2023.
- RedCLARA. Servicios. <https://redclara.net/index.php/es/red>. Accessed: Mar, 2023.
- R. Rodríguez and D. Javier. *Implentación de una MIB para la generación de mensajes de alerta para la administración de un servidor de correo electrónico*. PhD thesis, Feb. 2009.
- E. Rosen, A. Viswanathan, and R. Callon. Multiprotocol label switching architecture. Technical report, 2001.
- G. Sain. Historia de internet (i). *Revista pensamiento penal*, 2015.
- J. I. C. Velázquez. Redes de datos contexto y evolución. 2<sup>a</sup>, 2016.
- J. I. C. Velázquez. *Redes de datos: Contexto y Evolución*. México, 2019.