



**UNIVERSIDAD ESTATAL
PENÍNSULA DE SANTA ELENA**

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TELECOMUNICACIONES

TRABAJO DE INTEGRACIÓN CURRICULAR

previo a la obtención del título de:

INGENIERA EN TELECOMUNICACIONES

**“DISEÑO E IMPLEMENTACIÓN DE MECANISMOS DE CONVERGENCIA
BRINDANDO CONEXIONES GPON PARA LA COMPARATIVA IPV4 E IPV6 EN
EL LABORATORIO DE TELECOMUNICACIONES.”**

AUTOR:

NATHALY NICOLE ORRALA VILLÓN

TUTOR:

ING. LUIS AMAYA FARIÑO, MGT

LA LIBERTAD – ECUADOR

2022-1



DEDICATORIA

A mi madre, por brindarme su apoyo incondicional, por no dejarme sola en este transcurso, por ser mi inspiración y mayor ejemplo a seguir, por enseñarme a ser una persona fuerte y valiente, por siempre salir adelante a pesar de los momentos difíciles.

A mi padre, que me enseñó a luchar por mis sueños, por haber tenido fe en mí siempre y que a pesar de que ya no está físicamente conmigo sigue siendo mi motivación para cumplir cada una de mis metas.

A mis hermanos, que siempre han estado presentes para aconsejarme y ayudarme, por ser el motivo para culminar este proyecto y poder brindarles un ejemplo de esfuerzo y constancia.

Nathaly Orrala Villón.

AGRADECIMIENTO

A Dios, por haberme brindado fortaleza, paciencia y sabiduría durante el desarrollo de este proyecto y por permitirme culminarlo con éxito.

A mis padres, Leonardo y Gloria, por su apoyo, esfuerzo y sacrificio para que pueda cumplir esta meta.

A mis hermanos Carmen y Peter, por su cariño y siempre confiar en mí.

A mis compañeros, por haberme ayudado en toda circunstancia y brindarme momentos y recuerdos inolvidables.

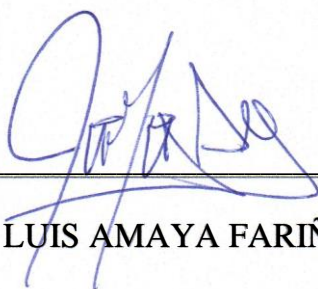
A mi tutor, por su paciencia y consejos brindados para poder culminar este proyecto.

Nathaly Orrala Villón.

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de titulación denominado “DISEÑO E IMPLEMENTACIÓN DE MECANISMOS DE CONVERGENCIA BRINDANDO CONEXIONES GPON PARA LA COMPARATIVA IPV4 E IPV6 EN EL LABORATORIO DE TELECOMUNICACIONES. ”, Elaborado por la estudiante Orrala Villón Nathaly Nicole, de la carrera de Telecomunicaciones de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes y autorizo al estudiante para que inicie los trámites legales correspondientes.

La Libertad, 1 de septiembre del 2022



ING. LUIS AMAYA FARIÑO, MGT



TRIBUNAL DE GRADO

Ing. Ronald Rovira Jurado, Ph. D.
DIRECTOR DE LA CARRERA
DE TELECOMUNICACIONES

Ing. Vladimir García Santos, Mgt.
DOCENTE ESPECIALISTA

Ing. Luis Amaya Fariño, Mgt.
DOCENTE TUTOR UIC

Ing. Corina Gonzabay De La A, Mgt.
SECRETARIA

RESUMEN

Desde la creación de Internet se ha desarrollado una gran demanda en cuestiones de conectividad, ancho de banda y direccionamiento IP para dispositivos finales, pues esto ha requerido que instituciones empiecen a migrar sus infraestructuras basadas en cableados de cobre a fibra óptica, así como también la implementación de mecanismos de transición para lograr la coexistencia de los protocolos IPv4 e IPv6 con la finalidad de obtener conexiones óptimas en diversos dispositivos electrónicos.

En la presente propuesta tecnológica se pretende diseñar e implementar una red con nuevo equipamiento que brinde conexiones de fibra óptica basado en un diseño previo en el software de Sketchup y en las normativas y estándares requeridos para su respectiva implementación, ya que mediante ello se podrá obtener una conectividad amplia y segura, además se pretende la implementación de direccionamiento IPv6 para la red interna del laboratorio de telecomunicaciones basado en la red actual con protocolo IPv4 mediante mecanismos de transición para la coexistencia de los mismos.

La finalidad de esta propuesta tecnológica es obtener una mejora en la infraestructura de la red interna del laboratorio, analizar el comportamiento y las diferencias de los protocolos al transmitir paquetes entre dispositivos finales, el paso al desarrollo de prácticas del direccionamiento IPv6 y el alcance de nuevos proyectos para los estudiantes de la carrera de telecomunicaciones.

ABSTRACT

Since the creation of the Internet, a great demand has developed in terms of connectivity, bandwidth and IP addressing for end devices, as this has required institutions that also begin to migrate their infrastructures based on copper wiring to fiber optics, as well as the Implementation of transition mechanisms to achieve the coexistence of IPv4 and IPv6 protocols in order to obtain optimal connections in various electronic devices.

In this technological proposal, it is intended to design and implement a network with new equipment that provides fiber optic connections based on a previous design in the Sketchup software and in the regulations and standards required for its respective implementation, since through this it will be possible to obtain a wide and secure connectivity, in addition, the implementation of IPv6 addressing for the internal network of the telecommunications laboratory based on the current network with IPv4 protocol is intended through transition mechanisms for their coexistence.

The purpose of this technological proposal is to obtain an improvement in the infrastructure of the internal network of the laboratory, to analyze the behavior and the differences of the protocols when transmitting packets between final devices, the step towards the development of IPv6 addressing practices and the scope of new projects for students of the telecommunications career.



DECLARACIÓN

El contenido del presente Trabajo de Graduación es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.

Nathaly Orrala

Nathaly Nicole Orrala Villón
AUTOR



INDICE DE CONTENIDO

DEDICATORIA.....	I
AGRADECIMIENTO	II
APROBACIÓN DEL TUTOR.....	III
TRIBUNAL DE GRADO	IV
RESUMEN.....	V
ABSTRACT.....	VI
DECLARACIÓN	VII
ÍNDICE DE FIGURAS.....	XIII
ÍNDICE DE TABLAS.....	XVI
ÍNDICE DE ABREVIATURAS.....	XVII
ÍNDICE DE ANEXOS.....	XIX
CAPÍTULO I.....	1
INTRODUCCIÓN	1
MARCO REFERENCIAL	2
1.1. ANTECEDENTES	2
1.2. DESCRIPCIÓN DEL PROYECTO	3
1.3. OBJETIVOS DEL PROYECTO	5
1.3.1. OBJETIVO GENERAL	5
1.3.2. OBJETIVOS ESPECÍFICOS.....	5
1.4. RESULTADOS ESPERADOS.....	5
1.5. JUSTIFICACIÓN	6
1.6. METODOLOGÍA	7
CAPÍTULO II.....	10
2.1. MARCO CONTEXTUAL	10
2.2. MARCO CONCEPTUAL	11
2.2.1. REDES DE COMUNICACIÓN	11
2.2.2. TIPOS DE REDES.....	11
2.2.2.1. REDES LAN	11

2.2.2.2.	REDES MAN	12
2.2.2.3.	REDES WAN	13
2.2.3.	TOPOLOGÍAS DE RED.....	14
2.2.3.1.	TOPOLOGÍA EN ESTRELLA.....	14
2.2.3.2.	TOPOLOGÍA EN BUS	14
2.2.3.3.	TOPOLOGÍA EN ANILLO	15
2.2.4.	REDES DE FIBRA ÓPTICA.....	16
2.2.4.1.	FIBRA ÓPTICA	16
2.2.4.2.	TIPOS DE CABLES DE FIBRA ÓPTICA	18
2.2.4.3.	TIPOS DE FIBRA ÓPTICA.....	18
2.2.5.	REDES GPON.....	20
2.2.5.1.	ESQUEMA DE RED GPON	21
2.2.5.2.	ELEMENTOS QUE COMPONEN LA RED GPON.....	22
2.2.6.	ESTÁNDARES Y ORGANISMOS DE ESTANDARIZACIÓN.....	26
2.2.6.1.	EIA	27
2.2.6.2.	TIA	27
2.2.6.3.	ANSI.....	27
2.2.6.4.	IEEE.....	27
2.2.6.5.	ITU	28
2.2.7.	NORMAS DE CABLEADO ESTRUCTURADO	28
2.2.7.1.	ANSI/TIA/EIA 568A	28
2.2.7.2.	ESTÁNDAR ANSI/TIA/EIA-568-B3.....	29
2.2.7.3.	ESTÁNDAR ANSI/TIA-568- C.....	29
2.2.7.4.	ANEXO ANSI/TIA/EIA-568-B.3-1	30
2.2.7.5.	CARACTERÍSTICAS ANSI/TIA/EIA-568-B.3-1.....	30
2.2.7.6.	ITU-T G.984x.....	31
2.2.8.	TCP/IP	32
2.2.8.1.	TCP/IP VERSIÓN 4.....	33
2.2.8.2.	TCP/IP VERSIÓN 6.....	35

2.2.9.	IPV6.....	37
2.2.9.1.	CARACTERÍSTICAS DE IPV6	37
2.2.9.2.	AUMENTO DE DIRECCIONES IP.....	38
2.2.9.3.	DIRECCIONAMIENTO IPv6	38
2.2.9.4.	PREFIJOS IPv6.....	39
2.2.10.	TIPOS DE DIRECCIONES.....	39
2.2.10.1.	MULTICAST.....	40
2.2.10.2.	UNICAST.....	41
2.2.10.3.	ANYCAST.....	42
2.2.11.	PROTOCOLO ICMP.....	44
2.2.11.1.	ICMPv4	44
2.2.11.2.	ICMPV6	46
2.2.12.	MECANISMOS DE TRANSICIÓN	48
2.2.12.1.	DUAL STACK.....	49
2.2.12.2.	TUNELIZACIÓN.....	50
2.2.12.3.	TRADUCCIÓN	56
2.2.12.4.	ELECCIÓN Y MECANISMO DE TRANSICIÓN A UTILIZAR	61
2.3.	MARCO TEÓRICO	62
CAPÍTULO III.....		64
3.1.	COMPONENTES DE LA PROPUESTA	64
3.1.1.	COMPONENTES FÍSICOS	64
3.1.1.1.	DREAM MACHINE PRO	64
3.1.1.2.	EDGEROUTER 4.....	64
3.1.1.3.	FIBER MEDIA CONVERTER.....	65
3.1.1.4.	UNIFI AC LITE.....	65
3.1.1.5.	MÓDULO DE FIBRA MULTIMODO 1G	66
3.1.1.6.	PATCHCORD DÚPLEX	67
3.1.2.	COMPONENTES LÓGICOS.....	67
3.1.2.1.	UNMS	67

3.1.2.2.	WIRESHARK	67
3.1.2.3.	SKETCHUP PRO	69
3.1.3.	DISEÑO Y DESPLIEGUE DE RED CON FIBRA ÓPTICA.....	69
3.1.3.1.	DISEÑO EN SKETCHUP PRO	71
3.1.3.2.	DESCRIPCIÓN DE UBICACIÓN Y CONEXIONES DE EQUIPOS	73
3.1.4.	SITUACIÓN DE LA RED ACTUAL DEL LABORATORIO DE TELECOMUNICACIONES.....	75
3.1.5.	CONFIGURACIÓN DE EQUIPOS	76
3.1.5.1.	CONFIGURACIÓN IPV4 EDGEROUTER.....	76
3.1.5.2.	CONFIGURACIÓN DE IPV4 EN UDM PRO	78
3.1.5.3.	CONFIGURACIÓN DE IPV4 EN AP AC-LITE	79
3.1.5.4.	CONFIGURACIÓN DE IPV4 EN RB2011 MIKROTIK.....	82
3.1.5.5.	DISEÑO LÓGICO DE RED IPV4 DEL LABORATORIO DE TELECOMUNICACIONES.....	85
3.1.6.	DESARROLLO DEL MECANISMO DE TRANSICIÓN	86
3.1.6.1.	ASIGNACIÓN DE DIRECCIONES	89
3.1.6.2.	DISEÑO LÓGICO DE RED IPV6 DEL LABORATORIO DE TELECOMUNICACIONES.....	93
3.1.7.	CONFIGURACIÓN DEL PROTOCOLO DE TRANSICIÓN	94
3.1.7.1.	CONFIGURACIÓN DE IPV6 EN EDGEROUTER.....	94
3.1.7.2.	CONFIGURACIÓN DE IPV6 EN UDM PRO	100
3.1.7.3.	CONFIGURACIÓN DE IPV6 EN RB MIKROTIK.....	102
3.1.7.4.	CONFIGURACIÓN DE DISPOSITIVOS FINALES.....	102
3.1.8.	ESTUDIO DE FACTIBILIDAD	105
3.1.8.1.	COSTO DE LA PROPUESTA.....	105
CAPÍTULO IV		107
4.1.	PRUEBAS DE FUNCIONALIDAD	107
4.1.1.	FUNCIONALIDAD IPV4 E IPV6 DEL AP UBIQUITI	107
4.1.2.	FUNCIONALIDAD IPV4 E IPV6 DEL AP MIKROTIK	110
4.2.	ANÁLISIS DE RESULTADOS	113



UPSE

Facultad de Sistemas y Telecomunicaciones Telecomunicaciones

4.2.1. ANÁLISIS DE LATENCIA Y PÉRDIDA DE PAQUETES DE LA RED UBIQUITI.....	113
4.2.2. ANÁLISIS DE LATENCIA Y PÉRDIDA DE PAQUETES DE LA RED MIKROTIK.....	116
4.3. COMPARATIVA DE LATENCIA EN UBIQUITI Y MIKROTIK.....	118
4.4. CAPTURA Y ANÁLISIS DE PAQUETES EN WIRESHARK.....	119
4.4.1. ANÁLISIS DE TRAMAS DE DIRECCIONAMIENTO	119
4.4.1.1. TRAMAS IPV4.....	120
4.4.1.2. TRAMAS IPV6.....	120
4.4.2. ANÁLISIS DE ESTRUCTURA DE PAQUETES	121
4.4.3. ANÁLISIS DEL PROTOCOLO ICMP.....	123
4.4.3.1. ANÁLISIS DE ICMPV4	123
4.4.3.2. ANÁLISIS DE ICMPv6	125
CONCLUSIONES.....	128
RECOMENDACIONES.....	129
BIBLIOGRAFÍA.....	130
ANEXOS.....	133

ÍNDICE DE FIGURAS

Figura 1 Diagrama de bloques de las fases del proyecto.....	8
Figura 2 Red LAN	12
Figura 3 Red MAN	13
Figura 4 Red WAN.....	13
Figura 5 Topología en estrella	14
Figura 6 Topología en bus	15
Figura 7 Topología en Anillo.....	15
Figura 8 Estructura del cable de fibra óptica	17
Figura 9 Fibra monomodo	19
Figura 10 Fibra multimodo	20
Figura 11 Esquema de una red GPON.....	22
Figura 12 OLT de 4 puertos PON.....	23
Figura 13 Divisor óptico	24
Figura 14 Conector de fibra óptica de tipo SC	25
Figura 15 Conector de fibra óptica tipo LC/PC.....	26
Figura 16 Segmento IPv4	33
Figura 17 Formato de cabecera IPv6	36
Figura 18 Formato de IPv6	38
Figura 19 Multicast.....	41
Figura 20 Unicast.....	42
Figura 21 Anycast.....	43
Figura 22 Formato de mensajes ICMPv4	45
Figura 23 Formato de mensajes ICMPv6	47
Figura 24 Funcionamiento de Dual Stack.....	49
Figura 25 Funcionamiento de tunelización.....	50
Figura 26 Funcionalidad de Tunnel Broker.....	52
Figura 27 Funcionamiento de túnel 6to4	54
Figura 28 Funcionamiento de ISATAP	55
Figura 29 Túnel TEREDO.....	56
Figura 30 Funcionamiento de NAT-PT	57
Figura 31 Traducción SIIT	58
Figura 32 Funcionamiento NAT64.....	59
Figura 33 Traducción BIS.....	60
Figura 34 UDM Pro-Ubiquiti	64
Figura 35 EdgeRouter 4 Ubiquiti.....	65
Figura 36 Fiber Media Converter	65
Figura 37 Unifi AC Lite – Ubiquiti	66



UPSE

Figura 38 Interfaz gráfica de Wireshark	68
Figura 39 Interfaz gráfica de SketchUp Pro	69
Figura 40 Diseño de la propuesta	70
Figura 41 Ubicación del rack.....	71
Figura 42 Ubicación de equipos	72
Figura 43 Vista general del diseño del laboratorio	72
Figura 44 Polaridad de conexión para cable multimodo	74
Figura 45 Conexiones del transceiver.....	74
Figura 46 Ingresar a configuración básica.....	76
Figura 47 Configuración puerto WAN	77
Figura 48 Configuración puertos LAN.....	77
Figura 49 Interfaces del EdgeRouter	78
Figura 50 Dirección IPv4 del UDM Pro.....	79
Figura 51 Red LAN Ipv4 UDM Pro	79
Figura 52 Configuración UAP AC Lite.....	80
Figura 53 Configuración UAP AC Lite.....	81
Figura 54 Características de la configuración del UAP AC Lite.....	81
Figura 55 Lista de direcciones IPv4 Mikrotik	82
Figura 56 Añadir DHCPv4 en Mikrotik	83
Figura 57 Ventana DHCP Setup.....	83
Figura 58 Configuración DNS.....	84
Figura 59 Configuración de interfaz inalámbrica	84
Figura 60 Configuración de seguridad del AP.....	85
Figura 61 Diseño nuevo de red IPv4 en el laboratorio	86
Figura 62 Mapeo de dirección IPv4 pública.....	88
Figura 63 Mapeo de dirección IPv4 privada.....	89
Figura 64 Diseño de red IPv6 en el laboratorio.....	93
Figura 65 Interfaz de línea de comandos del EdgeRouter	94
Figura 66 Configuración del túnel.....	96
Figura 67 Interfaces del router configuradas	96
Figura 68 Configuración de IPv6 en bridge.....	97
Figura 69 Bridge en IPv4 e IPv6	97
Figura 70 Configuración DHCPv6	98
Figura 71 Configuración de anuncios de enrutador.....	99
Figura 72 Tabla de rutas IPv6.....	99
Figura 73 Ingreso a la configuración de la red	100
Figura 74 Configuración avanzada de la red LAN	100
Figura 75 Configuración de IPv6 en UDM Pro.....	101



UPSE

Figura 76 Configuración IPv6 en RB Mikrotik.....	102
Figura 77 Habilitar protocolo IPv6 en PC	103
Figura 78 Asignación de dirección IPv6.....	104
Figura 79 Detalles de la red en IPv4 e IPv6	104
Figura 80 Detalles de la red mediante símbolo del sistema.....	105
Figura 81 Direcciones IPv4 e IPv6 del Host 1 de la red Ubiquiti	108
Figura 82 Direcciones IPv4 e IPv6 del Host 2 de la red Ubiquiti	108
Figura 83 Prueba 1 de red Ubiquiti.....	109
Figura 84 Prueba 2 de red Ubiquiti.....	109
Figura 85 Prueba 3 de red Ubiquiti.....	110
Figura 86 Direcciones IPv4 e IPv6 del Host 1 de la red Mikrotik.....	111
Figura 87 Direcciones IPv4 e IPv6 del Host 2 de la red Mikrotik.....	111
Figura 88 Prueba 1 de red Mikrotik.....	112
Figura 89 Prueba 2 de red Mikrotik.....	112
Figura 90 Prueba 3 de red Mikrotik.....	113
Figura 91 Comparativa de latencia Ubiquiti y Mikrotik.....	119
Figura 92 Tramas en direccionamiento IPv4	120
Figura 93 Tramas en direccionamiento IPv6.....	121
Figura 94 Paquete IPv4.....	122
Figura 95 Paquete IPv6.....	122
Figura 96 Captura del protocolo ICMP para IPv4.....	123
Figura 97 Solicitud de eco en IPv4.....	124
Figura 98 Respuesta de eco en IPv4.....	125
Figura 99 Captura del protocolo ICMP para IPv6.....	125
Figura 100 Solicitud de eco en IPv6.....	126
Figura 101 Respuesta de eco en IPv6.....	127

ÍNDICE DE TABLAS

Tabla 1	Ventajas y limitaciones de la fibra óptica	17
Tabla 2	Características técnicas y mecánicas de la fibra óptica	30
Tabla 3	Normativa ITU-T G.984x	31
Tabla 4	Diferencias de IPv4 e IPv6 en los tipos de direccionamiento.....	44
Tabla 5	Mensajes ICMPv4.....	46
Tabla 6	Mensajes ICMPv6.....	48
Tabla 7	Tiempos de convergencia de tunelización	53
Tabla 8	Tabla comparativa de mecanismos de transición.....	60
Tabla 9	Características del módulo SFP 1G MM	66
Tabla 10	Características del cable patchcord dúplex	67
Tabla 11	Conexión de equipos mediante puertos	71
Tabla 12	Equipos de la red del laboratorio	75
Tabla 13	Dispositivos finales.....	76
Tabla 14	Asignación de direcciones IPv6.....	90
Tabla 15	Creación de subredes	91
Tabla 16	Direccionamiento IPv6	92
Tabla 17	Consideraciones para configurar 6to4	95
Tabla 18	Costo de equipos.....	106
Tabla 19	Latencia con protocolo IPv4	114
Tabla 20	Latencia con protocolo IPv6	115
Tabla 21	Latencia con protocolo IPv4	116
Tabla 22	Latencia con protocolo IPv6	117
Tabla 23	Diferencias de latencia en las redes implementadas	118

ÍNDICE DE ABREVIATURAS

ABREVIATURA	SIGNIFICADO
ANSI	American National Standards Institute Instituto Americano de Estándares Nacionales
APC	Angled Physical Contact Contacto físico anulado
DHCPv6	Dynamic Host Configuration Protocol version 6 Protocolo de Configuración dinámica de Host
DNS	Domain Name System Sistema de Nombres de Dominio
EIA	Electronic Industries Alliance Alianza de Industrias Electrónicas
GPON	Gigabit Passive Optical Network Red Óptica Pasiva con Capacidad de Gigabit
ICMP	Internet Control Message Protocol Protocolo de Mensaje de Control de Internet
IEEE	Institute of Electrical and Electronics Engineers Instituto de Ingenieros Eléctricos y Electrónicos
IETF	Internet Engineering Task Force Grupo de Trabajo de Ingeniería de Internet
IPv4	Internet Protocol Version 4 Protocolo de Internet Versión 4
IPv6	Internet Protocol Version 6 Protocolo de Internet Versión 6
ITU	International Telecommunication Union Unión Internacional de Telecomunicaciones
LAN	Local Area Network Red de Área Local
LC	Lucent Connector Conector lucent
MAN	Metropolitan Area Network Red de Área Metropolitana
NAT	Network Address Translation Traducción de direcciones de red
OLT	Optical Line Terminal Terminal de Línea Óptica
ONT	Optical Network Terminal Terminal de Red Óptica
RA	Router advertisement





Facultad de Sistemas y Telecomunicaciones Telecomunicaciones

	Anuncio de enrutador
RFC	Request for Comments Solicitud de comentarios
SC	Suscriptor Conector Conector de suscriptor
SFP	Small Form Factor Pluggable Factor de forma pequeño conectable
TCP/IP	Transfer Control Protocol/Internet Protocol Protocolo de Control de Transmisión/Protocolo de Internet
TIA	Telecommunications Industry Association Asociación de la Industria de Telecomunicaciones
TTL	Time To Live Tiempo de vida
UPC	Ultra Physical Contact Contacto Ultra Físico
UPSE	Universidad Estatal Península de Santa Elena
WAN	Wide Area Network Red de Área Amplia





ÍNDICE DE ANEXOS

Anexo 1: Configuración de firewall en las máquinas para permitir comunicación IPv4 e IPv6 en la red LAN. 133
Anexo 2 Ubicación de UAP AC Lite 135
Anexo 3 Conexión de cable multimodo 136
Anexo 4 Conexión de equipos..... 136
Anexo 5 Armado final del Rack 137



CAPÍTULO I

INTRODUCCIÓN

En la actualidad es necesario estar a la vanguardia de las tecnologías de telecomunicaciones ya que mediante él se brindan diversos tipos de servicios indispensables en el diario vivir, también se debe considerar que dichos servicios requieren de múltiples dispositivos conectados a la red por ello es importante optar por la adquisición de nuevas tecnologías y la implementación de mecanismos de convergencia que permitan aumentar la conectividad de una alta cantidad de dispositivos sin tener problemas de direccionamiento.

El presente proyecto consta de cuatro capítulos. El capítulo I detalla puntos importantes acerca de la implementación del proyecto en el que se mencionan los antecedentes, la descripción del proyecto, objetivos, justificación y metodología.

El capítulo II se compone de marco contextual, conceptual y teórico, se detallan conceptos y bases teóricas que sirven para el conocimiento y la implementación adecuada del proyecto.

El capítulo III muestra el desarrollo de la propuesta, se presenta el diseño de la red en Sketchup, la ubicación de equipos, la conexión e instalación basado en los estándares, las configuraciones para brindar direccionamiento en IPv4 e IPv6 y el estudio de factibilidad del proyecto.

El capítulo IV se basa en presentar las pruebas de funcionamiento en la red implementada, además de realizar análisis de paquetes en Wireshark y comparativa entre redes Ubiquiti y Mikrotik.

MARCO REFERENCIAL

1.1. ANTECEDENTES

La evolución de las telecomunicaciones que se ha dado durante los últimos años ha requerido que los usuarios necesiten conexiones a altas velocidades en la transmisión de información, esto ha provocado que las redes tradicionales se saturen de forma que se deba buscar alternativas con tecnología actual que brinde un mayor ancho de banda.

Una de las alternativas implementada actualmente es el despliegue de GPON la cual utiliza tecnología de acceso a través de fibra óptica, la fibra óptica es un medio guiado para transmitir información mediante ella se han podido obtener ventajas importantes como: inmunidad a interferencias electromagnéticas, mayor ancho de banda, disminución en la degradación de señales, entre otras.

El crecimiento de usuarios y dispositivos con nuevas tecnologías que requieren de acceso a los servicios de Internet ha provocado un agotamiento de direcciones IPv4, las cuales se han utilizado desde su creación hace más de 20 años, esta versión utiliza un espacio de direcciones de 32 bits, por lo que tiene un límite de 4.294.967.296 direcciones, debido a esto el IETF habría estado trabajando en una nueva versión de IP desde el año 1994, denominada IPV6 permitiendo el crecimiento de internet con sus direcciones.

La coexistencia entre las dos versiones de direccionamiento mencionadas surgió con el fin de no pasar de una manera abrupta desde una versión a otra, de tal manera que se propuso y se diseñó diversos mecanismos de transición, que se clasifican en: Dual Stack, tunelización y mecanismo basado en traducción.



UPSE

La adopción de IPv6 en el Ecuador se da a finales del 2011 cuando el Ministerio de Telecomunicaciones y de la Sociedad de la Información realizó un diseño y construcción de políticas con diferentes entidades del país para la transición y coexistencia entre IPv4 e IPv6 de manera ordenada, de tal manera que hasta el año 2020 Ecuador representaba un 17% en la adopción de IPv6 en el ámbito regional de Sudamérica y en la actualidad representa un 40% en la adopción a nivel nacional.

El laboratorio de telecomunicaciones de la Universidad Estatal Península de Santa Elena situada en el cantón La Libertad de la Provincia de Santa Elena brinda una cantidad de equipos de diversas marcas que ayudan al fortalecimiento y la aplicación de conocimientos prácticos y teóricos de los estudiantes.

Es importante destacar que el laboratorio tiene una red en funcionamiento utilizando direcciones IPv4 para los equipos o dispositivos que se conectan a dicha red, el presente proyecto busca mediante mecanismos de transición la coexistencia entre IPv4 e IPv6 mediante la implementación de nuevos equipos y tecnologías que permitirán a los estudiantes de la carrera de telecomunicaciones realizar diversas prácticas para la adquisición de aprendizaje de forma dinámica e intuitiva.

1.2. DESCRIPCIÓN DEL PROYECTO

La idea principal en este proyecto tecnológico es poder realizar un diseño e implementación de una red con fibra óptica en el laboratorio de telecomunicaciones que permita una tasa alta de transmisión de información con direccionamiento IPv6 para conectar múltiples dispositivos a la red interna, además se pretende la adquisición, y configuración de nuevos equipos y herramientas para los estudiantes.



UPSE

El presente proyecto consiste en brindar soluciones para el mejoramiento en el aprendizaje de los estudiantes que conforman la carrera de telecomunicaciones mediante nuevos equipos y el desarrollo de prácticas en el área de redes como configuración y direccionamiento en IPv6, métodos de coexistencia e implementación adecuada de redes de fibra de modo que se pueda contribuir al aumento de prácticas en el laboratorio.

Se pretende crear una red GPON que cumpla con los estándares emitidos por la unión Internacional de Telecomunicaciones como es el estándar ITU-T G.984 que describe de manera general las características de redes de acceso de fibra, medios físicos, convergencia de transmisión, entre otros; para poder realizar un correcto cableado estructurado en el laboratorio se deberá aplicar el estándar ANSI/TIA/EIA 568 A.

El estándar ANSI/TIA/EIA 568 B.3 – 1 permitirá conocer y aplicar los requerimientos y elementos de transmisión para realizar el cableado de la red de fibra.

Luego que se haya implementado la red GPON con los estándares y normativas mencionadas se deberá hacer las respectivas configuraciones en los equipos para el correcto funcionamiento de la red, en este punto se realizará la implementación de puntos de acceso.

Posteriormente, se deberá configurar el mecanismo de transición que hará la coexistencia entre la red IPv4 e IPv6 del laboratorio, para ello se optó por la utilización de equipos de la marca Ubiquiti, ya que estos admiten y soportan ambos direccionamientos, la línea de equipos cuenta con interfaces amigables para realizar configuraciones rápidas y sencillas, además se puede tener un control en tiempo real de nuestra red en su interfaz gráfica principal.

Por último, se deberá demostrar que la red del laboratorio admite direccionamiento IPv4 e IPv6, esto se puede realizar mediante capturadores de paquetes cuando un dispositivo compatible con IPv6 se conecte a la red.



UPSE

El proyecto permitirá desarrollar prácticas relacionadas al área de telecomunicaciones tales como: conocimiento y uso correcto de los estándares de cableado estructurado, configuración de mecanismos de transición, entre otros.

1.3. OBJETIVOS DEL PROYECTO

1.3.1. OBJETIVO GENERAL

Diseñar e implementar mecanismos de convergencia brindando conexiones GPON para la comparativa ipv4 e ipv6 en el laboratorio de Telecomunicaciones.

1.3.2. OBJETIVOS ESPECÍFICOS

- Aplicar técnicas y normativas en redes para establecer comunicación a gran velocidad entre una red de fibra y un sistema de cableado estructurado.
- Efectuar mecanismos de transición para brindar el servicio de enrutamiento a través de IPV6.
- Evaluar la fluctuación de la red IPv4 e IPv6 basadas en promedios de latencia y en las tramas de direccionamiento.

1.4. RESULTADOS ESPERADOS

Una vez concluida la propuesta tecnológica con la implementación de una red con direccionamiento IPV6 ejecutando mecanismos de transición y con conexiones GPON, se espera obtener los siguientes resultados:

- Permitir un correcto funcionamiento de las conexiones de fibra óptica con respecto a los estándares en la coexistencia de la red a implementar.

- Proporcionar a los dispositivos finales conexiones a frecuencias de 5 GHz y direccionamiento en IPv4 e IPv6.
- Adquirir valores de latencias de paquetes en IPv4 y en IPv6 que permitan evidenciar la comparativa de los direccionamientos.

1.5. JUSTIFICACIÓN

Las conexiones a alta velocidad juegan un papel importante en la actualidad, por lo que la implementación de una red de fibra óptica puede brindar a los usuarios del laboratorio el acceso a servicios de Internet con una gran capacidad de ancho de banda, evitando saturaciones, pérdidas de conexión en la red y ayudando a mejorar las necesidades tecnológicas.

El transporte de datos con fibra óptica tiene una gran acogida en el ámbito de las comunicaciones, ya que además de altas velocidades de transmisión también ofrece una subida y bajada rápida de información, mejora la calidad de audio y video de transmisiones online, minimiza interferencias electromagnéticas y es más segura que otros medios de transmisión.

El internet es una herramienta fundamental hoy en día, por lo que su crecimiento a nivel mundial ha provocado que las direcciones IPv4 se agoten limitando el desarrollo progresivo de nuevas tecnologías como es el Internet de las Cosas (IoT), debido a esto las entidades buscan implementar un nuevo protocolo de direccionamiento en sus infraestructuras de comunicaciones que garantice cubrir las falencias del protocolo antecesor y mejorar la seguridad de la red.

Ante la problemática descrita surge el protocolo de internet versión 6, que busca satisfacer las necesidades de IPv4 permitiendo generar más de 340 sextillones de direcciones IP diferentes utilizando un tamaño de 128 bits, además se pueden mencionar otras ventajas como: mayor



UPSE

seguridad de información y autenticación de paquetes para una transmisión confiable y segura de datos, mecanismo sencillo de autoconfiguración, velocidad de transmisión, eficiencia en la gestión de paquetes, entre otras.

Es fundamental considerar que la red interna del laboratorio de telecomunicaciones de la Universidad Estatal Península de Santa Elena se actualice y asegure su funcionamiento a largo plazo, por ello es importante implementar un método de coexistencia para que la red interna admita direccionamiento IPv4 e IPv6, el uso de nuevo equipamiento tecnológico actualizado y con tendencia en el mercado hará que la red sea optimizada, segura y permitirá una conectividad a dispositivos y servicios que continúan utilizando direccionamiento IPV4, al incorporar una nueva marca de dispositivos se podrá realizar la comparativa con equipos ya disponibles en el laboratorio como es la marca Mikrotik obteniendo así un análisis de como ambas marcas manejan la coexistencia de direcciones en la red interna.

Con la implementación de este proyecto, se pretenderá mejorar la calidad de aprendizaje de los estudiantes desarrollando nuevas prácticas en las materias relacionadas, además por medio de estudiantes se podrán crear nuevos proyectos experimentales y de investigación desplegándose en diferentes aplicaciones que tiene el direccionamiento IPv6, consiguiendo un mejor desarrollo intelectual de los estudiantes y el crecimiento tecnológico del laboratorio de Telecomunicaciones.

1.6. METODOLOGÍA

El presente proyecto se regirá mediante las siguientes metodologías de investigación:

- Investigación Exploratoria

Comprende la recopilación de información de fuentes documentales basado en redes de fibra óptica, estándares adecuados para fibra óptica, direccionamiento IPv6 y diferentes métodos de coexistencia.

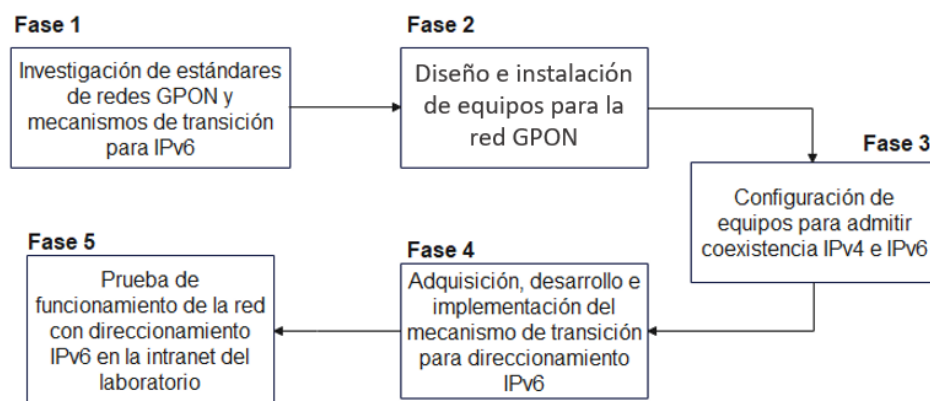
- Investigación Aplicada

La información que se obtenga ayudará a definir y aplicar el contenido necesario para implementar el tema propuesto, con la implementación se pretenderá realizar diferentes pruebas de los equipos que comprueben el correcto funcionamiento de la red de fibra óptica con direccionamiento IPV6 en el laboratorio.

A continuación, se presentan las fases del proyecto que harán posible el cumplimiento de los objetivos:

Figura 1

Diagrama de bloques de las fases del proyecto



Elaborado por el autor

Fase 1: Investigación de estándares de redes GPON y mecanismos de transición para IPv6

Se analizarán y estudiarán los estándares necesarios para la correcta implementación de la red GPON como son el ITU-T G.984, ANSI/TIA/EIA 568 A y ANSI/TIA/EIA 568 B.3 – 1, así mismo la investigación acerca de los mecanismos de transición más conocidos como dual stack, tunelización y traducción, para así obtener un mayor conocimiento e implementar la propuesta de manera correcta.



UPSE

Fase 2: Diseño e instalación de equipos para la red GPON

Se realizará un diseño previo a la implementación mediante el software Sketchup, el cual se basará en los estándares y normativas estudiadas en la primera fase, de esta manera se podrá obtener un esquema claro de la ubicación de los equipos en el rack del laboratorio.

Fase 3: Configuración de equipos para admitir coexistencia IPv4 e IPv6

En esta sección se deberá habilitar el direccionamiento IPv6 en cada componente hardware y software que formará parte de la nueva red del laboratorio, además de la activación del tipo de mecanismo a utilizar para su posterior configuración.

Fase 4: Adquisición, desarrollo e implementación del mecanismo de transición para direccionamiento IPv6

Se deberá adquirir un nuevo plan de direccionamiento IPv6 que se registrará bajo los tipos de direccionamiento anycast, multicast y unicast; el bloque de direcciones IPv6 dependerá de la red IPv4 del laboratorio. Para la configuración se hará uso de protocolos de enrutamiento y el nuevo diseño topológico de la red, lo cual permitirá la coexistencia de la infraestructura actual con IPv6.

Fase 5: Prueba de funcionamiento de la red con direccionamiento IPv6 en la intranet del laboratorio

Se deberá comprobar la conectividad de la red interna a Internet por medio de fibra óptica, las pruebas de funcionamiento de IPv6 y la coexistencia de IPv4 e IPv6 permitirán comprobar que cada equipo de la red admita y soporte el nuevo protocolo de direccionamiento de manera que se pueda realizar una comparativa.

CAPÍTULO II

2.1. MARCO CONTEXTUAL

La Universidad Estatal Península de Santa Elena ubicada en el cantón La Libertad, está orientada a formar profesionales de excelencia en las diferentes carreras que ésta oferta, a partir del año 2018 se dio apertura a nuevas carreras, en la cual la facultad de Sistemas y Telecomunicaciones empezó a ofertar la carrera de Telecomunicaciones, en la actualidad la carrera mencionada brinda un laboratorio con equipos como switch, routers, OLT, clouds, cámaras, entre otros; destacando las marcas de Cisco y Mikrotik.

Por otro lado, el laboratorio mantiene una red en funcionamiento con direccionamiento IPV4 utilizando para esto las marcas mencionadas anteriormente, es importante que el laboratorio de telecomunicaciones esté constituido de una gran variedad de equipos con diferentes interfaces, modos de configuración y principalmente que tengan un gran alcance en el mercado de forma general, ya que de esta manera los docentes que imparten las materias de unidad profesional de la malla curricular de la carrera y los estudiantes obtengan una mayor eficacia en sus conocimientos prácticos.

El laboratorio de telecomunicaciones de la universidad requiere de una propuesta e implementación para la respectiva coexistencia de IPV4 e IPV6 utilizando mecanismos de transición, la implementación de IPV6 requiere de equipos con tecnología avanzada que permita y soporte configuraciones IPV6, por lo que se optará la adquisición de una nueva marca de equipos para el laboratorio como es Ubiquiti.

Este proyecto se basa en crear una red que brinde conexiones por medio de fibra óptica y admitir el direccionamiento IPV6 en la intranet mediante métodos de transición para obtener una



UPSE

convergencia entre las dos versiones de direccionamiento, ampliación de las direcciones IP y un mejor rendimiento de la red que se encuentra en el laboratorio.

2.2. MARCO CONCEPTUAL

2.2.1. REDES DE COMUNICACIÓN

Una red de comunicación es un conjunto de hosts conectados entre sí a través de un medio físico, tiene como finalidad optimizar y compartir información, juegan un papel importante en la facilitación de la comunicación en redes globales y proporcionan una plataforma de servicios que permite conectarnos, local y globalmente con otros usuarios.

Los elementos que aseguran la transmisión de información en una red de datos son los medio al que se conectan los dispositivos de la red que cumplen con acuerdos y estándares que disponen su funcionamiento.

2.2.2. TIPOS DE REDES

Para que exista una comunicación entre dispositivos de una red, es necesario que éstos se conecten de forma independiente entre sí permitiendo el intercambio de información, los tipos de redes según su alcance más conocidos y utilizados se detallan a continuación.

2.2.2.1. REDES LAN

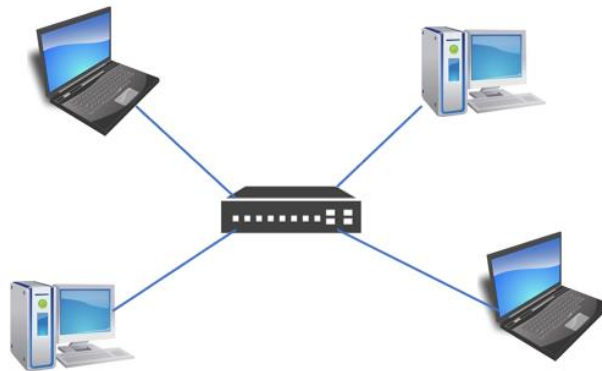
Una red de Área Local (Local Area Network) conecta uno o más dispositivos en un espacio limitado como una oficina, una planta de un edificio o un campus universitario, este tipo de red alcanza una velocidad de hasta 10 Gbps.

UPSE

La tecnología que emplea las redes LAN para la interconexión de dispositivos mediante ethernet, es decir, redes cableadas que facilitan su uso, y mediante Wi-Fi en el que los dispositivos se conectan de forma inalámbrica a un punto de acceso. (Santos, 2015)

Figura 2

Red LAN



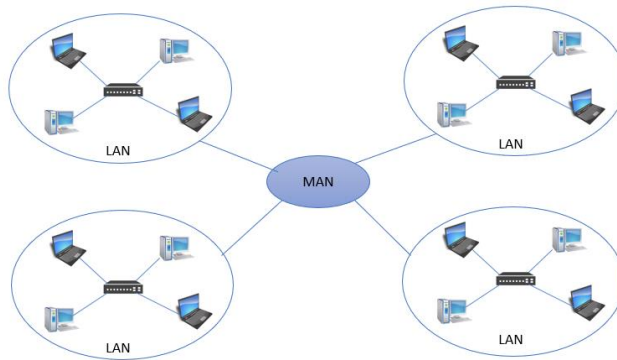
Elaborado por el autor

2.2.2.2. REDES MAN

Una red de Área Metropolitana (Metropolitan Area Network) es un conjunto de redes LAN conectadas, por lo que contribuye un área más extensa, su uso se da en diferentes ubicaciones dentro de un centro de población o en varios centros muy próximos donde todos pertenecen a una misma unidad organizativa. En su mayoría las redes MAN utilizan cables de fibra óptica para emplear interconexiones entre las LAN. (Santos, 2015)

UPSE
Figura 3

Red MAN



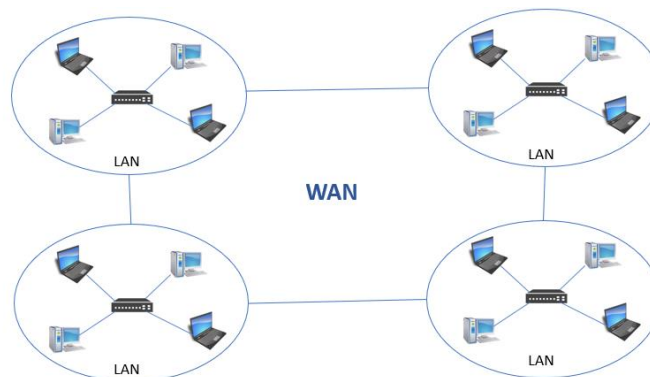
Elaborado por el autor

2.2.2.3. REDES WAN

La Red de Área Ampla (Wide Area Network) permite interconectar hosts de diversas zonas geográficas separadas por enormes distancias, su medio de transmisión puede ser la fibra óptica, cable coaxial o cables telefónicos, un ejemplo común de red WAN es Internet que conecta a miles de usuarios por medio de redes WAN regionales. (Santos, 2015)

Figura 4

Red WAN



Elaborado por el autor

2.2.3. TOPOLOGÍAS DE RED

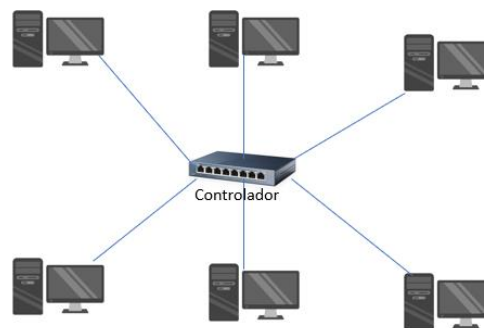
En redes de comunicaciones topología indica la forma física o lógica en la que está diseñada la red o la manera en la que se conectan los dispositivos, se pueden distinguir tres topologías básicas que se detallan a continuación.

2.2.3.1. TOPOLOGÍA EN ESTRELLA

La topología en estrella conecta estaciones entre sí por medio de un controlador central, es decir, cada estación deberá estar conectado a dicho concentrador, es utilizado en redes LAN y tiene las ventajas de fácil administración y optimización de recursos, en cuanto a su mayor desventaja es que si el concentrador falla toda la red tiende a fallar ocasionando la pérdida de conexión entre hosts. (Abad Domingo, 2013)

Figura 5

Topología en estrella



Elaborado por el autor

2.2.3.2. TOPOLOGÍA EN BUS

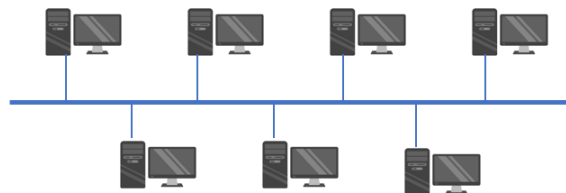
La forma de conexión de los dispositivos es mediante un medio de transmisión común por lo que la información se direcciona en ambos sentidos por toda la red haciendo que todos los dispositivos

UPSE

que conforman la red reciban la información enviada por uno, su principal desventaja es que si el cable que interconecta a los hosts se avería ya no habrá conexión. (Abad Domingo, 2013)

Figura 6

Topología en bus



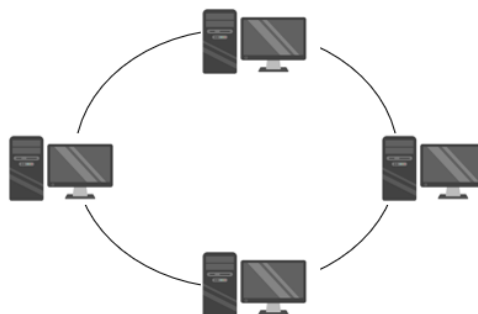
Elaborado por el autor

2.2.3.3. TOPOLOGÍA EN ANILLO

Los hosts se conectan en torno a un anillo físico, por lo que todos están conectados entre sí haciendo que el último host se conecte con el primero y la información circule en una misma dirección, tiene la desventaja de que si el anillo se avería en algún punto toda la red fallaría perdiendo conexión. (Abad Domingo, 2013)

Figura 7

Topología en Anillo



Elaborado por el autor



UPSE

2.2.4. REDES DE FIBRA ÓPTICA

La red de fibra óptica es una red de telecomunicaciones que permite la transferencia de datos a altas velocidades mediante tecnología basada en fibra óptica, este tipo de medio de transmisión sustituye a los tradicionales radioenlaces y redes de cobre utilizadas desde la invención del teléfono para la transmisión de voz y posteriormente mejoradas para soportar la transmisión de datos.

La principal ventaja de una red de fibra es una tasa alta de transferencia de datos con respecto a su ancho de banda, además las redes de fibra óptica utilizan una única red de transporte para brindar servicios de voz, datos y video permitiendo reducir costos de instalación y mantenimiento.

Definitivamente las redes de fibra permiten desarrollar, implementar y brindar una gama de servicios como una buena velocidad de bajada y subida de información, televisión en alta definición y juegos online.

2.2.4.1. FIBRA ÓPTICA

Es un medio de transmisión guiado que hace posible la comunicación a largas distancias y a velocidades altas (Gbps), se propaga mediante pulsos de luz y está fabricada por una fibra de vidrio silíceo en su interior que tiene una forma cilíndrica muy delgada y un revestimiento que protege la luz en el interior haciendo posible los fenómenos de reflexión y refracción.

Los cables ópticos están diseñados para admitir señales de luz, se trata de tres capas como se puede observar en la figura 8, la primera es un cilindro con una pequeña sección transversal flexible, llamado núcleo que tiene un diámetro de 8 a 125 μm a través del cual puede viajar la luz, la siguiente capa denominada revestimiento asegura que toda la luz se mantenga en el núcleo de

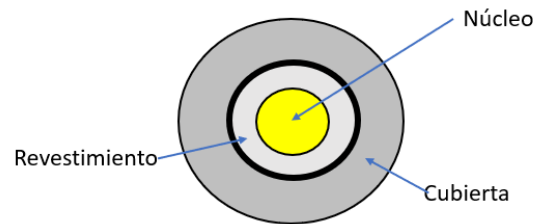
UPSE

manera uniforme y la tercera capa es una cubierta plástica que protege a la fibra de daños externos.

(Santos, 2015)

Figura 8

Estructura del cable de fibra óptica



Elaborado por el autor

Tabla 1

Ventajas y limitaciones de la fibra óptica

Ventajas	Limitaciones
Mayor ancho de banda y gran velocidad de transmisión	Requiere de equipos, herramientas y personal capacitado para su manipulación.
La baja atenuación y dispersión reduce pérdidas de la señal.	Si la distancia entre Tx y Rx es significativamente amplia se necesitará repetidores.
Diámetro y peso reducido por lo que ocupa menos espacio.	El servicio de transmisión de datos resulta costoso.
Mayor seguridad durante la transmisión	Altos costos para su implementación

La inmunidad a las EMI (Interferencias electromagnéticas) evita ruidos o perturbaciones durante la transmisión de información.

Es de material muy sensible por lo que puede averiarse y su reparación es dificultosa.

Nota: La table muestra las ventajas y limitaciones importantes que se deben considerar de la fibra óptica. (Tomasi, 2003)

2.2.4.2. TIPOS DE CABLES DE FIBRA ÓPTICA

Existen diversos tipos de fibra que se pueden clasificar generalmente en tres categorías detalladas a continuación:

Simples: Está compuesto por una sola fibra que permite transmitir información en un solo sentido y se emplea para interconectar equipos en áreas reducidas.

Dobles: Se compone de dos fibras, permite una transmisión full-duplex, es utilizado en redes LAN o para interconectar equipos en racks.

Multifibras: El cable multifibra está compuesta por varias fibras en ocasiones agrupadas una al lado de la otra y se usa comúnmente para establecer una red o un sistema de comunicación que procesa una gran cantidad de información y/o conecta varios nodos, terminales o dispositivos.

(Grazzini, 2020)

2.2.4.3. TIPOS DE FIBRA ÓPTICA

Los cables de fibra óptica se clasifican en dos tipos importantes más comunes y utilizados en comunicaciones de redes de fibra óptica, como son multimodo y monomodo, cada una se emplea acorde al modo y necesidad de transmisión de la red, las del tipo monomodo se encuentra

UPSE

especificada en la normativa UIT-T G.652 y las multimodo en la normativa ITU-T G. 651, en estas normativas se pueden encontrar conceptos básicos, características, especificaciones para la fabricación, aplicaciones, entre otros.

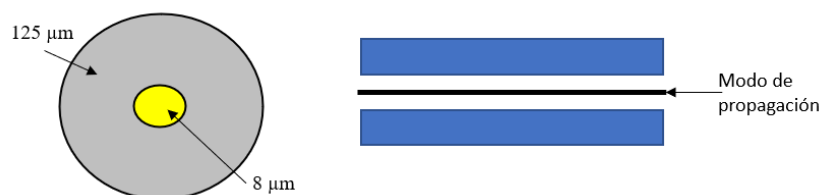
Monomodo

Este tipo de fibra se caracteriza por su especial diseño, las ondas se propagan en una sola dirección de forma recta, este modo de propagación hace que su transmisión sea paralela al eje de la fibra, puede alcanzar distancias de hasta 300km y predomina un ancho de banda desde 5 GHz hasta 100 GHz.

Está estandarizada en la UIT-T G.652 el cual indica que el diámetro de revestimiento es de aproximadamente $125 \mu\text{m}$ (micrómetros) y el diámetro del núcleo de este tipo de fibra varía entre 8 a $12 \mu\text{m}$, tiene un coeficiente de atenuación que varía de 0.35 dB/km en una región máxima de 1550 nm. (ITU, 2016)

Figura 9

Fibra monomodo



Elaborado por el autor

Multimodo

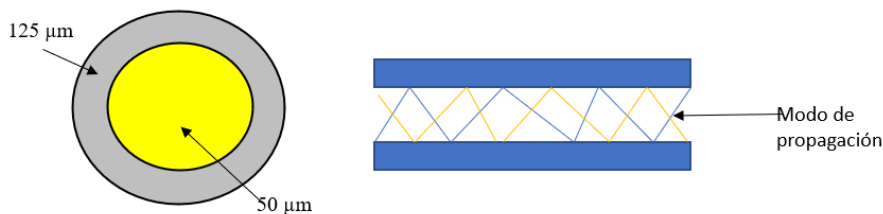
UPSE

Este tipo de fibra puede emitir varios rayos de luz ocasionado que la luz circule por más de un modo, se utilizan en instalaciones que requieren distancias menores a 2km, es económico con simplicidad de diseño y se usa comúnmente en aplicaciones locales.

Está estandarizada en la ITU-T G. 651 en donde indica que la fibra multimodo está compuesta por un núcleo con diámetro de 50 μm y un revestimiento con diámetro de 125 μm , el coeficiente de atenuación es inferior a 4 dB/km en una longitud de onda de 850 nm.

Figura 10

Fibra multimodo



Elaborado por el autor

2.2.5. REDES GPON

La tecnología GPON (Gigabit Passive Optic Network o Red de fibra óptica pasiva con capacidad de Gigabit) se encuentra especificada en los estándares de la ITU-T G.984x (G.984.1, G.984.2, G.984.3 y G.984.4), se trata de una red totalmente pasiva que no requiere de repetidores ni de alimentación externa para su funcionamiento, ofrece un mayor ancho de banda en comparación con sus antecesoras.

Una red GPON tiene la estructura básica de una red PON, está formado por equipos activos en sus extremos y equipos pasivos que transmiten y distribuyen señales desde la central hasta el usuario suscriptor.



UPSE

El objetivo de las redes GPON es reemplazar redes tradicionales (redes de cobre), ofrecer un incremento en su ancho de banda, eficiencia para transportar servicios IP y una mejor calidad de servicios de voz, datos y video; GPON al tener una comunicación punto a multipunto permite la reducción de costos en instalaciones de fibra óptica. (Huidobro, 2014)

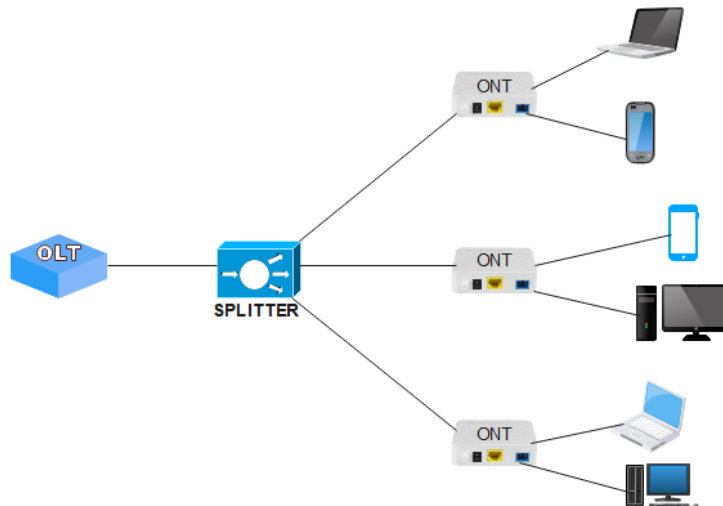
La información que se transmite en una red GPON se realiza por medio de fibra óptica en la que su distancia puede alcanzar hasta 20 km desde la central hasta el usuario final, la velocidad de transmisión supera los 1 Gbps, además la velocidad de subida y de bajada es de 1.25 Gbps y 2.5 Gbps respectivamente, aunque la velocidad más utilizada actualmente es de 2,488 Gbps.

2.2.5.1. ESQUEMA DE RED GPON

La red GPON está conformada principalmente por una OLT (Terminal de Línea Óptica) ubicada en las instalaciones del operador y ONTs (Terminación de Red Óptica) en las instalaciones de los suscriptores de fibra óptica hasta el hogar. La OLT contiene varios puertos de línea GPON, cada uno permite conectar hasta 6 ONT.

Para que la OLT y la ONT se conecten y transfieran datos se utilizan cables de fibra óptica que permitirá transportar una longitud de onda descendente, mediante un divisor óptico es posible dividir la señal de entrada en varias señales de salida se puede distribuir el tráfico descendente de la OLT. El divisor es una arquitectura punto a multipunto que puede dividirse de 1 entrada hasta n (2, 4, 8, 16, 32 o 64) salidas que conectan a los clientes a la red. (Huidobro, 2014)

Esquema de una red GPON



Nota: La figura muestra un esquema básico para el despliegue de redes GPON

2.2.5.2. ELEMENTOS QUE COMPONEN LA RED GPON

OLT

El Terminal de Fibra Óptica (Optical Line Terminal) es un dispositivo activo, se encuentra en la parte superior de la red y en una oficina central desde donde partirán las distintas líneas de fibra al divisor óptico con la finalidad de brindar servicio a múltiples usuarios. (España, 2005)

Tiene como función principal gestionar y enrutar el tráfico generado por las ONTs, admite servicios Triple-Play. Las OLT están constituidas por varios puertos PON que permite dar servicios a múltiples clientes por puerto y puertos SFP que permiten ofrecer conexiones de hasta 20 Gbps.

UPSE

Figura 12

OLT de 4 puertos PON



Nota: Se muestra una OLT de la marca Ubiquiti compuesto por 4 puertos PON capaz de brindar servicios a 128 usuarios por puerto. Fuente: (Ubiquiti, s.f.)

ONT

El Terminal de Red Óptica (Terminal Optical Network) es un equipo terminal situado al final de la red de fibra óptica (hasta el cliente), que convierte señales ópticas en señales eléctricas, sirve como intermediario entre la red y los equipos de los usuarios. Se encarga de recibir y enviar información destinada a los registrantes provenientes de una OLT, además, su objetivo es encapsular la información proveniente de un usuario y enviarla a la OLT para que sea redirigida a la red correspondiente.

La conversión de señales eléctricas a ópticas la realiza mediante dos puertos importantes de la ONT, como es un puerto para cable óptico que llega desde la OLT y un puerto LAN Ethernet RJ45 que se conecta con los usuarios.

Splitter

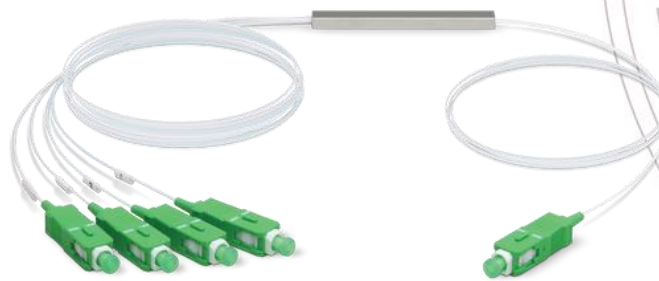
UPSE

También conocido como divisores ópticos, encargados de dividir la señal enviada por el OLT hacia las ONT donde se encargará de dividir la señal de bajada del cable óptico en más señales, pero con menor potencia para llegar a los usuarios, por lo que este divisor reducirá significativamente los costos y mantendrá mejor la infraestructura.

Los splitters suelen componerse de una variedad de puertos de salida como son de 1:2, 1:3, 1:4, 1:8, 1:16, 1:32 o 1:64 en el cual sus pérdidas por inserción son casi iguales en todas sus salidas, por ejemplo, un splitter de 1:4 separa una señal de entrada de un solo cable en cuatro señales de salida para cuatro cables de fibra, por lo tanto, si la señal de entrada tiene un ancho de banda de 2 Gbps cada salida tendrá una velocidad de 500 Mbps. (Szymanczyk, 2014)

Figura 13

Divisor óptico



Nota: La figura muestra un divisor óptico de 1:4 que permite dar conectividad a 4 usuarios. Fuente: (Ubiquiti, s.f.)

Patch cord de fibra óptica

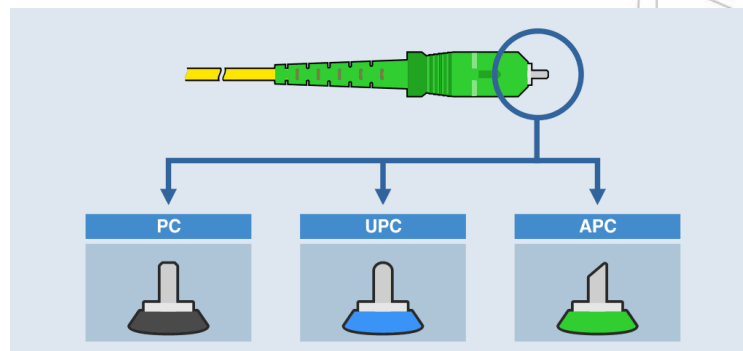
También llamado cable de conexión, se utilizan para interconectar toda la red de fibra en divisores ópticos, equipos terminales, distribuidores móviles y oficinas centrales; pueden ser simplex, dúplex o multifibra. Entre los modelos a considerar se encuentran:

Conector de suscriptor (Subscriber Connector) se aplica ampliamente para fibras monomodo de 125 μm y multimodo de 126 μm , tiene una pérdida por inserción menor a 0.1 dB y una pérdida por refracción mayor a 55 dB en fibras monomodo. Se utilizan para conectar equipos de telecomunicaciones, en redes LAN y WAN, equipos terminales, centrales telefónicas, entre otras.

Por otro lado, las abreviaturas PC (Contacto físico), UPC (Ultra Contacto físico) y APC (Control físico en ángulo) hacen referencia al tipo de forma del terminal óptico, esto se puede observar en la figura 14.

Figura 14

Conector de fibra óptica de tipo SC



Nota: La figura muestra el tipo de conector SC con los pulidos PC, UPC y APC en el terminal óptico. Fuente:

(PROMAX, 2019)

Conectores LC/PC y LC/APC

Lucent Connector o Local Connector es un conector utilizado para terminaciones y conexiones especialmente en transceivers, aplicados en redes de telecomunicaciones, redes LAN, televisión por cable y distribuciones locales.

UPSE

Pueden ser monomodo o multimodo, éstas tienen una pérdida por inserción de 0.15 y 0.3 respectivamente, y pérdidas por reflexión de 55/65 dB.

Figura 15

Conector de fibra óptica tipo LC/PC



Nota: Se muestra en la figura un conector tipo LC/PC que tiene un acabado uniforme. Fuente: (TECNIT, s.f.)

2.2.6. ESTÁNDARES Y ORGANISMOS DE ESTANDARIZACIÓN

Con la gran cantidad de redes disponibles en el mercado, se plantea la necesidad de estandarización y diferentes organizaciones se interesan por ello. Los dos principales beneficios de la estandarización son:

- Asegura la comunicación entre diferentes dispositivos.
- Impedir que los intereses privados definan las normas.

En esta sección se detallan los organismos encargados de la normalización y estandarización únicamente utilizados para el cableado de fibra óptica, mediante ellos es posible conocer los objetivos de cada organización y el conocimiento necesario para la aplicación del presente proyecto.

2.2.6.1. EIA

La Alianza de Industrias Electrónica (Electronic Industry Alliance), conocida hasta 1997 como Electronic Industry Association, es una organización formada por la asociación de empresas de electrónica y alta tecnología de Estados Unidos. Su misión es desarrollar estándares de cableado estructurado para estudiar métodos de cableado para construir sistemas de cableado estándar unificado para establecer y respaldar productos de múltiples proveedores.

2.2.6.2. TIA

Asociación de la Industria de las Telecomunicaciones (Telecommunications Industry Association) es una asociación comercial acreditada por el Instituto Nacional Estadounidense de Estándares (ANSI) para desarrollar estándares de la industria para productos de tecnología de la información y la comunicación (TIC) como de telefonía móvil, datos, equipos de VoIP, satélites, terminales telefónicas, entre otros. tiene como objetivo mejorar el entorno comercial para las organizaciones involucradas en banda ancha, telecomunicaciones, tecnología de la información, movilidad inalámbrica, por cable y satelital, redes, comunicaciones unificadas, entre otros servicios.

2.2.6.3. ANSI

Instituto Nacional Estadounidense de Estándares (American National Standards Institute) es una organización fundada por empresarios e industriales norteamericanos, dedicada a desarrollar estándares en comercio y comunicación. Coordina estándares de Estados Unidos, con estándares internacionales para que los productos tengan uniformidad y puedan usarse en todo el mundo.

2.2.6.4. IEEE

Instituto de Ingenieros en Electricidad y Electrónica (Institute of Electrical and Electronics Engineers) es una asociación dedicada a la normalización promover la creación, el desarrollo y la



UPSE

integración, el intercambio y la aplicación de los avances en tecnología de la información, la electrónica y la ciencia en general en beneficio de la humanidad y sus expertos. Está conformado por profesionales en el campo de las nuevas tecnologías, como ingenieros eléctricos, ingenieros electrónicos, ingenieros de sistemas, ingenieros de telecomunicaciones y muchos más.

2.2.6.5. ITU

Unión Internacional de Telecomunicaciones (International Telecommunication Union) es responsable de la normalización, coordinación y desarrollo de la infraestructura internacional de telecomunicaciones, sus actividades incluyen la coordinación del uso global del espectro radioeléctrico, la promoción de la cooperación internacional en la asignación de órbitas de satélites y la mejora de la infraestructura de telecomunicaciones en los países en desarrollo, y establece estándares globales para una fácil conexión a una variedad de sistemas de comunicación.

2.2.7. NORMAS DE CABLEADO ESTRUCTURADO

Un cableado estructurado está conformado por un sistema basado en normativas para la correcta instalación y administración de cables, conectores, canalizaciones, espacios, soportes y dispositivos, los elementos mencionados permiten la constitución de una infraestructura de telecomunicaciones y la distribución de señales para la comunicación.

2.2.7.1. ANSI/TIA/EIA 568A

El cableado estructurado horizontal se encuentra definido en la norma EIA/TIA 568A está conformado por cables distribuidos horizontalmente, terminaciones mecánicas y puntos de acceso, el mismo consta de dos componentes básicos que son las rutas y los espacios horizontales, los cuales son utilizados para distribuir el cableado horizontal y para la conexión entre equipos del área de trabajo y el cuarto de telecomunicaciones ya sea por suelo o techo.



UPSE

En esta normativa se especifican tres tipos de cables para su respectiva distribución como son los UTP, los STP y los de fibra, la distancia horizontal máxima para este tipo de cableado no debe sobrepasar los 90 metros por cable.

2.2.7.2. ESTÁNDAR ANSI/TIA/EIA-568-B3

El estándar ANSI/TIA/EIA-568-B3 se basa en los componentes de cableado de fibra óptica en el que se utilizan cables, conectores, patch cords, hardware de conexión y diversos instrumentos de prueba, además se mencionan los tipos de fibra óptica reconocidos como son los multimodos y monomodo, se especifica el ancho de banda para la fibra en sus respectivos tamaños y la atenuación dependiendo de los largos de onda.

- Multimodo: 62.5/125 μm
- Monomodo: 50/125 μm
- Ancho de banda: 160/500 MHz para fibra de 62.5/125 μm y 500/500 MHz para fibra de 50/125 μm .
- Atenuación: 3.5/1.5 dB/Km para longitud de onda de 850/1300 nm, aplica en los dos tipos de fibra.

2.2.7.3. ESTÁNDAR ANSI/TIA-568- C

El estándar ANSI/TIA-568- C contiene las especificaciones necesarias acerca del cableado para la respectiva instalación de los clientes, en este estándar se considera el 568-C.3 que se basa en los componentes de cableado de fibra óptica donde se especifica la correcta polaridad para la conexión entre dispositivos por medio de patchcords multimodo o dúplex.

Al conectar un patchcord multimodo se debe considerar la polaridad del mismo, ya que este tipo de cable contiene dos fibras normalmente etiquetadas por A y B en cada extremo del cable. Para



UPSE

asegurar una polaridad apropiada la conexión debe ser cruzada de manera que en un cable de fibra un extremo funcione como trasmisor mientras que el otro extremo del cable funcione como receptor, en el caso de la otra fibra se maneja la misma funcionalidad.

2.2.7.4. ANEXO ANSI/TIA/EIA-568-B.3-1

En este anexo se definen algunas descripciones adicionales para la fibra óptica con dimensión 50/125 µm para brindar una velocidad de Tx de 10 Gbps utilizando tecnología VCSEL desde una distancia de 850 nm hasta 300 m, distancia máxima para el backbone exterior. (Sánchez J. , 2019)

2.2.7.5. CARACTERÍSTICAS ANSI/TIA/EIA-568-B.3-1

Las características para este estándar se dividen en características técnicas y mecánicas, las cuales se detallan a continuación:

Tabla 2

Características técnicas y mecánicas de la fibra óptica

Características técnicas	Características mecánicas
Geometría de la fibra.	Tensión: al momento de contraer o estirar el cable de fibra, éste se puede romper si sobrepasa el porcentaje de elasticidad.
Propiedades de los materiales con lo que se realiza la fibra.	Compresión: Se refiere al esfuerzo transversal.
Anchura espectral de la fibra con respecto a la fuente de luz utilizada (a mayor	Impacto: Se debe a la protección de la fibra óptica.

anchura menor capacidad de transmisión
de información.

Soporta temperaturas desde -150 °C hasta +125°C.

Enrollamiento: es necesario limitar el ángulo de curvatura del cable, aunque la existencia de dicho enrollamiento evita que sobrepase el ángulo de curvatura.

Nota: La table 2 muestra diferentes características técnicas y mecánicas que tiene la fibra óptica. Fuente: (Coyachamin & Delgado, 2016)

2.2.7.6. ITU-T G.984x

Se indican las recomendaciones ITU-T G.984.1, G.984.2, G.984.3 y G.984.4, estas permiten brindar orientación al tomar decisiones sobre el despliegue de la red GPON, mediante las recomendaciones mencionadas es posible implementar un diseño óptimo en recursos y en cuestión de funcionamiento de la red.

Tabla 3

Normativa ITU-T G.984x

ITU-T G.984x	
G.984.1	Indica características generales de la fibra óptica
G.984.2	Especifica el correcto manejo de la capa dependiente de los medios físicos, las

	velocidades que ocupa en servicios de voz y dato
G.984.3	Indica los pasos a considerar en una estructura GPON y especifica las distancias, funciones y seguridad.
G.984.4	Especificaciones de interfaz de control y gestión de los equipos terminales de la red.

Nota: Se muestra la normativa ITU -T G.984.1, G.984.2, G.984.3 y G.984.4 que permiten realizar el despliegue de redes GPON de forma óptima.

2.2.8. TCP/IP

El protocolo de Control de Transmisión/Protocolo de Internet es el encargado de permitir y asegurar el intercambio de información entre ordenadores de una misma red, representa un conjunto de reglas de comunicación para Internet y se basa en el concepto de una dirección IP, es decir, en la idea de dar a cada computadora en la red una dirección IP para que los paquetes puedan enrutar datos.

TCP/IP está diseñado para ser compatible con cualquier sistema operativo, hardware o software, define cómo se fragmentan los datos en piezas manejables o paquetes de información y luego se envían individualmente a través de Internet. Por su parte, el protocolo IP controla el camino de los paquetes hacia su destino, como si fuera una especie de sistema de direccionamiento periódico basado en números IP.

El direccionamiento IP se maneja en la capa de Internet de este protocolo, pues su función es encaminar los paquetes o datos desde un origen hacia un destino en el que para llegar a su destino se debe identificar la cabecera IP. (Valdivia Miranda, 2019)

2.2.8.1. TCP/IP VERSIÓN 4

El protocolo TCP/IP versión 4 es la versión utilizada actualmente y se empezó a implementar desde 1981, consta de 32 bits asociados en cuatro grupos binarios y separados por un punto (.), cada agrupación contiene 8 bits por lo que su formato expresado en binario es 11000000.10101000.00000000.00000000, y 192.168.0.0 sería su formato en decimal.

Cabecera o segmento TCP versión 4

El segmento TCP consta de campos que contienen información acerca del paquete, en la siguiente figura se muestra el formato de cabecera.

Figura 16

Segmento IPv4

Versión 4 bits	IHL 4 bits	Tipo de servicio 8 bits	Longitud total 16 bits	
Identificación 16 bits			Bandera 3 bits	Compensación de fragmentos 13 bits
Tiempo de vida (TTL) 8 bits	Protocolo 8 bits		Checksum 16 bits	
IP de origen 32 bits				
IP de destino 32 bits				

Nota: El gráfico muestra los campos que existen en el encabezado de un paquete IPv4. Tomado de (Prado, 2014)

- Versión: Consta de un tamaño de cuatro bits, debido al número de versión IP.

- IHL: Significa Internet Header Length – Longitud del encabezado de Internet, este campo tiene un tamaño de cuatro bytes y palabras con 32 bits que indican el encabezado, el valor máximo para una cabecera correcta es de 5 y el valor mínimo es de 15.
- Tipo de servicio: Contiene un byte que equivale a 8 bits, encargado de gestionar y dar prioridad en casos de congestión, además de dar indicaciones al nivel requerido de retardo, coste, rendimiento y fiabilidad.
- Longitud total: Este campo contiene una longitud de 16 bits (2 bytes) indica el tamaño total del paquete incluyendo el tamaño de cabecera y los datos encapsulados.
- Identificación: Longitud de 16 bits (2 bytes), su valor permite un re-ensamblado en la recepción de fragmentos del paquete IP.
- Banderas (Flags): Contiene tres bits que se utilizan como se describe a continuación:
 - Bit en 0, el primer bit siempre se encuentra en este estado.
 - Bit DF (Don't Fragment – No Fragmentado): Autoriza según su estado la fragmentación, si es cero autoriza, si es uno no autoriza.
 - Bit MF (More Fragment – Más fragmentado): Identifica el último fragmento si el bit es cero, si el bit es uno se trataría de un fragmento intermedio.
- Compensación de fragmentos: Contiene 12 bits e indica en el paquete inicial la posición del fragmento y el primer fragmento tiene un valor de 0.

- Tiempo de vida (TTL): Contiene el número máximo de saltos (routers) que debe realizar un paquete y evita la sobrecarga de la red con datagramas perdidos.
- Protocolo: Este campo se compone de un byte equivalente a 8 bits, mediante un valor ayuda a autenticar el tipo de datos encapsulados por la cabecera.
- Checksum: Su objetivo es comprobar que el segmento ha llegado a su destino sin modificarse mediante su transmisión y para la protección de errores, suma uno a uno los bits de la cabecera y el resultado aparece en la sección checksum.
- IP de origen: En este campo de cuatro bytes (32 bits) se tiene la dirección IPv4 del origen del paquete.
- IP de destino: En este campo de cuatro bytes se tiene la dirección IPv4 del destino del paquete. (Pérez, 2020)

2.2.8.2. TCP/IP VERSIÓN 6

Cabecera o segmento versión 6

En IPv6 el segmento es simplificado y de longitud fija en comparación a IPv4, por lo que, tiene una gran ventaja con respecto a la velocidad. Está compuesta de 40 octetos y un tamaño de 16 bytes.

Formato de cabecera IPv6

Versión 4 bits	Clase de tráfico 8 bits	Etiqueta de flujo 20 bits	
Longitud de campo de Datos 16 bits		Cabecera siguiente 8 bits	Límite de saltos 8 bits
IP de origen 128 bits			
IP de destino 128 bits			

Nota: El gráfico muestra los campos que existen en el encabezado de un paquete IPv6. Tomado de (Prado, 2014)

- Versión: Consta de cuatro bits y muestra la versión IP a utilizar, en este caso 6.
- Clase de tráfico: Su campo tiene un byte (8 bits), especifica la clase de tráfico de los paquetes, si se trata de tráfico de datos con control de congestión el rango de valor asignado es del 0 al 7 y del 8 al 15 para tráfico de audio y video sin control de congestión.
- Etiqueta de flujo: Su tamaño es de 20 bits, contiene un valor específico para identificar paquetes pertenecientes a una misma transmisión. Tiene el propósito de facilitar la tarea de los routers y QoS.
- Longitud de carga útil: El campo es de dos bytes (16 bits) y especifica el tamaño del paquete que incluye la cabecera y datos, destacando que este campo es diferente a la longitud total de la cabecera IPv4.

- Cabecera siguiente: este campo es de un byte (8 bits) e indica la cabecera siguiente de los datos encapsulados, se pueden definir algunos valores para este campo como el número 58 que encapsula mensajes ICMv6.
 - Límite de saltos: el campo es de un byte, sustituye al campo TTL del segmento IPv4. El límite de saltos se define por un valor máximo por el origen del paquete, si su valor tiende a disminuir el paquete se descarta.
 - IP de origen: es un campo de 16 bytes que muestra la dirección IPv6 del origen del paquete.
 - IP de destino: campo de 16 bytes que muestra la dirección IPv6 del destino del paquete.
- (Pérez, 2020)

2.2.9. IPV6

IPv6 también denominada IP next generation (IPng) es una etiqueta única para cada equipo que permite se identificación y hace posible el envío de paquetes de información, la nueva versión de protocolo de internet sustituirá al protocolo antecesor IPv4, el objetivo de IPv6 es cubrir las falencias de su predecesor adhiriendo nuevas funcionalidades.

Una de las significativas características que trae IPv6 es el aumento de espacio de asignación de direcciones en el que pasa de 32 bits a 128 bits, albergando aproximadamente 340 sextillones de direcciones IP diferentes en la que cada una está constituida de 32 dígitos hexadecimales formado por ocho grupos de cuatro dígitos y separados por dos puntos. (Dordoigne, 2018)

2.2.9.1. CARACTERÍSTICAS DE IPV6

Algunas características fundamentales de IPV6 son las siguientes:

2.2.9.2. AUMENTO DE DIRECCIONES IP

En IPv6 se incrementa el tamaño de bits a 128 dando paso a más de 340 sextillones de direcciones disponibles haciendo posible la conexión de múltiples dispositivos a Internet, estas direcciones se pueden llegar a simplificar empleando las reglas del RFC 2373 – “IP versión 6 Addressing Structure”.

El aumento de direcciones hace posible la autoconfiguración y garantiza que cada dispositivo en la red obtenga una dirección IP pública única.

Formato de cabecera

Algunos campos de la cabecera en IPv6 se simplificaron o son de uso opcional consiguiendo un tamaño fijo y simple con el fin de limitar el coste de ancho de banda en el header de IPv6.

2.2.9.3. DIRECCIONAMIENTO IPv6

El direccionamiento IPv6 tiene una longitud de 128 bits que se dividen el bloque de 16 bits separados por dos puntos (:), es decir, que cada bloque contiene 4 dígitos que son valores hexadecimales, su representación en formato completo es:

Figura 18

Formato de IPv6

FF80:00D3:AA12:00FF:0000:0000:AC34:0D1D

Prefijo global	ID de red	ID de interfaz
-----------------------	------------------	-----------------------

Elaborado por el autor



UPSE

Como se puede observar en la figura 18 los primeros tres grupos identificados con color negro equivalen a 48 bits que corresponden al prefijo global, éste es asignado por el RIR (Registro Regional de Internet) y una vez asignado no se pueden realizar cambios, los siguientes 16 bits que corresponden al cuarto grupo se encuentra resaltado de color azul e identifican la red que es asignada por el administrador de red a un sitio específico y los últimos cuatro grupos que equivalen a 64 bits comprenden la identificación de interfaz.

Si alguna dirección IPv6 contiene ceros en el inicio de algún grupo éstos se pueden simplificar, tomando el ejemplo de la dirección mostrada en la figura 18 se simplificaría de la siguiente manera:

FF80: D3:AA12: FF:0:0:AC34:0D1D

Otra forma de simplificar el direccionamiento es cuando se tiene un grupo solo de ceros (0000), éstas se simplifican mediante "::", por ejemplo:

FF80: D3:AA12: FF::AC34:0D1D

2.2.9.4. PREFIJOS IPv6

En IPv4 se denominaba máscara de subred, mientras que en IPv6 se lo conoce como tamaño de prefijo, se representan mediante una barra invertida seguida de un número “n” y se utiliza para identificar las porciones de red y de host. Por ejemplo considérese la siguiente dirección para un host FF80:00D3:AA12:00FF:0000:0000:AC34:0D1D/64, en el que /64 hace referencia que este host pertenece a un prefijo en el que se encuentran más hosts con dirección similar pero con igual prefijo.

El prefijo de una dirección IPv6 indica la dirección de la red.

2.2.10. TIPOS DE DIRECCIONES

En esta sección se detallan los tipos de direccionamiento en IPv4 e IPv6 para posteriormente establecer sus diferencias y mejoras.

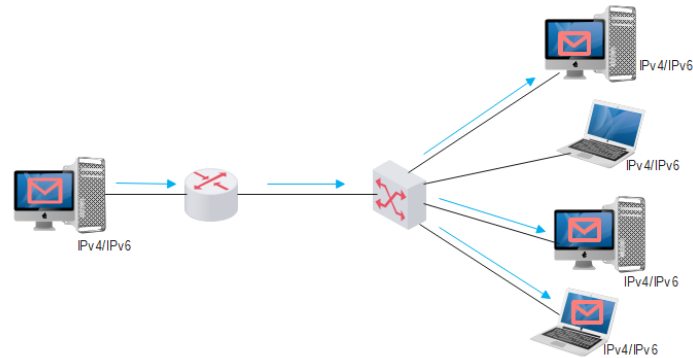
2.2.10.1. MULTICAST

Multicast consiste en enviar un paquete desde un servidor a múltiples destinos identificados por una dirección IP, para el tipo de direccionamiento IPv4 se utiliza el rango de direcciones de 224.0.0.0 hasta 239.255.255.255, se conservan algunas direcciones IP para usos específicos debido a su limitación

Los hosts que reciben los paquetes utilizan los servicios solicitados por parte de un programa cliente para asociarse al grupo Multicast, en el que cada grupo se identifica por una única dirección de destino.

Las direcciones multicast utiliza el prefijo FF00::/8 para IPv6 y sirve para identificar a los hosts que pertenecen al grupo de multicast, tienen los primeros ocho bits establecidos en uno (1111 1111 o 0xFF) identifican que el mensaje pertenece a multicast, seguido de cuatro bits para identificar banderas compuesto por 000T donde los cero se mantienen porque están reservados y T puede variar en 0 o 1 según la dirección que se asigna, por consiguiente contiene cuatro bits de scope que indican el alcance de las direcciones multicast y un grupo ID que identifica el grupo multicast.

En este caso no es necesario reservar direcciones, ya que IPv6 tiene un amplio rango de direcciones. (Vélez & Gutiérrez, 2016)



Elaborado por el autor

2.2.10.2. UNICAST

Identifican una sola interfaz, es decir, que el tráfico se envía únicamente a una dirección unicast, este tipo de direcciones no contienen una estructura interna, por lo que los hosts pueden tener diferentes longitudes de prefijo.

En IPv4 el rango de direcciones para unicast es de 1.1.1.1 hasta 223.255.255.255 en el que se asignan direcciones de origen y destino, durante la transmisión el dispositivo de origen coloca su dirección IP en el encabezado del paquete.

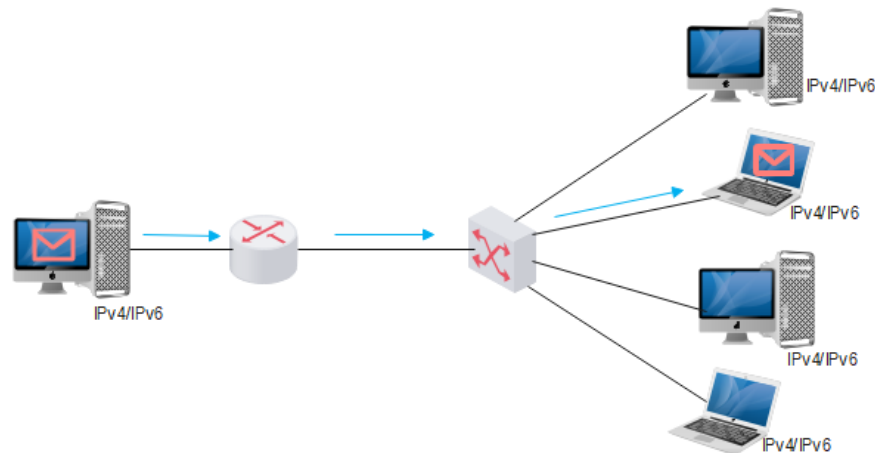
En IPv6 las direcciones unicast son las siguientes:

- Enlace local (link-local): Tienen formato FE80::/10 son de uso local para enlaces sencillos y se generan por el propio host.
- Unique Local: Su formato es de FD00::/8 utilizado en organizaciones privadas que no deben ser anunciadas en Internet

- Global IPv6 unicast addresses: Utiliza prefijo 2000::<3 es fundamental en una arquitectura IPv6 ya que se utilizan para el tráfico de internet.
- Loopback: Su prefijo abreviado es de ::1/128 y es utilizado para enviar un paquete de un host o nodo a sí mismo. (Carrera, 2018)
- Embedded IPv4: Las direcciones IPv4 embebidas son direcciones IPv6 utilizadas para permitir la transmisión de datos de IPv4 a IPv6, IPv4 contiene 32 bits que se usan para representar dicha dirección dentro de una dirección IPv6 de 128 bits.

Figura 20

Unicast



Elaborado por el autor

2.2.10.3. ANYCAST

Anycast se designan a más de una interfaz que es utilizada para enviar paquetes desde un nodo a una de las direcciones más cercanas, es decir, se basa en una comunicación punto a punto entre cliente y servidor, este tipo de dirección ocupa parte del direccionamiento unicast. (Sánchez G. , 2012)

UPSE

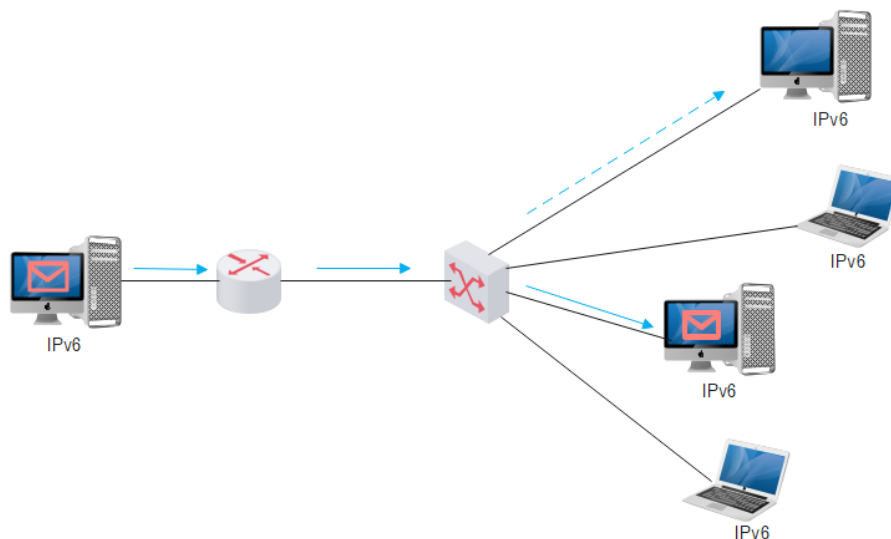
En IPv4 no se utilizan direcciones Anycast, aunque existe otro tipo de direccionamiento denominado Broadcast que se encarga de transmitir información desde un servidor a todos los hosts que conforman la red.

En IPv6 este tipo de dirección se utilizan como direcciones de destino asignados únicamente en routers, la asignación de direcciones Anycast se encuentran ya definidas en unicast que son: local única, enlace local e IPv6 global.

Anycast se utiliza para establecer comunicación con el servidor más cercano, descubrimiento de servicios mediante direccionamiento anycast y para comunicaciones entre routers disponibles en la misma red. (Vélez & Gutiérrez, 2016)

Figura 21

Anycast



Elaborado por el autor



UPSE
Tabla 4

Diferencias de IPv4 e IPv6 en los tipos de direccionamiento.

Tipo de direccionamiento	IPv4	IPv6
Multicast	224.0.0.0/24 se conservan direcciones IP	ff00::/8 no es necesario conservar direcciones IP
Unicast	Rango de direcciones: 1.1.1.1 - 223.255.255.255	Utiliza 4 formatos de direcciones: enlace local, local única, IPv6 global y loopback.
Anycast	No utiliza este tipo de direccionamiento	Las direcciones se asignan únicamente a routers.

Nota: La tabla muestra los diferentes tipos de direccionamiento en cada protocolo y el formato que utiliza cada uno, a excepción de Anycast para IPv4 ya que no lo utiliza.

2.2.11. PROTOCOLO ICMP

El Protocolo de Mensaje de Control de Internet (Internet Control Message Protocol) sirve para intercambiar datos de un host a otro mediante la capa de red y es utilizado con la finalidad de notificar acerca de problemas en los datagramas, en él se constituye un mecanismo de gestión para identificar incidencias suscitadas durante la transmisión d paquetes. (Íñigo Griera, 2013)

2.2.11.1. ICMPv4

ICMPv4 utiliza un formato que contiene tres campos mostrados en la figura 22, el cual facilitará la identificación del uso de paquetes ICMP, cada campo tiene su propia funcionalidad que se explicarán posteriormente.



UPSE
Figura 22

Formato de mensajes ICMPv4

Bit 0-7	Bit 8-15	Bit 16-31
Tipo	Código	Checksum
Mensaje		

Elaborado por el autor

- **Tipo:** Contiene 8 bits e indica el tipo de mensaje mediante un valor de bit, de este valor depende el formato del resto de la cabecera, existen dos tipos de mensajes ICMPv4, los que informan acerca de errores (entre 0-127 bits) y los que realizan petición de una información (entre 128 y 255 bits).
- **Código:** Contiene 8 bits, este campo depende del tipo de mensaje y su uso se da para crear una jerarquía para clasificar mensajes.
- **Checksum:** Contiene 16 bits para detectar errores en un mensaje ICMPv4.
- **Mensaje:** Se detallan los datos del mensaje ICMPv4.

En la siguiente tabla se muestran los diferentes mensajes del protocolo ICMPv4 que se determinan por el tipo, código y descripción del mensaje, es importante mencionar que los primeros 8 bits ayudarán a identificar la causa de un error en un datagrama. Los mensajes de Eco son utilizados para verificar la conectividad entre hosts mediante el protocolo IP.



UPSE
Tabla 5

Mensajes ICMPv4

Tipo	Código	Descripción
0	0	Respuesta de eco
8	0	Petición de eco
3	0-15	Destino inalcanzable
4	0	Destino inalcanzable por subred, estación, protocolo o puerto
5	0-3	Petición de control de flujo
9	0	Redireccionamiento
10	0	Publicación de rutas
11	0-1	Tiempo de vida expirado
12	0-1	Cabecera IP incorrecta
13	0	Respuesta de hora
14	0	Respuesta de hora
17	0	Petición de máscara de subred
18	0	Respuesta de máscara de subred

Nota: En la tabla se pueden identificar todos los tipos de mensajes ICMP y la información acerca de lo que realiza cada tipo y código. Obtenido de: (Íñigo Griera, 2013)

2.2.11.2. ICMPV6

Es un protocolo utilizado para informar por parte de los enrutadores y hosts acerca de errores que pueden ocurrir en algún tramo de la red, para el caso de IPv6 se emplea ICMPv6 es importante la implementación de este protocolo a la red, el protocolo mencionado contiene un listado de

UPSE

mensajes identificados por medio de un código que sirven para distinguir errores que se pueden producir durante la transmisión de paquetes además de realizar otras funciones relacionadas a la capa Internet.

El formato de mensajes ICMPv6 es idéntico al formato ICMPv4 y cada campo maneja el mismo concepto, la diferencia se encuentra en la clasificación de los mensajes.

Figura 23

Formato de mensajes ICMPv6

Bit 0-7	Bit 8-15	Bit 16-31
Tipo	Código	Checksum
Mensaje		

Elaborado por el autor

- **Tipo:** Contiene 8 bits e indica el tipo de mensaje mediante un valor de bit, de este valor depende el formato del resto de la cabecera, existen dos tipos de mensajes ICMPv6, los que informan acerca de errores (entre 0-127 bits) y los que realizan petición de una información (entre 128 y 255 bits).
- **Código:** Contiene 8 bits, este campo depende del tipo de mensaje y su uso se da para crear una jerarquía para clasificar mensajes.
- **Checksum:** Contiene 16 bits para detectar errores en un mensaje ICMPv6.
- **Mensaje:** Se detallan los datos del mensaje ICMPv6.

Los mensajes de ICMPv6 se clasifican en dos partes, la primera contiene mensajes de error y la segunda mensajes informativos, la siguiente tabla muestra los mensajes para ICMPv6.



UPSE
Tabla 6

Mensajes ICMPv6

Mensaje de error		
Tipo	Código	Descripción
1	0-4	Destino inaccesible
2		Paquete demasiado grande
3	0-1	Tiempo excedido
4	0-2	Problemas de parámetros
Mensajes informativos		
128	0	Solicitud de eco
129	0	Respuesta de Eco

Nota: En la tabla se puede identificar la clasificación de los tipos de mensajes ICMPv6 y la información acerca de lo que realiza cada tipo y código. Obtenido de: (Silva Bracero, 2012)

2.2.12. MECANISMOS DE TRANSICIÓN

Ante la problemática del agotamiento de direcciones IPv4 se ha empezado el cambio respectivo a IPv6, el objetivo de los mecanismos de transición es hacer que ambos protocolos convivan por un determinado tiempo, de tal manera que el cambio a IPv6 sea de forma progresiva.

Para poder realizar una transición satisfactoria se debe considerar que el proveedor de servicio de Internet soporte direccionamiento IPv6, en caso de que no lo haga se deberá implementar IPv6 por medio de túneles, otro punto a considerar es que los equipos como routers o switches que se encargan del enrutamiento y los dispositivos finales como PC's también soporten el protocolo nombrado.

Los mecanismos de transición se clasifican en 3 grupos importantes:

- Dual Stack (doble pila)
- Tunelización
- Traducción

2.2.12.1. DUAL STACK

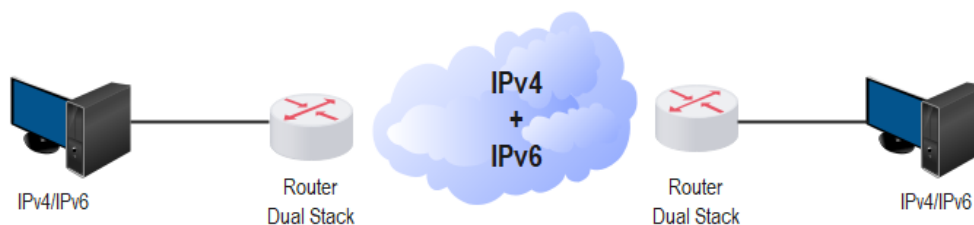
Uno de los mecanismos más utilizados para la transición de manera progresiva a IPv6 es el denominado dual stack o pila doble, el cual se describe en el RFC 2893, se fundamenta en la completa implementación de los protocolos IPv4 e IPv6 en una misma red.

Mediante la implementación de dual stack un host o un router puede contener las pilas de protocolo IPv4 e IPv6, en el que cada nodo IPv4/IPv6 debe estar configurado con ambos protocolos de direccionamiento, las pilas IPv4 e IPv6 pueden enviar y recibir datagramas de forma simultánea, de tal manera que pueda lograrse una comunicación con cada nodo IPv4 e IPv6 en la red.

El funcionamiento de doble pila se basa en que si se requiere comunicación IPv4 se utilizará la pila de protocolos IPv4, así mismo con la pila de protocolo IPv6 en caso de que se requiera comunicación IPv6. (Robert, Nordmark, & Gilligan, 2005)

Figura 24

Funcionamiento de Dual Stack



Nota. El gráfico muestra la funcionalidad del mecanismo de transición Dual Stack, en el que intervienen los protocolos IPv4 e IPv6. Tomado de (Martínez Yelmo & Riaño Vílchez, 2016)

2.2.12.2. TUNELIZACIÓN

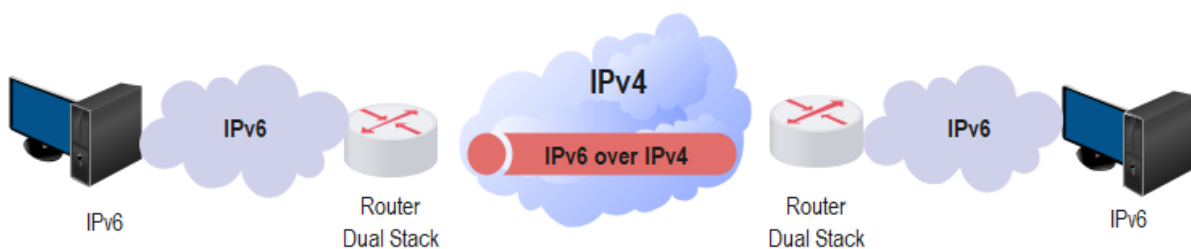
Este tipo de mecanismo de transición está basado en encapsular paquetes IPv6 dentro de paquetes IPv4 y transportarlos mediante una infraestructura IPv4 existente para poder llegar a su destino, este mecanismo se aplica para atravesar redes que no estén manejando IPv6, por lo que el tráfico IPv6 deberá cruzar una red IPv4 existente, esto se puede llevar a cabo mediante la técnica de tunneling o tunelización.

También es posible encapsular paquetes IPv4 sobre redes IPv6, este método se aplica cuando se requiere de nuevas redes IPv6 que aún necesiten conectividades en IPv4.

El proceso en general que realiza un túnel para el envío de paquetes consisten en tres pasos que son: encapsular, desencapsular y administrar el túnel. (Taffernaberry, 2011)

Figura 25

Funcionamiento de tunelización



Nota: La figura muestra un esquema general de tunelización donde se implementa redes IPv6 sobre infraestructura IPv4 existente. (Martínez Yelmo & Riaño Vílchez, 2016)

Existen tipos de túneles que pueden ser configurados, semi-configurados o automáticos.



UPSE

Túneles configurados o manuales

Se encuentra descrito en el RFC 4213, su configuración se realiza manualmente con rutas estáticas y son punto a punto, es decir, se deben configurar de forma manual en los dos extremos, este tipo de túnel se implementa para proveer conexiones IPv6 para una red completa.

Para poder realizar su configuración es importante definir una interfaz túnel, establecer el tipo de encapsulación para el túnel, en este caso se utiliza “ipv6ip”, y hacer visible la topología en IPv6 con la interfaz túnel.

Túnel Broker

Este tipo de túnel está descrito en el RFC 3053, requiere de una configuración manual de los equipos que se utilizarán para la aplicación del túnel, la asignación de direcciones IP y la creación de túneles para IPv6 se da mediante el denominado Tunnel Broker.

En primer lugar, el usuario deberá solicitar a un proveedor de TB la creación del túnel, luego elige un prefijo IPv6 que puede ser un valor entre 0 y 128, se proporcionará instrucciones para la creación del túnel, en consecuencia, se registra de forma automática en el DNS las direcciones IPv6 globales a los nodos finales del túnel y por último se configura el lado del servidor del túnel.

Una vez realizada las configuraciones respectivas, el túnel IPv6 sobre IPv4 estará en funcionamiento y permitirá al usuario una comunicación por IPv6. (Durand, Fasano, Guardini, & Lento, 2001)

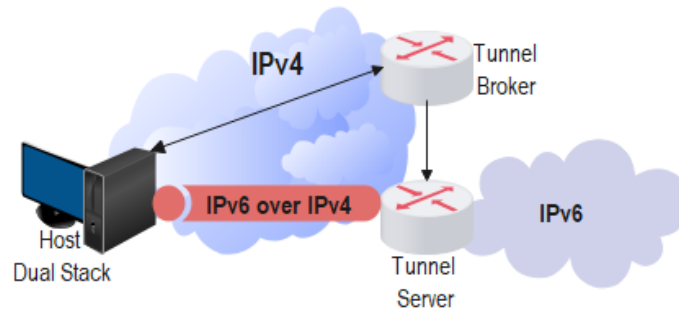
Existen diversos proveedores de Tunnel Broker a nivel mundial en el que se destacan los siguientes:

- Freenet6 para Canadá
- SixXS para Europa

- Hurricane Electric para Estados Unidos

Figura 26

Funcionalidad de Tunnel Broker



Nota. El gráfico describe la funcionalidad de un Tunnel Broker mediante un router y redes IPv4 e IPv6. Tomado de (Lin, 2014)

Túneles automáticos

Se configuran de forma automática y dinámica, su configuración solo puede realizarse de router a router (los routers IPv6 están separados por un entorno IPv4, por lo que se pueden encapsular paquetes IPv6 e IPv4 sin realizar una configuración extra en la red IPv4), de host a router (el host solo trabaja en IPv6 y encapsula paquetes para ser enviados a un router que admita IPv4 e IPv6 y permita hacer un ruteo en IPv4), de host a host (los paquetes que se envían de un host a otro host requieren de una configuración manual que permitan interconectar redes IPv4 e IPv6 entre ellos) y de Router a host (requiere de configuración manual en los routers para encapsular paquetes IPv6 y llegar a su destino). (Taffernaberry, 2011)

Tiempos de convergencia de los túneles

El tiempo de convergencia consiste en determinar el tiempo en que los routers se tardan en enviar información, calcular métricas y actualizar tablas con respecto a enrutamiento.



UPSE

Los tiempos de convergencia de los túneles automáticos suelen ser tiempos de convergencia simultáneos, mientras que en los túneles manuales los tiempos de convergencia depende del tiempo de respuesta del equipo de soporte. (Girón, 2015)

Se presenta una tabla con diferentes tiempos de convergencia utilizando diferentes protocolos como OSPF, HSRP, entre otros:

Tabla 7

Tiempos de convergencia de tunelización

Escenarios de falla	Protocolos	Tiempos de convergencia
1	HSRP	15 segundos
5	OSPF	40 segundos
2	HSRP+OSPF	40 segundos
3	Túnel Back up	Inmediato
6	HSRP+ Túnel Back up	15 segundos
4	HSRP+ Túnel Back up+OSPF	40 segundos

La tabla muestra diferentes tipos de convergencia para el método de tunelización según los protocolos de enrutamiento a utilizar. Fuente: (Girón, 2015)

Túneles 6to4

Permite una interconexión dinámica, su comunicación es punto a punto (router a router), utiliza un prefijo IPv6 (2002::/16) asignado por IANA, este tipo de túnel permite que islas con dominio IPv6 se comuniquen con otros dominios IPv6 mediante una configuración mínima.

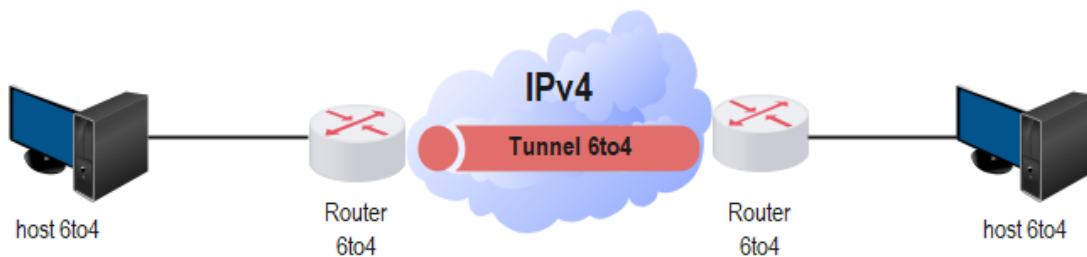
Los routers 6to4 no requieren de ningún protocolo de enrutamiento para IPv6, ya que el enrutamiento IPv4 es el encargado de realizar la tarea. Para que los hosts y las redes que utilicen 6to4 puedan intercambiar paquetes con redes IPv6 nativas se deberá hacer uso de Routers Relay,

UPSE

el cual se encuentra especificado en el RFC 3068, si una interfaz IPv4 envían paquetes 6to4 hacia un Router Relay los paquetes se desencapsularán y continuarán su camino hacia la red IPv6 nativa, por otro lado, si se envían paquetes IPv6 que tengan como destino una dirección IPv4 con el prefijo anteriormente mencionado, los paquetes se encapsularán en IPv4 hacia la red IPv4. (Taffernaberry, 2011)

Figura 27

Funcionamiento de túnel 6to4



Nota. La gráfica muestra la funcionalidad 6to4, donde Site 1 de la red 6to4 se comunica con Site 2 y Site 3 por medio de un túnel 6to4. Fuente: (TechHub, 2016)

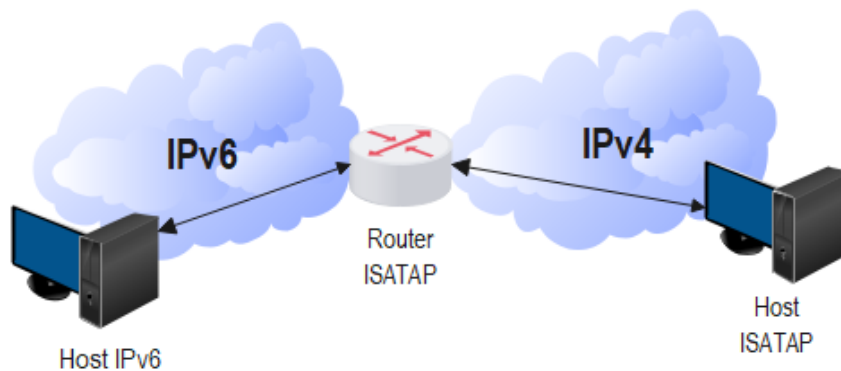
Túnel ISATAP

Protocolo de direcciones de túnel automático entre sitios (Inter Site Automatic Tunneling Address Protocol) está definido en el RFC 4212, es un túnel punto a multipunto que permite implementar IPv6 a través de infraestructura IPv4, utiliza el tipo de dirección unidifusión global (global unicast) con formato especial para el ID de interfaz.

El túnel ISATAP permite que los hosts que están a varios saltos de distancia de un enrutador IPv6 se unan a una red IPv6 al enrutar automáticamente los paquetes IPv6 a través de IPv4 a un enrutador IPv6 como la dirección del siguiente salto. (Vélez & Gutiérrez, 2016)

UPSE
Figura 28

Funcionamiento de ISATAP



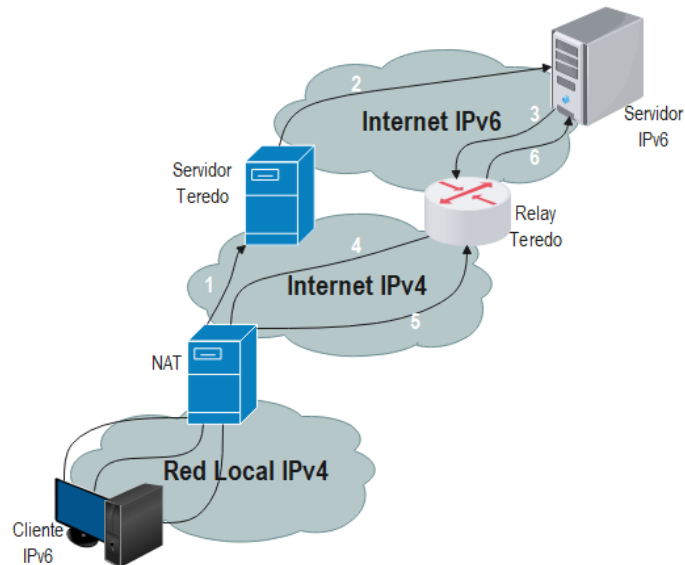
Nota: ISATAP permite la comunicación de redes IPv4 e IPv6 mediante un router ISATAP. Fuente: (Vélez & Gutiérrez, 2016)

TEREDO

Se especifica en la RFC 4380, permite encapsular paquetes IPv6 dentro de paquetes UDP/IPv4 para traspasar dispositivos NAT, esto se debe emplear cuando no sea posible transformar NAT IPv4 en un router IPv6. Mediante la implementación de Teredo se debe considerar un Servidor Teredo que permitirá controlar el tráfico de los usuarios que tengan conexión a Internet, un Cliente Teredo que se encuentra detrás de una NAT y debe tener conexión a Internet, por último, un Teredo de Reenvío que se conecta a IPv6 y actúa como router para brindar conexiones a clientes Teredo. (Vélez & Gutiérrez, 2016)

Es similar al tipo de tunelización 6to4 y utiliza el prefijo 2001:0000::/32 para clientes Teredo, es necesario considerar que un dispositivo de la red convierta paquetes de IPv6 a IPv4 o viceversa de tal manera que exista una conexión para la comunicación.

Túnel TEREDO



Nota: La figura muestra el proceso en el que se basa el tipo de tunelización Teredo para obtener conexiones de IPv4 e IPv6. Fuente: (Vélez & Gutiérrez, 2016)

2.2.12.3. TRADUCCIÓN

Para aplicar este mecanismo de transición es necesario que un dispositivo en la red se encargue de convertir paquetes IPv4 a paquetes IPv6 y de paquetes IPv6 a paquetes IPv4 de tal manera que pueda existir una comunicación.

El método de traducción también es conocido como AFT (Address Family Translation – Traducción de la familia de direcciones) su función se basa en permitir enviar información entre nodos IPv6 nativos a nodos IPv4, contiene dos tipos de traducción que se pueden mencionar como son el NAT-PT y NAT64.

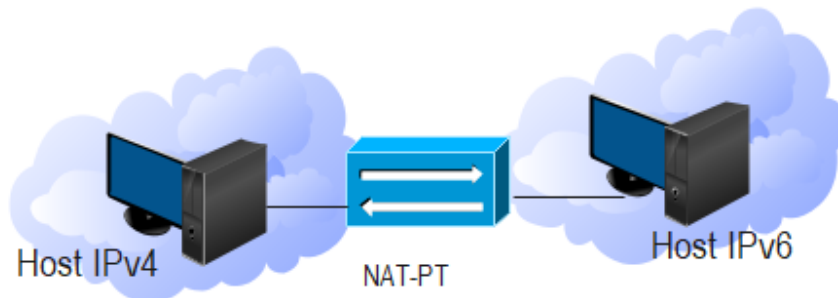
UPSE NAT-PT

Está definido en la IETF RFC 2766, el Network Address Translation – Protocol Translation (Traducción de direcciones de red - Traducción de protocolos) se basa en un enrutamiento transparente y en la traducción del direccionamiento IPv4 a IPv6 sin que exista modificaciones en las aplicaciones de los protocolos antes mencionados. Es el encargado de establecer una conexión desde un host con IPv6 a un host con IPv4. (Tsirtsis, 2000)

A pesar de ser uno de los primeros mecanismos de traducción actualmente ha sido descartado para su implementación debido a las fallas mencionadas en el RFC 4966 como son los protocolos de direccionamiento, la pérdida de información y selección al enviar paquetes a un destino, limitación en la seguridad DNS, entre otras. (Cedric Aoun & Davies, 2007)

Figura 30

Funcionamiento de NAT-PT



Nota. En la figura se muestra un diagrama acerca del mecanismo NAT-PT para la convergencia de redes IPv4 e IPv6.

Fuente: (Ogunleye, 2016)

SIIT

Traducción de IP/ICMP sin estado (Stateless IP/ICMP Translation) especificada en el RFC 6145 y creado para reemplazar NAT-PT, permite traducir cabeceras IPv4 en IPv6 o viceversa y mediante

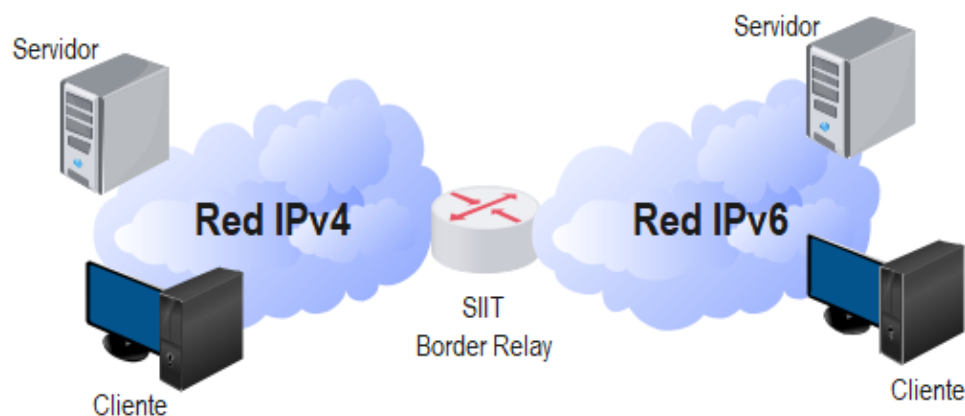
UPSE

ello establecer comunicación entre nodos IPv4 e IPv6. Para realizar el proceso de traducción se necesita una dirección IPv4 mapeada en formato IPv6 que podrá identificar al destino IPv4, además una IPv4 traducida en formato IPv6 para identificar al destino IPv6. (Vélez & Gutiérrez, 2016)

En la traducción de IPv4 a IPv6 cuando un paquete IPv4 se transmite hacia un dominio IPv6 se traduce primero el encabezado IPv4 en un encabezado IPv6, por lo que el encabezado IPv4 tiende a eliminarse y ser reemplazado por el de IPv6.

Figura 31

Traducción SIIT



Nota: SIIT requiere de servidores en cada punto de la red para hacer posible la traducción de IPv4 a IPv6 mediante un router SIIT. Fuente: (LACNIC)

NAT64

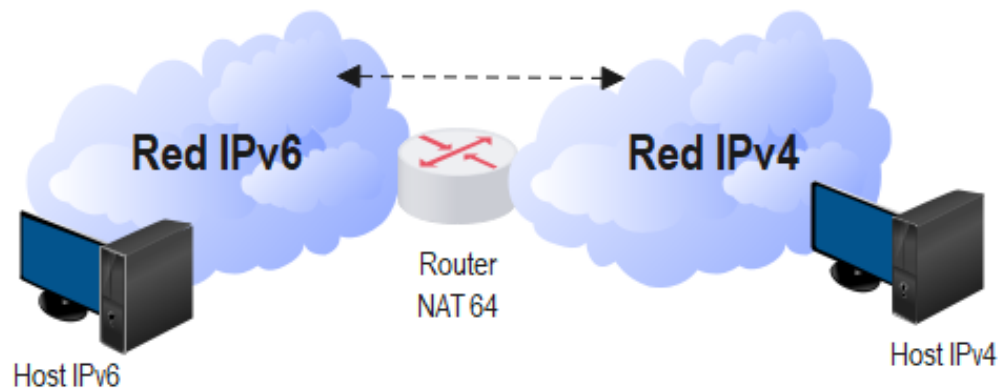
Se utiliza únicamente para IPv6, consiste en obtener una puerta de enlace con dos interfaces, una con red IPv4 y otra con red IPv6, los paquetes IPv6 se enruta por medio de la puerta de enlace que realiza las traducciones para transferir los paquetes de una red a otra.

UPSE

Existen dos estados de aplicación con respecto al mecanismo NAT64, uno con estado, el cual se define en el RFC 6146 en el que menciona que el mapeo de las direcciones se establece con un algoritmo estático o manual, realiza traducción de IPv6 a IPv6 y viceversa, mientras se realiza la traducción el estado de sesión cambia; el NAT64 sin estado se define en el RFC 6145, requiere de que el mapeo de las direcciones se establezca de forma automática y no mantiene enlaces ni estados de sesión en las redes.

Figura 32

Funcionamiento NAT64



Nota. La figura muestra la traducción para la comunicación IPv4 e IPv6 mediante el mecanismo NAT64. Fuente:

(Interpolados, 2017)

BIS

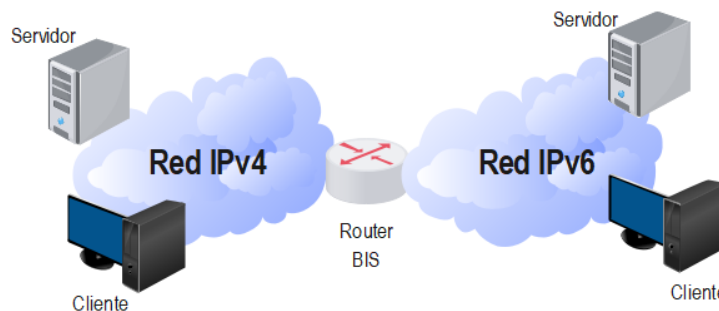
Bump in the Stack está definido en el RFC 2767, permite la comunicación de un nodo IPv4 con nodos IPv6 permitiendo utilizar aplicaciones IPv4 existentes que no puedan ser actualizadas a IPv6. Es importante considerar que cada nodo tenga una pila dual, es decir, que implemente pila

UPSE

para los dos protocolos. Su funcionamiento se basa en que cuando un host IPv4 requiera comunicarse con un host IPv6 se le asignará una dirección IPv4, la traducción de paquetes se realiza de acuerdo con el mecanismo SIIT mencionado anteriormente.

Figura 33

Traducción BIS



Nota: Mediante la figura es posible distinguir el funcionamiento de BIS que requiere un router que admita BIS para realizar la traducción de direccionamiento. Fuente: (LACNIC)

Una vez estudiado y conceptualizado los tipos de mecanismos de transición que existen y que están definidos por el IEFT es importante destacar los que más se implementan actualmente y realizar una comparativa sobre las ventajas, desventajas y formas de operación de estos para poder obtener un análisis conveniente del tipo de mecanismo a utilizar en este proyecto.

Tabla 8

Tabla comparativa de mecanismos de transición

	Dual Stack	Tunelización	Traducción
Modo de operación	Implementa IPv4 e IPv6 en cada punto de la red para	Encapsula paquetes IPv4 en paquetes IPv6 y viceversa	Convierte cabeceras IPv4 en IPv6 y viceversa para

	comunicarse con sobre redes IPv4 permitir
	otros nodos IPv4 e para brindar comunicación de
	IPv6. conectividad. nodos IPv4 a IPv6.
	Transmite paquetes Permite una
	migración gradual
Ventajas	Sencillo de IPv6 sobre haciendo que redes
	implementar y infraestructuras IPv4 IPv6 accedan a
	optimiza el proceso de y existen varios tipos servicios de Internet
	comunicación. de túneles disponibles que mantienen
	para implementar. IPv4.
	No es recomendable
	para usos futuros y
Desventajas	Presenta problemas de requiere de altos
	Requiere que todos los escalabilidad y
	dispositivos de la red y costos de
	soporten IPv4 e IPv4 retardos mediante la implementación de
	en conjunto. transmisión de acuerdo con la
	información. necesidad de los
	equipos.

Nota: La tabla muestra tres tipos de mecanismos de transición como son dual stack, tunelización y traducción en el que se destaca su modo de operación, ventajas y desventajas de cada uno.

2.2.12.4. ELECCIÓN Y MECANISMO DE TRANSICIÓN A UTILIZAR

El modo de elección del mecanismo de transición a implementar en este proyecto se basó bajo un estudio previo de todos los mecanismos utilizados en la actualidad y que han sido implementados



UPSE

en diversas universidades y entidades del país, se destacó los resultados que se obtuvieron en cada implementación, las ventajas, desventajas y funcionalidad de cada uno de ellos.

Para la elección es importante mencionar que el proyecto maneja equipamiento de la marca Ubiquiti, por lo que se investigó los tipos de mecanismos de transición que esta tecnología admite.

En la investigación de lo mencionado se pudo encontrar que el equipo a utilizar de la marca Ubiquiti para la respectiva transición permite configurar dual stack y tunelización, en el caso de tunelización admite Tunnel Broker y 6to4.

Analizando también las ventajas, desventajas de los mecanismos de transición mencionados para los equipos Ubiquiti y considerando que el Proveedor de Internet de la universidad (CEDIA) no asigna un prefijo IPv6 a la universidad se optó por el método de tunelización ya que por medio de un proveedor de tunnel broker se puede obtener un bloque de direcciones IPv6 con prefijo de /48 independientemente del ISP de la universidad.

2.3. MARCO TEÓRICO

En esta sección se detallan diversas publicaciones relevantes revisados por el autor y acorde a la propuesta tecnológica de este proyecto:

En el año 2015, en Perú se realizó una tesis de grado titulada “Migración de IPV4 a IPV6 para mejorar la seguridad y velocidad de la red Telemática de la Universidad Pedro Ruiz Gallo”, el cual constituye principalmente de un análisis detallado del protocolo IPv4 e IPv6, destacando las ventajas del nuevo protocolo. Por otro lado, se efectúa una simulación basada en la red Telemática de la universidad utilizando el software de Packet Tracert, para la simulación se usa el método de transición Dual Stack, con la finalidad de obtener la convergencia entre IPv4 e IPv6. (Manayay & Olivera, 2015)



UPSE

En el año 2018, en Bolivia se realizó un trabajo de grado de maestría titulada “Integración del protocolo IPv6 a la red de Internet y Datos de COTAS R.L”, el cual consiste en rediseñar la red de Internet y datos de la empresa integrando el protocolo IPv6 utilizando métodos de transición como Dual Stack y traducción, obteniendo como resultado un mayor uso de direcciones IP’s y un buen funcionamiento del servicio que brinda la empresa. (Salvatierra, 2018)

En la ciudad de Ibarra en 2018 se realizó un trabajo de titulación titulado “Transición de Protocolo IPv4 a Protocolo IPv6 para la red inalámbrica EDUROAM dentro de la Universidad Técnica del Norte”, la cual realiza la respectiva implementación de coexistencia utilizando dispositivos de marca Cisco y la metodología Dual Stack, lo cual dio como resultado la garantía de conectar más dispositivos a la red de una manera segura, además de un mayor ancho de banda y velocidades en los dispositivos con IPV6. (Carrera, 2018)

CAPÍTULO III

3.1. COMPONENTES DE LA PROPUESTA

3.1.1. COMPONENTES FÍSICOS

Para esta propuesta se consideraron los siguientes equipos de la marca Ubiquiti debido a su gran capacidad:

3.1.1.1. DREAM MACHINE PRO

Es un dispositivo switch de 8 puertos que tiene múltiples funcionalidades, viene incorporado con dos puertos WAN, uno de 10 G SFP+ y un puerto Gigabit RJ45, además contiene puertos LAN, uno de 10 G SFP+ y ocho puertos Gigabit RJ45.

Figura 34

UDM Pro-Ubiquiti



Nota: Equipo Ubiquiti a utilizar que permitirá administrar los dispositivos de la red. Fuente: (Ubiquiti, s.f.)

3.1.1.2. EDGEROUTER 4

El EdgeRouter 4 ofrece un alto rendimiento para aplicaciones de enrutamiento, capaz de enrutar hasta 3,4 millones de paquetes por segundo para paquetes de 64 bits, este router incorpora 3 puertos Gigabit RJ45, un puerto Gigabit SFP y un puerto consola.

Ofrece direccionamiento estático IPv6, enrutamiento OSPFv3 y BGP, por lo que es posible aplicar mecanismos de transición como Dual stack y tunelización.

UPSE

Figura 35

EdgeRouter 4 Ubiquiti



Nota: El equipo que se muestra en la figura consta de varios puertos que ayudarán a la conectividad de la red.

Fuente: (Ubiquiti, s.f.)

3.1.1.3. FIBER MEDIA CONVERTER

Cuenta con dos puertos, uno para cable UTP y el otro puerto es SFP para conectar cables de fibra óptica ya sea multimodo o monomodo, su función es convertir señales eléctricas y ópticas provenientes de los cables para conectarlo con otro equipo y obtener una transmisión óptima.

Figura 36

Fiber Media Converter



Elaborado por el autor

3.1.1.4. UNIFI AC LITE

Es un punto de acceso con un alto rendimiento de hasta 1,2 Gbps en bandas de 5 GHz y rendimiento de 300 Mbps en bandas de 2,4 GHz. Se puede montar en paredes o techos para ampliar la cobertura

65

UPSE

de la señal, se puede configurar y administrar de forma fácil mediante la aplicación web o móvil.

Permite conectividad de hasta 100 usuarios.

Figura 37

Unifi AC Lite – Ubiquiti



Nota: La figura muestra un punto de acceso de la marca Ubiquiti. Fuente: (Ubiquiti, s.f.)

3.1.1.5. MÓDULO DE FIBRA MULTIMODO 1G

Los SFP multimodo son un tipo de módulo que permiten la transmisión de datos a corta distancia, el módulo de Ubiquiti de 1G contiene las características que se muestran en la tabla 9.

Tabla 9

Características del módulo SFP 1G MM

Descripción	Característica
Tipo de conector	LC
Longitud de onda Tx	850 nm
Longitud de onda Rx	850 nm
Velocidad de datos	1.25 Gbps
Distancia del cable	550 m

Nota: La table muestra las características generales del módulo SFP 1G mm de Ubiquiti. (Ubiquiti, s.f.)

3.1.1.6. PATCHCORD DÚPLEX

Contiene dos hilos de fibra con cubiertas independientes pero unidos entre sí, el patchcord a utilizar tiene sus terminaciones en LC/UPC y permitirá interconectar dos equipos que contengan puertos y módulos SFP, las características del cable se muestran en la tabla 10.

Tabla 10

Características del cable patchcord dúplex

Tipo	SM	Length	3M
Insertion loss (dB)	A (1)	0.26	B (1) 0.14
	A (2)	0.10	B (2) 0.11
Return loss (dB)	A (1)	55.6	B (1) 56.4
	A (2)	55.8	B (2) 56.6

Elaborado por el autor

3.1.2. COMPONENTES LÓGICOS

Se utilizará programas que facilitará la configuración, análisis y verificación de diversos parámetros para la ejecución del proyecto.

3.1.2.1. UNMS

El Sistema de Gestión de Red Ubiquiti es un sistema gratuito utilizado por usuarios y proveedores que permite realizar configuraciones de redes Ubiquiti, monitorear y verificar el rendimiento de las redes en tiempo real, gestión de dispositivos y exploración de funcionalidades de los equipos.

3.1.2.2. WIRESHARK

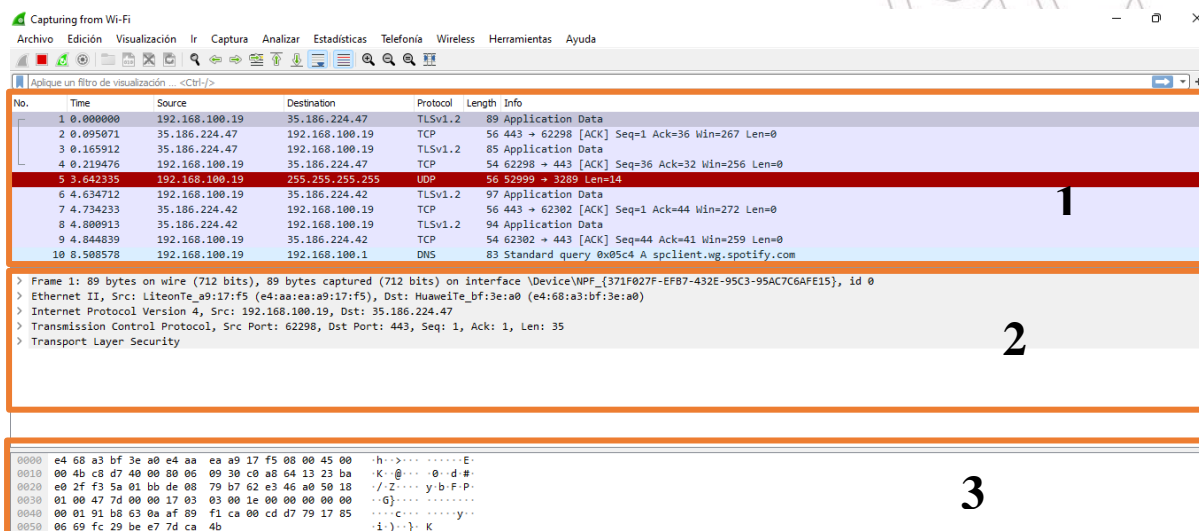
Wireshark permite capturar, mostrar y analizar todos los paquetes transmitidos y recibidos de una tarjeta de red cableada o inalámbrica, se compone de una librería de captura de paquetes y un analizador de paquetes.

Wireshark es una herramienta que soporta más de 480 protocolos en el que se incluye IPv6, permite analizar todo el tráfico de la red mediante una interfaz gráfica, permite aplicar filtros para obtener solo los paquetes que se quieren analizar y mediante Wireshark es posible detectar y resolver fallos o anomalías en la red.

La interfaz de Wireshark se divide en tres secciones, en la primera se encuentra el listado de los paquetes que fueron capturados y se especifica el número, tiempo, fuente, destino, protocolo, longitud e información de cada paquete; la segunda sección muestra información detallada en forma de árbol acerca del paquete que se selecciona y es una parte importante al momento de analizar paquetes, por último, se tiene una sección compuesta por datos formato hexadecimal, cuando se selecciona alguna fila de la sección dos en la parte inferior se resaltarán los bytes para lo seleccionado.

Figura 38

Interfaz gráfica de Wireshark



Elaborado por el autor

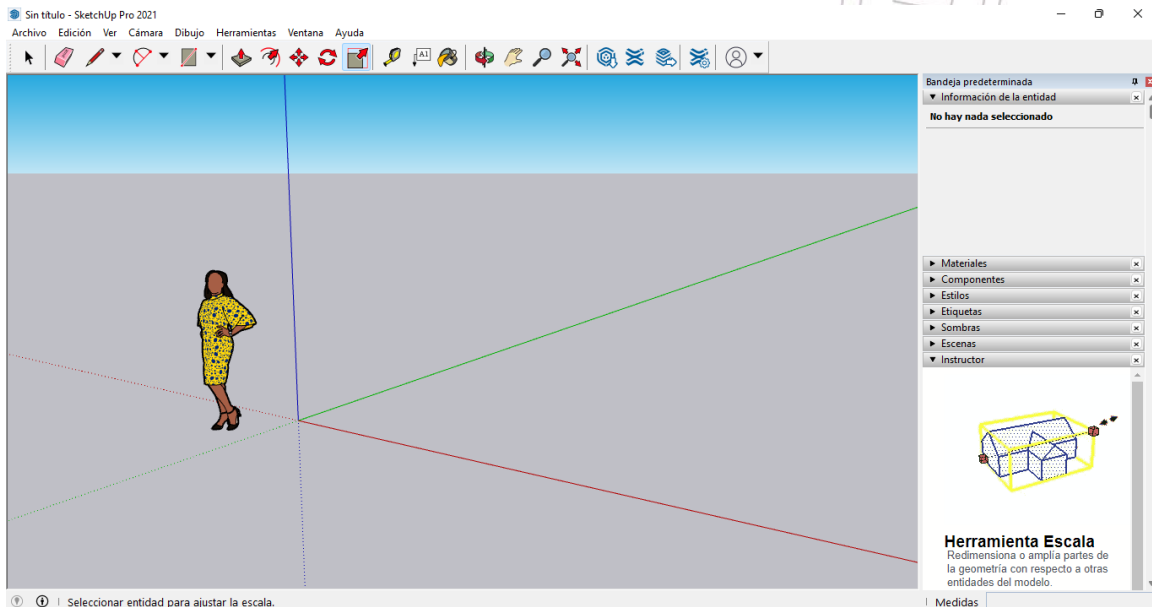
3.1.2.3. SKETCHUP PRO

El software de SketchUp Pro permite realizar esquemas, planos, diagramas y diseños en general basado en el modelado 3D mediante él es posible crear desde modelos simples hasta modelos con grandes estructuras, es mayormente utilizado por arquitectos en lo que respecta a diseño de interiores y exteriores.

Para el diseño del laboratorio de telecomunicaciones se utilizará SketchUp Pro que permitirá realizar un modelado 3D del mismo y de los equipos que se implementarán con sus respectivas dimensiones de manera que se pueda obtener una visión del proyecto previo a la implementación.

Figura 39

Interfaz gráfica de SketchUp Pro



Elaborado por el autor

3.1.3. DISEÑO Y DESPLIEGUE DE RED CON FIBRA ÓPTICA

En el diseño de la propuesta se presenta una topología en árbol con los componentes que se muestran en la figura 40, la topología en árbol también es denominada topología jerárquica, y es

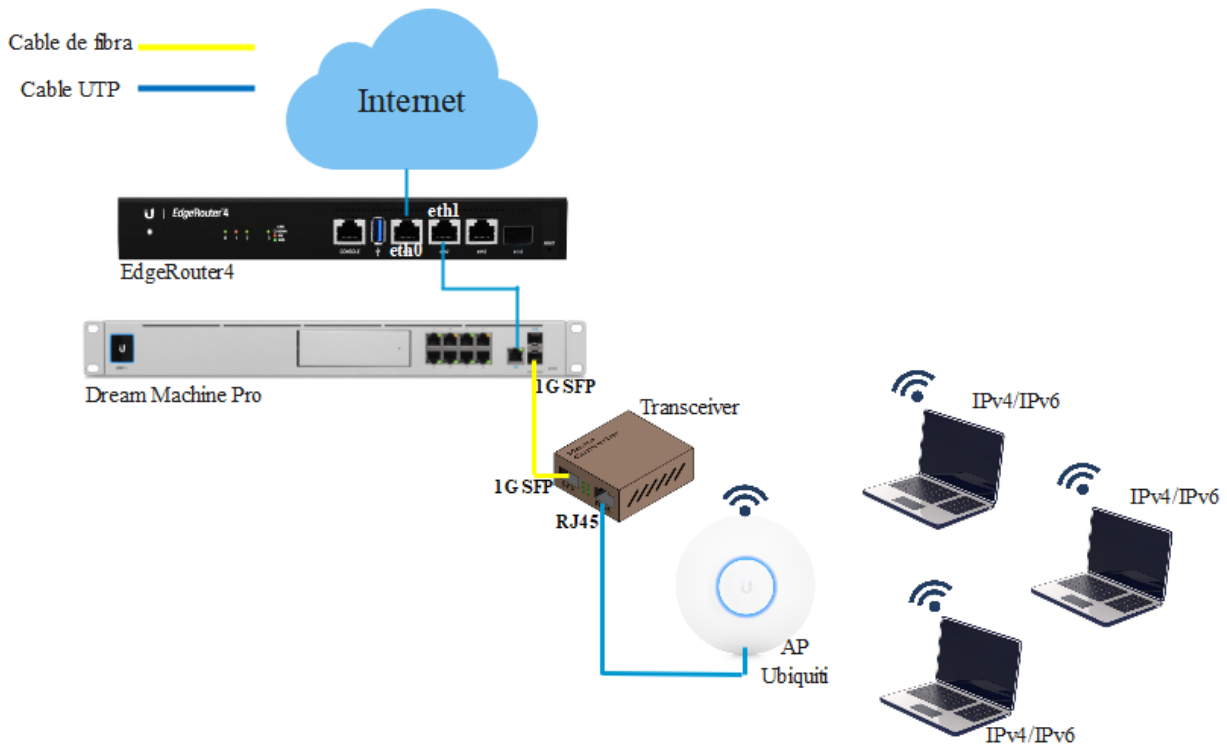
UPSE

una combinación de varias redes en estrella, esta topología consiste en un nodo central al que se conectan los demás equipos en la red.

El diseño de la red que se muestra en la figura 40 contiene dos partes, la red cableada y la red inalámbrica en el que un segmento está compuesto por cable de fibra óptica y cable UTP, mientras que la otra parte se compone de los dispositivos finales conectados inalámbricamente a la red.

Figura 40

Diseño de la propuesta



Elaborado por el autor.

Para obtener un esquema claro de la forma en la que se conectan los equipos con sus respectivos puertos con la finalidad de brindar una conexión óptima de los dispositivos finales se presenta la tabla 11 en la que se describen los puertos a utilizar y su respectiva descripción.

UPSE
Tabla 11

Conexión de equipos mediante puertos

Equipo	Puerto	Descripción
EdgeRouter 4	Ethernet0	ISP
	Ethernet1	Conexión con UDM Pro
UDM Pro	Puerto 9	RJ45 Internet
	Puerto 11	1G SFP LAN conectado al transceiver
Transceiver	Puerto SFP	Conexión con UDM Pro
	Puerto RJ45	Conexión con UAP AC-Lite
UAP AC-Lite	Puerto RJ45	Conexión con transceiver

Elaborado por el autor

3.1.3.1. DISEÑO EN SKETCHUP PRO

Para realizar el diseño del laboratorio de telecomunicaciones se utilizó el software de SketchUp Pro, pues de esta manera se tiene un panorama claro de donde se encontraría ubicado el rack con los respectivos equipos a implementar y el orden de los mismos, como se observa en la figura 41 el rack se ubicará del lado derecho de una estación de trabajo.

Figura 41

Ubicación del rack



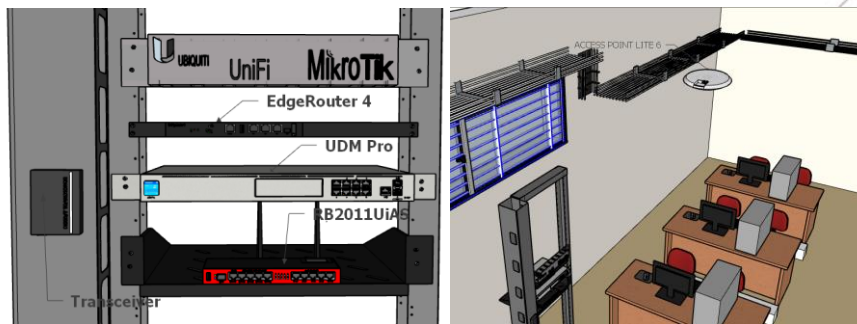
Elaborado por el autor

UPSE

El orden y la ubicación de los equipos se muestran en la figura 42 como se puede observar la mayoría de los equipos se ubicarán en el rack de piso, mientras que el AP al ser un dispositivo que propaga su señal en un ángulo de 360 grados deberá ubicarse de forma estratégica en el tumbado del laboratorio de manera que cumpla el estándar TIA/EIA 568 A.

Figura 42

Ubicación de equipos

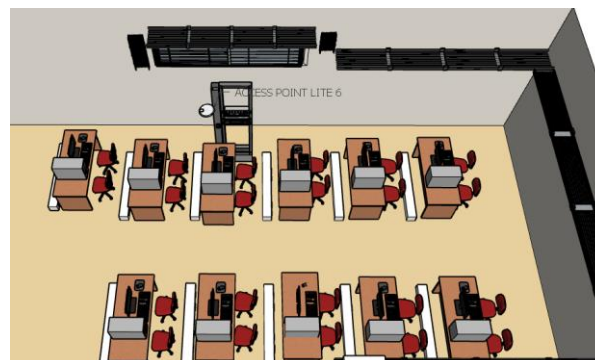


Elaborado por el autor

En la figura 43 se observa de manera general una vista completa del laboratorio de telecomunicaciones en donde se puede apreciar de mejor manera la ubicación del rack de piso y el AP Ubiquiti.

Figura 43

Vista general del diseño del laboratorio



Elaborado por el autor

3.1.3.2. DESCRIPCIÓN DE UBICACIÓN Y CONEXIONES DE EQUIPOS

El proyecto desarrolla un cableado estructurado en el laboratorio de telecomunicaciones que contiene cables UTP categoría 6 y cable de fibra óptica escogido basado en el estándar UIT-T G.651 el cual es el de multimodo, pues este es óptimo para la comunicación a distancias menores a 2 Km y es implementado en las comunicaciones de redes LAN.

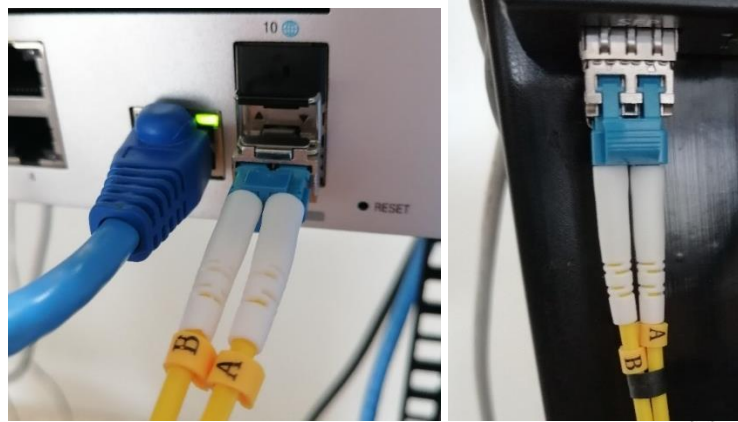
En el laboratorio de telecomunicaciones se encuentra un rack de piso que se utilizará para la instalación de los equipos, es importante mencionar que la mitad del rack está ocupado por equipos de la marca Mikrotik por lo que la implementación de los equipos de la marca Ubiquiti se realizará debajo de los equipos Mikrotik, para ello se consideró el orden de equipos mostrado en la figura 42 empezando por el EdgeRouter que se conecta a Internet desde su puerto eth0 empleando cable UTP, el segundo equipo en la ubicación del rack es el Dream Machine Pro, su conexión a Internet se realiza mediante el puerto 9 que se conecta con el puerto eth1 del router a través de cable UTP. También se hace uso del puerto 11 (SFP LAN) en el que se insertará un módulo SFP multimodo de 1G para la implementación de fibra óptica del laboratorio, la conexión de este puerto se dirige hacia el puerto de fibra del transceiver en el que también se insertará un módulo SFP multimodo para que los equipos se puedan conectar por cable de fibra, en este punto hay que considerar que al utilizar módulos multimodo el cable de fibra óptica también debe ser multimodo.

El cable de fibra multimodo está compuesto por dos fibras en el que se debe considerar la polaridad de los extremos para mantener una conexión, cada extremo del cable está compuesto por un transmisor y un receptor etiquetados como B y A respectivamente, para mantener una correcta polaridad se emplea la normativa TIA 568-C.3.

UPSE

Figura 44

Polaridad de conexión para cable multimodo



Elaborado por el autor

La ubicación del transceiver se colocará en el extremo izquierdo del rack, ya que al ser un dispositivo pequeño se puede adaptar en cualquier lugar.

En el transceiver se hace una segunda conexión por el puerto RJ45 que se dirigirá al AP Ubiquiti para poder brindar conexiones inalámbricas en la red del laboratorio.

Figura 45

Conexiones del transceiver



Elaborado por el autor



UPSE

3.1.4. SITUACIÓN DE LA RED ACTUAL DEL LABORATORIO DE

TELECOMUNICACIONES

Una vez implementada la red de fibra óptica es importante destacar las funcionalidades de cada equipo para el soporte de IPv6, en la siguiente tabla se detallan los equipos utilizados en la red y sus respectivas características para el despliegue del mecanismo de transición:

Tabla 12

Equipos de la red del laboratorio

Equipo	Marca/Modelo	Observación
Router	Ubiquiti/EdgeRouter 4	Soporta IPv6
UDM Pro	Ubiquiti/UDM Pro	Soporta IPv6
Transceiver	-----	Soporta IPv6
Access Point	Ubiquiti/ UNIFI AC LITE	Soporta IPv6
Access Point	Mikrotik/RB2011UiAS-2HnD	Soporta IPv6

Elaborado por el autor

Para el usuario final se utilizarán laptops en el que sus sistemas operativos admitan la coexistencia de IPv4 e IPv6, de tal manera que se pueda tener conectividad a la red y poder realizar las respectivas pruebas, la siguiente tabla muestra las características de los dispositivos finales a utilizar.

UPSE
Tabla 13

Dispositivos finales

Equipo	Marca	Característica	Sistema Operativo	Observación
Computadora portátil	Lenovo	Core i5 10th Gen	Windows 11	Soporta IPv6
Computadora portátil	Dell	Core i3 7ma Gen	Windows 10	Soporta IPv6

Elaborado por el autor

3.1.5. CONFIGURACIÓN DE EQUIPOS

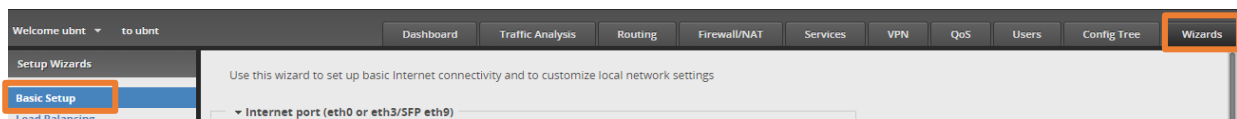
Para la conectividad a Internet del laboratorio el departamento de TIC's proporcionó un puerto para dar salida a Internet por medio de ethernet hacia el puerto eth0 del router, como se trata de la implementación de nuevos equipos para el laboratorio, es importante considerar las configuraciones iniciales que se realizaron en cada uno de ellos.

3.1.5.1. CONFIGURACIÓN IPV4 EDGEROUTER

En primer lugar, se configuró el EdgeRouter, para su configuración se ingresa a la interfaz del router por medio de un navegador e ingresando la dirección por defecto 192.168.1.1 y el usuario y contraseña por defecto que es ubnt para ambos, en la interfaz se escoge en la pestaña Wizards y luego en Basic Setup como se muestra en la figura 46.

Figura 46

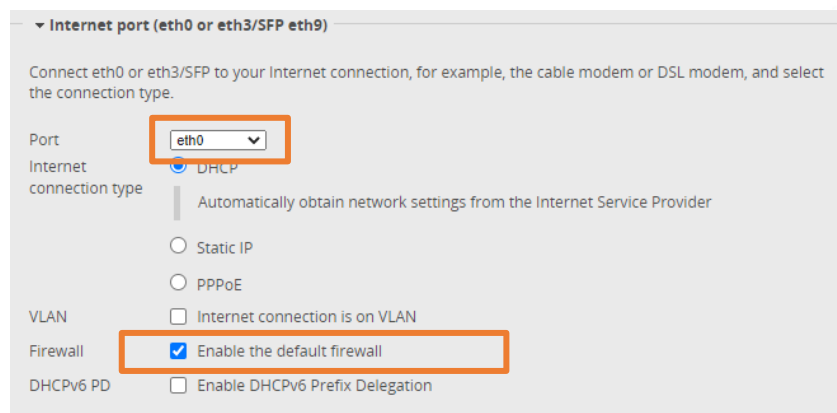
Ingresar a configuración básica



En este caso el puerto eth0 es establecido como WAN y se asigna una dirección IPv4 por DHCP habilitando la opción de firewall para dar seguridad a la red, lo mencionado se muestra en la figura 47.

Figura 47

Configuración puerto WAN

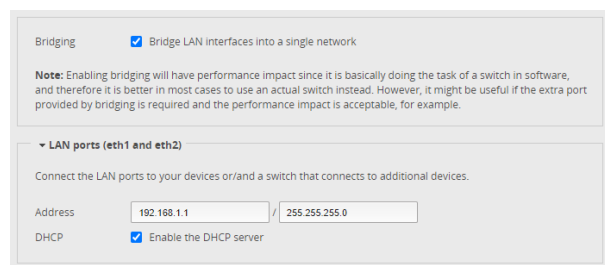


Elaborado por el autor

Los puertos eth1 y eth2 del EdgeRouter se establecen como LAN, por lo que en este proyecto ambos puertos se configuraron como bridge (puente), el bridge permite interconectar los segmentos eth1 y eth2 formando una única subred, lo mencionado se muestra a continuación.

Figura 48

Configuración puertos LAN



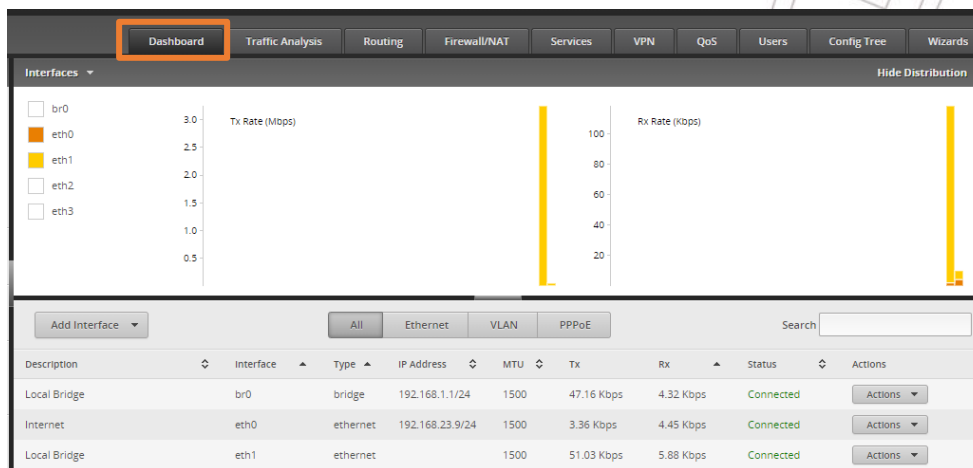
Elaborado por el autor

Al realizar los cambios para los puertos es necesario reiniciar el equipo para que se guarden los cambios, para ello se debe colocar un usuario y una contraseña, en este caso se colocó de usuario ubnt y de contraseña ubnt.

Al reiniciar el equipo se deberá acceder con los datos mencionados, en la figura 49 se muestra el estado de todas las interfaces configuradas como se puede observar la interfaz eth0 (WAN) toma la dirección por DHCP 192.168.23.9/24 de la red 192.168.23.0/24 y las interfaces eth1 y eth2 al estar puenteadas toman una sola dirección la 192.168.1.1/24.

Figura 49

Interfaces del EdgeRouter



Elaborado por el autor

3.1.5.2. CONFIGURACIÓN DE IPV4 EN UDM PRO

Al conectar el puerto eth1 al puerto WAN RJ45 (puerto 9) del UDM Pro, esta toma una dirección por DHCP para proporcionar conectividad a Internet, en este caso fue la dirección IP 192.168.1.40 de la red 192.168.1.0/24, la figura 50 muestra a detalle características como la dirección IP que toma, el proveedor de servicio, la ubicación del proveedor y la utilización máxima de subida y descarga.



UPSE

Figura 50

Dirección IPv4 del UDM Pro

Internet					
NAME	IP ADDRESS	SERVICE PROVIDER	LOCATION	UPTIME	PEAK UTILIZATION (UL / DL)
● Default (WAN...	192.168.1.40	CEDIA	Cuenca	100%	7%/8%
● Backup (WAN...	-	-	-	-	-

Elaborado por el autor

El bloque de direcciones de la red LAN que parte del UDM Pro se puede observar en la figura 51, la cual es 192.168.0.0/24 teniendo un rango de direcciones desde 192.168.0.2 – 192.168.0.254 con la máscara de subred 255.255.255.0

Figura 51

Red LAN Ipv4 UDM Pro

Networks					
NAME	ROUTER	SUBNET	IP LEASES	INTERNET	BACKUP
● Default	UDM PRO - T...	192.168.0.0/24	13 (249)	Default (WAN1)	-

[+ Create New Network](#)

Elaborado por el autor

3.1.5.3. CONFIGURACIÓN DE IPV4 EN AP AC-LITE

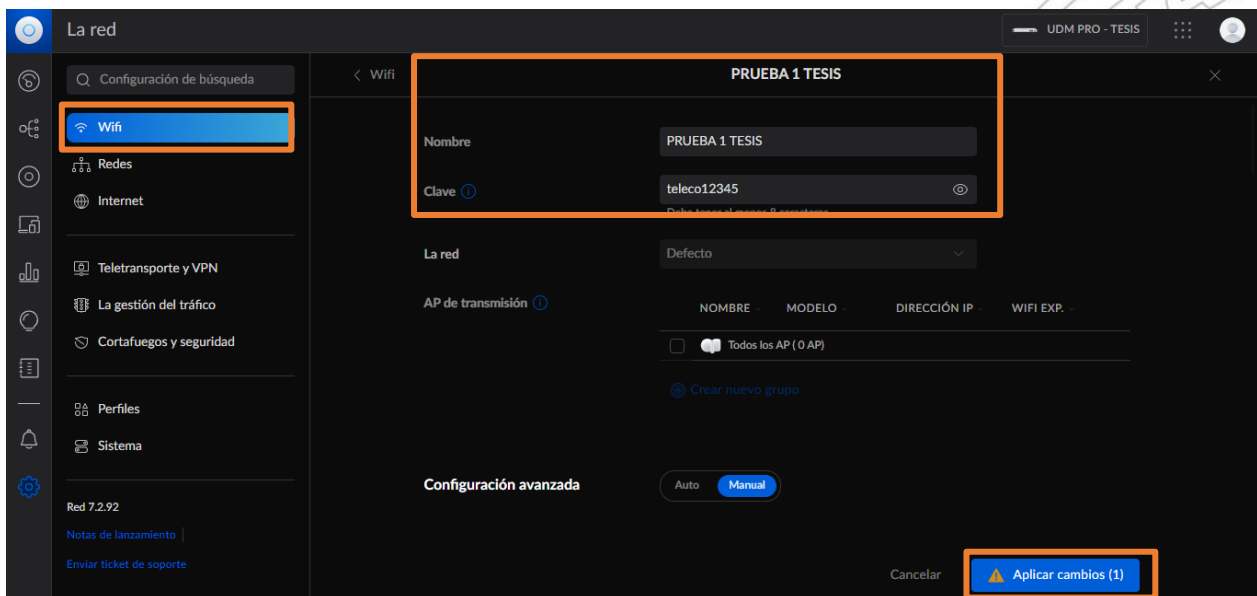
Se deberá conectar el punto de acceso al transceiver para inicializar la respectiva configuración, esto se lo puede realizar mediante la interfaz gráfica del UDM Pro debido a que el transceiver se

UPSE

encuentra conectado a este equipo, para ello nos dirigimos a la ventana de red elegimos la opción de Wifi, aquí aparecerá el AP que se conectó, al seleccionarlo se deberá especificar el nombre de la red y la clave de seguridad, en este caso el SSID será PRUEBA 1 TESIS y la contraseña teleco12345, a continuación seleccionar en aplicar cambios para guardar la configuración.

Figura 52

Configuración UAP AC Lite

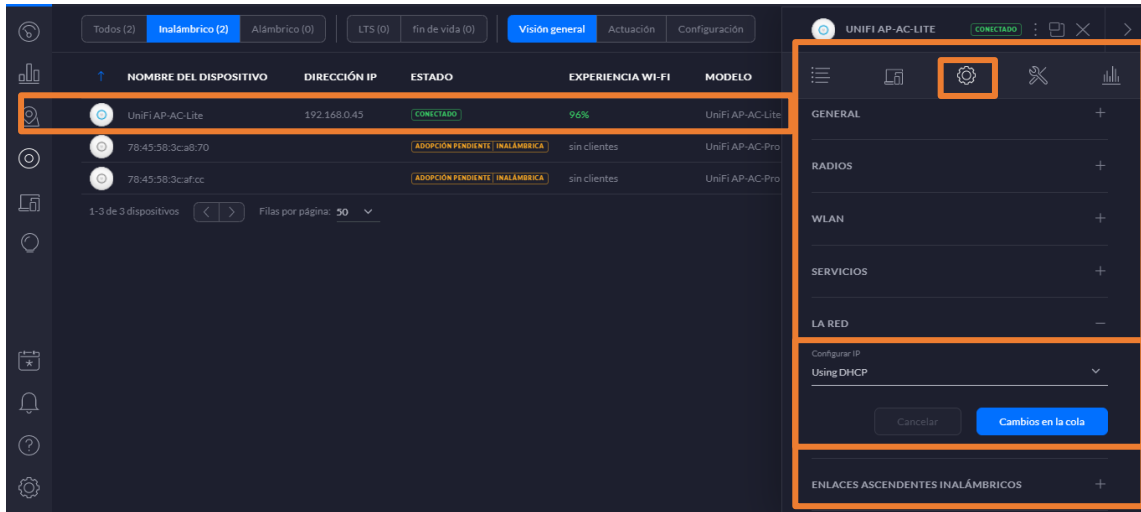


Elaborado por el autor

Al regresar a la interfaz principal encontraremos el punto de acceso, al seleccionarlo en el apartado derecho se mostrarán algunas opciones en la que seleccionaremos el ícono de configuración, aquí nos dirigimos a la sección de “La red” y colocaremos la configuración de la dirección IP mediante DHCP como se muestra en la siguiente figura.

UPSE
Figura 53

Configuración UAP AC Lite

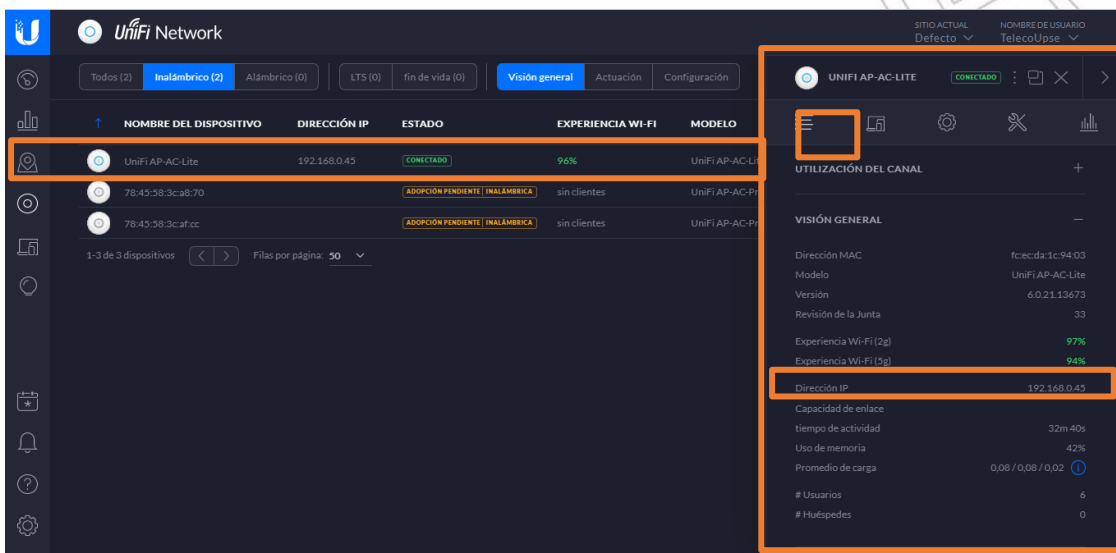


Elaborado por el autor

Ahora seleccionamos el primer ícono del apartado derecho para observar las características de la red y la dirección IPv4 que toma, lo mencionado se muestra en la siguiente figura.

Figura 54

Características de la configuración del UAP AC Lite



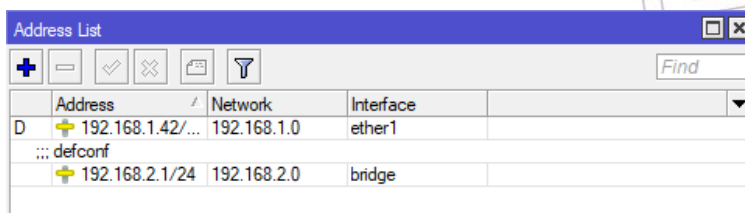
3.1.5.4. CONFIGURACIÓN DE IPV4 EN RB2011 MIKROTIK

El equipo Mikrotik se conecta al UDM Pro mediante el puerto SFP+ LAN (puerto 11) y el puerto eth1 del RB2011 utilizando un transceiver para hacer posible la comunicación por fibra óptica, una vez conectado se procede a configurar el equipo haciendo uso del Winbox.

Al abrir la aplicación del winbox aparecerá el equipo, lo seleccionamos para ingresar y realizar la configuración, en el menú de la izquierda seleccionar address list deberá aparecer la dirección IPv4 por DHCP que proviene del UDM Pro, también es necesario añadir una dirección para la red LAN, la cual se configurará en todos los puertos mediante un puente (bridge), la dirección de red a utilizar es la 192.168.2.0/24, el address list se muestra en la figura 55.

Figura 55

Lista de direcciones IPv4 Mikrotik

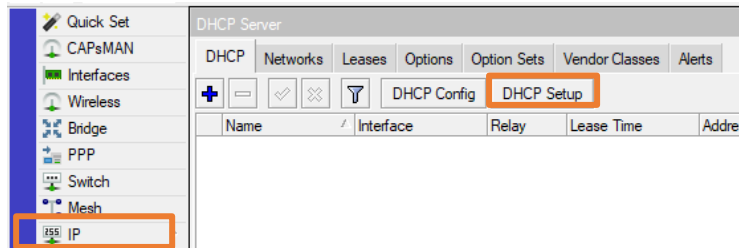


	Address	Network	Interface
D	192.168.1.42/...	192.168.1.0	ether1
defconf	192.168.2.1/24	192.168.2.0	bridge

Elaborado por el autor

Para que los dispositivos finales puedan obtener direccionamiento IPv4 de forma automática se debe crear un DHCP server con la dirección de la red LAN ingresada anteriormente, para configurar se dirige al menú izquierdo en IP, luego a DHCP Server y hacer clic en DHCP Setup como se muestra en la figura 56.

Añadir DHCPv4 en Mikrotik

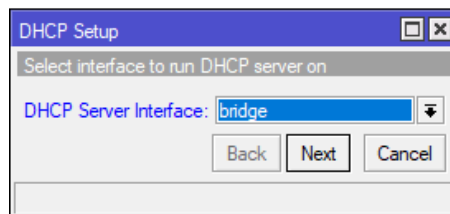


Elaborado por el autor

Al seleccionar DHCP Setup se abre una pequeña ventana como se muestra en la figura 57 en la que se deberá especificar mediante un paso a paso la interfaz a aplicar en este caso bridge, el espacio de direcciones (192.168.2.0/24), la puerta de enlace para la red (192.168.2.1), el rango de direcciones (192.168.2.2 – 192.168.2.254) y el DNS Server (192.168.1.0), si lo indicado se realizó de forma correcta al finalizar aparecerá un mensaje señalando que la configuración se completó exitosamente.

Figura 57

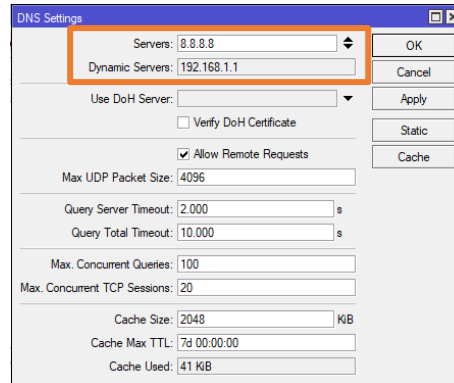
Ventana DHCP Setup



Elaborado por el autor

Luego se agrega la configuración DNS, este apartado lo encontramos en el menú IP en DNS, en la ventana que aparece se debe especificar la dirección del servidor DNS de Google 8.8.8.8 y la dirección del servidor dinámico, para guardar los cambios seleccionamos en Apply, luego en OK.

Configuración DNS

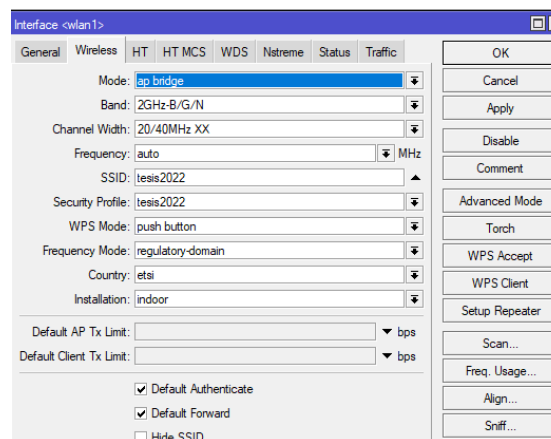


Elaborado por el autor

Ahora debemos configurar el equipo para crear un punto de acceso y poder conectarse a la red de forma inalámbrica, para ello seleccionamos Wireless del menú del Winbox aparecerá una ventana llamada Wireless Tables en la pestaña de WiFi Interfaces se configura la interfaz wlan 1 especificando el modo, la banda de frecuencia, la frecuencia y el SSID, la selección de las características mencionadas se muestra a continuación.

Figura 59

Configuración de interfaz inalámbrica

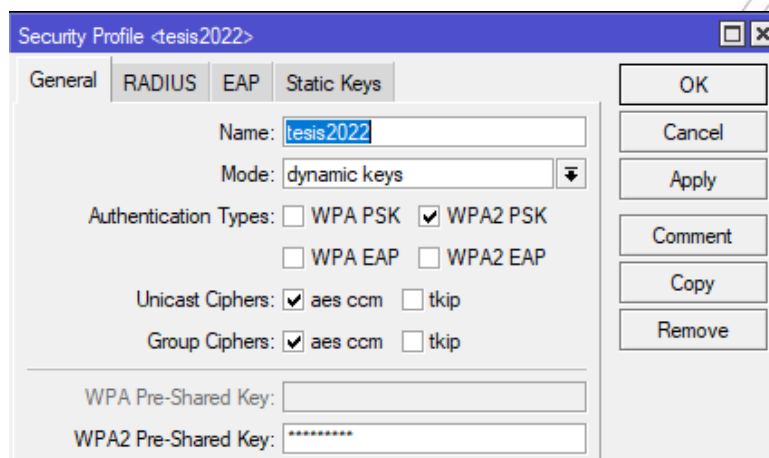


Elaborado por el autor

Por último, debemos agregar la seguridad al AP en la misma ventana de Wireless Tables seleccionamos la pestaña de Security Profiles, luego el botón agregar para crear un nuevo perfil aquí se especifica el nombre, en este proyecto se utilizará el nombre de la red tesis2022, el tipo de seguridad será WPA2 PSK y la contraseña tesis2022, una vez colocado todos los parámetros seleccionamos en Apply, luego en OK para guardar la configuración.

Figura 60

Configuración de seguridad del AP

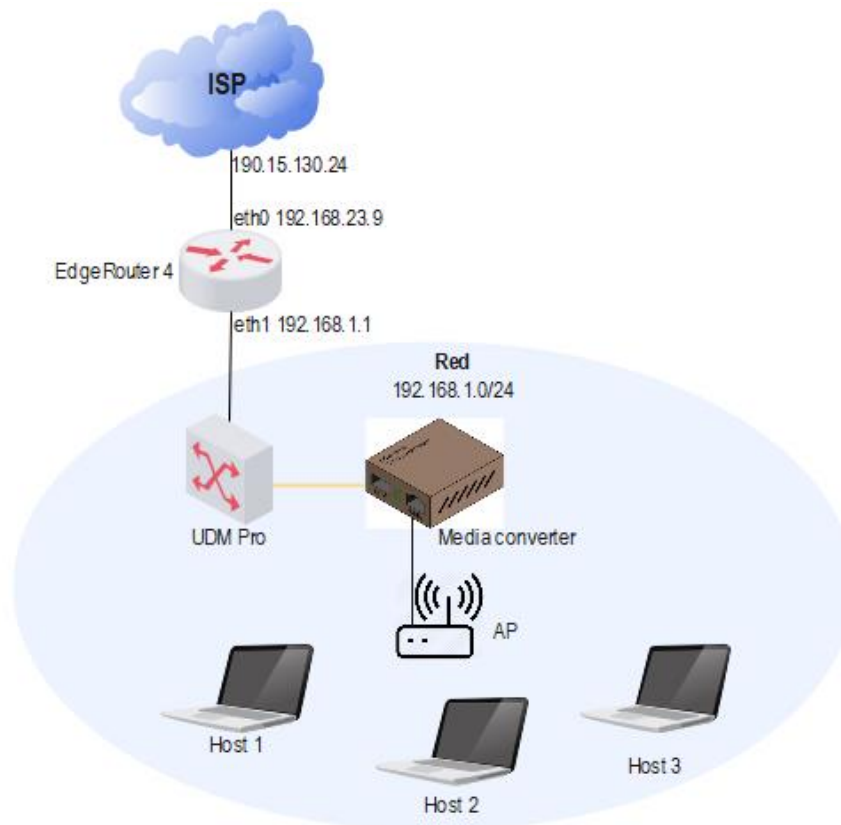


Elaborado por el autor

3.1.5.5. DISEÑO LÓGICO DE RED IPV4 DEL LABORATORIO DE TELECOMUNICACIONES

Una vez configurada la red en IPv4 para que los dispositivos puedan conectarse de forma inalámbrica, se procede a elaborar el diseño lógico del mismo considerando el AP inalámbrico de la marca Mikrotik.

Diseño nuevo de red IPv4 en el laboratorio



Elaborado por el autor

3.1.6. DESARROLLO DEL MECANISMO DE TRANSICIÓN

En este proyecto se consideraron dos puntos importantes, el primero realizar el modelo de uno de los mecanismos de transición para la futura salida a Internet por IPv6 en el laboratorio de telecomunicaciones de la universidad y el segundo la creación de la red interna con direccionamiento IPv6, para el primer punto se consideró el mecanismo de tunelización que hará factible la coexistencia de los protocolos de direccionamiento IPv4 e IPv6, como se estudió anteriormente en la sección 2.2.12 existen varios tipos de túneles que se pueden implementar, para el modelo se optó por utilizar un túnel denominado tunnel 6to4.



UPSE

La elección del mecanismo mencionado se debió a que el ISP (Proveedor de Servicio de Internet) aún no ha proporcionado direcciones IPv6 nativas a la universidad, por lo que mediante la utilización del túnel sería posible lograr la conectividad de una red IPv6 a otras redes que manejan IPv6 a través de la infraestructura IPv4 que se emplea.

Para la obtención del bloque de direccionamiento IPv6 se utilizó el prefijo asignado para túneles 6to4 (2002::/16) y la dirección IPv4 pública, la dirección IPv4 pública que tiene la universidad es la 190.15.130.24, además se utiliza el prefijo de sitio /64 al tratarse del laboratorio, esto se debe a que es un campus limitado comparado a una empresa.

Para obtener la dirección IPv6 global y hacer que la red del laboratorio pueda comunicarse con otros dominios IPv6 habrá que autoasignarle una dirección global que contenga el prefijo mencionado para túneles, en este caso el formato de la dirección IPv6 sería 2002:ADD-IPv4::/48, en ADD-IPv4 se considera la dirección IPv4 que contiene el router para dar acceso a internet a la red (IPv4 pública), esta dirección es transformada a formato IPv6, a este tipo de formato se les denomina dirección IPv4 mapeada.

De la dirección IPv4 pública se escogen los dos primeros octetos para formar el segundo hexteto de la dirección IPv6 seguido del prefijo 2002, así mismo se escogen los dos octetos restantes del IPv4 para formar el tercer hexteto para la dirección IPv6 global, los octetos se deben transformar a formato hexadecimal, por lo que la dirección IPv4 pública mapeada o transformada a IPv6 sería como se muestra en la figura 62.

Mapeo de dirección IPv4 pública

IPv4 privada:

190.15.130.24

IPv4 en binario:

1011 1110.0000 1111.1001 0010.0001 1000

IPv4 en hexadecimal:

be 0f 82 18

Dirección IPv6:

2002:be0f:8218::/48

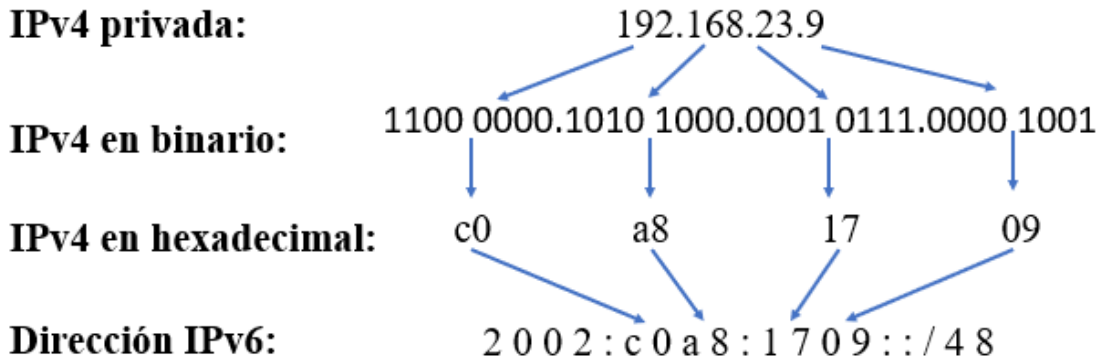
Elaborada por el autor

Del prefijo IPv6 global 2002:be0f:8218::/64 se obtiene la primera dirección 2002:be0f:8218:0001::1 que deberá ser agregada en el router de frontera para comunicación con otras redes en IPv6 y la segunda dirección 2002:be0f:8218:0001::2 para la comunicación del router de frontera con los hosts.

Para el segundo punto que se mencionó anteriormente se hará uso de la dirección IPv4 privada mediante el cual se deberá obtener un prefijo IPv6 para la asignación de direcciones en las redes internas, al realizar la configuración inicial del router se obtuvo la dirección 192.168.23.9.

Se realiza el mismo proceso con el que se obtuvo la IPv6 global pero ahora utilizando la dirección IPv4 privada por lo que la dirección IPv6 obtenida para los dispositivos finales, el proceso de conversión sería como se muestra en la figura 63.

Mapeo de dirección IPv4 privada



Elaborada por el autor

La dirección IPv6 obtenida que se muestra en la figura 63 será destinada para la red LAN y mediante ella se podrán crear diferentes subredes para diferentes fines dentro del laboratorio.

3.1.6.1. ASIGNACIÓN DE DIRECCIONES

Cuando se realizaba el direccionamiento IPv4 existían dos segmentos, uno para la parte de red y otro para la parte de host en el que la máscara de subred definía cual pertenecía a la parte de red y cual a la parte de host y la división de la red en subredes se hacía mediante subnetting.

Para IPv6 también se tienen dos segmentos que se los denomina ID de red e ID de interfaz, se debe considerar que al tratarse de un laboratorio las subredes tendrán un prefijo de /64 que identificarán el ID de interfaz, se tiene que por dichas subredes se podrían conectar un aproximado de dieciocho trillones de dispositivos o hosts debido al total de direcciones que este prefijo permite (2^{64}).

El hecho de tener una cantidad muy grande de direcciones no indica un desperdicio de las mismas, ya que se pueden administrar de forma que las direcciones se utilicen de manera óptima, además



UPSE

es importante mencionar que la disponibilidad total de direcciones IPv6 es muy alta, por lo que el grupo de direcciones para este proyecto es relativamente pequeño.

Entonces se establece que todas las subredes tendrán un prefijo de /64, esto quiere decir que los primeros 64 bits serán para identificar a la red y los 64 restantes identificarán la interfaz, para obtener el total de subredes se tiene que toda la red tiene un prefijo de /48 y para las subredes se utilizará un prefijo de /64 por lo que su diferencia es de 16 bits lo que equivale a un total de 65536 subredes (2^{16}) que podrá tener el laboratorio.

Una vez realizado el análisis y la obtención de prefijos en IPv6 se presenta la forma en la que se asignarán las direcciones IPv6 a los equipos, en el router se configurará la dirección de forma manual mientras que en los demás equipos se les asignará por DHCPv6.

En la tabla 14 se especifican las direcciones IPv6 a utilizar obtenidas anteriormente que se aplicarán en la red del laboratorio.

Tabla 14

Asignación de direcciones IPv6

Direccionamiento IPv4 e IPv6		
Descripción	IPv4	IPv6
IPv4 pública	190.15.130.24	
Dirección WAN	192.168.23.9	
IP pública mapeada		2002:be0f:8218::/64
IPv4 privada	192.168.1.1	
IP privada mapeada		2002:c0a8:1709::/64
Prefijo /48		2002:c0a8:1709::/48

Elaborado por el autor



UPSE

Como se mencionó anteriormente se utilizará un prefijo /64 para crear las respectivas subredes, para ello habrá que definir el cuarto hexteto de 2002:c0a8:1709::/48 para cada subred, el método que se utiliza es mediante la combinación y el manejo de bits (desde el bit 56 al 64), en la tabla 15 se muestra la forma en la que se obtiene el cuarto hexteto para las subredes.

Tabla 15

Creación de subredes

Laboratorio /48	Subred/64	Bits restantes
2002:c0a8:1709:	0000 0000 0000 0000	64
2002:c0a8:1709:	0000 0000 0000 0001	64
2002:c0a8:1709:	0000 0000 0000 0010	64
2002:c0a8:1709:	0000 0000 0000 0011	64
2002:c0a8:1709:	0000 0000 0000 0100	64
2002:c0a8:1709:	0000 0000 0000 0101	64
2002:c0a8:1709:	0000 0000 0000 0110	64
2002:c0a8:1709:	0000 0000 0000 0111	64
2002:c0a8:1709:	0000 0000 0000 1000	64
2002:c0a8:1709:	0000 0000 0000 1001	64
2002:c0a8:1709:	0000 0000 0000 1010	64
2002:c0a8:1709:	64
2002:c0a8:1709:	1111 1111 1111 1111	64

Elaborado por el autor

La representación de las subredes en formato hexadecimal de la tabla 16 se muestra a continuación.



UPSE
Tabla 16

Direccionamiento IPv6

Dirección subred	Prefijo	Rango de direcciones
2002:c0a8:1709:0001::	64	2002:c0a8:1709:1::2 2002:c0a8:1709:1:ffff:ffff:ffff:ffff
2002:c0a8:1709:0002::	64	2002:c0a8:1709:2::2 2002:c0a8:1709:2:ffff:ffff:ffff:ffff
2002:c0a8:1709:0003::	64	2002:c0a8:1709:3::2 2002:c0a8:1709:3:ffff:ffff:ffff:ffff
2002:c0a8:1709:0004::	64	2002:c0a8:1709:4::2 2002:c0a8:1709:4:ffff:ffff:ffff:ffff
2002:c0a8:1709:0005::	64	2002:c0a8:1709:5::2 2002:c0a8:1709:5:ffff:ffff:ffff:ffff
2002:c0a8:1709:0006::	64	2002:c0a8:1709:6::2 2002:c0a8:1709:6:ffff:ffff:ffff:ffff
2002:c0a8:1709:0007::	64	2002:c0a8:1709:7::2 2002:c0a8:1709:7:ffff:ffff:ffff:ffff
2002:c0a8:1709:0008::	64	2002:c0a8:1709:8::2 2002:c0a8:1709:8:ffff:ffff:ffff:ffff
2002:c0a8:1709:0009::	64	2002:c0a8:1709:9::2 2002:c0a8:1709:9:ffff:ffff:ffff:ffff
2002:c0a8:1709:000a::	64	2002:c0a8:1709:a::2 2002:c0a8:1709:a:ffff:ffff:ffff:ffff
2002:c0a8:1709:.....:	64	2002:c0a8:1709:.....:2 2002:c0a8:1709:.....:ffff:ffff:ffff:ffff
2002:c0a8:1709:ffff::	64	2002:c0a8:1709:ffff:2 2002:c0a8:1709:ffff:ffff:ffff:ffff

Elaborado por el autor

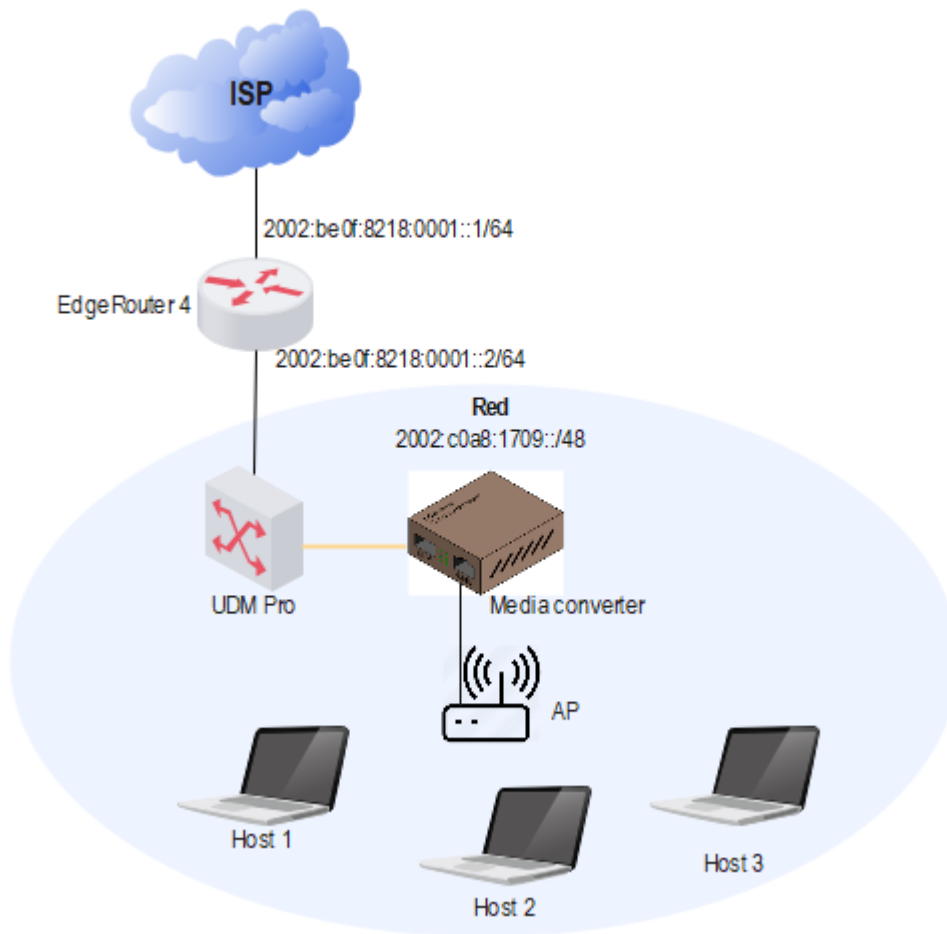
Para el proyecto se hará uso de dos subredes, debido a la cantidad de equipos que se está utilizando, pues al tener una subred de prefijo 64 ésta será suficiente para conectar dichos equipos a la red, la primera subred 2002:c0a8:1709:0001::/64 estará dedicada a la red interna dominada por el AP Ubiquiti y la segunda subred 2002:c0a8:1709:0002::/64 se le asignará a la red interna que maneja el AP Mikrotik, al utilizar únicamente dos subredes se podría decir que las subredes restantes se reservarán para futuros proyectos del laboratorio en IPv6.

3.1.6.2. DISEÑO LÓGICO DE RED IPV6 DEL LABORATORIO DE TELECOMUNICACIONES

En la figura 64 se observa el diseño lógico de la red, el cual incluye los equipos a utilizar y el direccionamiento IPv6 para cada interfaz.

Figura 64

Diseño de red IPv6 en el laboratorio



Elaborado por el autor

3.1.7. CONFIGURACIÓN DEL PROTOCOLO DE TRANSICIÓN

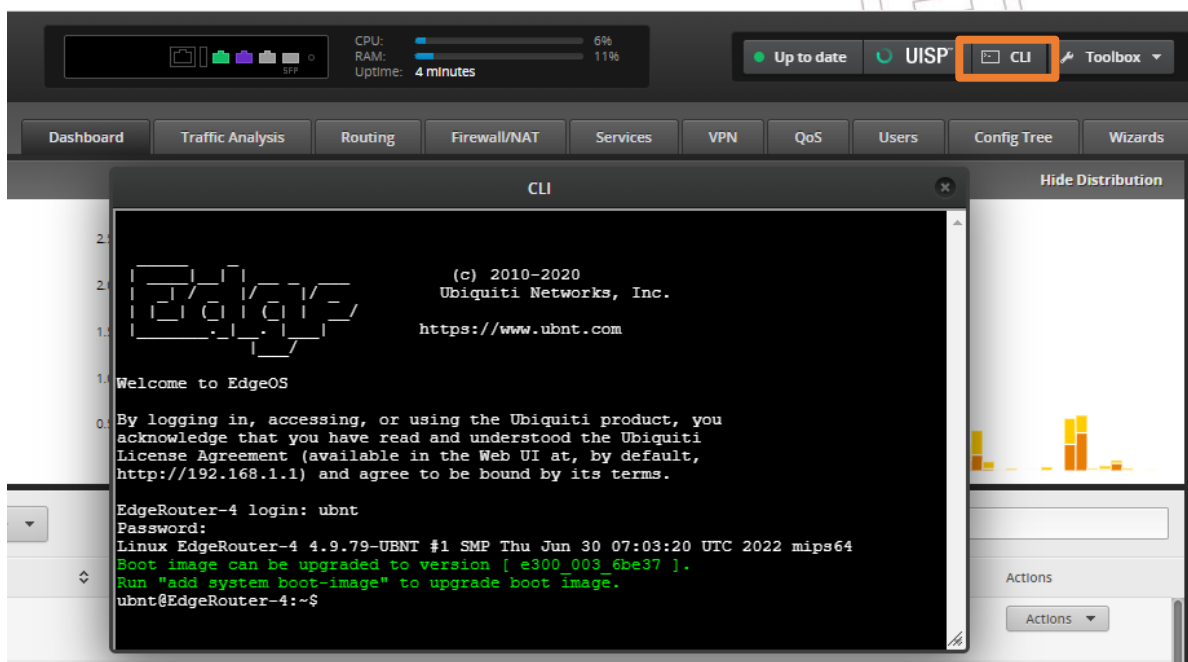
Una vez establecida la asignación de direcciones IPv6 para el laboratorio de telecomunicaciones se procede a realizar el primer punto que es el desarrollo del modelo de túnel 6to4 mediante el proceso de configuración de los equipos Ubiquiti.

3.1.7.1. CONFIGURACIÓN DE IPV6 EN EDGEROUTER

El primer equipo para configurar la red en IPv6 es el EdgeRouter, ya que mediante él se establecerá el túnel 6to4 y las respectivas direcciones IPv6 para la red, para la configuración se utilizó líneas de comandos a través del CLI del router, esta herramienta se encuentra en la interfaz principal, la figura 65 muestra la pantalla del CLI en el que para realizar las configuraciones se debe ingresar el usuario y la contraseña del router (ubnt para ambos).

Figura 65

Interfaz de línea de comandos del EdgeRouter



Elaborado por el autor



UPSE

El primer paso es realizar la configuración del túnel 6to4 en el que se deberá considerar los datos de la tabla 17, la IP 192.88.99.1 es una dirección anycast que funciona como una puerta de enlace entre IPv4 e Iv6.

Tabla 17

Consideraciones para configurar 6to4

Descripción	Dirección
Remote any local/dirección pública	190.15.130.24
Dirección IPv6	2002:be0f:8218::1/48
6to4 relay router	192.88.99.1

Elaborado por el autor

La figura 66 muestra los comandos necesarios para configurar el túnel, para ello se debe ingresar al modo de configuración del router e introducir el comando configure, seguidamente se crea la interfaz del túnel al que se le llamará tun0, la segunda línea de comando sirve para configurar un túnel estático IPv6 en IPv4 usando la interfaz tun0, aquí se coloca la IPv4 pública de la red para indicar la dirección de entrada del túnel.

En la tercera línea de comandos se debe especificar el valor de MTU debido a que se está utilizando direccionamiento IPv6 éste emplea el valor de 1280 para fragmentar los paquetes, luego se debe agregar la dirección IPv6 al túnel, se utilizó la dirección IPv4 pública mapeada, en la quinta línea se agrega la ruta por defecto para IPv6 ::/0 junto con la puerta de enlace del túnel.

UPSE

Figura 66

Configuración del túnel

```
ubnt@EdgeRouter-4:~$ configure
[edit]
ubnt@EdgeRouter-4# ip tunnel add tun0 mode sit remote any local 190.15.130.24
[edit]
ubnt@EdgeRouter-4# ip link set dev tun0 mtu 1280 up
[edit]
ubnt@EdgeRouter-4# ip -6 addr add 2002:be0f:8218::1/48 dev tun0
[edit]
ubnt@EdgeRouter-4# ip -6 route add ::/0 via ::192.88.99.1 dev tun0
[edit]
```

Elaborado por el autor

Para verificar que el túnel se ha creado se inserta el comando `show interfaces` este comando muestra el estado y las configuraciones de las interfaces del router, como se puede observar en la figura 67 el túnel se ha configurado correctamente con su respectiva dirección IPv6 y la dirección de puerta de enlace del túnel.

Figura 67

Interfaces del router configuradas

```
ubnt@EdgeRouter-4# exit
exit
ubnt@EdgeRouter-4:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface      IP Address          S/L  Description
-----
br0            192.168.1.1/24      u/u   Local Bridge
eth0           192.168.23.9/24     u/u   Internet
eth1           -                   u/u   Local Bridge
eth2           -                   u/D   Local Bridge
eth3           -                   u/D
lo             127.0.0.1/8        u/u
tun0           ::1/128
               2002:be0f:8218::1/48 u/u
               ::190.15.130.24/96
```

Elaborado por el autor

Como anteriormente se configuró un puente con IPv4 entre dos interfaces de la misma manera se debe agregar una dirección en IPv6, para ello se utiliza las líneas de comandos que se muestran en

96

UPSE

la figura 68, la primera línea indica la dirección IPv6 a agregar para la red LAN, el comando aging 300 indica el tiempo límite en que la dirección MAC permanece en la tabla de direcciones y el valor de 300 es el predeterminado el cual es medido en segundos.

Figura 68

Configuración de IPv6 en bridge

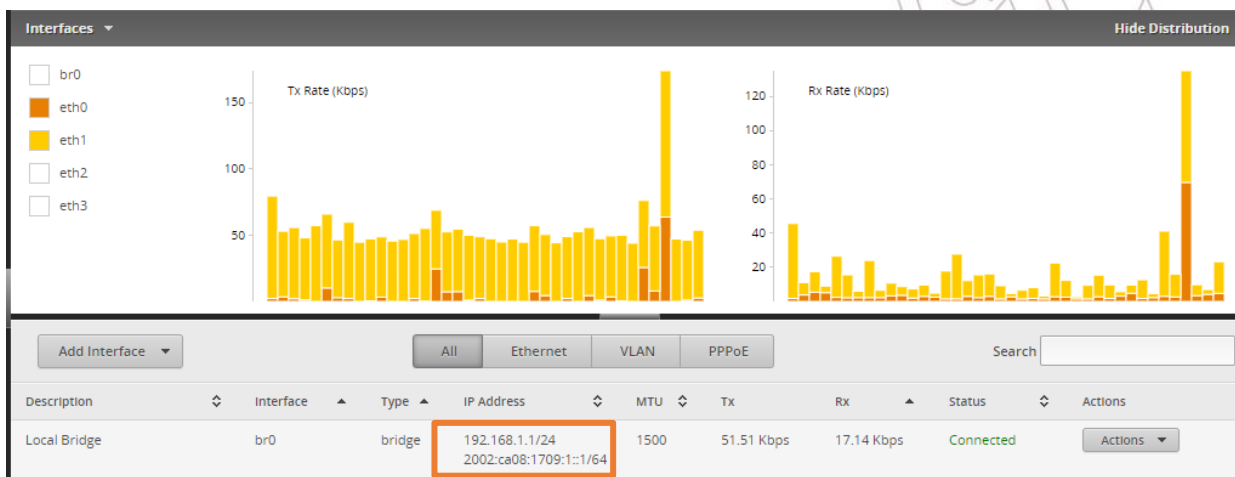
```
ubnt@EdgeRouter-4# set interfaces bridge br0 address '2002:ca08:1709:1::1/64'  
[edit]  
ubnt@EdgeRouter-4# set interfaces bridge br0 aging 300  
[edit]
```

Elaborado por el autor

Al guardar los cambios para la dirección del puente br0 se podrá visualizar ambas direcciones de IPv4 e IPv6 en la interfaz principal del EdgeRouter, lo cual indica que es posible la coexistencia para este equipo.

Figura 69

Bridge en IPv4 e IPv6



Elaborado por el autor

En la configuración del bridge se debe especificar la forma en que un dispositivo final adquiere una dirección por DHCPv6, en el comando de la figura 70 aquello se establece mediante dhcpv6-

UPSE

options, en el que parameters-only indica la adquisición de solo parámetros configurados por parte del servidor DHCPv6.

Figura 70

Configuración DHCPv6

```
[edit]  
ubnt@EdgeRouter-4# set interfaces bridge br0 dhcpv6-options parameters-only  
[edit]
```

Elaborado por el autor

Mediante las líneas de comando que se muestran en la figura 71 se configura el anuncio de enrutador (Router-Advert) el cual se utiliza para proporcionar información a los hosts acerca del prefijo de subred, el RA es derivado de las rutas de las tablas de enrutamiento y contiene la opción de MTU, como se está utilizando un anuncio de enrutador IPv6 el valor de MTU es 1280 (comando router-advert link-mtu 1280), además se deberá especificar la preferencia alta (high) para los mensajes de RA (comando router-advert default-preference high) y el límite de saltos de los paquetes salientes del router (comando cur-hop-limit).

Antes de anunciar la dirección IPv6 también es importante indicar a los dispositivos finales que recibirán una dirección con estado de forma automática (comando router-advert managed-flag), luego autorizar que los dispositivos adjuntos puedan recibir otra información utilizando configuración automática (comando router-advert other-config-flag), cuando se anuncia el prefijo con la dirección '2002:c0a8:1709:1::/64' se debe activar la autoconfiguración de direcciones (autonomous-flag true), habilitar el prefijo anunciado como enlace (on-link-flag true) e indicar el tiempo de vida del prefijo anunciado (valid-lifetime).

En este caso se configuró un valor predeterminado de 0 segundos para que un host IPv6 se considere accesible (comando reachable-time 0), así mismo para la retransmisión de mensajes del

router advert (retrans-timer 0), por último, es necesario habilitar los anuncios mediante el comando

send-advert true.

Figura 71

Configuración de anuncios de enrutador

```
ubnt@EdgeRouter-4# set interfaces bridge br0 ipv6 router-advert cur-hop-limit 64
[edit]
ubnt@EdgeRouter-4# set interfaces bridge br0 ipv6 router-advert default-preferen
ce high
[edit]
ubnt@EdgeRouter-4# set interfaces bridge br0 ipv6 router-advert link-mtu 1280
[edit]
ubnt@EdgeRouter-4# set interfaces bridge br0 ipv6 router-advert managed-flag fal
se
[edit]
ubnt@EdgeRouter-4# set interfaces bridge br0 ipv6 router-advert max-interval 600
[edit]
ubnt@EdgeRouter-4# set interfaces bridge br0 ipv6 router-advert other-config-fla
g true
[edit]
ubnt@EdgeRouter-4# set interfaces bridge br0 ipv6 router-advert prefix '2002:c0a
8:1709:1::/64' autonomous-flag true
[edit]
ubnt@EdgeRouter-4# set interfaces bridge br0 ipv6 router-advert prefix '2002:c0a
8:1709:1::/64' on-link-flag true
[edit]
ubnt@EdgeRouter-4# set interfaces bridge br0 ipv6 router-advert prefix '2002:c0a
8:1709:1::/64' valid-lifetime 2592000
[edit]
ubnt@EdgeRouter-4# set interfaces bridge br0 ipv6 router-advert reachable-time 0
[edit]
ubnt@EdgeRouter-4# set interfaces bridge br0 ipv6 router-advert retrans-timer 0
[edit]
ubnt@EdgeRouter-4# set interfaces bridge br0 ipv6 router-advert send-advert true
[edit]
```

Elaborado por el autor

Para comprobar que la configuración se ha realizado de manera exitosa se procede a mostrar la tabla de rutas para IPv6 mediante el comando show ipv6 route, como se puede observar en la figura

72 se tiene la ruta estática de IPv6, la dirección del túnel, la dirección del puente para la red LAN y la ruta por defecto del túnel.

Figura 72

Tabla de rutas IPv6

```
ubnt@EdgeRouter-4:~$ show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
IA - OSPF inter area, E1 - OSPF external type 1,
E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
S ::/0 [1/0] via ::, tun0, 00:01:50
C ::1/128 via ::, lo, 30w3d23h
C 2002:be0f:8218::/48 via ::, tun0, 00:01:50
C 2002:ca08:1709:1::/64 via ::, br0, 00:19:09
C fe80::/64 via ::, tun0, 00:01:50
```

Elaborado por el autor

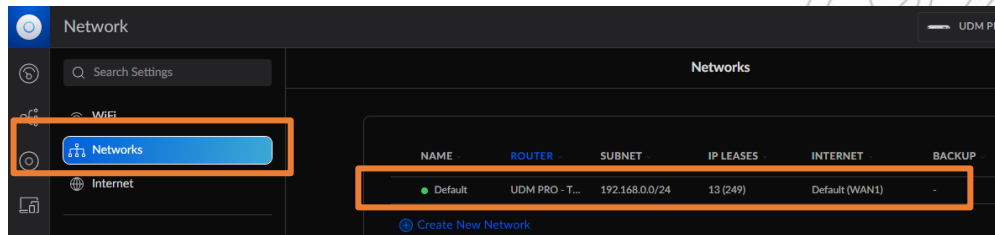
3.1.7.2. CONFIGURACIÓN DE IPV6 EN UDM PRO

En esta sección se desarrolla el punto dos que consiste en la configuración de la red interna para que los equipos admitan direccionamiento IPv4 e IPv6, este proceso se lleva a cabo en el UDM Pro y se realiza mediante su interfaz gráfica.

Primero se selecciona Networks del menú izquierdo, en el lado derecho aparecerá la red LAN en IPv4 que se creó anteriormente procedemos a seleccionar la red.

Figura 73

Ingreso a la configuración de la red

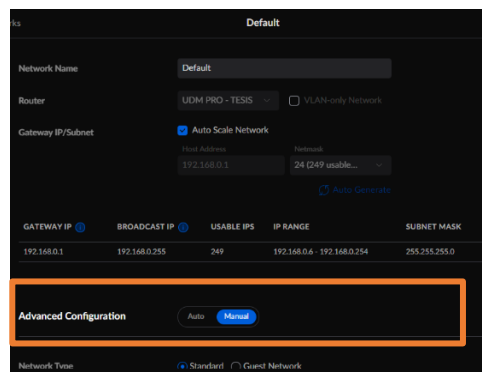


Elaborado por el autor

Al ingresar a la red se observa a detalle las características de la red en IPv4 y la configuración avanzada de forma automática, para habilitar el direccionamiento IPv6 se deberá cambiar la configuración avanzada a manual como se muestra a continuación.

Figura 74

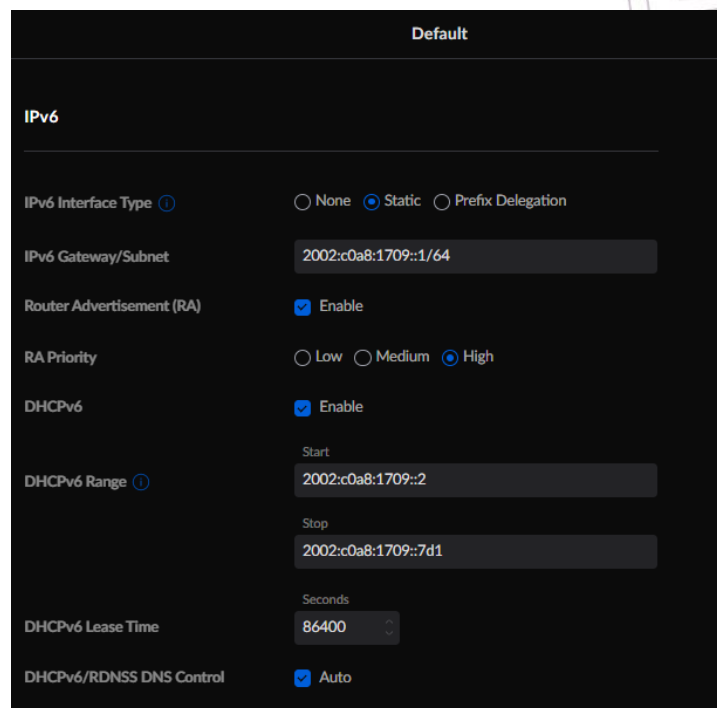
Configuración avanzada de la red LAN



Una vez cambiada la configuración deslizamos hacia abajo hasta encontrar un apartado denominado IPv6, aquí se debe especificar algunos parámetros los cuales harán la posible comunicación entre hosts para poder ingresar la dirección IPv6 calculada anteriormente es necesario colocar el tipo de interfaz de forma estático, a continuación ingresamos la puerta de enlace IPv6 2002:c0a8:1709::1/64, habilitamos el anuncio de enrutador para esta dirección con prioridad alta (high), además debemos habilitar el DHCPv6 y especificar el rango de direcciones aunque el UDM también lo coloca automáticamente, el tiempo de arriendo del DHCP se lo deja por defecto y por último se habilita el automático del control DNS, lo mencionado anteriormente se muestra en la siguiente figura.

Figura 75

Configuración de IPv6 en UDM Pro



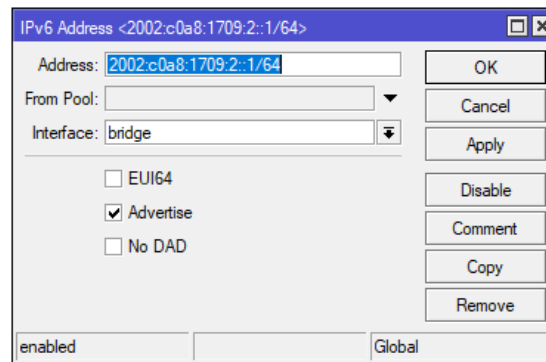
Elaborado por el autor

3.1.7.3. CONFIGURACIÓN DE IPV6 EN RB MIKROTIK

En el menú de la interfaz gráfica del Winbox existe una opción denominada IPv6, al seleccionarlo encontramos la opción llamada addresses seleccionamos y se abre una ventana en la que podemos añadir nuestra propia dirección, nos dirigimos a agregar y colocamos la dirección de la segunda subred de la tabla 16 a la interfaz de bridge, activamos la casilla de Advertise para anunciar a los dispositivos finales una dirección automática a través del protocolo ICMPv6.

Figura 76

Configuración IPv6 en RB Mikrotik

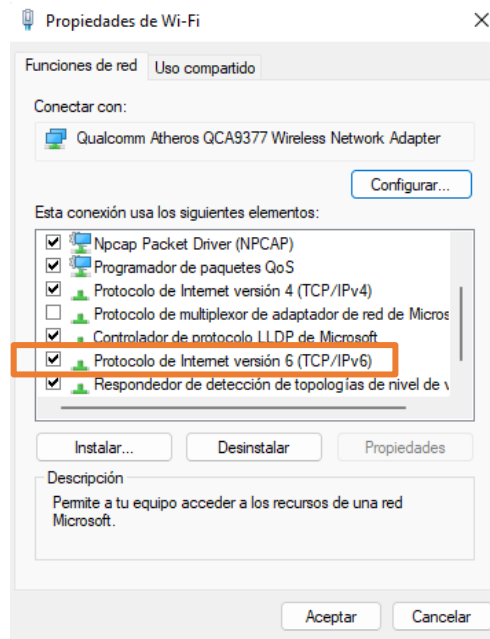


Elaborado por el autor

3.1.7.4. CONFIGURACIÓN DE DISPOSITIVOS FINALES

Como se mostró en la tabla 13 los hosts a utilizar tienen sistema operativo de Windows en sus versiones 10 y 11 los cuales incluyen soporte para IPv6 y funcionalidad en Dual Stack, es decir que permite la activación de los dos protocolos al mismo tiempo haciendo posible la coexistencia. Antes de realizar la configuración de IPv6 debemos verificar que el protocolo IPv6 esté habilitado, para ello nos dirigimos a las conexiones de red, seleccionamos red local o inalámbrica dependiendo de la conexión, luego en propiedades como se puede observar en la figura 77 el protocolo IPv6 está habilitado.

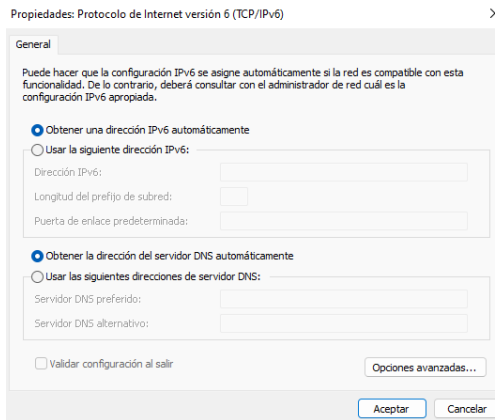
Habilitar protocolo IPv6 en PC



Elaborado por el autor

Al seleccionar Protocolo de Internet versión 6 se abre una ventana con ciertas propiedades para la configuración del protocolo, teniendo la opción de obtener una dirección IPv6 y un servidor DNS de forma automática (DHCPv6) o en otro caso ingresar manualmente las direcciones que se requiere, para este proyecto se utilizará la asignación de direcciones IPv6 de forma automática ya que la red está configurada de esta manera.

Asignación de dirección IPv6

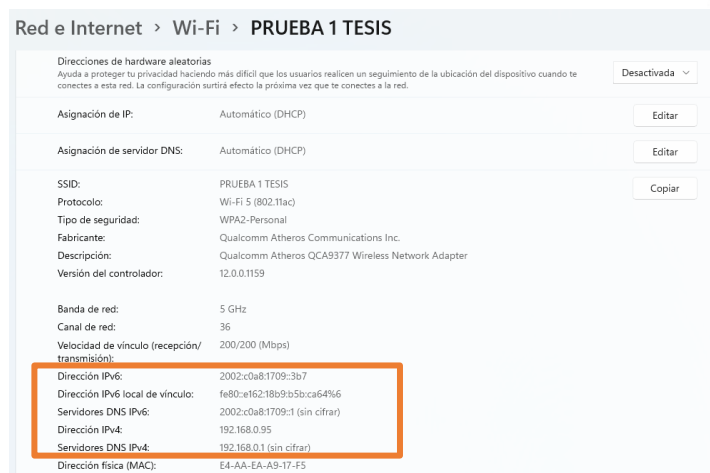


Elaborado por el autor

Para verificar que la PC haya obtenido el direccionamiento IPv6 por DHCP se puede realizar de dos formas, seleccionando las propiedades de la red a la que estamos conectados o por el símbolo del sistema insertando el comando ipconfig, lo mencionado se muestra en las figuras 79 y 80 respectivamente.

Figura 79

Detalles de la red en IPv4 e IPv6



Elaborado por el autor

Detalles de la red mediante símbolo del sistema

```
Adaptador de LAN inalámbrica Wi-Fi:

Sufijo DNS específico para la conexión. . . : localdomain
Dirección IPv6 . . . . . : 2002:c0a8:1709::3b7
Vínculo: dirección IPv6 local. . . : fe80::e162:18b9:b5b:ca64%6
Dirección IPv4. . . . . : 192.168.0.95
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : fe80::74ac:b9ff:fe3b:58bc%6
                                           192.168.0.1
```

Elaborado por el autor

3.1.8. ESTUDIO DE FACTIBILIDAD

El estudio de factibilidad de esta propuesta tecnológica permite demostrar la viabilidad para su implementación además de conocer el equipamiento y herramientas necesarias para armar una red con fibra óptica.

En el laboratorio de telecomunicaciones se implementó una red con equipos de la marca Ubiquiti en el que se dio a conocer el proceso de instalación considerando un orden correcto de los equipos y su conectividad para su funcionamiento mediante el cual se aplicaron algunos estándares que permitieron establecer una comunicación óptima en los dispositivos.

La implementación de nuevos equipos requirió de un estudio previo de los mismos ya que al implementar mecanismos de coexistencia todos los equipos deben soportar direccionamiento IPv6.

3.1.8.1. COSTO DE LA PROPUESTA

Para la propuesta tecnológica se utilizaron los equipos que se muestran en la tabla 18 se especifica el valor unitario por equipo.



UPSE
Tabla 18

Costo de equipos

Cant.	Descripción	Marca	Valor Unitario	Valor Total
1	EdgeRouter 4	Ubiquiti	\$130	\$130
1	Dream Machine Pro	Ubiquiti	\$360	\$360
1	Fiber Media Converter	-----	\$20	\$20
1	Acces Point WiFi 6 Lite	Ubiquiti	\$100	\$100
2	Módulo SFP 1G	Ubiquiti	\$19	\$38
1	Patchord dúplex LC/UPC	-----	\$3	\$3
1	RB2011UiAS	Mikrotik	\$150	\$150
			TOTAL	\$801

Elaborado por el autor

CAPÍTULO IV

4.1. PRUEBAS DE FUNCIONALIDAD

Mediante las pruebas de funcionalidad del direccionamiento IPv6 se podrá determinar que los dispositivos finales de la red interna del laboratorio admitan el nuevo protocolo de red y comprobar que por medio de los mecanismos de coexistencia se puede tener una red en funcionamiento con ambos protocolos y mantener una comunicación continua.

Las pruebas se realizarán entre máquinas mediante el símbolo del sistema haciendo uso del comando ping, en primer lugar, se ejecutarán pruebas para los dispositivos que se conectan al AP de la marca Ubiquiti y posteriormente a los que se conectan al AP Mikrotik con la finalidad de establecer diferencias del manejo de los dos protocolos de direccionamiento en las marcas mencionadas.

4.1.1. FUNCIONALIDAD IPV4 E IPV6 DEL AP UBIQUITI

Para realizar las pruebas es necesario conocer las direcciones de los hosts asignados por DHCP y DHCPv6 mediante el AP Ubiquiti, para ello nos dirigimos al símbolo del sistema e insertamos el comando ipconfig al presionar enter se despliega una lista de los adaptadores e interfaces de red del host como el dispositivo se conecta de forma inalámbrica deslizamos hasta encontrar Adaptador de LAN inalámbrica Wi-Fi aquí obtendremos las direcciones en IPv4 e IPv6 de los hosts.

Se tomará un primer dispositivo al cual le asignaremos el nombre de Host 1 el cual tiene las direcciones mostradas en la siguiente figura.

Direcciones IPv4 e IPv6 del Host 1 de la red Ubiquiti

```
Adaptador de LAN inalámbrica Wi-Fi:

Sufijo DNS específico para la conexión. . . : localdomain
Dirección IPv6 . . . . . : 2002:c0a8:1709::3b7
Vínculo: dirección IPv6 local. . . : fe80::e162:18b9:b5b:ca64%6
Dirección IPv4. . . . . : 192.168.0.95
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : fe80::74ac:b9ff:fe3b:58bc%6
                                           192.168.0.1
```

Elaborado por el autor

El segundo dispositivo se lo denominará Host 2 y tendrá las direcciones que se muestran en la siguiente figura 82.

Figura 82

Direcciones IPv4 e IPv6 del Host 2 de la red Ubiquiti

```
Adaptador de LAN inalámbrica Wi-Fi:

Sufijo DNS específico para la conexión. . . : localdomain
Dirección IPv6 . . . . . : 2002:c0a8:1709::61f
Vínculo: dirección IPv6 local. . . : fe80::511e:b50e:ef77:84a%15
Dirección IPv4. . . . . : 192.168.0.15
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : fe80::74ac:b9ff:fe3b:58bc%15
                                           192.168.0.1
```

Elaborado por el autor

Una vez conocida las direcciones de los dos dispositivos se debe verificar que ambos puedan comunicarse, la forma de comprobarlo es realizando un ping del host 1 al host 2 utilizando Dirección IPv4 y luego Dirección IPv6, para ello se realizarán tres pruebas enviando cuatro paquetes con tamaño de 32, 512 y 8000 bytes en la red Ubiquiti. A continuación, se muestran las tres pruebas realizadas con la red de Ubiquiti.



UPSE

Figura 83

Prueba 1 de red Ubiquiti

```
C:\Users\ >ping 192.168.0.15

Haciendo ping a 192.168.0.15 con 32 bytes de datos:
Respuesta desde 192.168.0.15: bytes=32 tiempo=6ms TTL=128
Respuesta desde 192.168.0.15: bytes=32 tiempo=4ms TTL=128
Respuesta desde 192.168.0.15: bytes=32 tiempo=4ms TTL=128
Respuesta desde 192.168.0.15: bytes=32 tiempo=4ms TTL=128

Estadísticas de ping para 192.168.0.15:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 4ms, Máximo = 6ms, Media = 4ms

C:\Users\ >ping -6 2002:c0a8:1709::61f

Haciendo ping a 2002:c0a8:1709::61f con 32 bytes de datos:
Respuesta desde 2002:c0a8:1709::61f: tiempo=4ms
Respuesta desde 2002:c0a8:1709::61f: tiempo=4ms
Respuesta desde 2002:c0a8:1709::61f: tiempo=4ms
Respuesta desde 2002:c0a8:1709::61f: tiempo=4ms

Estadísticas de ping para 2002:c0a8:1709::61f:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 4ms, Máximo = 4ms, Media = 4ms
```

Elaborado por el autor

Figura 84

Prueba 2 de red Ubiquiti

```
C:\Users\ >ping 192.168.0.15 -l 512

Haciendo ping a 192.168.0.15 con 512 bytes de datos:
Respuesta desde 192.168.0.15: bytes=512 tiempo=5ms TTL=128
Respuesta desde 192.168.0.15: bytes=512 tiempo=4ms TTL=128
Respuesta desde 192.168.0.15: bytes=512 tiempo=4ms TTL=128
Respuesta desde 192.168.0.15: bytes=512 tiempo=4ms TTL=128

Estadísticas de ping para 192.168.0.15:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 4ms, Máximo = 5ms, Media = 4ms

C:\Users\Gloria Villon>ping -6 2002:c0a8:1709::61f -l 512

Haciendo ping a 2002:c0a8:1709::61f con 512 bytes de datos:
Respuesta desde 2002:c0a8:1709::61f: tiempo=4ms
Respuesta desde 2002:c0a8:1709::61f: tiempo=4ms
Respuesta desde 2002:c0a8:1709::61f: tiempo=4ms
Respuesta desde 2002:c0a8:1709::61f: tiempo=4ms

Estadísticas de ping para 2002:c0a8:1709::61f:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 4ms, Máximo = 4ms, Media = 4ms
```

Elaborado por el autor



UPSE

Figura 85

Prueba 3 de red Ubiquiti

```
C:\Users\ >ping 192.168.0.15 -l 8000

Haciendo ping a 192.168.0.15 con 8000 bytes de datos:
Respuesta desde 192.168.0.15: bytes=8000 tiempo=7ms TTL=128
Respuesta desde 192.168.0.15: bytes=8000 tiempo=6ms TTL=128
Respuesta desde 192.168.0.15: bytes=8000 tiempo=6ms TTL=128
Respuesta desde 192.168.0.15: bytes=8000 tiempo=13ms TTL=128

Estadísticas de ping para 192.168.0.15:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 6ms, Máximo = 13ms, Media = 8ms

C:\Users\ >ping -6 2002:c0a8:1709::61f -l 8000

Haciendo ping a 2002:c0a8:1709::61f con 8000 bytes de datos:
Respuesta desde 2002:c0a8:1709::61f: tiempo=6ms
Respuesta desde 2002:c0a8:1709::61f: tiempo=7ms
Respuesta desde 2002:c0a8:1709::61f: tiempo=8ms
Respuesta desde 2002:c0a8:1709::61f: tiempo=7ms

Estadísticas de ping para 2002:c0a8:1709::61f:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 6ms, Máximo = 8ms, Media = 7ms
```

Elaborado por el autor

4.1.2. FUNCIONALIDAD IPV4 E IPV6 DEL AP MIKROTIK

Se realiza el mismo procedimiento para el AP Mikrotik, conectamos los hosts de forma inalámbrica a la red tesis2022, una vez establecida la conexión se deberá abrir el símbolo del sistema e insertar ipconfig para conocer las direcciones IPv4 e IPv6 de los hosts.

Las direcciones del host 1 se muestran en la figura 86 mediante el Adaptador de LAN inalámbrica Wi-Fi, de las cuales se considerará Dirección IPv4 y Dirección IPv6.

UPSE
Figura 86

Direcciones IPv4 e IPv6 del Host 1 de la red Mikrotik

```
Adaptador de LAN inalámbrica Wi-Fi:

Sufijo DNS específico para la conexión. . . :
Dirección IPv6 . . . . . : 2002:c0a8:1709:2:511e:b50e:ef77:84a
Dirección IPv6 temporal. . . . . : 2002:c0a8:1709:2:c:258:d58a:1135
Vínculo: dirección IPv6 local. . . : fe80::511e:b50e:ef77:84a%15
Dirección IPv4. . . . . : 192.168.2.252
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : fe80::ba69:f4ff:feb3:3d41%15
192.168.2.1
```

Las direcciones del host 2 se muestran en la figura 87 mediante el Adaptador de LAN inalámbrica Wi-Fi, de las cuales se considerará Dirección IPv4 y Dirección IPv6.

Figura 87

Direcciones IPv4 e IPv6 del Host 2 de la red Mikrotik

```
Adaptador de LAN inalámbrica Wi-Fi:

Sufijo DNS específico para la conexión. . . :
Dirección IPv6 . . . . . : 2002:c0a8:1709:2:e162:18b9:b5b:ca64
Dirección IPv6 temporal. . . . . : 2002:c0a8:1709:2:f06e:cd05:1e3d:b859
Vínculo: dirección IPv6 local. . . : fe80::e162:18b9:b5b:ca64%6
Dirección IPv4. . . . . : 192.168.2.253
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : fe80::ba69:f4ff:feb3:3d41%6
192.168.2.1
```

La comprobación de la comunicación de los dispositivos por medio de la red es realizada mediante ping del host 1 al host 2 tanto en IPv4 como en IPv6, para ello se envían cuatro paquetes con tamaño de 32, 512 y 8000 bytes; las figuras 88, 89 y 90 muestran que los cuatro paquetes transmitidos desde el host 1 al host 2 para ambas direcciones son recibidos completamente y sin tener pérdida de paquetes.

A continuación, se muestran las tres pruebas realizadas con la red de Ubiquiti.

Prueba 1 de red Mikrotik

```
C:\Users\ >ping 192.168.2.252
Haciendo ping a 192.168.2.252 con 32 bytes de datos:
Respuesta desde 192.168.2.252: bytes=32 tiempo=7ms TTL=128
Respuesta desde 192.168.2.252: bytes=32 tiempo=5ms TTL=128
Respuesta desde 192.168.2.252: bytes=32 tiempo=4ms TTL=128
Respuesta desde 192.168.2.252: bytes=32 tiempo=4ms TTL=128

Estadísticas de ping para 192.168.2.252:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 4ms, Máximo = 7ms, Media = 5ms

C:\Users\Gloria Villon>ping -6 2002:c0a8:1709:2:511e:b50e:ef77:84a
Haciendo ping a 2002:c0a8:1709:2:511e:b50e:ef77:84a con 32 bytes de datos:
Respuesta desde 2002:c0a8:1709:2:511e:b50e:ef77:84a: tiempo=4ms
Respuesta desde 2002:c0a8:1709:2:511e:b50e:ef77:84a: tiempo=4ms
Respuesta desde 2002:c0a8:1709:2:511e:b50e:ef77:84a: tiempo=5ms
Respuesta desde 2002:c0a8:1709:2:511e:b50e:ef77:84a: tiempo=4ms

Estadísticas de ping para 2002:c0a8:1709:2:511e:b50e:ef77:84a:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 4ms, Máximo = 5ms, Media = 4ms
```

Figura 89

Prueba 2 de red Mikrotik

```
C:\Users\ >ping 192.168.2.252 -l 512
Haciendo ping a 192.168.2.252 con 512 bytes de datos:
Respuesta desde 192.168.2.252: bytes=512 tiempo=7ms TTL=128
Respuesta desde 192.168.2.252: bytes=512 tiempo=12ms TTL=128
Respuesta desde 192.168.2.252: bytes=512 tiempo=7ms TTL=128
Respuesta desde 192.168.2.252: bytes=512 tiempo=8ms TTL=128

Estadísticas de ping para 192.168.2.252:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 7ms, Máximo = 12ms, Media = 8ms

C:\Users\Gloria Villon>ping -6 2002:c0a8:1709:2:511e:b50e:ef77:84a -l 512
Haciendo ping a 2002:c0a8:1709:2:511e:b50e:ef77:84a con 512 bytes de datos:
Respuesta desde 2002:c0a8:1709:2:511e:b50e:ef77:84a: tiempo=5ms
Respuesta desde 2002:c0a8:1709:2:511e:b50e:ef77:84a: tiempo=8ms
Respuesta desde 2002:c0a8:1709:2:511e:b50e:ef77:84a: tiempo=4ms
Respuesta desde 2002:c0a8:1709:2:511e:b50e:ef77:84a: tiempo=12ms

Estadísticas de ping para 2002:c0a8:1709:2:511e:b50e:ef77:84a:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 4ms, Máximo = 12ms, Media = 7ms
```

Elaborado por el autor

Prueba 3 de red Mikrotik

```
C:\Users\ >ping 192.168.2.252 -l 8000
Haciendo ping a 192.168.2.252 con 8000 bytes de datos:
Respuesta desde 192.168.2.252: bytes=8000 tiempo=13ms TTL=128
Respuesta desde 192.168.2.252: bytes=8000 tiempo=7ms TTL=128
Respuesta desde 192.168.2.252: bytes=8000 tiempo=7ms TTL=128
Respuesta desde 192.168.2.252: bytes=8000 tiempo=7ms TTL=128

Estadísticas de ping para 192.168.2.252:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
  (0% perdidos),
  Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 7ms, Máximo = 13ms, Media = 8ms

C:\Users\Gloria Villon>ping -6 2002:c0a8:1709:2:511e:b50e:ef77:84a -l 8000
Haciendo ping a 2002:c0a8:1709:2:511e:b50e:ef77:84a con 8000 bytes de datos:
Respuesta desde 2002:c0a8:1709:2:511e:b50e:ef77:84a: tiempo=7ms
Respuesta desde 2002:c0a8:1709:2:511e:b50e:ef77:84a: tiempo=9ms
Respuesta desde 2002:c0a8:1709:2:511e:b50e:ef77:84a: tiempo=12ms
Respuesta desde 2002:c0a8:1709:2:511e:b50e:ef77:84a: tiempo=8ms

Estadísticas de ping para 2002:c0a8:1709:2:511e:b50e:ef77:84a:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
  (0% perdidos),
  Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 7ms, Máximo = 12ms, Media = 9ms
```

Elaborado por el autor

4.2. ANÁLISIS DE RESULTADOS

En esta sección se analizan los resultados obtenidos de la sección 4.1 de las tres pruebas realizadas para cada red, además se realiza una captura de paquetes mediante el software de Wireshark consiguiendo diferentes parámetros para su respectivo análisis.

4.2.1. ANÁLISIS DE LATENCIA Y PÉRDIDA DE PAQUETES DE LA RED UBIQUITI

Mediante este análisis se podrá determinar el tiempo en el que los paquetes se transmiten a través de la red hacia un destino y si durante la transmisión existen o no pérdidas de paquetes, las pruebas se realizaron empleando el comando ping en cmd con tres tamaños de paquetes diferentes, cabe mencionar que la herramienta ping permite enviar paquetes con tamaño aproximado de 65.527 bytes, esto se realiza con la finalidad de verificar la pérdida de paquetes en IPv4 e IPv6.

En las tablas 19 y 20 se muestran los datos obtenidos de las figuras 83, 84 y 85 de las tres pruebas mencionadas acerca del envío de paquetes del host 1 al host 2.



UPSE
Tabla 19

Latencia con protocolo IPv4

Tamaño del paquete	Latencia (ms)		Paquetes	
	Bytes	Mínimo	Máximo	Paquetes enviados
32	4	6	4	0
512	4	5	4	0
8000	6	13	4	0

Elaborado por el autor

Al realizar la primera prueba con un tamaño de 32 bytes se tiene una latencia que no sobrepasa los 20ms, por lo que no existen problemas durante la transmisión de paquetes, la latencia mínima obtenida es de 4ms, mientras que la máxima es de 6ms obteniendo 0 pérdidas de paquetes.

La segunda prueba se realizó con un tamaño de 512 bytes en el que se obtuvo valores de latencia mínima de 4 ms y máxima de 5ms con 0% de pérdidas de paquetes, esto indica que el protocolo IPv4 sigue siendo óptimo para este tamaño de paquetes.

En la tercera prueba con tamaño de paquetes de 8000 bytes se puede observar una subida de latencia máxima considerable de 13ms, esto se debe a que el protocolo IPv4 maneja un número limitado de bytes por lo que si se enviaban paquetes con tamaño superior a 8000 existirían latencias altas o pérdidas de paquetes.



UPSE
Tabla 20

Latencia con protocolo IPv6

Tamaño del paquete	Latencia (ms)		Paquetes	
	Bytes	Mínimo	Máximo	Paquetes enviados
32	4	4	4	0
512	4	4	4	0
8000	6	8	4	0

Elaborado por el autor

Para las pruebas en IPv6 se emplearon los mismos tamaños de paquetes, en el que la primera prueba realizada de 32 bytes produjo una latencia mínima y máxima de 4ms de la cual no se obtuvieron paquetes perdidos.

En la segunda prueba con tamaño de 512 bytes se obtiene una latencia igual a la primera prueba en la que tampoco existen paquetes perdidos y en comparación con IPv4 los resultados son similares.

La tercera prueba de tamaño 8000 bytes muestra una latencia mínima de 6ms y una máxima de 8ms, en este caso la latencia máxima se redujo con respecto a lo obtenido en IPv4, esto se debe a que IPv6 al ser un protocolo con más soporte de bytes permite la transferencia de paquetes con mayor tamaño.



UPSE

4.2.2. ANÁLISIS DE LATENCIA Y PÉRDIDA DE PAQUETES DE LA RED MIKROTIK

Se realizaron las mismas pruebas a la red de Mikrotik con los tres tamaños de paquetes mencionados anteriormente y utilizando el comando ping junto a las direcciones IPv4 e IPv6 de dos dispositivos que se encuentren conectados a la red, pues de esta manera se podrá obtener una comparativa entre los protocolos y una comparativa de como manejan los protocolos la red Ubiquiti.

En las tablas 21 y 22 se muestran los datos obtenidos de las figuras 88, 89 y 90 de las tres pruebas mencionadas acerca del envío de paquetes del host 1 al host 2.

Tabla 21

Latencia con protocolo IPv4

Tamaño del paquete	Latencia (ms)		Paquetes	
	Mínimo	Máximo	Paquetes enviados	Paquetes perdidos
32	4	7	4	0
512	7	12	4	0
8000	7	13	4	0

Elaborado por el autor

Aplicando las mismas pruebas en la red inalámbrica de Mikrotik se pudo obtener que para la primera prueba realizada que contiene un tamaño por paquete de 32 bytes la latencia en IPv4 mínima fue de 4ms mientras que la máxima de 7ms de forma que no existieron pérdidas de paquetes.



UPSE

En la segunda prueba con tamaño de 512 bytes se obtuvo una latencia mínima de 7ms, la latencia máxima determinada es de 12ms, lo cual aún se considera óptimo para la transmisión de paquetes, en esta prueba no se registran porcentajes de paquetes perdidos.

La tercera prueba de tamaño 8000 bytes muestra una latencia similar a la segunda prueba realizada sin registro de porcentaje de paquetes perdidos.

Tabla 22

Latencia con protocolo IPv6

Tamaño del paquete	Latencia (ms)		Paquetes	
	Bytes	Mínimo	Máximo	Paquetes enviados
32	4	5	4	0
512	4	12	4	0
8000	7	12	4	0

Elaborado por el autor

Se realizaron las mismas pruebas para IPv6 con los tamaños de paquetes mencionados anteriormente.

En el paquete de 32 bytes se obtuvo mejor resultado que en IPv4 ya que la latencia mínima se redujo a 4ms y la latencia máxima se redujo a 5ms, aunque en esta prueba tampoco existieron pérdidas de paquetes.

En segunda prueba con tamaño de 512 bytes se obtuvo un resultado similar a IPv4 en el que la latencia mínima fue de 4 ms y la máxima de 12 ms sin pérdidas de paquetes.



UPSE

La tercera prueba con tamaño de 8000 paquetes muestra una latencia mínima de 7ms y la latencia mínima es igual al tamaño de prueba de 512 bytes, en comparación con la prueba de IPv4 se observa una mínima diferencia en la latencia máxima.

4.3. COMPARATIVA DE LATENCIA EN UBIQUITI Y MIKROTIK

En la tabla 23 y la figura 91 se muestra una comparativa del promedio general de latencias de IPv4 e IPv6 que se realizaron en las tres pruebas tanto en Ubiquiti como en Mikrotik, como se puede observar la red de Ubiquiti maneja una latencia con diferencias mínimas que la red de Mikrotik, en la prueba de 32 y 512 bytes para IPv4 se observa un mejor desempeño en la red Ubiquiti, mientras que en la prueba de 8000 bytes se maneja un igual promedio de latencia. Para IPv6 se muestra un igual desempeño en la prueba de 32 bytes, en la prueba de 512 bytes se obtiene mejor resultado en la red de Ubiquiti al igual que la prueba de 8000 bytes.

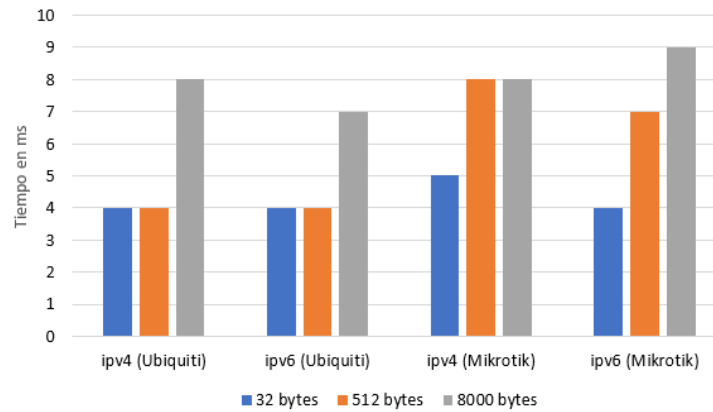
Tabla 23

Diferencias de latencia en las redes implementadas

N° de prueba	Tamaño de paquetes	Ubiquiti		Mikrotik	
		IPv4	IPv6	IPv4	IPv6
1	32 bytes	4ms	4ms	5ms	4ms
2	512 bytes	4ms	4ms	8ms	7ms
3	8000 bytes	8ms	7ms	8ms	9ms

Elaborado por el autor

Comparativa de latencia Ubiquiti y Mikrotik



Elaborado por el autor

4.4. CAPTURA Y ANÁLISIS DE PAQUETES EN WIRESHARK

En este apartado se realizan tres tipos de análisis tanto en IPv4 como en IPv6 con la finalidad de comparar y comprobar sus diferencias, el primer análisis se basa en las tramas IPv4 e IPv6, con el segundo análisis por medio de la estructura de paquetes se pretende evidenciar las diferencias de los campos de las cabeceras en ambas versiones y mediante el tercer análisis se pretende hacer uso del protocolo ICMP en versión 4 y 6 para el análisis de mensajes de solicitud y respuesta según el tipo y código definido en sus respectivos campos.

4.4.1. ANÁLISIS DE TRAMAS DE DIRECCIONAMIENTO

En este tipo de análisis se identifica el protocolo IP mediante la capa de enlace de datos y la identificación se da a conocer en las tramas a través del campo Ethertype, también se podrá identificar.

4.4.1.1. TRAMAS IPV4

En la figura 92 se muestran resaltados acerca de los datos importantes para la identificación del protocolo que se está utilizando, como se puede observar en el primer recuadro en Protocol in frame se tiene un ethertype:ip el cual hace referencia al protocolo IPv4, además en el segundo recuadro se muestra la encapsulación de IPv4 en Ethernet II en el que el valor de identificación para este tipo de direcciones es 0x0800.

Figura 92

Tramas en direccionamiento IPv4

```
▼ Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{371F027F-EFB7-432E-95C3-95AC7C6AFE15}, id 0
  > Interface id: 0 (\Device\NPF_{371F027F-EFB7-432E-95C3-95AC7C6AFE15})
  Encapsulation type: Ethernet (1)
  Arrival Time: Aug 5, 2022 12:50:31.320426000 Hora est. Pacífico, Sudamérica
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1659721831.320426000 seconds
  [Time delta from previous captured frame: 0.487718000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 3.723256000 seconds]
  Frame Number: 5
  Frame Length: 74 bytes (592 bits)
  Capture Length: 74 bytes (592 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:icmp:data]
  [Coloring Rule Name: ICMP]
  [Coloring Rule String: icmp || icmpv6]
  ▼ Ethernet II, Src: LiteonTe_a9:17:f5 (e4:aa:ea:a9:17:f5), Dst: HonHaiPr_c1:84:c3 (b0:52:16:c1:84:c3)
    > Destination: HonHaiPr_c1:84:c3 (b0:52:16:c1:84:c3)
    > Source: LiteonTe_a9:17:f5 (e4:aa:ea:a9:17:f5)
    Type: IPv4 (0x0800)
```

Elaborado por el autor

4.4.1.2. TRAMAS IPV6

La figura 93 muestra resaltados de datos importantes para la identificación del protocolo que se está utilizando, como se puede observar en el primer recuadro en Protocol in frame se tiene un ethertype:ipv6 el cual hace referencia al protocolo IPv6, además en el segundo recuadro se muestra la encapsulación de IPv6 en Ethernet II en el que el valor de identificación para este tipo de direcciones es 0x86dd.

Tramas en direccionamiento IPv6

```
▼ Frame 60: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{371F027F-EFB7-432E-95C3-95AC7C6AFE15}, id 0
  > Interface id: 0 (\Device\NPF_{371F027F-EFB7-432E-95C3-95AC7C6AFE15})
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 5, 2022 12:51:08.461753000 Hora est. Pacifico, Sudamérica
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1659721868.461753000 seconds
    [Time delta from previous captured frame: 0.269557000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 40.864583000 seconds]
    Frame Number: 60
    Frame Length: 94 bytes (752 bits)
    Capture Length: 94 bytes (752 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:icmpv6:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
  ▼ Ethernet II, Src: LiteonTe_a9:17:f5 (e4:aa:ea:a9:17:f5), Dst: HonHaiPr_c1:84:c3 (b0:52:16:c1:84:c3)
    > Destination: HonHaiPr_c1:84:c3 (b0:52:16:c1:84:c3)
    > Source: LiteonTe_a9:17:f5 (e4:aa:ea:a9:17:f5)
    Type: IPv6 (0x86dd)
```

Elaborado por el autor

4.4.2. ANÁLISIS DE ESTRUCTURA DE PAQUETES

Al capturar paquetes con direccionamiento IPv4 e IPv6 en Wireshark se puede obtener información detallada acerca de los campos que componen la estructura o el encabezado de un paquete en ambos protocolos, mediante ello es posible identificar las diferencias entre los campos.

En las figuras 94 y 95 se pueden distinguir mediante los recuadros los campos de los encabezados en el que los recuadros de color verde señalan los campos que se mantienen en ambos protocolos con la diferencia de que cada uno muestra su propia versión como por ejemplo en IPv4 se puede observar una versión de 4 con sus respectivas direcciones mientras que en IPv6 se muestra una versión de 6 con direcciones en dicha versión.

Los campos que se encuentran dentro del recuadro celeste en la figura 94 indica los campos que fueron eliminados y no aparecen en la estructura de IPv6, los recuadros de gris indican los campos que fueron modificados como la longitud del encabezado, en IPv4 es de 20 bytes mientras que en IPv6 aumenta a 40 bytes, también se puede mencionar que se ha modificado el campo de tipo de servicio en el que en IPv6 pasa a llamarse clase de tráfico, otro campo que se modificó fue el de



UPSE

tiempo de vida (time to live) en IPv4 que ahora en IPv6 pasa a llamarse límite de saltos (hop limit) y el campo de protocolo (protocol) en IPv4 fue renombrado a siguiente encabezado (next header) en IPv6.

Por otro lado, es importante mencionar que al eliminarse algunos campos en IPv4 se obtiene una simplificación en la cabecera de IPv6 haciendo óptima la velocidad de transmisión y la identificación de los paquetes.

Figura 94

Paquete IPv4

```
Internet Protocol Version 4, Src: 192.168.2.253, Dst: 192.168.2.252
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 60
  Identification: 0x42b5 (17077)
  > Flags: 0x00
  Fragment Offset: 0
  Time to Live: 128
  Protocol: ICMP (1)
  Header Checksum: 0x70c2 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.2.253
  Destination Address: 192.168.2.252
```

Elaborado por el autor

Figura 95

Paquete IPv6

```
Internet Protocol Version 6, Src: 2002:c0a8:1709:2:3103:5531:1c31:3756, Dst: 2002:c0a8:1709:2:511e:b50e:ef77:84a
  0110 .... = Version: 6
  > .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 0000 0000 0000 0000 = Flow Label: 0x000000
  Payload Length: 40
  Next Header: ICMPv6 (58)
  Hop Limit: 128
  Source Address: 2002:c0a8:1709:2:3103:5531:1c31:3756
  Destination Address: 2002:c0a8:1709:2:511e:b50e:ef77:84a
  [Source 6to4 Gateway IPv4: 192.168.23.9]
  [Source 6to4 SLA ID: 2]
  [Destination 6to4 Gateway IPv4: 192.168.23.9]
  [Destination 6to4 SLA ID: 2]
```

Elaborado por el autor

De la figura 95 el recuadro morado hace referencia al tipo de mecanismo al que se rige la dirección en la que se está trabajando, el primer hexteto más a la izquierda el cual es 2002 indica que se está utilizando las direcciones asignadas para túneles 6to4 cabe mencionar que esta dirección se obtuvo mediante la IPv4 privada 192.168.23.9.

4.4.3. ANÁLISIS DEL PROTOCOLO ICMP

La captura de paquetes para este análisis se da mediante el adaptador inalámbrico de dos hosts que se conectan a la red propuesta para este proyecto con la finalidad de poder realizar un análisis del tráfico haciendo uso del protocolo ICMP en versión 4 y 6.

4.4.3.1. ANÁLISIS DE ICMPV4

Para obtener la captura de los datos se realizó un ping desde una máquina a otra ejecutando al mismo tiempo el programa de Wireshark y haciendo uso de la dirección IPv4 en el que se transmitieron cuatro paquetes obteniendo así los paquetes solicitados (request) y la respuesta de los mismos (reply) como se observa en la siguiente figura en la columna de info.

Figura 96

Captura del protocolo ICMP para IPv4

No.	Time	Source	Destination	Protocol	Length	Info
5	3.723256	192.168.2.253	192.168.2.252	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 6)
6	3.728964	192.168.2.252	192.168.2.253	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=128 (request in 5)
8	4.728185	192.168.2.253	192.168.2.252	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in 9)
9	4.734097	192.168.2.252	192.168.2.253	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=128 (request in 8)
11	5.743485	192.168.2.253	192.168.2.252	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 12)
12	5.764382	192.168.2.252	192.168.2.253	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=128 (request in 11)
15	6.759160	192.168.2.253	192.168.2.252	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=128 (reply in 16)
16	6.769722	192.168.2.252	192.168.2.253	ICMP	74	Echo (ping) reply id=0x0001, seq=16/4096, ttl=128 (request in 15)

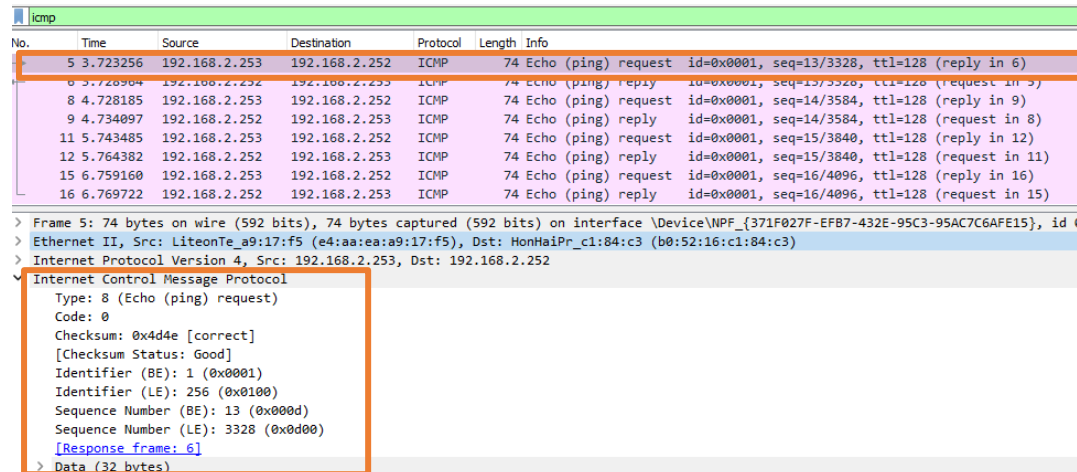
Elaborado por el autor

Al seleccionar el primer paquete de solicitud en la parte inferior aparecerá toda la información acerca de la solicitud realizada como se muestra en la figura 97, como el protocolo a analizar es

ICMP seleccionamos en Internet Control Message Protocol y a continuación de despliega un listado con campos importantes para este protocolo.

Figura 97

Solicitud de eco en IPv4



No.	Time	Source	Destination	Protocol	Length	Info
5	3.723256	192.168.2.253	192.168.2.252	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 6)
6	3.728904	192.168.2.252	192.168.2.253	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=128 (request in 5)
8	4.728185	192.168.2.253	192.168.2.252	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in 9)
9	4.734097	192.168.2.252	192.168.2.253	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=128 (request in 8)
11	5.743485	192.168.2.253	192.168.2.252	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 12)
12	5.764382	192.168.2.252	192.168.2.253	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=128 (request in 11)
15	6.759160	192.168.2.253	192.168.2.252	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=128 (reply in 16)
16	6.769722	192.168.2.252	192.168.2.253	ICMP	74	Echo (ping) reply id=0x0001, seq=16/4096, ttl=128 (request in 15)

```

> Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{371F027F-EFB7-432E-95C3-95AC7C6AFE15}, id 0
> Ethernet II, Src: LiteonTe_a9:17:f5 (e4:aa:ea:a9:17:f5), Dst: HonHaiPr_c1:84:c3 (b0:52:16:c1:84:c3)
> Internet Protocol Version 4, Src: 192.168.2.253, Dst: 192.168.2.252
  > Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d4e [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 13 (0x000d)
    Sequence Number (LE): 3328 (0x0d00)
    [Response frame: 6]
  > Data (32 bytes)
  
```

Elaborado por el autor

Para el análisis del protocolo se utiliza la tabla 5 que contiene los tipos de mensajes ICMPv4, en la figura 97 en el recuadro de Internet Control Message Protocol se muestran los campos del formato ICMP, la primera y segunda fila indica un mensaje tipo 8 y código 0 respectivamente los cuales son encargados de realizar una petición de eco desde un host, en el recuadro también se puede apreciar la suma de comprobación y el estado indicando que se realizó de forma correcta, por último se muestra el total de datos transmitidos, en este caso fue de 32 bytes.

Ahora seleccionamos el paquete de respuesta y nos dirigimos a Internet Control Message Protocol, como se observa en la figura 98 en el segundo recuadro ahora cambia el tipo de mensaje y el código, en este caso ambos son 0 e indican que se ha obtenido una respuesta al eco solicitado, además de que los datos también fueron de 32 bytes por lo que se puede decir que no existen pérdida de paquetes.

Respuesta de eco en IPv4

No.	Time	Source	Destination	Protocol	Length	Info
5	3.723256	192.168.2.253	192.168.2.252	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 6)
6	3.728964	192.168.2.252	192.168.2.253	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=128 (request in 5)
8	4.728185	192.168.2.253	192.168.2.252	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in 9)
9	4.734097	192.168.2.252	192.168.2.253	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=128 (request in 8)
11	5.743485	192.168.2.253	192.168.2.252	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 12)
12	5.764382	192.168.2.252	192.168.2.253	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=128 (request in 11)
15	6.759160	192.168.2.253	192.168.2.252	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=128 (reply in 16)
16	6.769722	192.168.2.252	192.168.2.253	ICMP	74	Echo (ping) reply id=0x0001, seq=16/4096, ttl=128 (request in 15)

> Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{371F027F-EF87-432E-95C3-95AC7C6AFE15}, id 0 > Ethernet II, Src: HonHaiPr_c1:84:c3 (b0:52:16:c1:84:c3), Dst: LiteonTe_a9:17:f5 (e4:aa:ea:a9:17:f5) > Internet Protocol Version 4, Src: 192.168.2.252, Dst: 192.168.2.253 > Internet Control Message Protocol Type: 0 (Echo (ping) reply) Code: 0 Checksum: 0x554e [correct] [Checksum Status: Good] Identifier (BE): 1 (0x0001) Identifier (LE): 256 (0x0100) Sequence Number (BE): 13 (0x000d) Sequence Number (LE): 3328 (0x0d00) [Request frame: 5] [Response time: 5,708 ms] Data (32 bytes)						
--	--	--	--	--	--	--

4.4.3.2. ANÁLISIS DE ICMPv6

En este caso se utiliza la tabla 6 que contiene los tipos de mensajes ICMPv6, se realizó un ping haciendo uso de la dirección IPv6 al mismo tiempo que se capturaban los paquetes en Wireshark, se transmitieron cuatro paquetes obteniendo así los paquetes solicitados (request) y la respuesta de los mismos (reply), para obtener solo los datos del protocolo a utilizar se realiza un filtrado insertando icmpv6 en este caso como se observa en la siguiente figura.

Figura 99

Captura del protocolo ICMP para IPv6

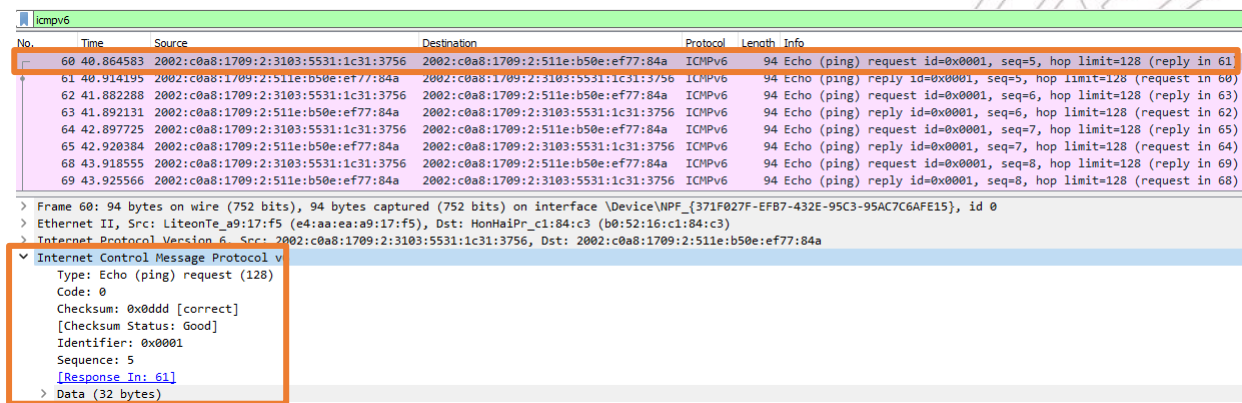
No.	Time	Source	Destination	Protocol	Length	Info
60	40.864583	2002:c0a8:1709...	2002:c0a8:1709...	ICMPv6	94	Echo (ping) request id=0x0001, seq=5, hop limit=128 (reply in 61)
61	40.914195	2002:c0a8:1709...	2002:c0a8:1709...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=5, hop limit=128 (request in 60)
62	41.882288	2002:c0a8:1709...	2002:c0a8:1709...	ICMPv6	94	Echo (ping) request id=0x0001, seq=6, hop limit=128 (reply in 63)
63	41.892131	2002:c0a8:1709...	2002:c0a8:1709...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=6, hop limit=128 (request in 62)
64	42.897725	2002:c0a8:1709...	2002:c0a8:1709...	ICMPv6	94	Echo (ping) request id=0x0001, seq=7, hop limit=128 (reply in 65)
65	42.920384	2002:c0a8:1709...	2002:c0a8:1709...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=7, hop limit=128 (request in 64)
68	43.918555	2002:c0a8:1709...	2002:c0a8:1709...	ICMPv6	94	Echo (ping) request id=0x0001, seq=8, hop limit=128 (reply in 69)
69	43.925566	2002:c0a8:1709...	2002:c0a8:1709...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=8, hop limit=128 (request in 68)

Elaborado por el autor

Al seleccionar el paquete de solicitud podremos analizar la sección de Internet Control Message Protocol v6 con sus respectivos campos, como se observa en la figura 100 la primera fila contiene un mensaje informativo tipo 128 y la segunda fila un código 0 las cuales indican que se está realizando una solicitud de eco, además se aprecia una correcta suma de verificación y el buen estado del mismo, por último, se tiene que el paquete solicitado tiene un tamaño de 32 bytes.

Figura 100

Solicitud de eco en IPv6



Elaborado por el autor

Ahora seleccionamos el paquete de respuesta como se observa en la figura 101 la primera fila contiene un mensaje informativo tipo 129 y la segunda fila un código 0 las cuales indican que se indica que se ha obtenido una respuesta al eco solicitado, además se aprecia una correcta suma de verificación y el buen estado del mismo, por último, se tiene que el paquete solicitado tiene un tamaño de 32 bytes.



UPSE

Figura 101

Respuesta de eco en IPv6

No.	Time	Source	Destination	Protocol	Length	Info
60	40.864583	2002:c0a8:1709:2:3103:5531:1c31:3756	2002:c0a8:1709:2:511e:b50e:ef77:84a	ICMPv6	94	Echo (ping) request id=0x0001, seq=5, hop limit=128 (reply in 61)
61	40.914195	2002:c0a8:1709:2:511e:b50e:ef77:84a	2002:c0a8:1709:2:3103:5531:1c31:3756	ICMPv6	94	Echo (ping) reply id=0x0001, seq=5, hop limit=128 (request in 60)
62	41.882288	2002:c0a8:1709:2:3103:5531:1c31:3756	2002:c0a8:1709:2:511e:b50e:ef77:84a	ICMPv6	94	Echo (ping) request id=0x0001, seq=6, hop limit=128 (reply in 63)
63	41.892131	2002:c0a8:1709:2:511e:b50e:ef77:84a	2002:c0a8:1709:2:3103:5531:1c31:3756	ICMPv6	94	Echo (ping) reply id=0x0001, seq=6, hop limit=128 (request in 62)
64	42.897725	2002:c0a8:1709:2:3103:5531:1c31:3756	2002:c0a8:1709:2:511e:b50e:ef77:84a	ICMPv6	94	Echo (ping) request id=0x0001, seq=7, hop limit=128 (reply in 65)
65	42.920384	2002:c0a8:1709:2:511e:b50e:ef77:84a	2002:c0a8:1709:2:3103:5531:1c31:3756	ICMPv6	94	Echo (ping) reply id=0x0001, seq=7, hop limit=128 (request in 64)
68	43.918555	2002:c0a8:1709:2:3103:5531:1c31:3756	2002:c0a8:1709:2:511e:b50e:ef77:84a	ICMPv6	94	Echo (ping) request id=0x0001, seq=8, hop limit=128 (reply in 69)
69	43.925566	2002:c0a8:1709:2:511e:b50e:ef77:84a	2002:c0a8:1709:2:3103:5531:1c31:3756	ICMPv6	94	Echo (ping) reply id=0x0001, seq=8, hop limit=128 (request in 68)

> Frame 61: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{371F027F-EF87-432E-95C3-95AC7C6AFE15}, id 0
> Ethernet II, Src: HonHaiPr_c1:84:c3 (b0:52:16:c1:84:c3), Dst: LiteonTe_a9:17:f5 (e4:aa:ea:a9:17:f5)
> Internet Protocol Version 6, Src: 2002:c0a8:1709:2:511e:b50e:ef77:84a, Dst: 2002:c0a8:1709:2:3103:5531:1c31:3756
Internet Control Message Protocol v6
Type: Echo (ping) reply (129)
Code: 0
Checksum: 0x0cdd [correct]
[Checksum Status: Good]
Identifier: 0x0001
Sequence: 5
[Response To: 60]
[Response Time: 49,612 ms]
> Data (32 bytes)

Elaborado por el autor

CONCLUSIONES

- Con el diseño elaborado en el software Sketchup se logró obtener una perspectiva de la ubicación del rack en el laboratorio de telecomunicaciones y el correcto orden de los equipos que se utilizaron para este proyecto.
- La estructura de la red de fibra funciona de manera óptima ya que se utilizó un cable de fibra multimodo basado en el estándar UIT-T G.652 el cual permite velocidades de hasta 10 Gb/s a distancias menores de 2km siendo ideal para el laboratorio de telecomunicaciones.
- El mecanismo de transición que se efectuó para la coexistencia de los protocolos IPv4 e IPv6 fue el de tunelización 6to4 debido a que este método permitió obtener un bloque de direcciones IPv6 a partir de la red IPv4 del laboratorio de tal manera que los dispositivos finales obtuvieron direccionamiento en ambas versiones.
- Al realizar las pruebas de latencia en la transmisión de paquetes IPv4 e IPv6 con tamaños de 32 bytes, 512 bytes y 8000 bytes se obtuvo una latencia promedio de 5,33ms para IPv4 mientras que para IPv6 la latencia promedio fue de 5ms concluyendo que IPv6 tiene una ligera ventaja en términos de latencia para la transmisión de paquetes.
- En la comparativa de latencia de las redes con equipos Ubiquiti y Mikrotik se consiguieron mejores promedios de latencia en la red de Ubiquiti con 5ms en comparación con Mikrotik que obtuvo un promedio de 7ms.

RECOMENDACIONES

- Para realizar mejoras en la red de fibra se puede adicionar módulos SFP+ de 10G de tal manera que se pueda conseguir mayores velocidades de transmisión, para ello se debe tomar en cuenta las características de los equipos y verificar si sus puertos admiten los módulos mencionados.
- Antes de la implementación del protocolo IPv6 se recomienda realizar un estudio de los diferentes mecanismos de transición y verificar si el proveedor de servicios de internet brinda bloques de direcciones IPv6 a sus clientes, en caso de no hacerlo se pueden utilizar túneles para brindar una navegación por IPv6.
- Se recomienda realizar pruebas de transferencia de paquetes con tamaño superior a 8000 bytes, considerando que el CMD de Windows tiene un límite de tamaño de paquetes de 65500 bytes.

BIBLIOGRAFÍA

- [1] Santos, M. (2015). Diseño de redes telemáticas. Madrid: RA-MA Editorial.
- [2] Abad Domingo, A. (2013). Redes locales. Madrid: McGraw-Hill Education.
- [3] Tomasi, W. (2003). Sistemas de Comunicaciones Electrónicas. México: Pearson Educación.
- [4] Grazzini, H. (2020). Fibras ópticas: conceptos teóricos y aplicaciones prácticas. Córdoba: Jorge Sarmiento Editor - Universitas.
- [5] ITU. (2016). ITU. Obtenido de <https://www.itu.int/rec/T-REC-G.652-201611-I/es>
- [6] Huidobro, J. (2014). Telecomunicaciones. Tecnologías, Redes y Servicios. Madrid: RA-MA S.A. Editorial.
- [7] España, M. (2005). Comunicaciones ópticas. Madrid: Ediciones Días de Santos S.A.
- [8] Szymanczyk, O. (Junio de 2014). Oscarszymanczyk. Obtenido de <http://www.oscarszymanczyk.com.ar/documentos/ANEXO%207.pdf>
- [9] PROMAX. (Septiembre de 2019). PROMAX. Obtenido de <https://www.promax.es/esp/noticias/578/tipos-de-conectores-de-fibra-optica-guia-sencilla/>
- [10] TECNIT. (s.f.). TECNIT. Obtenido de <https://tecnit.com.ec/producto/patch-cord-de-fibra-sm-lc-apc-a-lc-apc-9-125um-dx-25mts/>
- [11] Coyachamin, G., & Delgado, H. (Marzo de 2016). Repositorio Institucional UTC. Obtenido de <http://repositorio.utc.edu.ec/bitstream/27000/4945/1/T-003895.pdf>
- [12] Coyachamin, G., & Delgado, H. (Marzo de 2016). Repositorio Institucional UTC. Obtenido de <http://repositorio.utc.edu.ec/bitstream/27000/4945/1/T-003895.pdf>
- [13] Valdivia Miranda, C. (2019). Comunicaciones industriales. Madrid: Ediciones Parainfo, SA.
- [14] Pérez, A. (2020). La seguridad de las redes. London: ITSE International.



UPSE

- [15] Dordoigne, J. (2018). Redes Informáticas: nociones fundamentales. Barcelona: Ediciones ENI.
- [16] Vélez, F., & Gutiérrez, L. (2016). IPv6, una realidad. Bogotá: Ediciones de la U.
- [17] Carrera, J. J. (2018). Transición de protocolo IPV4 a protocolo IPV6 para la red inalámbrica EDUROAM dentro de la Universidad Técnica del Norte. Ibarra.
- [18] ñigo Griera, J. (2013). Estructura de redes de computadores. Barcelona: Editorial UOC.
- [19] Silva Bracero, L. (Febrero de 2012). Repositorio Digital EPN. Obtenido de <https://bibdigital.epn.edu.ec/handle/15000/4549?locale=de>
- [20] Robert, Nordmark, E., & Gilligan, R. (2005). Basic Transition Mechanisms for IPv6 Hosts and Routers. RFC 4213 (Proposed Standard).
- [21] Martínez Yelmo, I., & Riaño Vílchez, P. (2016). IPv6-Lab: entorno de laboratorio para la adquisición de competencias relacionadas con IPv6. Madrid: Universidad de Alcalá.
- [22] Taffernaberry, J. (Junio de 2011). Repositorio Institucional UNPL. Obtenido de <http://sedici.unlp.edu.ar/handle/10915/4193>
- [23] Durand, A., Fasano, P., Guardini, I., & Lento, D. (2001). IPv6 Tunnel Broker. en RFC 3053 (Informational).
- [24] Tsirtsis, G. (2000). Network Address Translation - Protocol Translation (NAT-PT). RFC 2766 (Historic).
- [25] Ogunleye, G. (Octubre de 2016). Infraestructura de la red NAT-PT. Obtenido de ResearchGate: https://www.researchgate.net/publication/342159046_PERFORMANCE_EVALUATION_OF_LINUX_AND_MICROSOFT_WINDOWS_OPERATI



UPSE

[26] Interpolados. (26 de Marzo de 2017). Traducción. Obtenido de Interpolados:

<https://interpolados.wordpress.com/2017/03/26/necesidad-de-utilizar-ipv6/>

[27] LACNIC. (s.f.). Obtenido de <https://www.lacnic.net/innovaportal/file/5495/1/siit-dc.pdf>

[28] Manayay, C., & Olivera, R. (Mayo de 2015). Repositorio Institucional UNPRG. Recuperado

el 6 de Enero de 2022, de

<https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/894/BC-TES-4177.pdf?sequence=1&isAllowed=y>

[29] Salvatierra, J. (Mayo de 2018). School of Engineering UAGRM. Obtenido de

<https://www.soe.uagrm.edu.bo/wp-content/uploads/2020/08/INTEGRACION-DEL-PROTOCOLO-IPv6-A-LA-RED-DE-INTERNET-Y-DATOS-DE-COTAS-RL.pdf>

[30] Ubiquiti. (s.f.). Obtenido de <https://store.ui.com/collections/unifi-network-unifi-os-consoles/products/udm-pro>

[31] Ubiquiti. (s.f.). Obtenido de https://store.ui.com/collections/routing-switching/products/edgerouter-4?_pos=5&_sid=e3b22f651&_ss=r

[32] Ubiquiti. (s.f.). Obtenido de https://dl.ubnt.com/qsg/UAP-AC-LITE/UAP-AC-LITE_ES.html

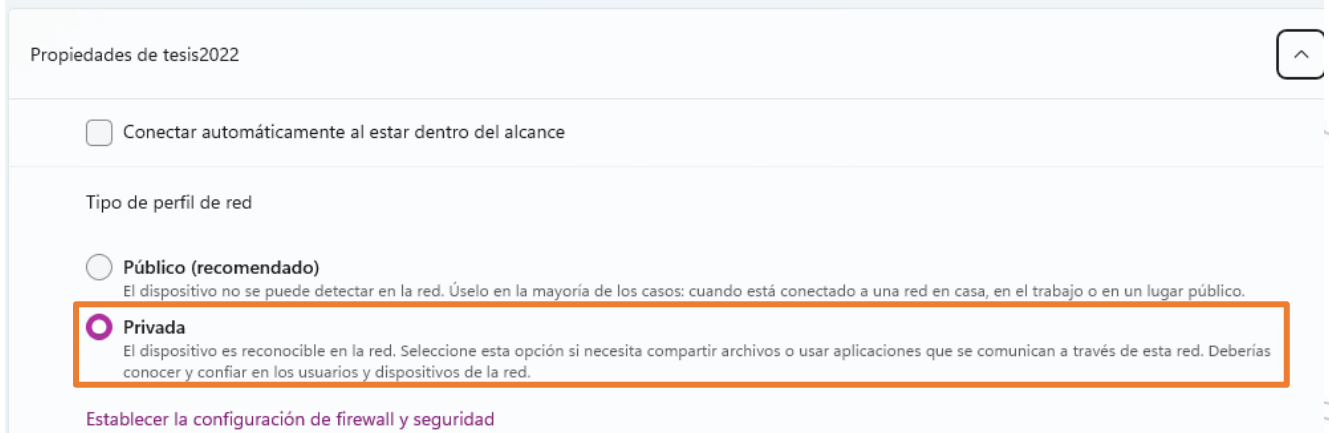
ANEXOS

Anexo 1: Configuración de firewall en las máquinas para permitir comunicación IPv4 e IPv6 en la red LAN.

En determinadas ocasiones al realizar ping desde un host a otro en el que ambos se encuentran en la misma red resulta imposible establecer una conexión para la transmisión de paquetes, esto se debe al tipo de perfil que maneja el usuario en la red o a las reglas de firewall que tienen las máquinas. Para poder solucionar este problema se realizan las siguientes instrucciones.

Se debe ingresar a las características de la red y seleccionar el tipo de perfil de red Privada, como se muestra en la siguiente figura.

Red e Internet > Wi-Fi > tesis2022



Ahora ingresamos al firewall de Windows defender, seleccionamos configuración avanzada y luego en reglas de entrada buscamos la opción de archivos e impresoras compartidos, se debe identificar el protocolo ICMP e ICMPv6 y en perfil deberá estar Público, privado; hacemos clic derecho sobre cada regla de entrada mencionada y seleccionamos en habilitar regla.

Windows Defender Firewall con seguridad avanzada

Archivo Acción Ver Ayuda

Windows Defender Firewall con seguridad avanzada

- Reglas de entrada
- Reglas de salida
- Reglas de seguridad de con...
- Supervisión

Nombre	Grupo	Perfil	Habilitado	Acción	Inv
Archivos e impresoras compartidos (petición eco: ICMPv6 de entrada)	Compartir archivos e impres...	Privado, Público	Sí	Permitir	No
Supervisión de máquina virtual (Solicitud de eco - ICMPv4 de entrada)	Supervisión de máquina virt...	Todo	No	Permitir	No
Redes principales: destino inaccesible fragment. necesaria (ICMPv4 de entrada)	Redes principales	Todo	Sí	Permitir	No
Diagnóstico de redes principales: solicitud de eco ICMP (ICMPv4 de entrada)	Diagnóstico de redes princi...	Dominio	No	Permitir	No
Diagnóstico de redes principales: solicitud de eco ICMPv4 de entrada	Diagnóstico de redes princi...	Privado, Público	No	Permitir	No
Archivos e impresoras compartidos (petición eco: ICMPv4 de entrada)	Compartir archivos e impres...	Privado, Público	Sí	Permitir	No
Archivos e impresoras compartidos (petición eco: ICMPv4 de entrada)	Compartir archivos e impres...	Dominio	No	Permitir	No
Enrutamiento y acceso remoto (GRE de entrada)	Enrutamiento y acceso rem...	Todo	No	Permitir	No
Xbox Game Bar	Xbox Game Bar	Todo	Sí	Permitir	No
Windows Search	Windows Search	Dominio, Privado	Sí	Permitir	No
Visor web de aplicación de escritorio	Visor web de aplicación de e...	Todo	Sí	Permitir	No
Uso del servicio de digitalización de Wi-Fi Direct (entrada)	Detección de redes Wi-Fi Dir...	Público	Sí	Permitir	No
Uso de administrador de trabajos en cola de Wi-Fi Direct (entrada)	Detección de redes Wi-Fi Dir...	Público	Sí	Permitir	No
Tu cuenta	Tu cuenta	Dominio, Privado	Sí	Permitir	No
Reproductor multimedia de Windows	Reproductor multimedia de ...	Dominio, Privado	Sí	Permitir	No
Películas y TV	Películas y TV	Dominio, Privado	Sí	Permitir	No
Paquete de experiencia de características de Windows	Paquete de experiencia de c...	Dominio, Privado	Sí	Permitir	No
Microsoft To Do	Microsoft To Do	Dominio, Privado	Sí	Permitir	No
Microsoft Store	Microsoft Store	Todo	Sí	Permitir	No
Microsoft Solitaire Collection	Microsoft Solitaire Collection	Dominio, Privado	Sí	Permitir	No
Microsoft Edge	Microsoft Edge	Dominio, Privado	Sí	Permitir	No
Instalador de aplicación	Instalador de aplicación	Dominio, Privado	Sí	Permitir	No
Inicio	Inicio	Dominio, Privado	Sí	Permitir	No
Fotos de Microsoft	Fotos de Microsoft	Todo	Sí	Permitir	No
Enlace Móvil	Enlace Móvil	Dominio, Privado	Sí	Permitir	No
Disney+	Disney+	Dominio, Privado	Sí	Permitir	No
Detección de redes Wi-Fi Direct (entrada)	Detección de redes Wi-Fi Dir...	Público	Sí	Permitir	No
Cortana	Cortana	Todo	Sí	Permitir	No
Correo y Calendario	Correo y Calendario	Todo	Sí	Permitir	No



UPSE
Anexo 2

Ubicación de UAP AC Lite





UPSE
Anexo 3

Conexión de cable multimodo



Anexo 4

Conexión de equipos





UPSE
Anexo 5

Armado final del Rack

