UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TÍTULO DEL TRABAJO DE TITULACIÓN

Modelo experimental de migración progresiva de IPv4 a IPv6 utilizando mecanismos de túnel y traducción aplicado al laboratorio de redes de FACSISTEL.

AUTOR

Soledispa Saltos Jorge Joel

EXAMEN COMPLEXIVO

Previo a la obtención del grado académico en
INGENIERO EN TECNOLOGÍA DE LA INFORMACIÓN

TUTOR

Lsi. Quirumbay Yagual Daniel Iván, Msia.

Santa Elena, Ecuador

2025

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez Aquino. Mgt.
DIRECTOR DE LA CARRERA

Lsi. Daniel Quirumbay Yagual, Msia.
TUTOR

Ing. Iván Coronel Suárez Mgt.
DOCENTE ESPECIALISTA

Ing. Marjorie Coronel Suárez . Mgt.
DOCENTE GUÍA UIC

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por Soledispa Saltos Jorge Joel, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 14 días del mes de noviembre del año 2025

TUTOR

Daniel Iván Quirumbay Yagual

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Jorge Joel Soledispa Saltos**

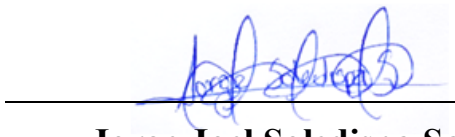
DECLARO QUE:

El trabajo de Titulación, Modelo experimental de migración progresiva de IPv4 a IPv6 utilizando mecanismos de túnel y traducción aplicado al laboratorio de redes de FACSISTEL, previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 14 días del mes noviembre del año 2025

EL AUTOR



Jorge Joel Soledispa Saltos

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado Modelo experimental de migración progresiva de IPv4 a IPv6 utilizando mecanismos de túnel y traducción aplicado al laboratorio de redes de FACSISTEL, presentado por el estudiante, Soledispa Saltos Jorge Joel fue enviado al Sistema Anti-plagio, presentando un porcentaje de similitud correspondiente al 6%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

TUTOR

Daniel Iván Quirumbay Yagual

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

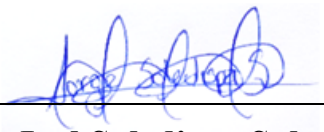
Yo, **Jorge Joel Soledispa Saltos**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales del presente trabajo de titulación con fines de difusión pública, además apruebo la reproducción dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 14 días del mes de noviembre del año 2025

EL AUTOR



Jorge Joel Soledispa Saltos

AGRADECIMIENTO

Agradezco a mi familia que ha sido siempre el motor que impulsa mis sueños y esperanzas, siempre han sido mis mejores guías de vida.

A mi tutor el Msia. Daniel Quirumbay por su apoyo en el desarrollo de este trabajo de titulación, a la Ing. Marjorie Coronel por compartir sus conocimientos y contribuir a mi formación profesional.

A mis amistades Jhonny Pérez, Miguel Carcelén, James Carvajal, Andrea Orrala, Jennifer Lopez, gracias por su amistad sincera, por todos los momentos compartidos, a la Ing. Emily Suarez por el apoyo y cariño brindado durante este proceso. A cada docente que formó parte de este proceso integral de formación.

A la Universidad Estatal Península de Santa Elena, por brindarme las herramientas y conocimientos necesarios para completar esta importante etapa de mi vida académica.

Jorge Joel, Soledispa Saltos

DEDICATORIA

Dedico este trabajo de titulación a mis padres Joffre y Norma por todo su apoyo, confianza, sacrificio y por enseñarme a ser la persona que soy hoy, mis principios, mis valores, mi perseverancia y mi empeño.

A mis hermanos Joffre, Agustín, Johana y la Ing. Verónica por su motivación y cariño a lo largo de mi vida y carrera universitaria. Y demás familiares que me han dado ejemplo de superación personal y profesional

Jorge Joel, Soledispa Saltos

ÍNDICE GENERAL

TRIBUNAL DE SUSTENTACIÓN	I
CERTIFICACIÓN	II
DECLARACIÓN DE RESPONSABILIDAD	III
CERTIFICACIÓN DE ANTIPLAGIO	IV
AUTORIZACIÓN	V
AGRADECIMIENTO	VI
DEDICATORIA	VII
ÍNDICE GENERAL	VIII
ÍNDICE DE TABLAS	XI
ÍNDICE DE FIGURA	XI
ÍNDICE DE ANEXOS	XIV
RESUMEN	XV
ABSTRACT	XVI
INTRODUCCIÓN	1
CAPITULO I	2
1.1 ANTECEDENTE	2
1.2 DESCRIPCIÓN DEL PROYECTO	5
1.3 OBJETIVOS	7
1.3.1 OBJETIVO GENERAL	7
1.3.2 OBJETIVOS ESPECÍFICOS	7
1.4 JUSTIFICACIÓN	7
1.5 ALCANCE DEL PROYECTO	8
CAPITULO II	10
2.1 MARCO CONCEPTUAL	10
2.1.1 DIRECCIONES IP	10

2.1.2 Protocolos de Internet IPv4 e IPv6 10
2.1.2.1 Protocolo IPv4 10
2.1.2.2 Tipos de comunicaciones IPv4 11
2.1.3 Protocolos de Internet IPv6 12
2.1.3.1 Tipos de comunicaciones IPv6 13
2.1.3.2 Tipos de direcciones 14
2.1.4 Bridge y LAN/WAN 15
2.1.5 Diferencia entre IPv4 e IPv6 16
2.1.6 Ventajas de IPv6 Sobre IPv4 16
2.1.7 Mecanismo de transición 17
2.1.7.1 Estrategias de transición IPv4 e IPv6 17
2.1.7.2 Traducción de direcciones IPv6 a IPv4 17
2.1.8 Mecanismo de transición 18
2.1.8.1 Dual Stack 18
2.1.8.2 Tunelización 19
2.1.8.3 Traducción 19
2.1.9 Segmentación de redes 19
2.1.9.1 DNS en redes IP 19
2.1.9.2 Tipo de servidores DNS 20
2.1.9.3 Tipos de resoluciones de nombres de dominio 20
2.1.9.4 Tipos de Registros DNS 21
2.1.9.5 Diferencias en el manejo de DNS para IPv4 e IPv6 21
2.2 Marco teórico 22
2.2.1 Fundamentos de redes y protocolos 22
2.2.1.1 Porque migrar IPv6 Sobre IPv4 22
2.2.1.2 Mecanismo de migración 23
2.2.1.3 Normas y estándares 24
2.2.1.4 Elección y mecanismo de transición a utilizar 24
2.3.1 Metodología de investigación 25
2.3.2 Técnicas e instrumentos de recolección de datos 28
2.3.2.1 Análisis de resultados de la encuesta 29
2.3.3 Metodología de desarrollo 36

CAPITULO III 38
3. REQUERIMIENTOS 38
3.1 REQUERIMIENTOS FUNCIONALES 38
3.1.1 REQUERIMIENTOS NO FUNCIONALES 38
3.2 FASE DE RECOLECCIÓN DE DATOS 40
3.2.1 OBJETIVOS DE LA ENCUESTA 40
3.2.2 LEVANTAMIENTO DE INFORMACIÓN 40
3.2.3 PRESUPUESTO 41
3.2.4 RECOLECCIÓN DE DATOS DE DUAL STACK Y TÚNEL. 41
3.2.5 CUADRO COMPARATIVO DE EQUIPOS PARA EL PROCESO DE MIGRACIÓN 44
3.4 FASE DE IMPLEMENTACIÓN 47
3.4.1 DEFINICIÓN DEL ENTORNO 47
3.4.2 PLAN DE PRUEBAS 48
3.4.3 INSTALACIÓN Y CONFIGURACIÓN DEL EQUIPO MIKROTIK 50
3.4.3.1 CONFIGURACIÓN DE PROTOCOLO DE MIGRACIÓN 52
3.4.3.2 DUAL STACK 52
3.4.3.3 TUNNELING 55
3.4.4 CONFIGURACIÓN DEL PORTAL CAUTIVO 57
3.4.5 CONFIGURACIÓN DE SSH 59
3.5 FASE DE PRUEBAS DE FUNCIONALIDAD IPV6 59
3.5.1 FUNCIONALIDAD IPV4 E IPV6 EN EL MIKROTIK 60
3.5.2 ANÁLISIS DE RESULTADOS 61
3.5.3 ANÁLISIS DE LATENCIA Y PÉRDIDA DE PAQUETES EN LA RED MIKROTIK 63
3.5.4 PRUEBA DE BLOQUEO DE CONEXIÓN 65
3.5.5 COMPARTIR ARCHIVOS POR SHH EN IPV6 65
CONCLUSIÓN 67
RECOMENDACIÓN 68
REFERENCIAS 69
ANEXOS 76

ÍNDICE DE TABLAS

Tabla 1 Clases de direcciones ipv4 11
Tabla 2 Clases de direcciones ipv4 12
Tabla 3 Esquema de direcciones ipv6 con subredes 13
Tabla 4 Cantidad de estudiantes a los que se les realizará la encuesta 28
Tabla 5 Uso de ipv6 29
Tabla 6 Laboratorio solo opera con ipv4 30
Tabla 7 Laboratorio solo opera con ipv4 31
Tabla 8 El uso de ipv6 mejorará el aprendizaje 32
Tabla 9 Considera que aprender ipv6 es necesario para la formación profesional 33
Tabla 10 Condiciones técnicas, control de acceso y velocidad de transferencia de datos 34
Tabla 11 Beneficios para implementar un modelo de transición ipv4 a ipv6 35
Tabla 12 Requerimientos funcionales 38
Tabla 13 Requerimientos no funcionales 39
Tabla 14 Requisitos de hardware para la migración de protocolos 39
Tabla 15 Requisito de software de migración 40
Tabla 16 Comparativa de equipos para ipv6 45
Tabla 17 Plan de pruebas 49
Tabla 18 Latencia del protocolo ipv4 64
Tabla 19 Latencia del protocolo ipv6 64

ÍNDICE DE FIGURAS

Figura 1 Funcionamiento de Multicast [17]. 13
Figura 2 Funcionamiento de Anycast [17]. 14
Figura 3: Diferencia entre la cabecera IPv4 e IPv6. 16
Figura 4 Uso de IPv6 29
Figura 5 Laboratorio solo opera con IPv4 30
Figura 6 Laboratorio solo opera con IPv4 31
Figura 7 El uso de IPv6 mejorará el aprendizaje 32
Figura 8 Considera que aprender IPv6 es necesario para la formación académica 33
Figura 9 Condiciones técnicas, control de acceso y velocidad de transferencia de datos 34
Figura 10 Beneficios para implementar un modelo de transición IPv4 a IPv6 35
Figura 11 Fases de migración IPv4 e IPv6 37
Figura 12 Conexión del equipo mikrotik al cable ethernet de la red de la universidad. 41
Figura 13 Método Dual Stack 41
Figura 14 Prueba desde PC a MIKROTIK por el método DUAL STACK 42
Figura 15 Consulta de IP publica 42
Figura 16 Ping desde el Mikrotik al túnel 43
Figura 17 Comprobar conexión ipv6 desde Túnel Broker Hurricane a la PC por medio del CMD43
Figura 18 Captura de tráfico con Wireshark IPv4 e IPv6 44
Figura 19 Arquitectura 46
Figura 20 Topología IPv4 e IPv6 47
Figura 21 Instalación de pantalla y equipo Mikrotik al RAD 48
Figura 22 Aplicación Winbox para administrar el equipo Mikrotik 50
Figura 23 Instalación del paquete IPv6 50
Figura 24 Interfaz de Hurricane Electric 51
Figura 25 Crear túnel con la IP publica de la universidad 51
Figura 26 IPv6 del túnel Hurricane con la IP publica 52
Figura 27 Habilitar protocolo IPv6 en la PC 52
Figura 28 Red en IPv4 e IPv6 53
Figura 29 Detalles de las direcciones por el símbolo del sistema y el comando IPCONFIG 53
Figura 30 Configuración Dual Stack 54
Figura 31 Conexión Dual Stack 54

Figura 32 Túnel IPIPv6 55
Figura 33 Asigna IPv6 al bridge 55
Figura 34 Configuración de la ruta 56
Figura 35 Consola de mikrotik con datos del túnel creado 56
Figura 36 túnel activo y funcional 57
Figura 37 Bloque de la página web con el Hotspot 58
Figura 38 Restablece la conexión. 58
Figura 39 Servidor SSH 59
Figura 40 Conexión SSH 59
Figura 41 Dirección IPv4 e IPv6 60
Figura 42 Envió de IPv4 e IPv6 en PC1 60
Figura 43 Envió de IPv4 e IPv6 en PC2 61
Figura 44 Envió de IPv4 e IPv6 en PC3 61
Figura 45 Análisis de ipv4 62
Figura 46 Análisis de IPv6 62
Figura 47 Bloque de hotspot 65
Figura 48 Interfaz Putty 65
Figura 49 Compartir archivo al NAS 66
Figura 50 Documentos recibidos en el NAS. 66
Figura 51 Equipo Mikrotik RB760IGS 82
Figura 55 Botón RESET 82
Figura 56 Modo reset configuration 83
Figura 57 Opciones de RESET 83
Figura 58 Activar paquete IPv6 84
Figura 59 Verificación de DHCP 84
Figura 60 Asignar IPv6 al puerto Ether y Bridge 85
Figura 61 Conexión entre mikrotik y pc dual Stack 85
Figura 62 Túnel Hurricane Electric 86
Figura 63 Crear el túnel con la IP pública 86
Figura 64 Dirección IP asignada por el túnel sobre IPv4 87
Figura 65 Crear túnel IPIPV6 87
Figura 66 Asignar la dirección al túnel 88

Figura 67 Asignación de rutas 88
Figura 68 Regla de firewall 88

ÍNDICE DE ANEXOS

Anexo 1 Encuesta dirigidas a estudiantes de Facsistel 76
Anexo 2 Permiso de uso de laboratorio de Redes 78
Anexo 3 Permiso de uso de laboratorio y uso de equipo 79
Anexo 4 Configuración del Mikrotik 80
Anexo 5 Armado final del RAD 80
Anexo 6 Configuración del túnel 80
Anexo 7 Manual de migración del protocolo ipv4 a ipv6 utilizando un router Mikrotik Hex S RB760IGS 81

RESUMEN

El crecimiento acelerado de Internet y el aumento de dispositivos conectados han evidenciado las limitaciones del protocolo IPv4 por la escasez de direcciones. Ante esta situación nace IPv6 como una solución que amplía la cantidad de direcciones que facilitan la conexión de nuevos equipos. Tiene como propósito diseñar un modelo experimental que permita la transición entre ambos protocolos mediante mecanismos de transición, garantizando la compatibilidad entre dispositivos. Para ello, se implementarán esquemas como Dual Stack y Tunneling, así como reglas de firewall y Hotspot para el control de tráfico. La investigación se desarrolla bajo un enfoque cuantitativo y un diseño experimental. Los resultados evidencian que la red ipv6 es más eficiente y estable con un 41,54% de pérdida de latencia, mientras que en IPv4 de 62,47% del total de latencias, con IPv6 se logró demostrar mayor estabilidad y coexistencia entre los dispositivos del laboratorio a través de ping y transmitir documento por SSH con direccionamiento IPv6. Se concluye que este modelo experimental permite mejoras en la infraestructura del laboratorio, analiza el comportamiento y las diferencias de los protocolos al momento de transmitir paquetes a los dispositivos finales, de esta manera, queda como un medio de prácticas de direccionamiento IPv6 para nuevos proyectos para los estudiantes de la carrera.

Palabras claves: laboratorio de redes, protocolo IPv6, transición, conectividad.

ABSTRACT

The rapid growth of the internet and the increase in connected devices have highlighted the limitations of the IPv4 protocol due to address scarcity. In response, IPv6 emerged as a solution that expands the number of addresses, facilitating the connection of new devices. The aim is to design an experimental model that allows the transition between both protocols through transition mechanisms, ensuring compatibility between devices. To this end, schemes such as Dual Stack and Tunneling will be implemented, as well as firewall and Hotspot rules for traffic control. The research is conducted using a quantitative approach and experimental design. The results show that the IPv6 network is more efficient and stable, with a 41.54% reduction in latency, compared to 62.47% for IPv4. IPv6 demonstrated greater stability and coexistence among the laboratory devices through ping tests and by transmitting documents via SSH using IPv6 addressing. It is concluded that this experimental model improves the laboratory's infrastructure, analyzes the behavior and differences between the protocols when transmitting packets to end devices, and serves as a practical tool for IPv6 addressing practices in future student projects.

Keywords: network laboratory, IPv6 protocol, transition, connectivity.

INTRODUCCIÓN

El crecimiento acelerado de Internet y el constante aumento de dispositivos conectados han puesto en evidencia las limitaciones del protocolo IPv4, cuyo espacio de direccionamiento resulta insuficiente frente a la demanda actual. Para dar respuesta a esta problemática se ha desarrollado IPv6 como un protocolo de nueva generación que amplía significativamente la capacidad de direccionamiento mejora los procesos de autoconfiguración y promueve una gestión más eficiente de la red. Sin embargo, la migración hacia IPv6 no puede realizarse a gran escala ya que la infraestructura mundial todavía se encuentra fuertemente basada en IPv4, lo que hace necesario implementar mecanismos de transición que permitan la coexistencia entre ambos protocolos.

El presente trabajo desarrolla un modelo experimental de migración progresiva del protocolo IPv4 al protocolo IPv6 en el que se va a aplicar mecanismos de túnel en el laboratorio de redes de FACSISTEL de la UPSE. Teniendo como objetivo diseñar un prototipo que permita a los estudiantes comprender los procesos de transición, así como los desafíos y beneficios asociados a los cambios a IPv6.

Para cumplir este propósito se tomará en cuenta la configuración de prototipos de Dual Stack y Tunneling en los equipos de red del laboratorio esto se hace con el fin de garantizar compatibilidad y conectividad entre dispositivos IPv4 e IPv6. Además, se implementará un mecanismo de control de acceso basado en firewall y Hotspot para que regule el tráfico. Después, se procederá a evaluar el rendimiento del prototipo mediante métricas comparativas antes y después de la migración para validar mejoras. Finalmente, se va a desarrollar un manual de funcionamiento en el que se va a documentar los procesos de instalación, configuración y pruebas en el que va a quedar como una guía práctica para futuras implementaciones.

Con este enfoque, el modelo experimental no solo busca demostrar el modelo de migración progresiva hacia IPv6 en un entorno académico, sino que también nos permite fortalecer las competencias de los estudiantes en el uso de tecnologías de transición y análisis de rendimiento de redes. En consecuencia, estas aportan un recurso didáctico de alto valor para la formación en telecomunicaciones, alineado con los desafíos actuales de la industria y el proceso global de aceptación de IPv6.

CAPITULO I

1.1 Antecedente

La transición de IPv4 a IPv6 presenta una alta complejidad ya que es necesario cumplir con varios requisitos antes de poder llevar a cabo la migración. Este proceso debe entenderse como algo que tomará tiempo ya que no es posible terminar una tarea tan extensa en poco tiempo y todavía está en marcha. Sin embargo, los progresos alcanzados hasta el momento han permitido abordar y simplificar numerosos problemas asociados con la comunicación en IPv4, además de ayudar a aliviar la situación del agotamiento de direcciones [1].

[2] menciona que:

> En la actualidad, internet es la plataforma principal de acceso al sistema en casi todo el mundo. Las redes son una parte indispensable de eso y, en gran medida, son responsables por la buena (o mala) experiencia de los usuarios. Dentro de ese contexto, es fundamental la implementación de IPv6 para mantener la calidad de los servicios.

Vélez Varela, Fernando y Gutiérrez Rancruel, Liliana [3] comentan sobre protocolos:

> El protocolo que se utiliza para dirigir y encaminar los paquetes en la red es IPv4, pero este protocolo ya no permite el crecimiento de la red, haciendo necesaria la migración a un estándar que proporcione los beneficios de IPv4, además de brindar un gran número de direcciones IP y una versión mejorada, presentando atributos como movilidad, seguridad, soporte para aplicaciones en tiempo real, extensibilidad, entre otras.

[4] menciona que:

> La Facultad de Sistemas y Telecomunicaciones (FACSISTEL) fue creada en el año 2010 y tiene cinco carreras vigentes. Actualmente dispone de cuatro laboratorios, 4 en el cual el servicio de internet se torna saturado sin conocerse cuales son las causas específicas de la ralentización de la conectividad generando malestar en la Facultad al no poder acceder de

> manera usual a los servicios ya que existe un número cada vez mayor de aplicaciones y de equipos terminales conectados a la misma.

En base a la observación (Ver anexo 1), la infraestructura desactualizada del laboratorio de Cisco en la Facultad de Sistemas y Telecomunicaciones de la UPSE ha generado múltiples problemas, siendo uno de los más críticos la interrupción en la conectividad. El uso excesivo de IPv4 y sus limitaciones ha provocado fallos repetidos en la red. Como resultado, los estudiantes enfrentan tienen varias dificultades ya que esta versión no permite un crecimiento ya sea en seguridad, actualización y funcionamiento lo que ha provocado que se opte por migrar el protocolo ipv6.

Los errores en la planificación en el proceso de la migración en el laboratorio de Redes nos han provocado un retraso significativo en la implementación para adaptarnos a las nuevas tecnologías tal es el caso de la transición de IPv4 a IPv6. La falta de una estrategia clara y una evaluación apropiada de los recursos ha generado problemas con el cumplimiento del proyecto lo que afecta a la continuidad del aprendizaje práctico de los estudiantes. Como consecuencia, la infraestructura sigue operando con configuraciones antiguas, lo que nos limita a el acceso a entornos de red modernas y dificulta la adquisición de capacidades actualizadas en el ámbito de las telecomunicaciones.

Juan Pablo [5] menciona:

> La configuración de IPv6 en entornos multiusuarios, redes de cobertura WAN y la implementación del (Network address translation-protocols translation) es un mecanismo que permite que los nodos IPv6 se comuniquen con nodos IPv4 de forma transparente utilizando una única dirección IPv4. También muestra la configuración de DNS IPv6 tanto en Cliente como Servidor. También permite identificar características propias de los túneles que proporcionan un componente que sirva para utilizar la infraestructura IPv4 mientras la infraestructura IPv6 está siendo implementada.

Para realizar este trabajo se hizo referencia con base a tres trabajos investigativos en los cuales tenía como propósito "Propuesta de migración del protocolo ipv4 a ipv6 en la infraestructura tecnológica de una organización caso de estudio" [6]. Con un enfoque exploratorio y descriptivo para hacer la migración del protocolo ipv4 a IPv6, este trabajo solo hacía hincapié en un diseño general del enrutamiento aplicado en packet trace mostrando toda su infraestructura.

Salgado, Lorena [6] menciona:

> El objetivo de establecer un marco de referencia para estudios futuros enfocados en diseñar un esquema de migración en el contexto de las PYME (Pequeña y Mediana Empresa) de manera rápida, efectiva y llevando un adecuado control de la información en la compañía. En el caso particular de la PYME, las características permiten concluir que la transición a IPv6 es posible ejecutando el Double Stack en los equipos de la LAN para lograr una isla IPv6 que permita posteriormente un enlace exterior con el método de transición "6to4" el cual accederá enlazar los dos protocolos.

Del trabajo de investigación titulado "Propuesta de migración del protocolo IPv4 a IPv6 de la red nacional de datos de la Agencia de Regulación y Control de Electricidad (ARCONEL)" [7]. Está enfocado en hacer la transición de la infraestructura basada en el protoc,olo IPv4 teniendo como objetivo la transformación de una red escalable. "Esta migración de protocolos beneficiado a los usuarios o funcionarios de la ARCONEL quienes serán los favorecidos directos" [7]. Este caso de estudio se enfocaba en crear una topología estrella combinada con equipos SWCORE Cisco 4500, Cisco 29600 y 3COM generando la alternativa de aplicar este tipo de migración con un equipo físico Mikrotik que soporta los cambios.

Juan Pablo [5] menciona del trabajo titulado "Propuesta para la migración del protocolo ipv4 a protocolo ipv6 para la secretaria del Sisbén de la alcaldía de Tunja", que:

> Corresponde a un estudio descriptivo, el cual busca especificar las propiedades importantes, personas, grupos. Identificando las características

principales de la red actual con el fin de caracterizar los elementos necesarios para el cambio progresivo de la red de comunicaciones y su migración de IPv4 a IPv6, esta propuesta de diseño topológico se va a aplicar de forma física y lógica.

Por los motivos expuestos, se vuelve evidente la importancia de actualizar la infraestructura del laboratorio Cisco de la Facultad de Sistemas y Telecomunicaciones. La migración del protocolo IPv4 a IPv6 no solo representa un avance en cuanto al rendimiento y la seguridad de la red, sino que también abre la puerta a una conectividad más ágil y preparada para los desafíos tecnológicos. Esta implementación permitirá gestionar de forma eficiente el tráfico y también fortalecerá la formación práctica de los estudiantes en tecnologías modernas y en línea con los estándares internacionales en telecomunicaciones.

1.2 Descripción del Proyecto

En los laboratorios de la Facultad de Sistemas y Telecomunicaciones (FACSISTEL), en este caso Redes se observa una constante presencia de dispositivos fijos y móviles pertenecientes a docentes, estudiantes e invitados que visitan la Facultad diariamente. Esto genera un alto tráfico de datos dentro de la infraestructura de red, lo que en varios momentos provoca una disminución en la velocidad de conexión a internet. Por esta razón se va a realizar la migración de protocolo IPv4 a IPv6 en el laboratorio de Redes de la Facultad de Sistemas y Telecomunicaciones (FACSISTEL), para poder mitigar las limitaciones de conectividad de dispositivos, configuración y mejorar la seguridad.

El proyecto consta de las siguientes fases descritas a continuación.

Fases de recolección de datos.

Este trabajo se va a realizar obteniendo información a través de encuesta con muestreo no probabilístico por conveniencia estratificada a los estudiantes que utilizan el laboratorio de redes (Ver anexo 1) con esto se podrá conocer las necesidades para poder realizar la migración del ipv4 a ipv6, mostrando las

limitaciones que se ha presentado en el laboratorio para poder hacer prácticas estudiantiles. Recolección de la información acerca de todo lo que tiene que ver con el estado del arte de la migración del protocolo IPv4 a IPv6.

- Encuesta dirigida a los diferentes semestres que utilizan el laboratorio de redes.
- Identificación de las limitaciones en la infraestructura de la red basada en ipv4.

- Revisión bibliográfica sobre casos y documentación de casos similares de la implementación.

Fase de diseño.

En esta fase se va a elegir un método que permita la migración de ipv4 a ipv6. Diseño del sistema general considerando los protocolos de enrutamiento, entre otros aspectos técnicos.

- Seleccionar la metodología de migración (Dual Stack y túnel).
- Definir los esquemas de direccionamiento ipv6.
- Consideraciones de seguridad en el diseño (firewall, control de acceso).

Fase de implementación.

Configurar el prototipo de la metodología elegida (Dual Stack, túnel) para asegurar la coexistencia entre IPv4 e IPv6 y asegurar que haya tráfico en las dos direcciones.

- Instalación y configuración de ipv6 en los diferentes dispositivos de la red.
- Configuración de los túneles y activación de los modos para la coexistencia de protocolos.
- Pruebas de conectividad.

Fase de pruebas de funcionalidad IPv6

Se generará un informe donde se puede evidenciar los procesos de la implementación de IPv6 en el laboratorio de Redes.

- Pruebas de conectividad local y remota.
- Comparación de las métricas claves antes y después de la migración.
- Verificación de los tráficos en ambas pilas ipv4 e ipv6.

- Elaboración de un uniforme con resultados, conclusiones y recomendaciones.

1.3 Objetivos

1.3.1 Objetivo general

Diseñar un prototipo que permita migrar del protocolo de internet IPv4 a IPv6 mediante esquemas de transición y configuración de equipos en la red para el laboratorio redes de la UPSE.

1.3.2 Objetivos específicos

- Configurar los prototipos funcionales (Dual Stack, Tunneling) en el dispositivo de red del laboratorio que ayude a integrar el protocolo IPv4 y IPv6 para garantizar compatibilidad y conectividad.
- Configurar el mecanismo de control de acceso a tráfico, mediante reglas de firewall que bloqueen las conexiones provenientes de Hotspot.
- Evaluar el rendimiento y la eficiencia del prototipo implementado, comparando métricas clave antes y después de la migración para validar mejoras.
- Elaborar un manual de funcionamiento para la migración del protocolo de internet IPv4 a IPv6 donde se muestren los procesos de instalación, configuración y pruebas.

1.4 Justificación

Con el crecimiento de dispositivos conectados a internet ha provocado la extenuación de direcciones disponibles de IPv4, por aquello se está optando por la transición a IPv6. La evolución del protocolo de Internet es una necesidad crítica frente al crecimiento exponencial de dispositivos conectados a nivel global. Según, [8] hoy en día, el protocolo IPv4, que solo admite unos 4. 3 mil millones de direcciones únicas, ya no basta para cubrir la necesidad de conexión en el mundo del Internet de las Cosas (IoT), la nube y los servicios digitales actuales. Por lo tanto, es fundamental pasarse a IPv6, un protocolo que ofrece una ampliación prácticamente ilimitada del direccionamiento IP.

La implementación de un prototipo funcional de la migración del protocolo IPv4 al protocolo IPv6 en el laboratorio cisco de la UPSE, no solo dará solución a una necesidad técnica, sino que también forma parte de una estrategia académicas que

nos permitirá a nosotros los estudiantes explorar y ampliar conocimiento antes las practicas que no se desarrollaban por las restricciones habidas en el laboratorio.

Según, [9] para poder lograr el cambio de IPv4 a IPv6, se implementarán estrategias de transición como Dual Stack y Tunelización, que nos ayudarán la coexistencia es decir que ambos protocolos operen juntos sin afectar los servicios de red actuales. Estas técnicas nos posibilitan la creación de una red híbrida que asegura la conectividad durante el proceso de innovación tecnológica eso si ajustándose a las limitaciones presentes en el laboratorio.

Además, la implementación de este proyecto ayudará a fortalecer las capacidades técnicas e investigativas de todos los estudiantes de la carrera y con esto promoviendo una cultura de innovación y adaptación tecnológica en relación con los estándares internacionales. La transición a IPv6 no solo responde a una necesidad operativa, sino que también impulsa el desarrollo de competencias en redes avanzadas, preparando a los estudiantes para enfrentar los desafíos que se aplicaran en su vida laboral profesional. Al integrar prácticas reales con tecnologías se podrá ayudar con un entorno educativo dinámico y alineado con las metas del desarrollo digital del país. Este proyecto está orientado al **Plan Nacional de Desarrollo Ecuador No Se Detiene 2025-2029**, descrito a continuación.

Eje Ambiente, Agua, Energía y Conectividad.

Objetivo 7.- "Impulsar el desarrollo de infraestructuras sostenibles y resilientes; y de la conectividad física y digital, que brinde condiciones de crecimiento y desarrollo económico" [10].

Política 7.1.- "Impulsar el desarrollo digital a través de la mejora en tecnología y la expansión de la conectividad en áreas geográficas no atendidas o con conectividad limitada en el país" [10].

1.5 Alcance del proyecto

El presente trabajo se enfoca en realizar un modelo experimental de migración progresiva de protocolo de internet IPv4 a IPv6, utilizando mecanismos de túnel. El estudio se realizará en el laboratorio de redes de FASCISTEL de la UPSE.

Este trabajo se basa en la configuración de prototipos utilizables en los equipos que se encuentren dentro de la red en el cual se busca integrar los dos protocolos que nos garanticen compatibilidad y conectividad dentro de la red. El proyecto constará de cuatro fases (Recolección de datos, Diseño, Implementación y pruebas de funcionalidad). Además, se configurarán reglas de control para el acceso de tráfico IPv6, mediante firewall y Hotspot, esto se realiza con la finalidad de establecer políticas de seguridad básicas.

Dentro del proyecto se incluirá evaluación del rendimiento del entorno con un antes y después de la migración, esto se plantea hacer utilizando las métricas claves que permitan medir la eficiencia a los cambios realizados, además se elaborará un manual técnico donde están todos los procedimientos a realizar para poder hacer réplicas de migración, este manual estará enfocado al personal académico o técnico.

Para este estudio no se considerará hacer la migración de las infraestructuras externas a la universidad, tampoco se hará la implementación en redes a gran escala. Otras consideraciones que se harán son que no se incluirá un análisis avanzado en la seguridad IPv6 ni pruebas de compatibilidad con servicios de otros proveedores externos. El trabajo se desarrollará en este periodo académico 2025-2.

CAPITULO II

2.1 Marco conceptual

El presente capítulo se enfocará en los servicios comunes sustentados en los Protocolos de Internet (IP) versiones 4 y 6. Además, vamos a presentar la estructura de direcciones que utiliza la IP y explicaremos cómo se dividen las distintas clases de direcciones IP. Adicionalmente, profundizaremos en cómo los protocolos TCP e IP ofrecen los métodos necesarios para la transmisión de mensajes y, crucialmente, analizaremos las normas de comunicación, sin importar el hardware empleado en la red.

2.1.1 Direcciones IP

[11] menciona que:

> El Protocolo de Internet (IP) es un protocolo[1], o conjunto de reglas, para enrutar y direccionar paquetes de datos, de modo que puedan viajar a través de las redes y llegar a su destino correcto. Los datos que viajan por Internet se dividen en fragmentos más pequeños, llamados paquetes.

Las direcciones IP nos permite recibir archivos que hemos solicitados como usuarios a través del host, esto se da para poder identificar y a la vez poder ser localizados. Dentro de la dirección IP del host, tenemos datos importantes como el número único, que se representa por cuatro cifras que son separadas por dos puntos, esta dirección identifica cualquier tipo de dispositivo que esté conectado en la red.

2.1.2 Protocolos de Internet IPv4 e IPv6

2.1.2.1 Protocolo IPv4

"Las direcciones IP tienen diferentes notaciones. Una dirección IPv4 en representación decimal[2] está compuesta por cuatro números enteros separados por un punto. Formando un conjunto de 4 números. Cada número entero tiene un valor comprendido entre 0 y 255" [7].

---

[1] Protocolo: Conjunto de reglas y métodos que permiten hacer intercambio datos en la red.

[2] Decimal: Compuesta de diez símbolos o dígitos (0, 1, 2, 3, 4, 5, 6, 7, 8 y 9)

Carlos Valdivia [12] comenta sobre las clases principales de IPv4:

> El espacio de direcciones IPv4 se divide en cinco clases principales de redes (A, B, C, D y E), donde cada clase tiene asignado un tamaño fijo de número de red. La clase, y por extensión la longitud de número de red y el número de host, se pueden determinar comprobando los bits más significativos (a la izquierda) de la dirección IP.

	0 1	8	16	24 31
Clase A	0	Número de Red	Número de host	
Clase B	10	Número de Red	Número de host	
Clase C	110	Número de Red	Número de host	
Clase D	1110	Dirección multicast		
Clase E	1111	Reservado		

Tabla 1 Clases de direcciones IPv4

Ernesto Ariganello [13] menciona:

> La RFC 1700[3] agrupa rangos de direcciones unicast en tamaños específicos llamados direcciones de clase. Las direcciones IPv4 se dividen en clases para definir las redes de tamaño pequeño, mediano y grande. Las direcciones Clase A se asignan a las redes de mayor tamaño. Las direcciones Clase B se utilizan para las redes de tamaño medio y las de Clase C para redes pequeñas. Dentro de cada rango existen direcciones llamadas privadas para uso interno que no veremos en Internet. Las direcciones de clase D son de uso multicast y las de clase E, experimentales.

2.1.2.2 Tipos de comunicaciones IPv4

Para los hosts existen tres maneras de comunicarse en una red IPv4:

[3] RFC 1700: Números asignados en protocolos, puertos y otros valores que se asignan en redes TCP/IP.

Unicast: "método que se envía paquete de un host individual a otro host individual. La comunicación unicast se usa para una comunicación normal de host a host, tanto en una red de cliente/servidor como en una red punto a punto." [13].

Broadcast: conexión multipunto en redes IP que permite llegar de forma automática a todos los usuarios de una red sin la necesidad de conocer las respectivas direcciones de destino. Esta conexión se establece mediante el uso de un broadcast IP reservada [14].

Multicast: "permiten el envío de datos desde un emisor a muchos receptores (uno-a-muchos), o desde muchos emisores a muchos receptores (muchos-a-muchos) si la gestión de los grupos se realiza de forma adecuada. Los envíos a muchos receptores se realizan de forma simultánea" [15].

Las clases de direcciones siempre se encuentran en una IP determinada, en un rango indicado el cual se va a mostrar en la tabla 2.

CLASE	Rango de direcciones	Máscara de red	Direcciones privadas
A	1.0.0.0 a 127.0.0.0	255.0.0.0 0/8	1.0.0.0 a 10.255.255.255
B	128.0.0.0 a 191.0.0.0	255.255.0.0 o /16	128.0.0.0 a 191.255.0.0
C	192.0.0.0 a 223.255.255.0	255.255.255.0 o /24	192.198.0.0 a 192.168.255.255
D	224.0.0.0 a 239.255.255.255	Uso multicast o multidifusión	
E	240.0.0.0 a 254.255.255.255	Uso experimental o científico	

Tabla 2 Clases de direcciones IPv4

2.1.3 Protocolos de Internet IPv6

El principal impulso de IPv6 es el aumento de direcciones, teniendo una longitud de 128 bits ubicadas en grupos de 16 bits dados en valores hexadecimales y a la vez están separados por dos puntos ":". "Puede utilizarse la notación comprimida de doble dos puntos ("::") para representar grupos de ceros consecutivos, pero sólo puede usarse una vez en la expresión (en la

secuencia más larga de ceros consecutivos)" [16]. En un formato de cada grupo lo ceros que se encuentres más a la izquierda se podrían suprimir.

IPv4	16 bit	8 bit	8 bit	
IPv6	48 bit		16 bit	64 bit

	Bits de la red asignado por el proveedor
	Bit de la subred autoasignados
	Host-Bits

Tabla 3 Esquema de direcciones IPv6 con subredes

2.1.3.1 Tipos de comunicaciones IPv6

Multicast: "Multi-difusión. En IPv6 no existen más las direcciones de broadcast. Para este propósito se deben utilizar direcciones de Multicast.

Prefijo/Rango: FF00::/8, FF00:: . . FFFF:...: FFFF" [16].

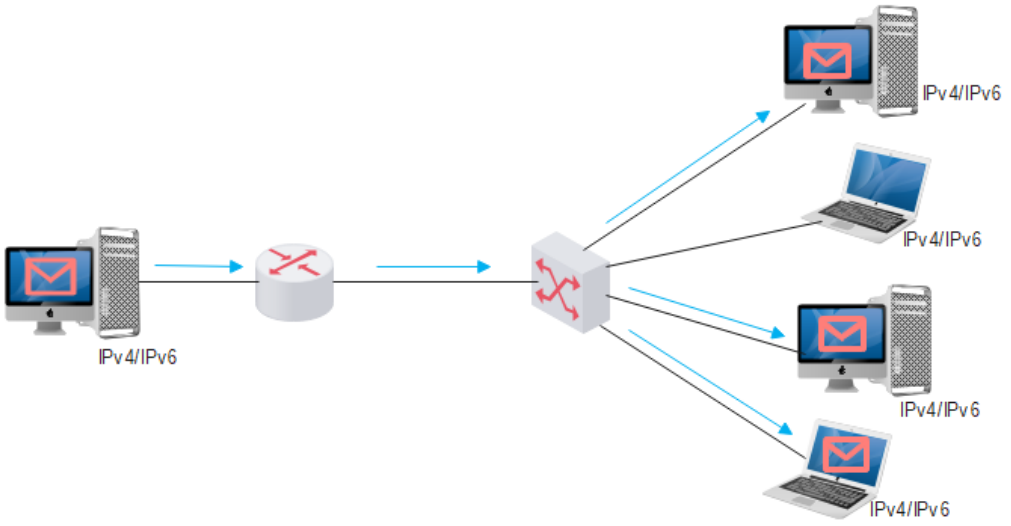


Figura 1 Funcionamiento de Multicast [17].

Anycast: "son direcciones especiales que indican un destino entre muchos posibles. Pueden ser utilizadas para cuestiones de balanceo de carga, por ejemplo, para consultar el DNS más cercano, o cualquiera dentro de un grupo de varios DNS" [16].

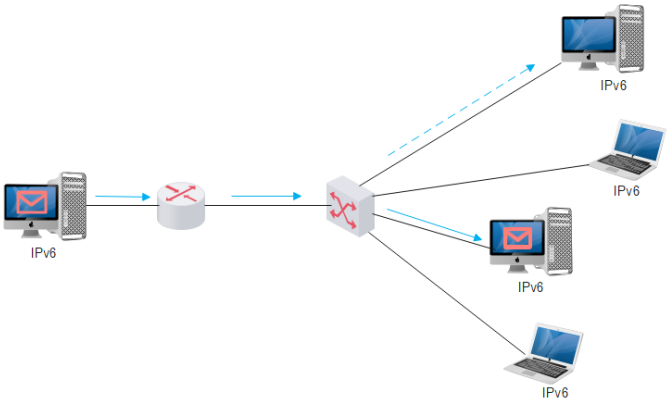


Figura 2 Funcionamiento de Anycast [17].

2.1.3.2 Tipos de direcciones

Alejandro Acosta *et al* [18] menciona, que:

> **Link local:** Las direcciones Link Local (o direcciones de Enlace Local) están definidas en el RFC 4291. Son utilizadas únicamente para direccionamiento unicast dentro de un mismo segmento de red, es decir, no son enrutadas, no pasan enrutadores. Su prefijo corresponde a FE8::/10 y su dirección puede ser construida de manera manual, automática derivada de un DHCP, de un algoritmo del S O entre otros. La manera actual es configurar esta dirección IP en base a algún tipo de algoritmo aleatorio para aumentar la seguridad y privacidad del usuario.

Loopback: "Los hosts utilizan la dirección de loopback para enviarse paquetes entre sí y no se puede asignar a una interfaz física. La dirección IPv6 de loopback está formada por todos ceros, excepto el último bit representado como ::1/128 simplemente ::1" [19].

6to4: "conecta hosts o sitios IPv6 a través de la infraestructura de Internet IPv4 existente. Usa prefijo de dirección único para proporcionar a los sitios IPv6 aislados su propio espacio de direcciones IPv6. 6to4 como un "pseudo-ISP" que proporciona conectividad IPv6" [20].

Documentación: "El prefijo utilizado mundialmente para documentación es 2001:db8::/32. La intención de esta dirección es utilizarla en libros, revistas,

documen-tación, ejemplos, entre otros. Este prefijo no debe ser utilizado en Inter-net ni como direcciones en nuestra red" [18].

[21] menciona, que:

> **Default Gateway**: Mientras que la puerta de enlace IPv4 utiliza direcciones de 32 bits, normalmente escritas como un conjunto de cuatro números decimales separados por puntos, la puerta de enlace IPv6 utiliza direcciones de 128 bits. En consecuencia, las direcciones IPv6 son mucho más largas y utilizan una configuración que se puede abreviar mediante los dos puntos dos veces y juntos (::) pero que desarrolladas serían, por ejemplo, 0000:0000:0000:0000:0000:ffff:cb00:7100.

[22] menciona, que:

> **No especifico (unspecified)** La dirección no especificada es 0:0:0:0:0:0:0:0. Puede abreviarla con dos puntos (::). La dirección no especificada indica la ausencia de una dirección y nunca puede asignarse a un host. Puede ser utilizada por un host IPv6 que aún no tenga una dirección asignada. Por ejemplo, cuando el host envía un paquete para detectar si otro nodo utiliza una dirección, utiliza la dirección no especificada como su dirección de origen.

2.1.4 Bridge y LAN/WAN

Brigde: "es un dispositivo de red de capa de datos. El puente conecta segmentos de red de diferentes topologías y arquitecturas. Los puentes de red reducen la carga en las redes, son extremadamente útiles para filtrar la carga de tráfico" [23].

LAN: "Para la interconexión de computadores personales y estaciones de trabajo Se caracterizan por tamaño restringido, tecnologia de transmisión, por lo general broadcast es decir, aquella en que a un sólo cable se conectan todas las máquinas, alta velocidad y topología" [24]. Mientras que la **WAN** es una "red de computadoras abarca varias ubicaciones físicas, proveyendo servicio a una zona,

un país, incluso varios continentes. Es cualquier red que une varias redes locales LAN, por lo que sus miembros no están todos en una misma ubicación física" [24].

2.1.5 Diferencia entre IPv4 e IPv6

Elena Limones [25] comenta sobre la diferencia entre IPv4 e IPv6:

> En IPv6 existirán únicamente Multicast, Unicast y Anycast. En IPv4 el Broadcast era un tráfico muy poco optimizado. Si teníamos una red muy grande con muchos dispositivos, cada vez que queríamos enviar un paquete este iba a todos. De esta forma, empleaba recursos de la red, tráfico y ancho de banda para procesar datos que nunca llegaban a ningún host, pero que a pesar de ello eran transmitidos por la red. En IPv6 esto será reemplazado por Multicast (transporte de un paquete de datos a un grupo de la red, de manera más optimizada).
>
> "El campo de "siguiente encabezado" es equivalente al de IPv4 y se utiliza para indicar qué protocolo sigue, incluyendo opciones como UDP o TCP" [25]. "UDP, es un protocolo más liviano, más simple de usar, no verifica el control de flujo, no verifica que los paquetes hayan llegado a destino como corresponde. Aunque, sin embargo, ofrece una facilidad de uso y es mucho más ligero" [26].

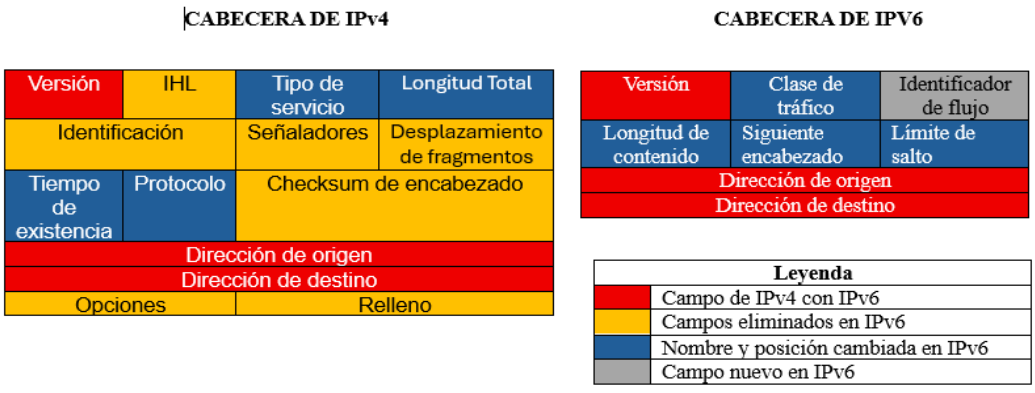


Figura 3: Diferencia entre la cabecera IPv4 e IPv6.

2.1.6 Ventajas de IPv6 Sobre IPv4

Dentro de las ventajas de IPv6 sobre IPv4 se pueden mencionar las siguientes: direcciones más largas, formatos de cabecera flexibles, fragmentación end-to-end, soporte para reserva de recursos, provisión de extensiones al protocolo y número

de saltos. Dentro de todos estos saltos, podemos decir que IPv6 cuadruplica todo el tamaño de IPv4 de 32 a 128 bits; también se considera la capacidad potencial para que el protocolo se adapte al hardware de la red [27].

2.1.7 Mecanismo de transición

Con el desafío del agotamiento de las direcciones IPv4, se ha comenzado la transición a IPv6. Los mecanismos de este cambio están diseñados para permitir que ambos protocolos operen simultáneamente por un tiempo determinado, facilitando así una adopción gradual de IPv6.

Para lograr una transición efectiva, es fundamental que el proveedor de servicios de Internet sea compatible con el direccionamiento IPv6. Si el proveedor no ofrece soporte, se deberá implementar IPv6 a través de túneles. Además, es importante que los dispositivos como enrutadores y conmutadores, responsables del enrutamiento, así como las computadoras y otros dispositivos finales, también sean compatibles con el protocolo mencionado.

2.1.7.1 Estrategias de transición IPv4 e IPv6

Yesica Maria Pérez Pérez y Andrés Mauricio Puentes Velásquez [28] mencionan:

> Debido a que IPv6 se diseñó sin compatibilidad, la transición de IPv4 a IPv6 necesita esencialmente una fase de "doble pila" durante la cual los hosts operen con ambas pilas de protocolos al mismo tiempo, utilizando la pila de protocolos IPv6 para hablar con otros hosts IPv6 y la pila de protocolos IPv4 a otros hosts IPv4. La disponibilidad (o la falta de ella) de direcciones IPv4 es, por lo tanto, un factor que continúa siendo importante durante el período de transición. Por el momento, no hay certeza sobre la duración de esta transición IPv4 / IPv6, expertos de LACNIC temen que el tiempo de esta transición se extienda indefinidamente.

2.1.7.2 Traducción de direcciones IPv6 a IPv4

"Consiste en utilizar algún dispositivo en la red que convierta los paquetes de IPv4 a IPv6 y viceversa. Ese dispositivo tiene que ser capaz de realizar la traducción en los dos sentidos de forma de permitir la comunicación" [29]. "La mayor parte de la

traducción de encabezados es sencilla. Por ejemplo, el campo "Protocolo" de IPv4 es básicamente el mismo que el campo "Siguiente encabezado" de IPv6. El campo "TTL" de IPv4 es el mismo que el campo "Límite de saltos" de IPv6, etc" [30].

Prefijo IPv6: "El prefijo de sitio de una dirección IPv6 ocupa como máximo los 48 bits de la parte más a la izquierda de la dirección IPv6. Por ejemplo, el prefijo de sitio de la dirección IPv6 2001:db8:3c4d:0015:0000:0000:1a2f:1a2b/48" [31]. Mientras que la **RFC (Request for Comments) "**describen los fundamentos técnicos de Internet, como las tecnologías de direccionamiento, enrutamiento y transporte. Las RFC también especifican protocolos como TLS 1.3, QUIC y WebRTC" [32].

DHCPv6: "Los paquetes DHCPv6 se transmiten a través de UDPv6. Los clientes DHCPv6 solo procesan paquetes DHCPv6 con el puerto UDP número 546. Los servidores DHCPv6 y los agentes de retransmisión solo procesan paquetes DHCPv6 con el puerto UDP número 547" [33].

Firewall IPv6: Activando la función de cortafuegos puede proteger su red de área local. El firewall puede segmentar la red en diversas zonas, cada una con diferentes permisos de acceso, lo que le permite limitar el acceso a ciertos servicios en la red, cumpliendo así con el objetivo de seguridad de las direcciones [34].

2.1.8 Mecanismo de transición

- Dual Stack
- Tunelización
- Traducción.

2.1.8.1 Dual Stack

Se refiere a la aptitud de un equipo dentro de una plataforma de comunicación tecnológica para implementar el protocolo TCP/IP, tanto en su versión 4 como en la 6. Este fue el enfoque inicial planteado para facilitar el cambio progresivo hacia IPv6. Para esto, es necesario tener un número adecuado de direcciones IPv4 para poder usar ambas versiones del protocolo a la vez en toda la red. Así, al conectarse a un destino que solo tiene IPv4, se usará la conexión IPv4, y si es hacia una dirección IPv6, se usará la red IPv6. Si el destino soporta ambos protocolos, se suele

intentar conectar primero por IPv6 y luego por IPv4, aunque esto ha cambiado para evitar problemas de tiempos de espera (ver “happy eyeballs”) [35].

2.1.8.2 Tunelización

Este tipo de sistema de transición consiste en encapsular paquetes IPv6 dentro de paquetes IPv4 y transportarlos a través de una infraestructura IPv4 existente para alcanzar su destino. Se utiliza cuando las redes no están utilizando IPv6, lo que implica que el tráfico IPv6 debe atravesar una red IPv4 ya existente. Esto se puede hacer utilizando la técnica de tunelización o tunneling. Encapsular paquetes IPv4 dentro de redes IPv6 también es factible, y este procedimiento se utiliza cuando las nuevas redes IPv6 que se crean todavía requieren conectividad a través de IPv4. El procedimiento general que un túnel sigue para la remisión de paquetes conlleva tres etapas: encapsulación, desencapsulación y administración del túnel [17].

2.1.8.3 Traducción

Para implementar este sistema de transición, es fundamental que un dispositivo presente en la red se encargue de transformar paquetes de IPv4 a IPv6 y viceversa, de modo que se pueda lograr una comunicación efectiva. Este enfoque de traducción es conocido como AFT (Traducción de la familia de direcciones), y su propósito es facilitar la transmisión de datos entre nodos que operan con IPv6 y aquellos que utilizan IPv4. Incluye dos tipos de traducción que se identifican como NAT-PT y NAT64. NAT-PT este concepto está especificado en la IETF RFC 2766. La traducción de direcciones de red y de protocolo se fundamenta en un enrutamiento que es transparente y permite convertir direcciones IPv4 a IPv6 sin requerir cambios en las aplicaciones de los protocolos previamente mencionados. Su función principal es establecer una conexión desde un host que utiliza IPv6 a uno que opera con IPv4 [17].

2.1.9 Segmentación de redes

2.1.9.1 DNS en redes IP

Domain Name System o DNS (sistema de nombres de dominio) conjunto de protocolos que nos permite a los usuarios obtener un único nombre para tener conexión a internet o a una red privada, teniendo como función llegar a la

traducción de los nombres intangibles al ser humano ya sea como los números binarios que se asocian al equipo que se encuentra conectado en la red de datos, esto se da con el fin de localizar y direccionar a la ruta que se le asigne [36].

2.1.9.2 Tipo de servidores DNS

Según [37], los tipos de servidores DNS pueden ser primarios o maestros y estos se clasifican como **secundarios o esclavos,** estos son lo que obtienen datos de los servidores principales que están en una transferencia zonal. Mientras, los **Locales o cache,** estos funcionan dentro del sistema operativo como el host, aún así no contienen los datos necesarios o bases para las resoluciones de los nombres. Estos sirven como transceptor ya que si se le hace una consulta esto a su vez consulta a los servidores DNS, que almacenan la respuesta en la base de datos para agilizar la respuesta en alguna futura consulta.

[36] menciona que:

> Existen diferentes tipos de registros utilizados para resolver nombres de dominio, los cuales contienen el nombre, la dirección y el tipo de registro. Algunos de estos de registros son los siguientes: A: Una dirección IPv4 de un dispositivo final, NS: Un servidor de nombres autorizado, AAAA: Una dirección IPv6 de un dispositivo final, MX: Un registro de intercambio de correo.

2.1.9.3 Tipos de resoluciones de nombres de dominio

RECURSIVA: Esto se da cuando un servidor recibe una consulta, obligado a responder con los datos que se están solicitando o a su vez especifica el error dentro del dominio o menciona que no existe el tipo de datos, dentro de esta existen las respuestas de consultas en el registro CNAME y cuando dice que no hay error o host no existe NXDOMAIN, mientras que las consultas **ITERATIVA:** esto se da cuando se obtiene una respuesta parcial o un error dado antes de la consulta. El servidor encargado da solución a la consulta realizada iterativamente por los diferentes servidores DNS [37].

2.1.9.4 Tipos de Registros DNS

- "A= Address – (Dirección): registro para traducir nombres de servidores de hospedaje a direcciones IPv4" [35].
- "AAAA= Address – (Dirección): Registro utilizado en IPv6 para la traducción de nombres de hosts a direcciones IPv6" [35].
- "CNAME= Canonical Name – (Nombre Canónico): El registro CNAME se usa para renombrar servidores como alias, especialmente para los de alojamiento de un dominio. Es muy importante especialmente si se están ejecuta múltiples servicios como ftp, web, entre otros en un servidor con una misma dirección IP" [35].
- "NS= Name Server – (Servidor de Nombres): Precisa la sociedad que existe entre un nombre de dominio y un DNS, es decir este registro especifica cual servidor DNS es autoritativo para el dominio solicitado" [35].
- "MX (registro)= Mail Exchange – (Registro de Intercambio de Correo): Se utiliza para el intercambio de correo, asocia un nombre de dominio a un listado de servidores de correo. Con la utilización del balanceo de carga, prioriza la utilización del o los servidores de correo específicos" [35].
- "TXT= TeXT – (Información textual): Contiene información de texto adicional, permite a los dominios identificarse en la red. Es utilizado, también, para verificar la procedencia de un dominio" [35].
- "SPF= Sender Policy Framework: Contribuye a prevenir el envío de correo no deseado (spam). Este registro indica qué servidores o equipos están autorizados para enviar correos electrónicos en nombre del dominio correspondiente. El servidor que recibe consulta SPF para comparar IP desde la cual le llega con los datos de este registro" [35].

2.1.9.5 Diferencias en el manejo de DNS para IPv4 e IPv6

Aunque IPv6 prometía más seguridad, varios ataques siguen siendo posibles como spoofing en solicitudes de capa de enlace, rastreo de nodos, etc y ha requerido contramedidas específicas [38]. Los mecanismos de transición (como túneles automáticos) introducen vectores de ataque, ya que pueden expander fallos o brechas de seguridad inherentes a IPv4 dentro de entornos IPv6 [39].

Mikrotik hex S: "es un router Gigabit Ethernet de cinco puertos para ubicaciones donde no se requiere conectividad inalámbrica. A diferencia del hEX, el hEX S también incluye un puerto SFP y una salida PoE en el último puerto" [40]. Mientras, **Winbox** "es una aplicación de Mikrotik RouterOS que nos permite administrar los equipos usando una interfaz gráfica. Incluye una sofisticada tecnología para realizar estas conexiones basada en el sistema operativo de RouterOS" [41].

Wireshark: una herramienta de análisis de paquetes de red que permite capturar y examinar el tráfico de datos con un alto nivel de detalle. Funciona como un instrumento de diagnóstico que muestra lo que ocurre dentro de un cable o conexión de red. Este programa se distribuye bajo la Licencia Pública General de GNU (GPL), lo que significa que es de código abierto y puede ser utilizado y modificado libremente [42].

2.2 Marco teórico

2.2.1 Fundamentos de redes y protocolos

En la actualidad, debido al aumento masivo en la cantidad de dispositivos que se conectan a internet, se ha vuelto importante cambiar al protocolo IPv6. Dado que ambos protocolos se ejecutarán juntos durante el cambio, necesitamos estrategias tecnológicas para asegurarnos de que todo siga funcionando bien en conjunto y de que los servicios no se interrumpan. Este estudio analiza los conceptos básicos, los métodos y la tecnología que necesitará para una transición paso a paso de IPv4 a IPv6, especialmente en configuraciones administradas como el laboratorio de redes (FACSISTEL) de la UPSE.

2.2.1.1 Porque migrar IPv6 Sobre IPv4

La migración de IPv4 a IPv6 es muy importante debido al agotamiento de las direcciones de IPv4 y a la vez por el crecimiento masivo de la conectividad global. IPv6 no solo es un espacio de direcciones infinitas, sino que también tiene entre sus virtudes mejores aspectos como la autoconfiguración, la eficiencia en el enrutamiento y la seguridad del protocolo, caso contrario es que, si nos mantenemos en IPv4 implicar depender de soluciones NAT, siendo esta un modelo de

comunicación de extremo a extremo que dificulta y rompe la integración en las nuevas aplicaciones. Con la transición, aunque sea progresiva, es impredecible para garantizar el soporte en la red [43].

Existen múltiples formas de hacer la migración a IPv6, siendo uno de los métodos que se adapta a diferentes escenarios y necesidades técnicas. Entre ellas existen las redes pilas (Dual Stack), estas permiten la coexistencia de IPv4 a IPv6, así mismo tenemos los mecanismos de túnel, tales como 6to4, GRE, IPIPv6, estos encapsulan paquetes de IPv6 en redes IPv4. La elección técnica depende del control que se desee tener en la infraestructura y compatibilidad [43].

2.2.1.2 Mecanismo de migración

Para llevar a cabo la transición de IPv4 a IPv6 se van a aplicar los métodos de conversión son cruciales si se necesita comunicación entre equipos que usan únicamente una de las dos versiones del protocolo, dado que IPv4 e IPv6 no son compatibles de forma directa. Esta clase de cambio funciona como un conector que modifica las direcciones y encabezados entre los dos formatos, garantizando que la información se pueda enviar y recibir sin que las aplicaciones finales noten variaciones en su operación. Entre las soluciones más comunes están túnel, que convierte direcciones IPv6 a IPv4 en la capa de red, dando posibilidad que clientes IPv6 accedan a servicios IPv4, y DNS, este servicio apoya el proceso creando registros inventados para nombres que solo tienen registros [44].

El mecanismo que más se utiliza es el Dual Stack que consiste en ejecutar los protocolos IPv4 e IPv6 en los mismos dispositivos y redes con este modelo permite que los equipos seleccionen automáticamente el protocolo adecuado que les permitan tener coexistencia ambos tipos de direccionamiento. Otro método es el Túnel IPIPv6, que se emplea para transportar paquetes IPv6 a través de una red IPv4 que ya existente con este mecanismo podemos encapsular los paquetes IPv6 dentro de cabeceras IPv4, que nos permite atravesar infraestructuras que

aún no soportan IPv6 de forma nativa. Con su implementación nos permitirá tener escenarios de migración progresiva, donde se busca conectar segmentos IPv6 separados mediante una red IPv4 intermedia [44].

2.2.1.3 Normas y estándares

El marco de apoyo para la migración de IPv4 a IPv6 ofrece una forma ordenada de trabajar que ayuda a reconocer y eliminar todo lo que todavía depende del protocolo IPv4 en los sistemas y programas. Este enfoque revisa el sistema en su conjunto, considerando todas las etapas de su desarrollo y no solo el código. A través de metarreglas predefinidas que son diseñadas según el contexto del producto, se detectan de manera precisa las áreas donde IPv4 está presente, lo que facilita priorizar acciones de corrección y adaptación [45].

2.2.1.4 Elección y mecanismo de transición a utilizar

La selección del mecanismo de transición para este proyecto se fundamentó en un análisis previo de los diferentes mecanismos en uso actualmente, así como en aquellos que se han aplicado en varias universidades del país. Se resaltaron los resultados alcanzados en cada caso, junto con las ventajas y desventajas de cada mecanismo y su operatividad.

Es relevante señalar que el proyecto utiliza equipamiento de la marca Mikrotik, por lo que se llevó a cabo una investigación sobre los tipos de mecanismos de transición que son compatibles. En esta investigación se descubrió que los dispositivos de Mikrotik para la transición específica permiten la configuración de Dual Stack y tunelización, y para el túnel, se aceptan opciones como Tunnel Broker y IPIPv6.

Al observar las ventajas y desventajas de los mecanismos de transición para los equipos de Mikrotik y teniendo en cuenta que el Proveedor de Internet de la universidad no proporciona un prefijo IPv6 a la institución, se tomó la decisión de utilizar el método de tunelización. Esto se debe a que, a través de un proveedor de tunnel broker, es posible obtener un bloque de direcciones IPv6 con un prefijo de /64.2.3 Metodología del proyecto.

2.3.1 Metodología de investigación

En el desarrollo del trabajo de investigación se va a desarrollar con un enfoque cuantitativo y un tipo de investigación experimental. En el que se va a realizar un prototipo de migración progresiva de IPv4 a IPv6 en el laboratorio de redes de FACSISTEL. Dentro de la metodología se consideran varias fases como recolección de datos, diseño, implementación y pruebas de funcionalidad IPv6. Con estos resultados se podrá validar la eficiencia del prototipo, además se contribuirá con un manual técnico para su futura implementación.

Esta investigación adopta un enfoque cuantitativo, centrado en la medición objetiva de factores vinculados al desempeño y eficacia del prototipo propuesto. De esta manera, se consiguen datos tangibles del comportamiento de la red, tanto antes como después de la modificación del protocolo IPv4 al IPv6. Para ello, se va a emplear herramientas de análisis como pruebas de conectividad, latencia, pérdida de paquetes. Además, con el estudio completa aspectos del enfoque aplicado ya que su propósito es solucionar un desafío técnico en particular mediante el diseño de un prototipo práctico en un contexto real de laboratorio.

Esta investigación es de tipo experimental porque implica la crear, configuración y valorar el modelo práctico de la transición progresiva de IPv4 a IPv6 en el que se emplea métodos de transición como túneles. La experimentación se llevará a cabo en un entorno controlado, el laboratorio de redes de la Facultad de Sistemas y Telecomunicaciones (FACSISTEL), lo cual posibilita la manipulación de variables independientes (métodos de transición y configuración de la red) para evaluar los efectos en las variables dependientes (conectividad, rendimiento, compatibilidad).

Las fases que se van a involucrar son las siguientes:

Fases de recolección de datos.

Esta fase tiene como finalidad obtener información relevante que sirva de base para el diseño del prototipo de migración del protocolo IPv4 a IPv6, considerando tanto aspectos técnicos como la experiencia de los usuarios del laboratorio.

Para ello, se utilizará un muestreo no probabilístico por conveniencia estratificada, aplicando una encuesta dirigida a los estudiantes de los diferentes niveles académicos que utilizan regularmente el laboratorio de redes (ver Anexo 1). Esta encuesta nos permitirá identificar las necesidades, así como las limitaciones existentes en la infraestructura de IPv4, siendo un obstáculo en la práctica relacionados con IPv6.

También se llevará a cabo una revisión bibliográfica en el que se obtenga información sobre la migración de IPv4 a IPv6 en la que se incluya casos de éxito, métodos aplicados en otras instituciones educativas y estándares técnicos internacionales.

- Aplicación de encuestas a estudiantes usuarios del laboratorio.
- Identificación de limitaciones técnicas y pedagógicas en la infraestructura de red IPv4.
- Revisión documental sobre métodos de transición IPv6 aplicados en entornos académicos.

Fase de diseño.

En esta etapa se definirán las estrategias que se van a realizar durante la migración. Aquí se procederá a elegir la metodología más adecuada para la transición progresiva de IPv4 a IPv6 teniendo en consideración la realidad del laboratorio y los equipos disponibles.

- El diseño contemplará aspectos clave como el esquema de direccionamiento IPv6, la configuración de protocolos de enrutamiento, y criterios de seguridad para proteger el entorno de pruebas, como el uso de firewall y hotspot.
- Selección de metodologías de transición: Dual Stack, Túneles.
- Definición del esquema de direccionamiento IPv6 (prefijos, subredes, asignación).
- Consideraciones de seguridad en la arquitectura (firewall, control de tráfico).

Fase de implementación.

En esta fase se procederá a la configuración y se iniciará con el prototipo de migración en la que se aplique la metodología de transición seleccionada. Se realizará la instalación de IPv6 en los dispositivos disponibles, la activación de túneles y el ajuste necesarios para garantizar la coexistencia funcional de los protocolos IPv4 e IPv6.

Durante esta etapa se documentará cada procedimiento técnico mediante capturas de configuración, con el fin de facilitar la elaboración del manual técnico.

- Instalación y configuración de ipv6 en los diferentes dispositivos de la red.
- Configuración de los túneles y activaciones de los modos para la coexistencia de protocolos.
- Pruebas de conectividad.

Fase de pruebas de funcionalidad IPv6

Una vez implementado el prototipo, se ejecutarán pruebas de funcionalidad, rendimiento y compatibilidad, con el objetivo de validar el correcto funcionamiento del entorno IPv6 y comparar las métricas obtenidas con el estado previo en IPv4. Se realizarán pruebas de conectividad local y remota en la que se verificará el tráfico en (IPv4 e IPv6) donde se recopilarán métricas y los resultados se analizarán en un informe final que incluirá conclusiones y recomendaciones para futuras implementaciones.

- Pruebas de conectividad local.
- Comparación de las métricas claves antes y después de la migración.
- Verificación del tráfico simultáneo en IPv4 e IPv6 (Dual Stack).
- Elaboración de informe técnico con resultados, análisis y recomendaciones.

Idea a defender

El modelo de migración progresiva del protocolo de redes IPv4 a IPv6 aplicado en el laboratorio de Redes, me permite evaluar de manera efectiva el funcionamiento de ambos protocolos, midiendo los indicadores como el tiempo de respuesta y la cantidad de paquetes enviados. Con estos resultados es posible demostrar que IPv6

ofrece mejoras significativas tanto en rendimiento como en el manejo de tráfico, con esto se puede validar el funcionamiento del modelo propuesto para procesos de transición en entornos académicos.

2.3.2 Técnicas e instrumentos de recolección de datos

En este proyecto los datos necesarios para el diagnóstico y análisis de la migración del protocolo IPv4 a IPv6 serán recolectados a través de diferentes técnicas. Los datos se obtendrán mediante encuestas dirigidas a los estudiantes en el laboratorio de redes de los diferentes semestres que realizan prácticas la Facultad de Sistemas y Telecomunicaciones. La encuesta tiene como objetivo conocer el nivel de uso, satisfacción y percepción del servicio de internet dentro de los laboratorios.

La encuesta con muestreo no probabilístico por conveniencia estratificada se va a aplicar en 4 semestres que utilizan el laboratorio del cual se va a elegir el 50% de estudiantes de cada asignatura, teniendo como resultado un total de 111 estudiantes. A continuación, se mencionarán los semestres, la asignatura y la cantidad de estudiantes.

SEMESTRE	ASIGNATURA	N° ESTUDIANTES	50% ESTUDIANTES
TERCER	Fundamentos de redes	24	12
CUARTO	Comunicación y enrutamiento de datos	28	14
	Ingeniería en software	44	22
SEXTO	Ethical hacking	27	13
	Internet de las Cosas	28	14
	Arquitectura y plataforma TI	44	22
SEPTIMO	Computación Forense	25	13
	Seguridad de TI	22	11
Total		**221**	**111**

Tabla 4 Cantidad de estudiantes a los que se les realizará la encuesta

2.3.2.1 Análisis de resultados de la encuesta

¿Ha trabajado o estudiado alguna vez con el protocolo IPv6?
○ Sí ○ No ○ Tal vez

Respuesta	Total	Porcentaje %
Si	85	76,6
No	11	9,9
Tal vez	15	13,5
Total	111	100%

Tabla 5 Uso de IPv6

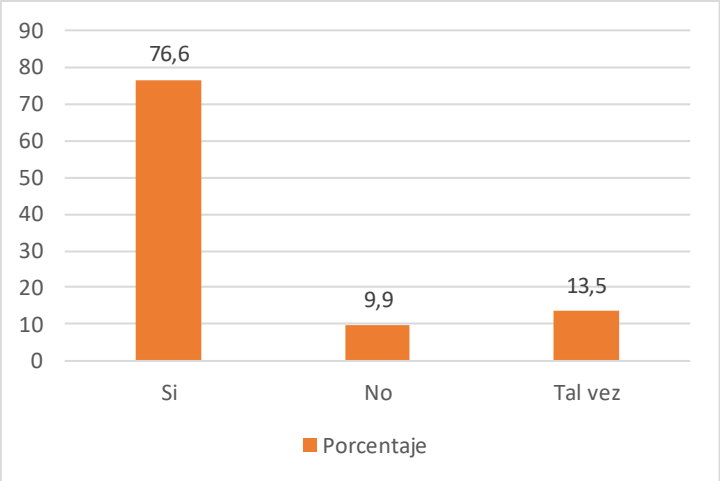


Figura 4 Uso de IPv6

INTERPRETACIÓN: Con el análisis de los estudiantes encuestados, podemos determinar que el 76,6 % de los estudiantes sí han trabajado con IPv6, el 9,9 % no, mientras que TAL VEZ el 13,5 %, como muestra la Figura 4. Es aquí donde la mayoría de los estudiantes encuestados ya ha tenido contacto con IPv6 (Tabla 5).

CONCLUSIÓN: Los resultados reflejan un nivel de familiaridad creciente con el protocolo. Esto facilita la implementación de un modelo experimental en el laboratorio, ya que los usuarios no parten de cero.

¿Está al tanto de que el laboratorio de redes solo opera actualmente con protocolo IPv4?
○ Sí ○ No ○ No estoy seguro/a

Respuesta	Total	Porcentaje %
Si	99	89,2
No	8	3,6
Tal vez	4	7,2
Total	111	100%

Tabla 6 Laboratorio solo opera con IPv4

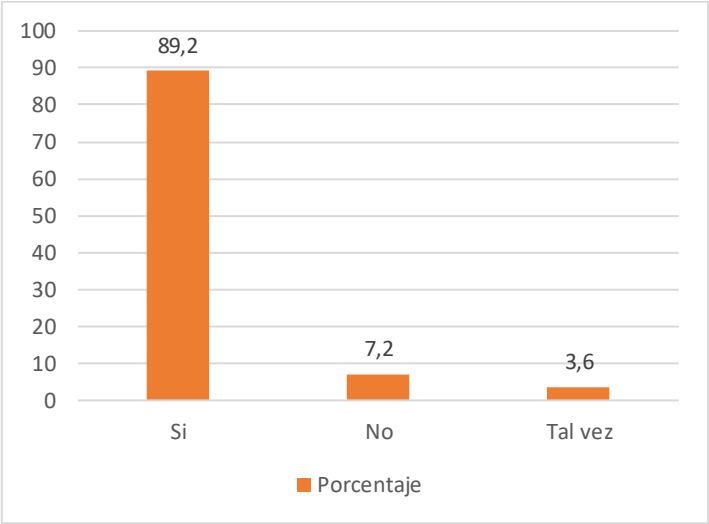


Figura 5 Laboratorio solo opera con IPv4

INTERPRETACIÓN: Los datos nos muestran, con el 89,2% (Figura 5), que la mayoría de los estudiantes están enterados de que el laboratorio solo opera en IPv4, datos obtenidos de la Tabla 6.

CONCLUSIÓN: Con los datos podemos verificar que los 99 estudiantes están enterados de qué protocolo se maneja en el laboratorio.

¿Considera importante que el laboratorio implemente soporte completo para IPv6?
○ Sí ○ No ○ No estoy seguro/a

Respuesta	Total	Porcentaje %
Si	96	90,6
No	2	1,9
Tal vez	13	7,5
Total	111	100%

Tabla 7 Laboratorio solo opera con IPv4

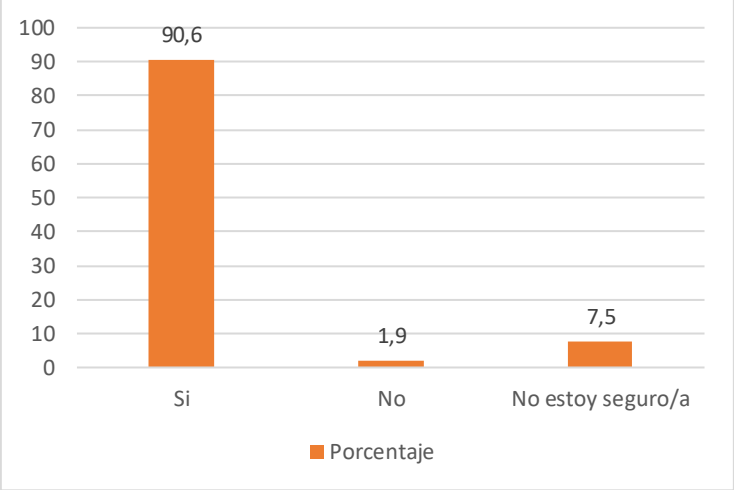


Figura 6 Laboratorio solo opera con IPv4

INTERPRETACIÓN: El 90,6 % están de acuerdo con la implementación del protocolo IPv6 en el laboratorio mientras que el 7,5 % no está seguro (Figura 6) (Tabla 6).

CONCLUSIÓN: Los usuarios del laboratorio de redes de FACISTEL están de acuerdo con la implementación del protocolo de IPv4 a IPv6.

¿Crees que el uso de IPv6 mejoraría la calidad del aprendizaje en redes?
○ Sí ○ No ○ Tal vez

Respuesta	Total	Porcentaje %
Si	97	87,4
No	0	0
Tal vez	14	12,4
Total	111	100%

Tabla 8 El uso de IPv6 mejorará el aprendizaje

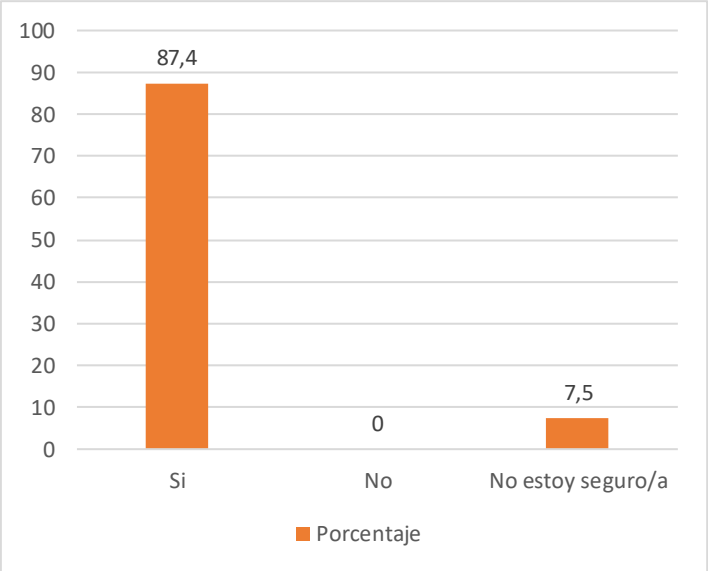


Figura 7 El uso de IPv6 mejorará el aprendizaje

INTERPRETACIÓN: considera el 87,4 % de los estudiantes que la implementación de IPv6 mejorará el aprendizaje, aunque el 7,5 % no está seguro, como muestra la Figura 7 en referencia a la Tabla 8.

CONCLUSIÓN: Se considera que el uso de IPv6 sería de gran ayuda, ya que nos permitirá aprender nuevas formas de estudio.

¿Consideras que aprender IPv6 es necesario para tu formación profesional en telecomunicaciones y sistemas?
○ Sí ○ No ○ No lo sé

Respuesta	Total	Porcentaje %
Si	103	92,8
No	0	0
Tal vez	8	7,2
Total	111	100%

Tabla 9 Considera que aprender IPv6 es necesario para la formación profesional

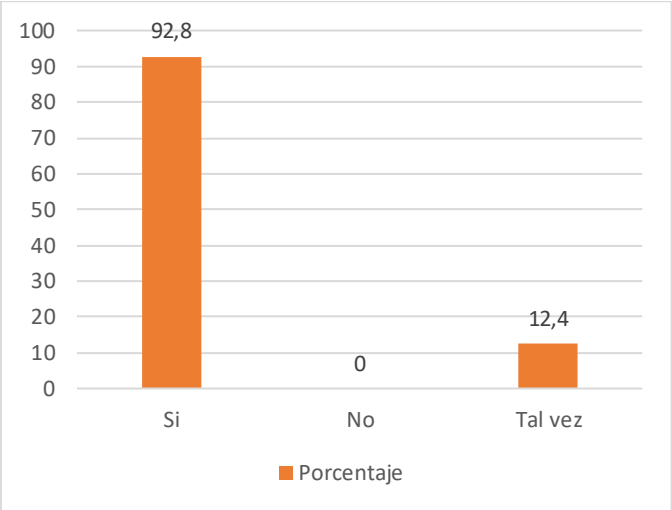


Figura 8 Considera que aprender IPv6 es necesario para la formación académica

INTERPRETACIÓN: consideran que el 92,8% debe aprender IPv6 ya que es útil para la formación académica, mientras que el 12,4% (Figura 8) tiene cierta duda sobre si debería estudiar o no (Tabla 9).

CONCLUSIÓN: Con la totalidad de los encuestados se puede determinar la importancia de implementar los protocolos IPv6 en el laboratorio, ya que nos ayuda tanto en conocimiento; sobre todo, es un plus para la formación profesional.

Con relación a la migración a IPv6, ¿considera que las condiciones técnicas del laboratorio permiten mantener un desempeño óptimo en términos de control de acceso y velocidad de transferencia de datos?
○ Sí ○ No ○ No lo sé

Respuesta	Total	Porcentaje %
Si	100	90,1
No	0	0
Tal vez	11	9,9
Total	111	100%

Tabla 10 Condiciones técnicas, control de acceso y velocidad de transferencia de datos

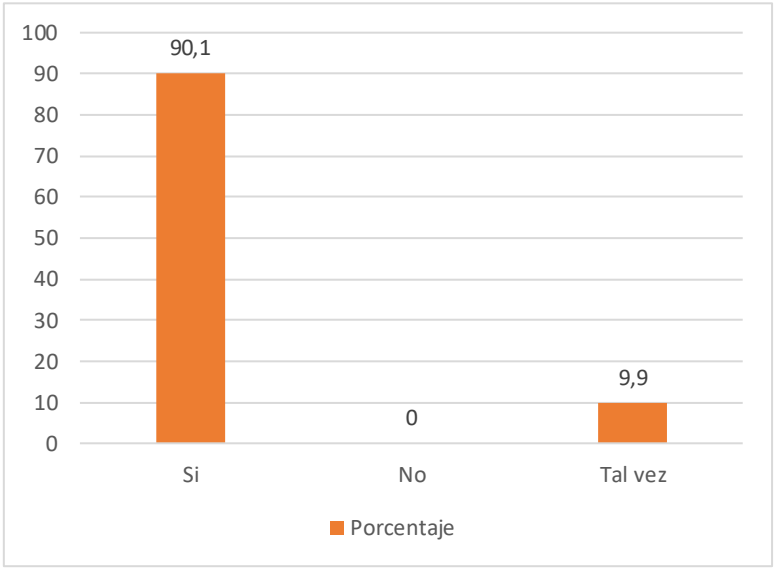


Figura 9 Condiciones técnicas, control de acceso y velocidad de transferencia de datos

INTERPRETACIÓN: El 98,75% está de acuerdo con las condiciones técnicas de la implementación de IPv6, mientras que el 9,9% tal vez está de acuerdo en referencia a la Figura 9.

CONCLUSIÓN: Con la totalidad de encuestado podemos ver que tan factible tener en cuenta los controles de acceso y el análisis de velocidad.

¿Cree que sería beneficioso implementar un modelo de prueba para la transición de IPv4 a IPv6 en el entorno del laboratorio de forma controlada?
○ Sí ○ No ○ Depende del presupuesto

Respuesta	Total	Porcentaje %
Si	103	87,4
No	0	0
Tal vez	8	12,6
Total	111	100%

Tabla 11 Beneficios para implementar un modelo de transición IPv4 a IPv6

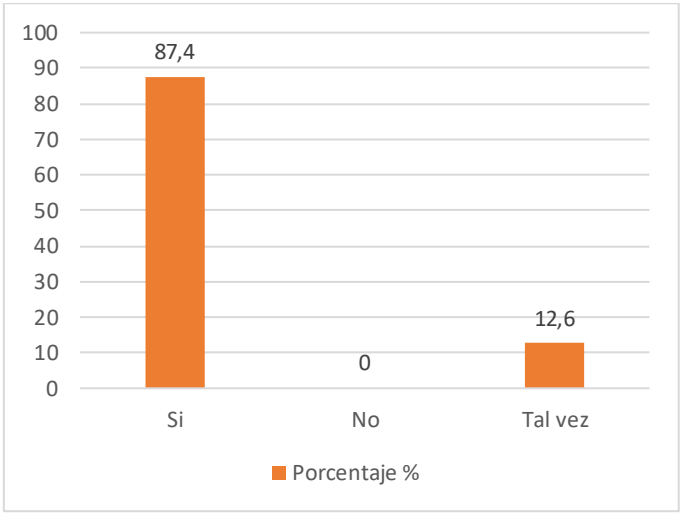


Figura 10 Beneficios para implementar un modelo de transición IPv4 a IPv6

INTERPRETACIÓN: El 87,4% de los usuarios encuestados manifiestan que la implementación de los protocolos se debe hacer y el 12,6% (Figura 10) no se decide si implementar o mantenerse como está en la Tabla 11.

CONCLUSIÓN: Los usuarios en su totalidad admiten que es beneficioso implementar el modelo de transición de IPv4 a IPv6.

2.3.3 Metodología de desarrollo

Este trabajo va a constar de cuatro fases las cuales son necesarias para la correcta implementación de migración de ipv4 a ipv6 para esto se acogió a las fases implementadas en los casos de estudio denominado, "Propuesta para la migración del protocolo ipv4 a protocolo ipv6 para la secretaria del sisben de la alcaldia de tunja" [5]. Por ello, Montañez Prieto Juan [5] indica las fases de este proyecto que consta de tres fases: "Planeación, Implementación del Protocolo IPV6 y Prueba de funcionalidad IPv6". Considero que estas fases son importantes, ya que me ayudarán a hacer la migración en el laboratorio de redes.

Siguiendo con la elección de fases que van a ser de consideración para el desarrollo de migración, se tomó como referencia el tema "Propuesta para la migración del protocolo ipv4 a ipv6 en la infraestructura tecnológica de una organización: caso de estudio" [7]. Esta tesis para su desarrollo consta de seis fases Investigación sobre informacion existente del tema; Según Cajamarca Remache Diana [7] indica el "Diseño del sistema general considerando los protocolos de enrutamiento, Reconocimiento de los requisitos que estructuran, Adquisición de herramientas, plataforma, Propuesta de las Metodologías Double Stack Y Tunelización y Diseño del plan de implementación con un manual de instrucciones", con las fases de los dos trabajos de titulación mostrada voy a unificar las fases que me van a ayudar a realizar mi trabajo.

El presente trabajo se desarrollará con un enfoque cuantitativo y un tipo de investigación experimental, en el que se va a enfocar en cuatro fases de las dos metodologías utilizadas en las tesis mencionadas, las cuales fueron adaptadas para realizar mi proyecto. A continuación, procederé a describir.

- **Fases de recolección de datos.** - se procederá a recolectar los datos a través de encuesta [7].
- **Fase de diseño. –** Se va a diseñar un sistema que nos permita los protocolos de enrutamiento en esta fase se va a determinar herramienta, desarrollo y bloque de direcciones IPv6 [7].

- **Fase de implementación. -** configurar la metodología elegida (Dual Stack, Tunelización) para asegurar la coexistencia entre IPv4 e IPv6 y asegurar que haya tráfico en las dos direcciones [7].
- **Fase de pruebas de funcionalidad IPv6.** - se harán pruebas de ping y tiempo de respuesta, además se generará manual de técnico donde se demuestre el proceso de migración de IPv4 a IPv6 [7].

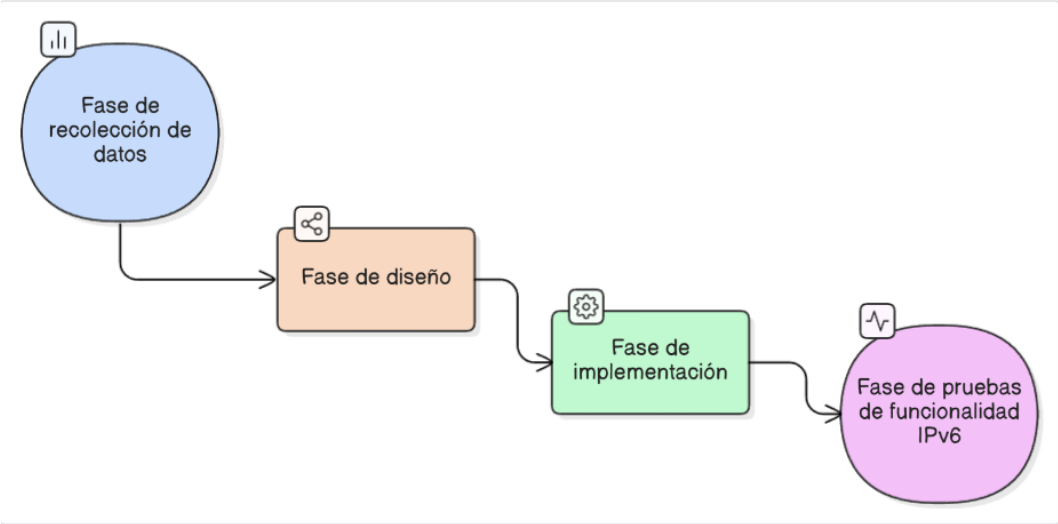


Figura 11 Fases de migración IPv4 e IPv6

CAPITULO III

3. Requerimientos

3.1 Requerimientos funcionales

CÓDIGO	DESCRIPCIÓN
Req-01	Habilitar Dual Stack entre IPv4 e IPv6 en segmentos del laboratorio
Req-02	Permitir pruebas de IPv6 en un segmento de pruebas
Req-03	Proveer al menos un túnel transportando tráfico IPv6.
Req-05	Asignar direcciones IPv6 vía DHCPv6.
Req-04	Debe hacer troubleshooting con ping
Req-05	Implementar firewall IPv6 filtros de entrada/salida y ND.
Req-06	Disponer de documentación con pasos reproducibles
Req-07	El sistema debe garantizar un tiempo de respuesta menor a 50 ms en la red local y no mayor a 150 ms en conexiones externas vía IPv6, para asegurar la calidad del servicio durante las pruebas de migración.
Req-08	El sistema debe integrar Hotspot para manejo de conexión y desconexión de la red sin perder el acceso de internet por cable ethernet
Req-09	Emitir informe final con hallazgos y mejoras propuestas.

Tabla 12 Requerimientos funcionales

3.1.1 Requerimientos no funcionales

CÓDIGO	DESCRIPCIÓN
Req-01	Los servicios del prototipo estarán operativos ≥ 95% del horario de laboratorio.
Req-02	Coexistencia sin impactos con la infraestructura IPv4 existente
Req-03	Manuales actualizados por versión; cambios con control de revisiones.
Req-04	El prototipo debe funcionar con el hardware y software actual del laboratorio (routers, switches, PCs, VMs).

CÓDIGO	DESCRIPCIÓN
Req-05	Debe incluir reglas básicas de firewall IPv6 para proteger los nodos de accesos no autorizados.
Req-06	El prototipo debe garantizar estabilidad durante las prácticas, minimizando caídas de conexión.

Tabla 13 Requerimientos no funcionales

Requisito de hardware

DISPOSITIVO	ESPECIFICACIÓN TECNICA	DESCRIPCIÓN FUNCIONAL
MIKROTIK HEX S	- Router con 5 puertos Gigabit Ethernet - 1 puerto SFP para fibra - CPU Dual Core 880 MHz - RAM: 256 MB - Soporta IPv4 e IPv6 - RouterOS con licencia. L4	Permite administrar la red e implementar esquemas de transición IPv4/IPv6 (dual stack, túneles) también aplicar reglas de firewall en un entorno de laboratorio académico.
PANTALLA	Monitor LED/LCD 56pulg" resolución 1366x768 o superior	Visualizar la interfaz de administración, configuración de servicios y resultados de pruebas de red.
CPU	- Procesador AMD Ryzen 5 - 8 GB RAM mínimo - 256 GB SSD - Tarjeta de red Gigabit - Sistema operativo: Windows	Equipo principal para ejecutar herramientas de análisis y simulación.
TECLADO	Teclado estándar USB	Permite la interacción y configuración manual de los equipos de laboratorio.
CABLE UTP	- Par trenzado, Cat6, con conectores RJ-45 - Soporte hasta 1 Gbps en 100 m.	Medio físico para interconectar el router MikroTik, CPU y demás dispositivos de red, asegurando estabilidad en las pruebas

Tabla 14 Requisitos de hardware para la migración de protocolos

Requisito de software

SOFTWARE	DESCRIPCIÓN FUNCIONAL
WINBOX	Herramienta gráfica de MikroTik para administrar y configurar el router de forma local, con interfaz amigable.
CLI MIKROTIK	Consola de comandos integrada en RouterOS que permite realizar configuraciones avanzadas, scripts y de pruebas.
WIRESHARK	Analizador de tráfico de red que nos permite capturar y examinar paquetes IPv4/IPv6 además, validar resolución DNS, ataques o anomalías.
NAVEGADORES WEB	Pruebas de resolución en entornos dual-stack y validación en clientes.

Tabla 15 Requisito de software de migración

3.2 Fase de recolección de datos

3.2.1 Objetivos de la encuesta

La encuesta realizada tuvo como finalidad recopilar datos que me permitieran evaluar las condiciones del laboratorio de redes, con énfasis en la infraestructura y su entorno para migrar los protocolos de red IPv4 a IPv6. Con las respuestas se pueden identificar las opciones y oportunidades para tener mayores oportunidades de prácticas académicas. Los datos que se obtuvieron serán utilizados en el entorno académico y se garantizará la confidencialidad de los estudiantes.

3.2.2 Levantamiento de información

Una vez aplicada la encuesta con la modalidad de muestreo no probabilístico por conveniencia estratificada a los estudiantes que hacen uso del laboratorio de Redes, con los resultados obtenidos, demuestra la necesidad de experimentar con nuevos

retos en el entorno de IPv6 dentro del laboratorio. Los resultados obtenidos son fundamentales para poder dar respaldo a la propuesta.

3.2.3 Presupuesto

Para la implementación del prototipo de migración de IPv4 a IPv6 en el laboratorio de redes de FACSISTEL, se considera como equipamiento principal un router MikroTik hEX S RB760IGS con un costo de USD $110, el cual permitirá configurar y simular los diferentes mecanismos de transición (Dual Stack y Tunneling). También, se contemplan otros recursos esenciales para el desarrollo y validación del modelo, tales como cables de red UTP categoría 6 (USD $8), que garanticen una conexión estable.

3.2.4 Recolección de datos de Dual Stack y túnel.

Figura 12 Conexión del equipo mikrotik al cable ethernet de la red de la universidad.

Se utilizo la interfaz gráfica del equipo mikrotik CLI y se inició con las credenciales del equipo mismo, una vez hecha la primera configuración se procede a configurar uno de los diferentes tipos de transición en este caso el Dual Stack, mostrando la coexistencia entre los dos puntos que se mostrara en la Figura 13, aquí podemos ver el funcionamiento de la IPv4 e IPv6 por medio del CMD de la laptop.

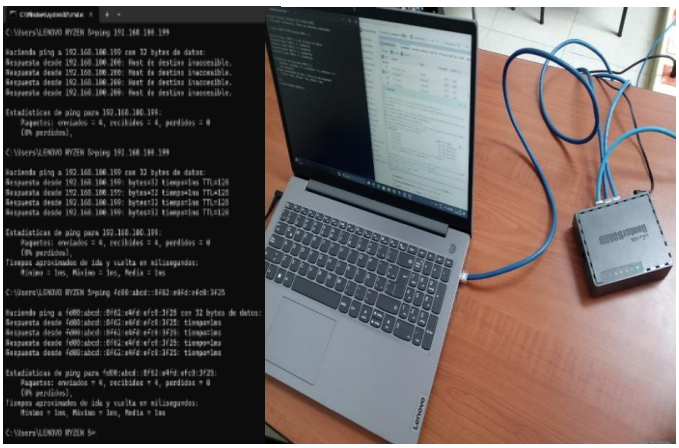


Figura 13 Método Dual Stack

En la Figura 14 se hicieron más pruebas de enlace Dual Stack en las que se comprueba su funcionalidad.

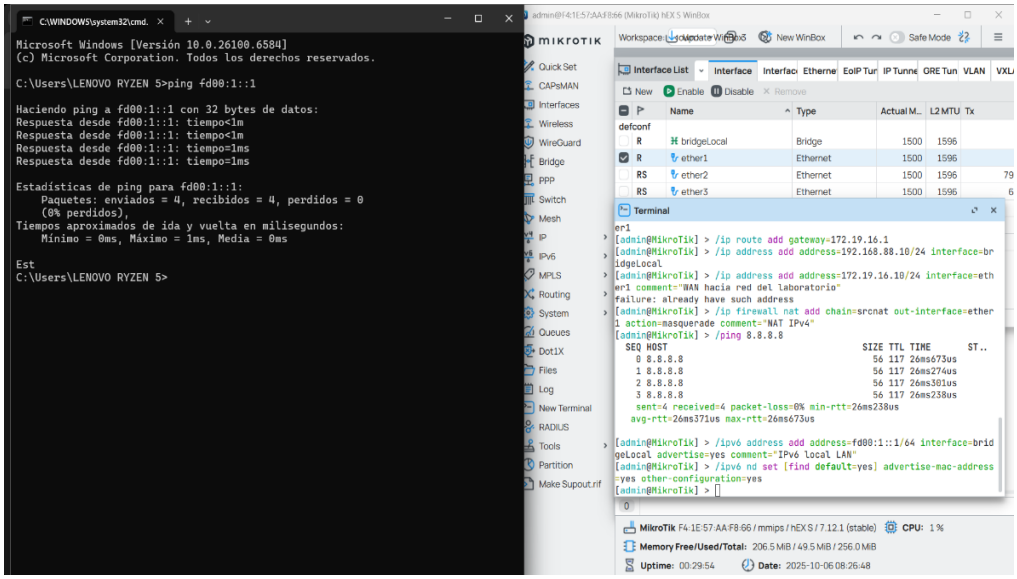


Figura 14 Prueba desde PC a MIKROTIK por el método DUAL STACK

Método túnel

En esta parte se hace las pruebas a través de Túnel Bróker Hurricane en el que se mostrara en la como adquiere la ipv6 partiendo desde la IP publica de la red, esto no ayudará hacer un enlace directo y no depender del ISP, primero se consulta cual es la IP publica Figura 15 para así poder crear el túnel y asigne la dirección ipv6 directamente.

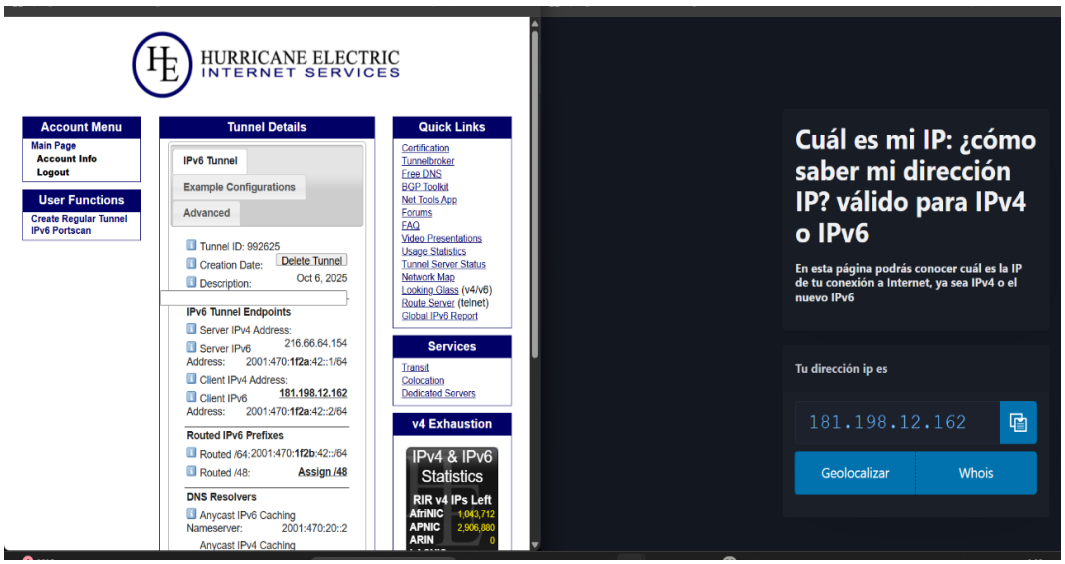


Figura 15 Consulta de IP publica

Se hace ping al túnel creado desde la terminal mikrotik y así poder comprobar la funcionalidad del túnel conectado a ipv4 en la dirección 216.66.64.154 en la Figura 16.

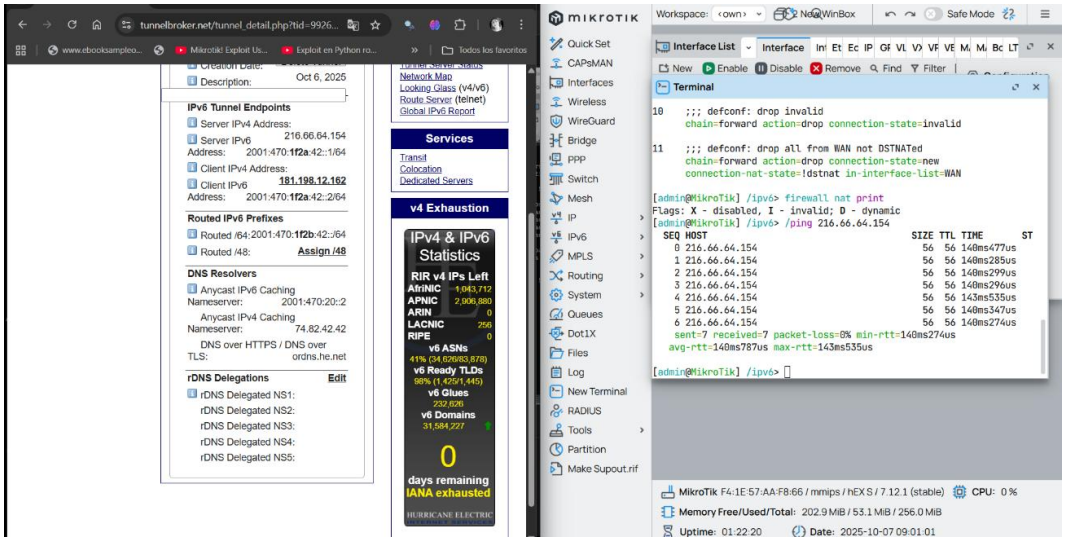


Figura 16 Ping desde el Mikrotik al túnel

En la Figura 17 se puede observar que la PC acepta el mismo rango de ipv6 que el túnel está distribuyendo para comprobar se hace una en el CMD un ipconfig .

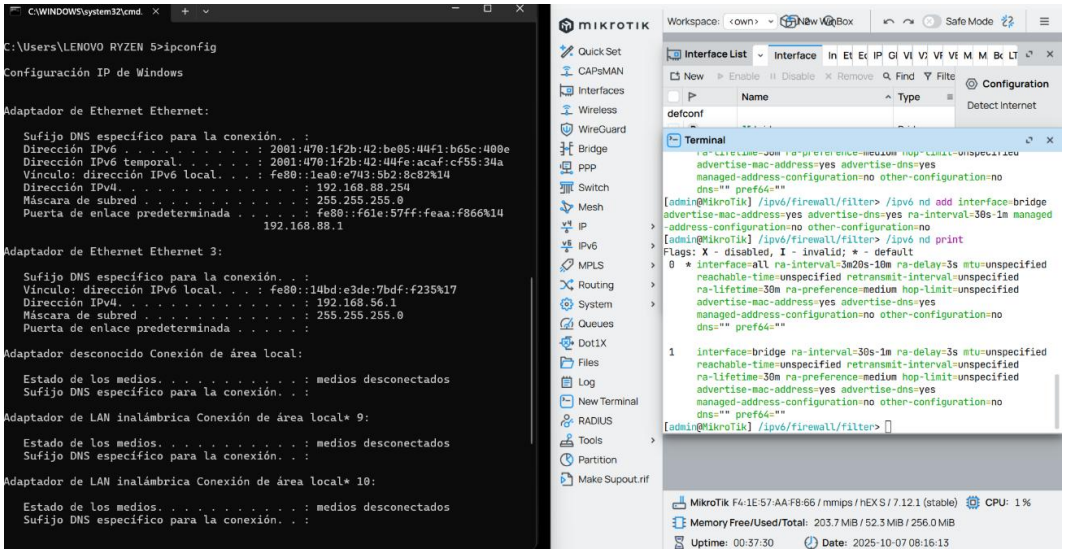


Figura 17 Comprobar conexión ipv6 desde Túnel Broker Hurricane a la PC por medio del CMD

Captura de tráfico ipv4 en ipv6 con el wireshark para esto se recurrió a utilizar esta herramienta en la que analiza el tráfico de la red de la PC que está conectada al cable ethernet que distribuye el dispositivo mikrotik.

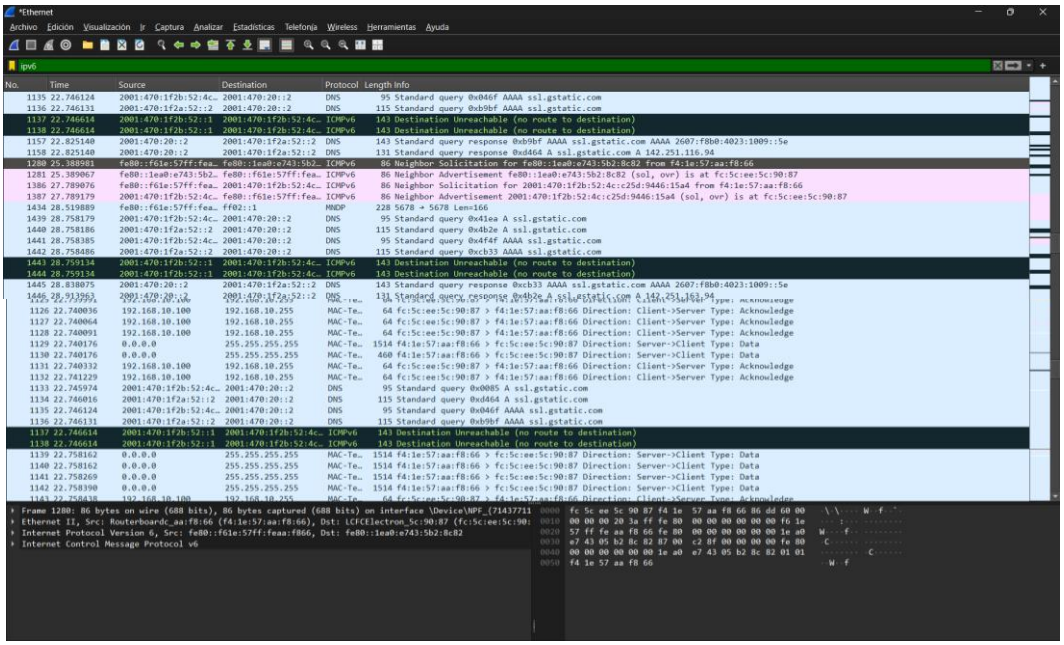


Figura 18 Captura de tráfico con Wireshark IPv4 e IPv6

3.2.5 Cuadro comparativo de equipos para el proceso de migración

Equipo	Descripción técnica	Parámetros
MikroTik hEX S (RB760iGS)	CPU dual-core 880 MHz, 256 MB RAM, 5 puertos Gigabit Ethernet, 1 puerto SFP, RouterOS con soporte nativo IPv4/IPv6, Dual Stack, túneles (IPIP, GRE, 6to4), NAT64.	✓ Soporte completo IPv4/IPv6 Configuración avanzada de firewall y portal cautivo ✓ Rendimiento estable en laboratorio ✓ Puerto SFP para fibra ✓ Económico y fácil de administrar X No incluye WiFi integrado
MikroTik hAP lite (RB941-2nD)	CPU 650 MHz, 32 MB RAM, 4 puertos Fast Ethernet + WiFi 2.4 GHz.	✓ Bajo costo ✓ Incluye WiFi ✓ Soporta dual-stack IPv4/IPv6 X Memoria muy limitada X Bajo rendimiento X No soporta alto tráfico ni firewall avanzado
Cisco 1841 ISR	Router de la serie ISR, 2 interfaces	✓ Documentación abundante

Equipo	Descripción técnica	Parámetros
	Fast Ethernet, IOS, soporte dual-stack IPv4/IPv6.	✓ Uso académico (Packet Tracer, laboratorios) ✓ Soporte nativo IPv6 X Solo Fast Ethernet X Hardware antiguo X Mayor consumo energético X Sin soporte de NAT64
Cisco 2901 ISR	Router modular, 2 interfaces Gigabit Ethernet, IOS 15.x, soporte dual-stack.	✓ Alto rendimiento en túneles ✓ Modular (tarjetas de expansión) ✓ Potente y robusto X Costoso X Alto consumo eléctrico X Configuración más compleja
TP-Link Archer C6 (AC1200)	Router doméstico, 4 puertos Gigabit, WiFi 2.4/5 GHz, soporte básico IPv6.	✓ Económico ✓ Fácil configuración web ✓ Buen alcance WiFi X Soporte IPv6 limitado (básico) X No soporta túneles X Poca utilidad en laboratorio avanzado
Ubiquiti EdgeRouter X	CPU dual-core, 256 MB RAM, 5 puertos Gigabit Ethernet, EdgeOS (Linux-based).	✓ Soporta IPv4/IPv6 dual-stack ✓ Interfaz web y CLI potente ✓ Buen rendimiento X No incluye WiFi X Documentación más limitada que Cisco/MikroTik X Curva de aprendizaje alta

Tabla 16 Comparativa de equipos para IPv6

El MikroTik hEX S (RB760iGS) fue seleccionado por su combinación de rendimiento, funcionalidad y costo, lo que lo hace ideal para un laboratorio académico de migración IPv4 a IPv6. Su CPU dual-core, 5 puertos Gigabit y puerto SFP permiten manejar configuraciones de dual-stack, túneles y firewall avanzado,

mientras que su RouterOS soporta de manera nativa IPv4 e IPv6 con herramientas de transición como NAT64 y DNS64.

Este equipo ofrece la flexibilidad necesaria para simular entornos reales, configurar portales cautivos y controlar el tráfico IPv6, al mismo tiempo que permite evaluar rendimiento y seguridad de la red. Su accesibilidad económica y facilidad de uso lo convierten en la opción más adecuada frente a routers domésticos limitados o equipos profesionales costosos, cumpliendo plenamente con los objetivos del laboratorio de FACSISTEL.

3.3 FASE DE DISEÑO

En esta fase, se plantea llevar a cabo la implementación de un diseño particular dentro del Laboratorio de Telecomunicaciones, con el fin de adaptarse a los cambios previamente planificados. Este enfoque renovado busca responder de manera efectiva el proceso de migración progresiva del protocolo IPv4 a IPV6 propuestas en la red del laboratorio de redes de FACISTEL. Es aquí donde se va a integrar el equipo Mikrotik hEX S RB760iGS como muestra la Figura 19.

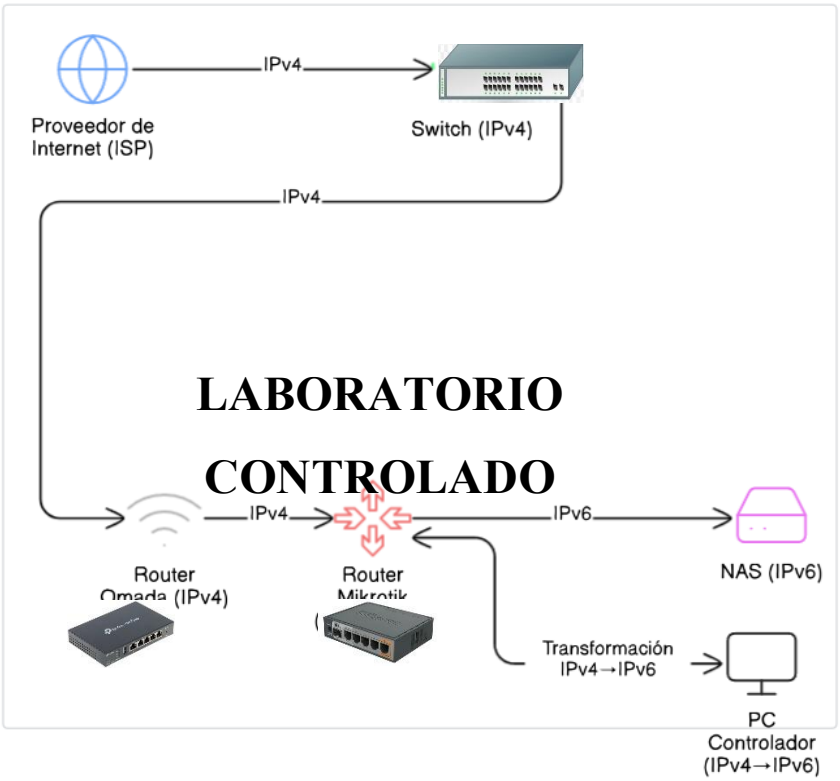


Figura 19 Arquitectura

Laboratorio controlado

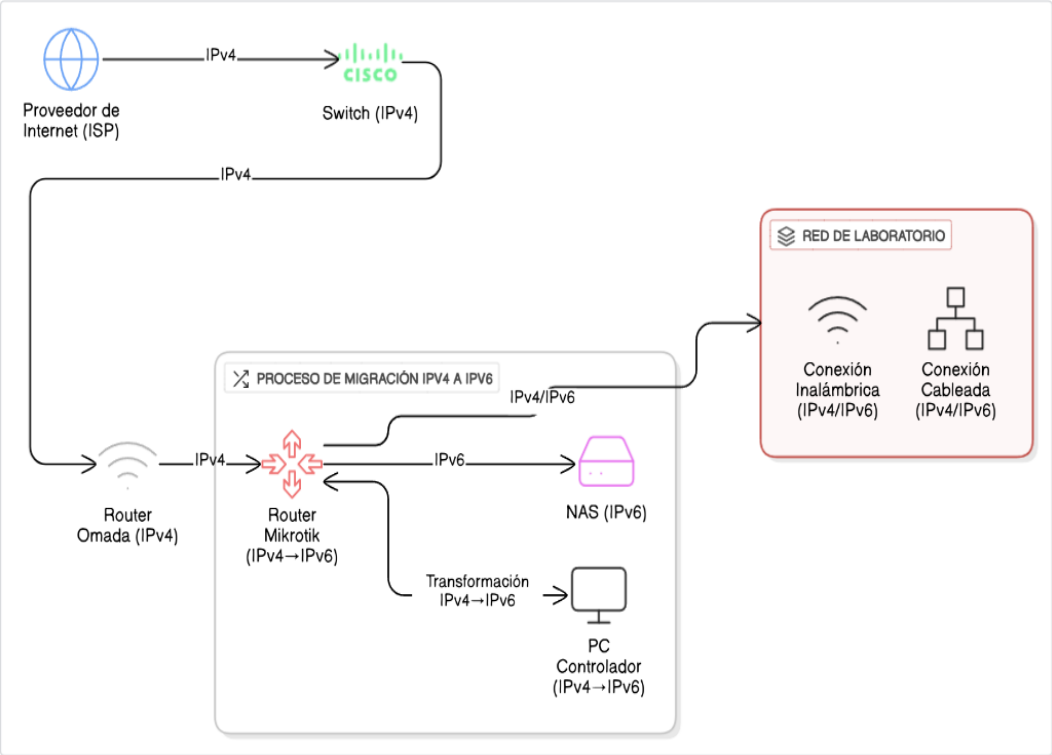


Figura 20 Topología IPv4 e IPv6

Como se puede apreciar en la Figura 20 partimos de la red del proveedor que tiene solo conectividad IPv4, este pasa por el switch Cisco que da internet al Omada y su vez se hace la integración del equipo **mikrotik** que básicamente nos va a migrar los protocolos de IPv4 a IPv6, una vez conectado solo podrá repartir IPv6 a los equipos dentro del laboratorio de redes que estén conectados por cable ethernet y wifi.

3.4 Fase de implementación

3.4.1 Definición del entorno

El entorno donde se implementó el proyecto de investigación se va a hacer de forma segura y con los permisos necesarios para poder cumplir con cada una de las pruebas y a su vez poder dar cumplimiento a su metodología y fases. Con el único fin de mostrar un entorno que permita seguir creciendo y a su vez mejorar la infraestructura de esta. Para la implementación de este modelo experimental progresivo en el laboratorio de redes de FACSITEL se ubicará en un RAD con los demás equipos que a su vez estarán conectados a la red principal.

Pruebas ejecutadas en el laboratorio

Figura 21 Instalación de pantalla y equipo Mikrotik al RAD

Durante la implementación se hizo varias pruebas integradas en el laboratorio en el cual se procedió con la instalación de una pantalla, ubicar un rad para poder trabajar con los distintos equipos del laboratorio para esto se hizo pruebas de forma local en el laboratorio ya que las restricciones de existentes del laboratorio no permitían que el dispositivo tenga el acceso para poder hacer el proceso de migración. Durante las pruebas se pudo determinar que accesos podemos tener dentro de la red universitaria y de las cuales se pido el permiso respectivo.

3.4.2 Plan de pruebas

Prueba	Objetivos	Procedimientos	Indicador
Configuración inicial del MikroTik	Preparar el router para la implementación de IPv4 e IPv6.	Acceder al MikroTik vía WinBox; asignar IP IPv4 a ether1_WAN y red local a bridgeLocal; habilitar servicios básicos (DNS, DHCP, firewall).	Conectividad IPv4 funcional en la red local.
Configuración de Dual Stack (IPv4/IPv6)	Permitir coexistencia de los protocolos IPv4 e IPv6.	Activar soporte IPv6; asignar direcciones IPv6 a las interfaces LAN y WAN; habilitar Neighbor Discovery y DNS IPv6.	El router responde a pings en ambas pilas (IPv4 e IPv6).

Prueba	Objetivos	Procedimientos	Indicador
Configuración de túnel IPv6 sobre IPv4	Encapsular tráfico IPv6 en IPv4 para conectividad hacia Internet.	Crear interfaz ipipv6-tunnel1 con direcciones locales y remotas; configurar prefijos 2001:470:1f2a:8a::/64 y 2001:470:1f2b:8a::/64; agregar ruta por defecto IPv6.	El túnel aparece como **RUNNING** y se logra conectividad IPv6 externa.
Configuración de túnel broker Hurricane Electric	Obtener conectividad IPv6 pública mediante un servicio externo.	Crear cuenta en tunnelbroker.net; registrar IP pública IPv4; configurar parámetros del túnel (cliente/servidor); verificar la conexión con ping ipv6.google.com.	Respuesta exitosa a pings IPv6 a través del túnel broker.
Creación del túnel IPIPv6 en MikroTik	Comprobar funcionamiento del mecanismo de transición IPIPv6.	Configurar manualmente la interfaz IPIPv6; asignar dirección local ::ffff:200.24.135.155; remota 216.66.64.154; verificar con /interface ipipv6 print y /ping.	Túnel activo y operativo (estado **R** RUNNING).
Análisis de ping en IPv4 e IPv6	Evaluar la conectividad y latencia en ambas pilas de red.	Realizar pruebas de ping a hosts internos y externos (8.8.8.8, ipv6.google.com); registrar tiempos de respuesta.	Diferencia de latencia entre IPv4 e IPv6 medida y registrada.
Direccionamiento IPv6 por Wi-Fi	Validar la asignación automática de direcciones IPv6 en la red inalámbrica.	Configurar ND y RA en la interfaz bridge; conectar un dispositivo Wi-Fi y comprobar asignación automática (SLAAC o DHCPv6).	Dispositivo Wi-Fi obtiene dirección IPv6 .

Tabla 17 Plan de pruebas

3.4.3 Instalación y configuración del equipo mikrotik

Para la implementación del equipo se efectuaron los siguientes pasos:

Abrir la aplicación **Winbox** que nos permite gestionar a través de una interfaz gráfica la configuración del equipo **mikrotik** como se muestra en la Figura 23**.**

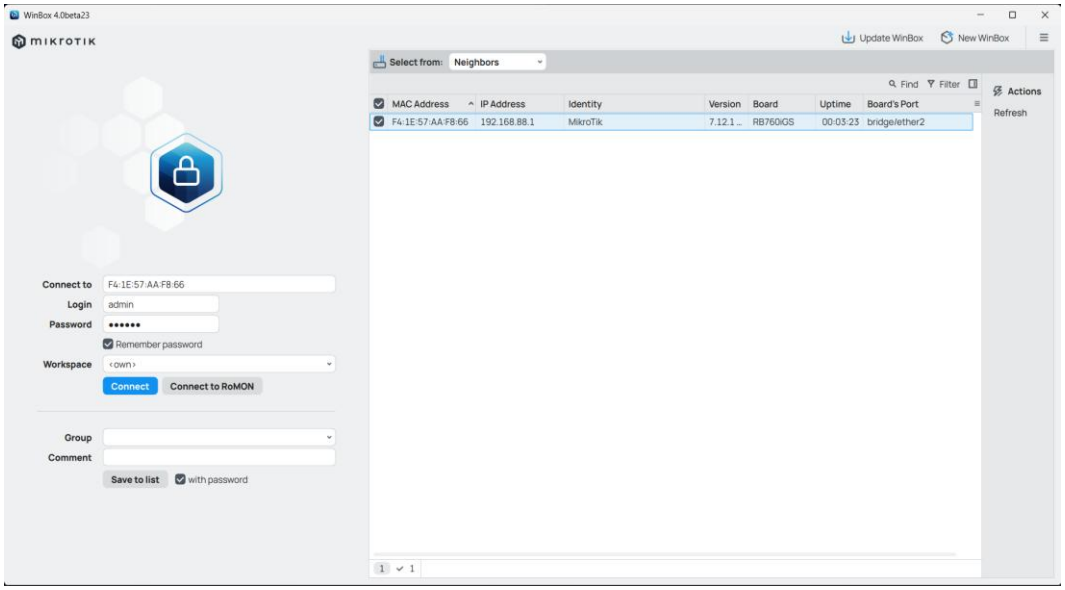


Figura 22 Aplicación Winbox para administrar el equipo Mikrotik

Una vez iniciado con las credenciales asignadas al equipo MikroTik, podemos acceder a la configuración de esta y a su vez activar los paquetes necesarios.

Nos dirigimos al menú, luego nos vamos a system y packages e instalamos la dependencia de IPv6 que viene desinstalada.

Ya instalado IPv6, podemos empezar con la configuración Figura 24.

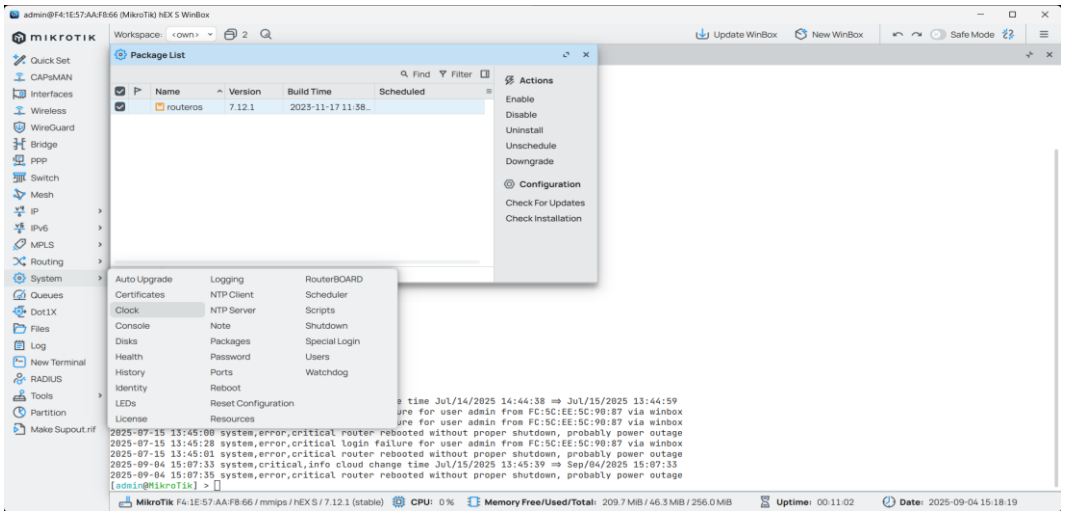


Figura 23 Instalación del paquete IPv6

Túnel Hurricane Electric

A continuación, se va a crear una cuenta en el **Túnel Hurricane (**Figura 25**)** este nos permitirá hacer una conexión externa ya que el proveedor no nos da una IP versión 6 de forma nativa.

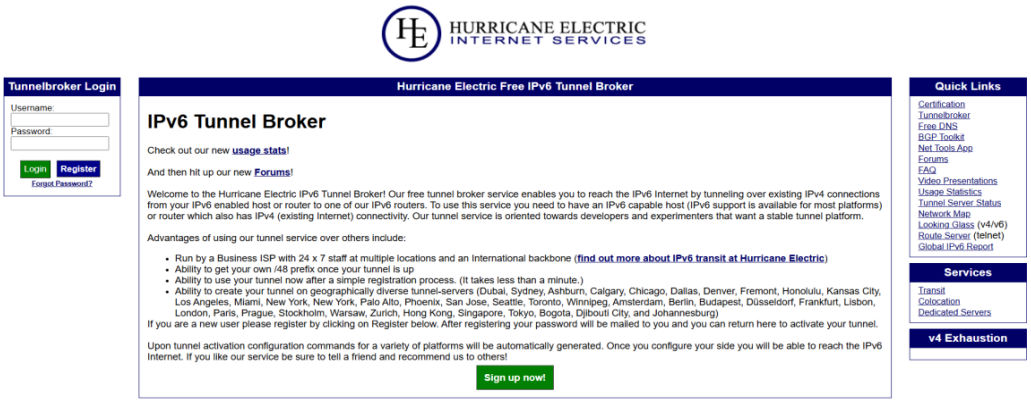


Figura 24 Interfaz de Hurricane Electric

Se procede a crear (Figura 26) el enlace del túnel con la IP pública de la universidad **181.198.12.162** y nos dé ya la ipv4 en ipv6.

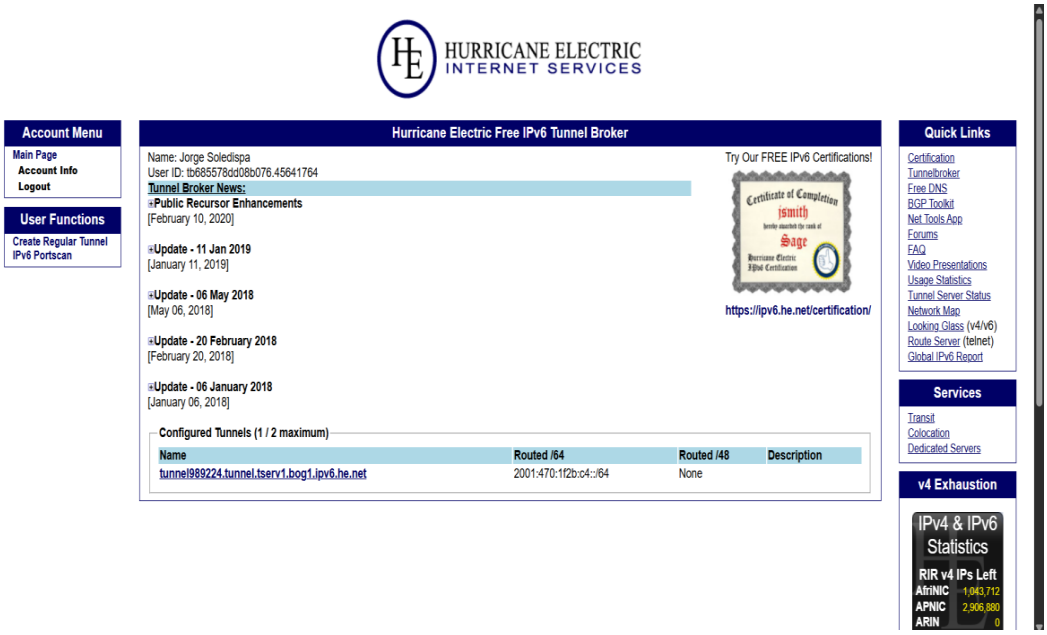


Figura 25 Crear túnel con la IP publica de la universidad

Una vez creado el túnel podemos ver las direcciones que me permitirán crear el túnel IPIPv6 en el equipo mikrotik, en la Figura 27 podemos ver

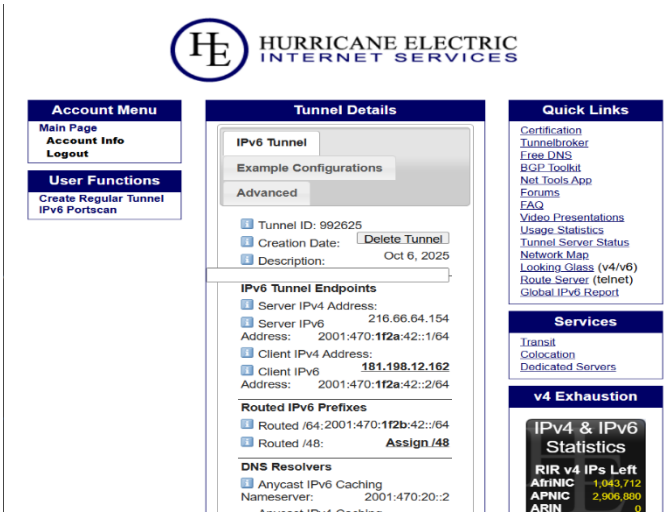


Figura 26 IPv6 del túnel Hurricane con la IP publica

3.4.3.1 Configuración de protocolo de migración

3.4.3.2 Dual Stack

Para iniciar con la configuración primero se ve la funcionalidad Dual Stack permite activar y utilizar simultáneamente los protocolos IPv4 e IPv6, garantizando su coexistencia en el mismo entorno de red.

Antes de proceder con la configuración de IPv6, es necesario comprobar que dicho protocolo esté habilitado. Para ello, se debe acceder a las conexiones de red, seleccionar la conexión correspondiente (ya sea cableada o inalámbrica) y abrir sus propiedades, donde, como se muestra en la Figura 28, se puede verificar que el protocolo IPv6 esté activado.

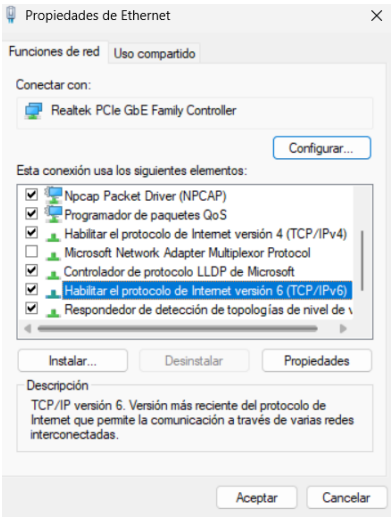


Figura 27 Habilitar protocolo IPv6 en la PC

Para poder verificar si la PC ha obtenido el direccionamiento IPv6 por DHCP se puede verificar de dos formas, la primera forma es seleccionando las propiedades del sistema y la otras son por el comando de símbolo como se muestra en la Figura 29 y 30

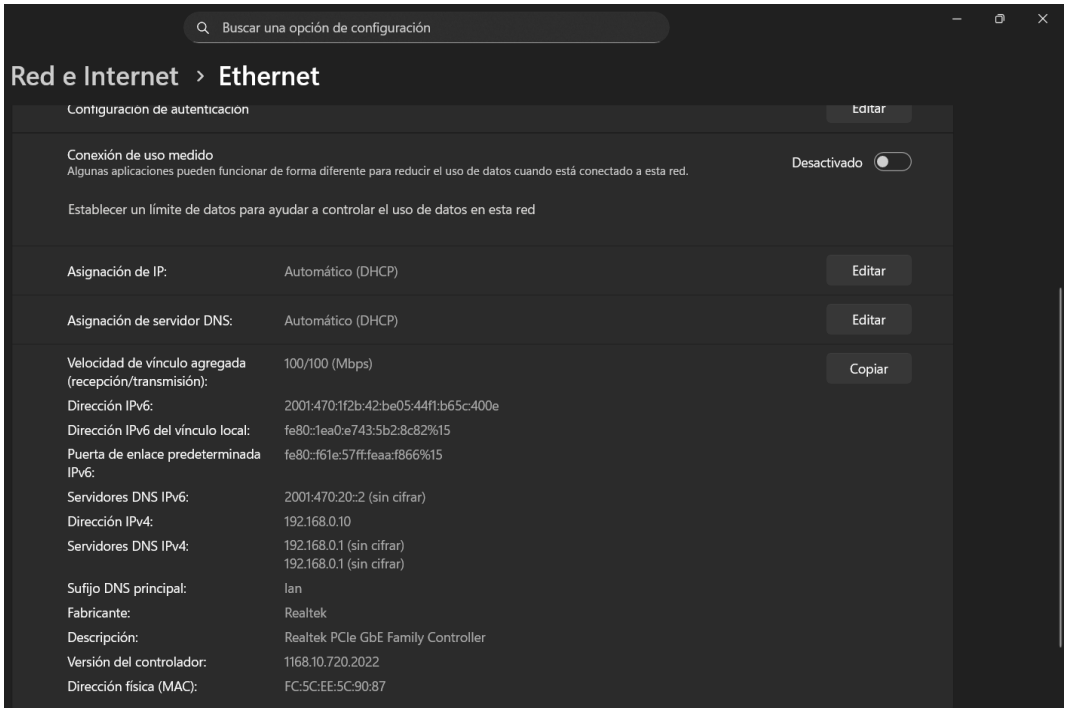


Figura 28 Red en IPv4 e IPv6

Además, se puede ver que las direcciones sí están siendo dadas por el DCHPv6 y siendo compartidas con las demás PC en el rango establecido en la Figura 29.

```
C:\Users\LENOVO RYZEN 5>ping 2001:470:1f2b:42:6842:88ee:4633:e3d3

Haciendo ping a 2001:470:1f2b:42:6842:88ee:4633:e3d3 con 32 bytes de datos:
Respuesta desde 2001:470:1f2b:42:6842:88ee:4633:e3d3: tiempo=1ms
Respuesta desde 2001:470:1f2b:42:6842:88ee:4633:e3d3: tiempo<1m
Respuesta desde 2001:470:1f2b:42:6842:88ee:4633:e3d3: tiempo<1m
Respuesta desde 2001:470:1f2b:42:6842:88ee:4633:e3d3: tiempo<1m

Estadísticas de ping para 2001:470:1f2b:42:6842:88ee:4633:e3d3:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\LENOVO RYZEN 5>ping 2001:470:1f2b:42:6842:88ee:4633:e3d3
```

Figura 29 Detalles de las direcciones por el símbolo del sistema y el comando IPCONFIG

En la Figura 31 podemos ver la configuración aplicada que nos verifica la funcionalidad del Dual Stack

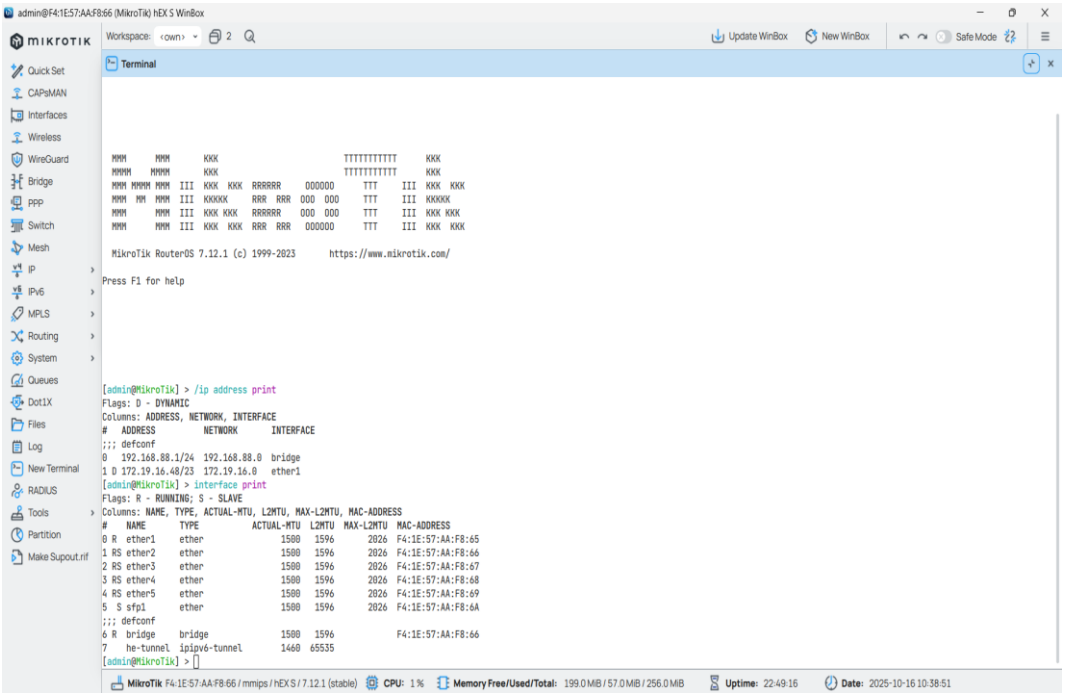


Figura 30 Configuración Dual Stack

En la Figura 32 se muestra la conexión existente en entre los diferentes dispositivos ya sea en IPv4 como IPv6.

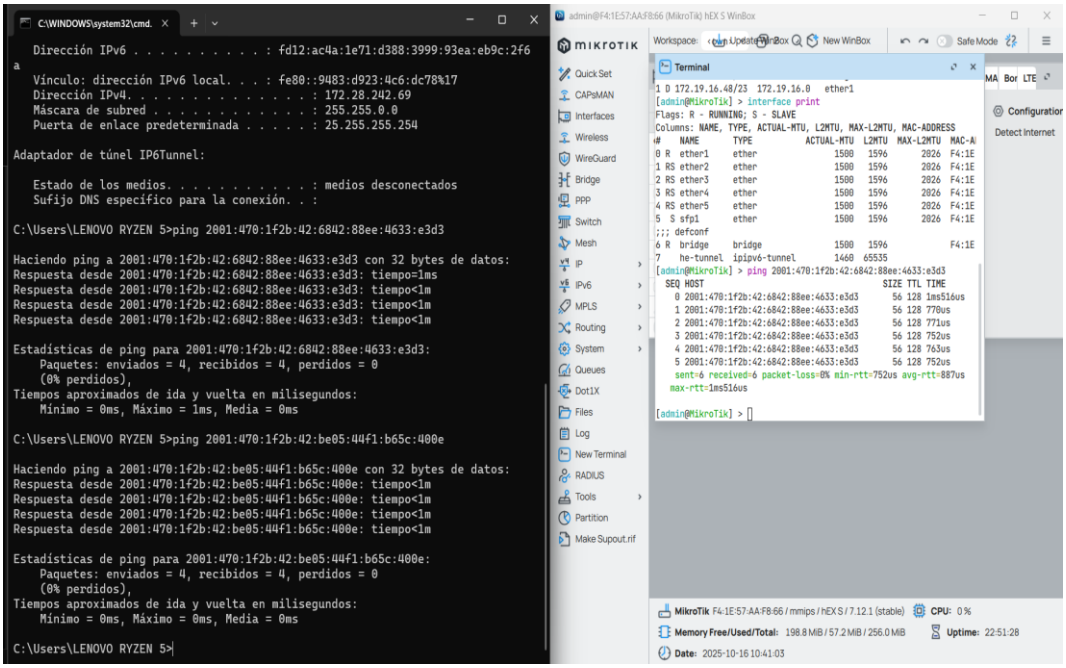


Figura 31 Conexión Dual Stack

3.4.3.3 Tunneling

Se procede a iniciar con la creación del túnel 6to4 en el que se le asigna la IP local y a su vez se va a enlazar con el túnel hurricane.

Crear el túnel IPIPV6

/interface IPIPv6 add name=IPIPv6 Tunnel comment="he-tunnel" \ local-address=::ffff:200.24.135.155 remote-address=216.66.64.154 mtu=1280

Asignar la IPv6 al túnel

/interface IPIPv6 add name=he-tunnellocal-address=::ffff:200.24.135.155 remote address=216.66.64.154 mtu=1280

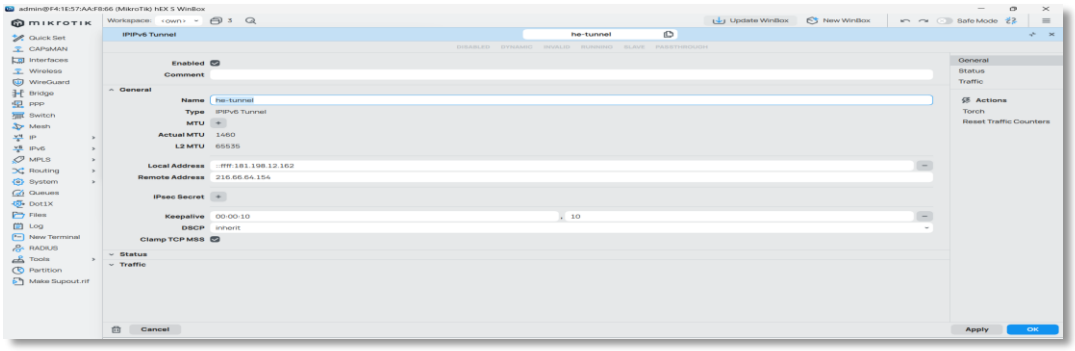


Figura 32 Túnel IPIPv6

En este caso se procede a asignar la dirección IPv6 a la brigde y a su vez la LAN, a continuación, se detalla por la línea de comando el ingreso.

/ipv6 address add address=2001:470:1f2a:52::2/64interface=bridge1 advertise=yes

/ipv6 nd set [find default=yes] advertise-dns=yes

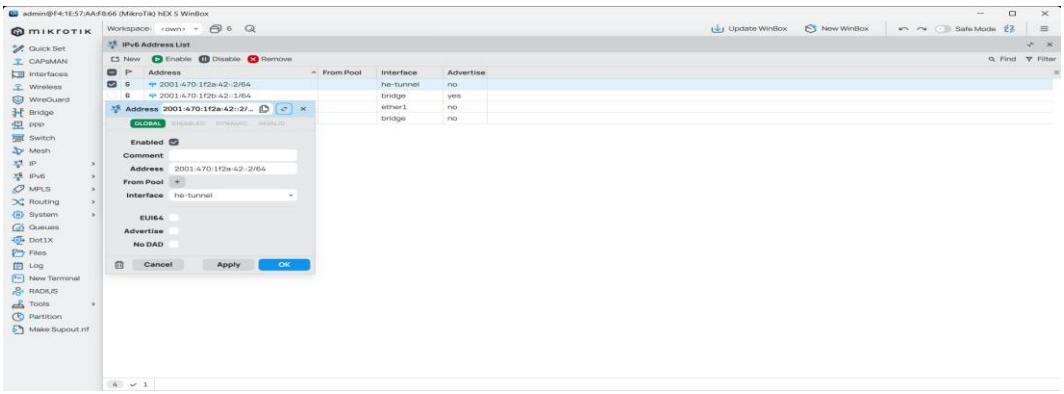


Figura 33 Asigna IPv6 al bridge

Configurar DNS IPv6

/ip dns set allow-remote-requests=yes

servers=2001:470:20::2,2001:4860:4860::8888

Finalmente procedemos a asignar la ruta de ipv6

/ipv6 address add address=2001:470:1f2a:c4::2/64 interface=sit1 advertise=no

/ipv6 route add dst-address=::/0 gateway=2001:470:1f2a:52::1

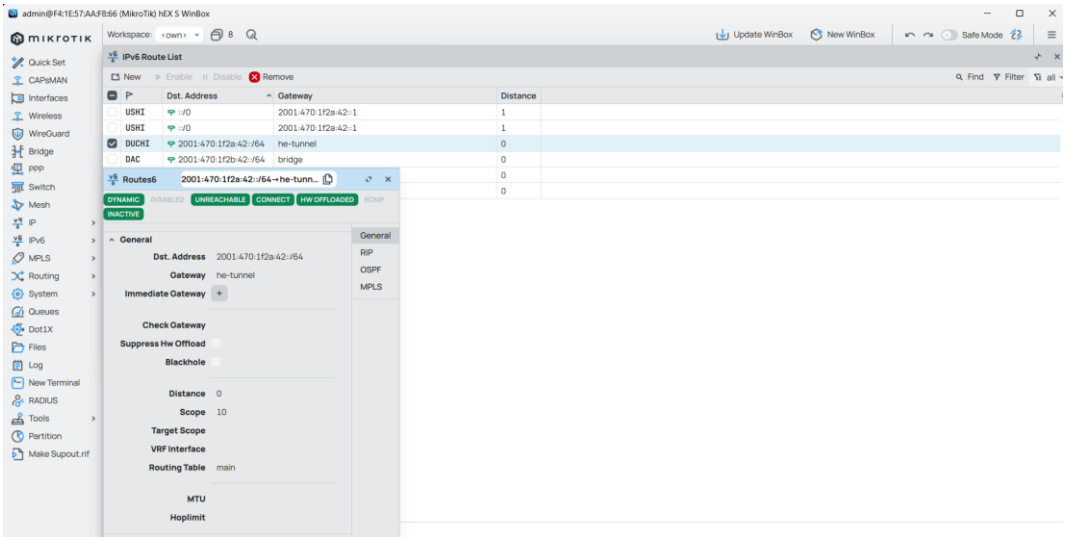


Figura 34 Configuración de la ruta

Como último paso tenemos la configurar firewall

/ip firewall filter add chain=input protocol=41 src-address=216.66.64.154

action=accept comment="HE proto41 in"

/ip firewall filter add chain=output protocol=41 dst-address=216.66.64.154

action=accept comment="HE proto41 out"

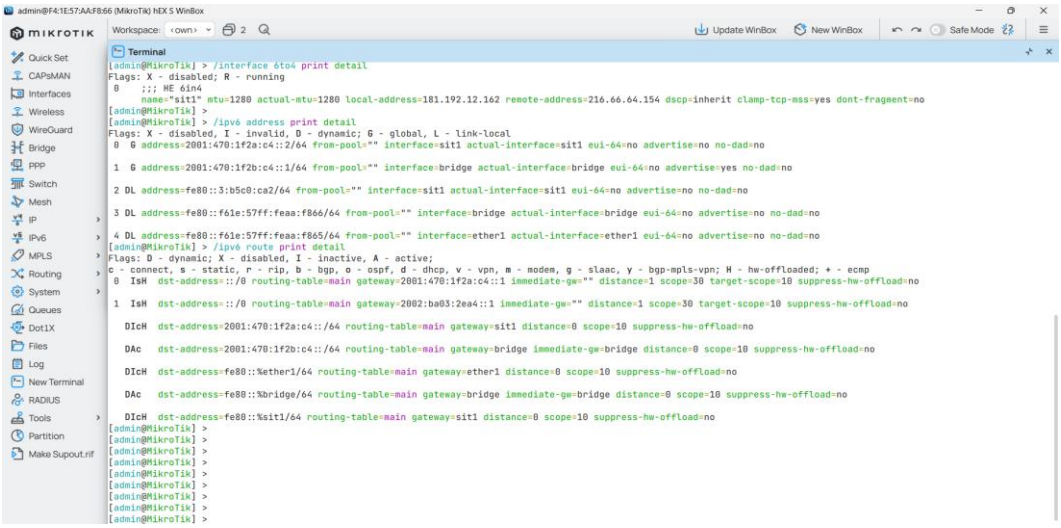


Figura 35 Consola de mikrotik con datos del túnel creado

En esta Figura se puede observar que el túnel está creado correctamente y activo en el cual se hace ping a al túnel entre los dispositivos del laboratorio.

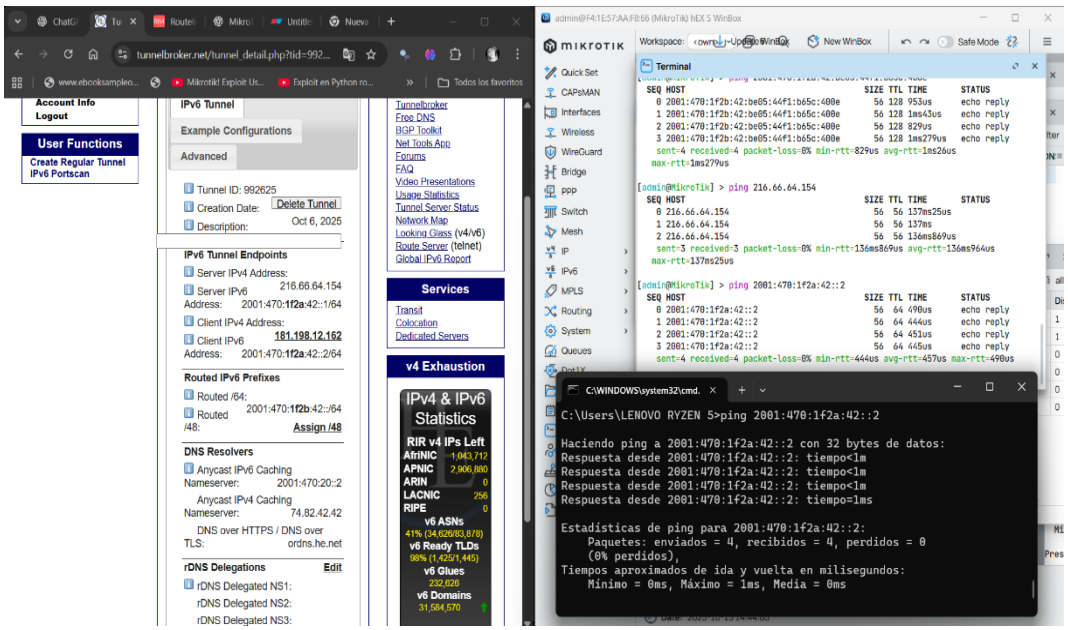


Figura 36 túnel activo y funcional

3.4.4 Configuración del portal cautivo

Se procede a crear el hotspot para el bloqueo masivo de toda la red. Por aquello, se creó el bloqueo hotspot. A continuación, se detallan los comandos de cómo crear y funcionar.

[admin@MikroTik] > /ip hotspot setup

Select interface to run HotSpot on

hotspot interface: bridge1

Set HotSpot address for interface

local address of network: 192.168.10.1/24

masquerade network: yes

Set pool for HotSpot addresses

address pool of network: 192.168.10.10-192.168.10.100

Select hotspot SSL certificate

select certificate: none

Select SMTP server

ip address of smtp server: 0.0.0.0

Setup DNS configuration

dns servers: 8.8.8.8,1.1.1.1

DNS name of local hotspot server

dns name: portal.lan

Create local hotspot user

name of local hotspot user: admin

password for the user: admin

Hotspot

A continuación, se mostrará la línea de código para bloquear la conexión a las páginas web /ip hotspot disable [find] aquí se deshabilita la navegación como se puede apreciar en la Figura 43.

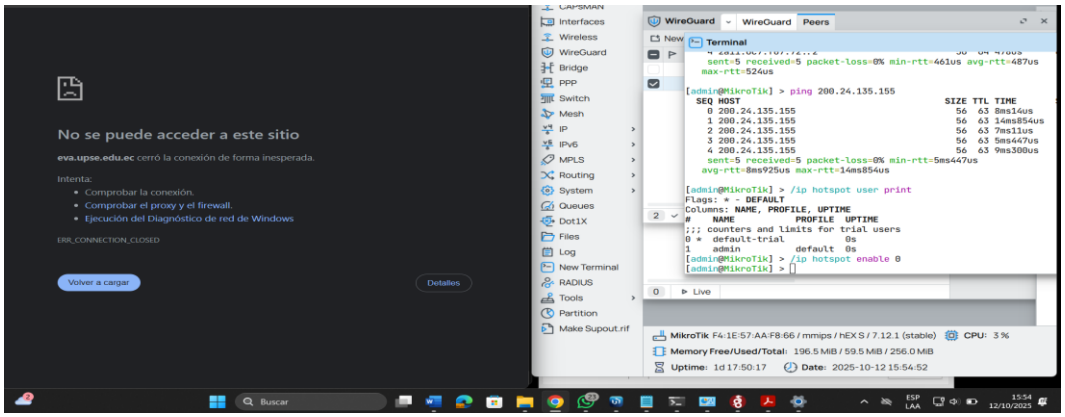


Figura 37 Bloque de la página web con el Hotspot

En la Figura 44 ya habilitamos la conexión con el comando /ip hotspot enable [find], para más detalle diríjase a Anexo 8.

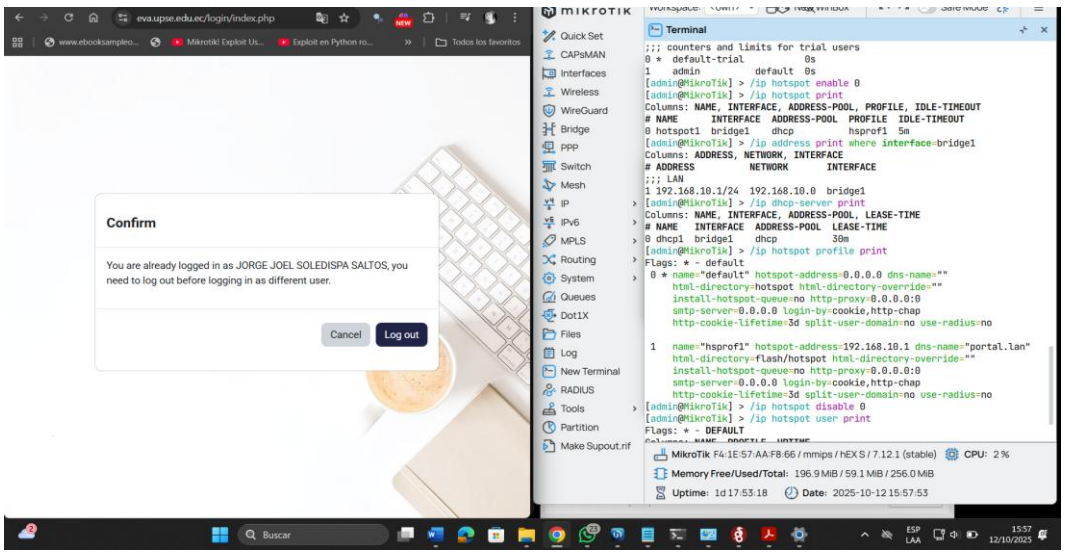


Figura 38 Restablece la conexión.

3.4.5 Configuración de SSH

Se procede a verificar si está instalado el servicio SSH, si no está procedemos a instalar con el PowerShell como muestra la Figura 38.

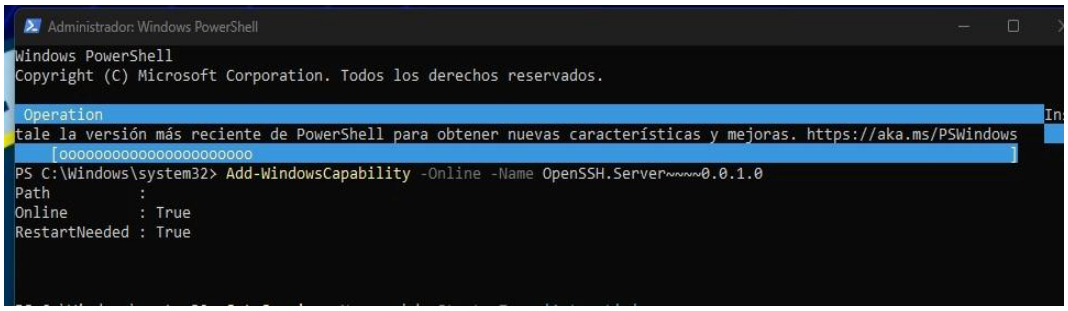


Figura 39 Servidor SSH

Verificamos la conexión por vía SSH entre los dispositivos y así confirmamos la funcionalidad de los mismos como muestra la Figura 39.

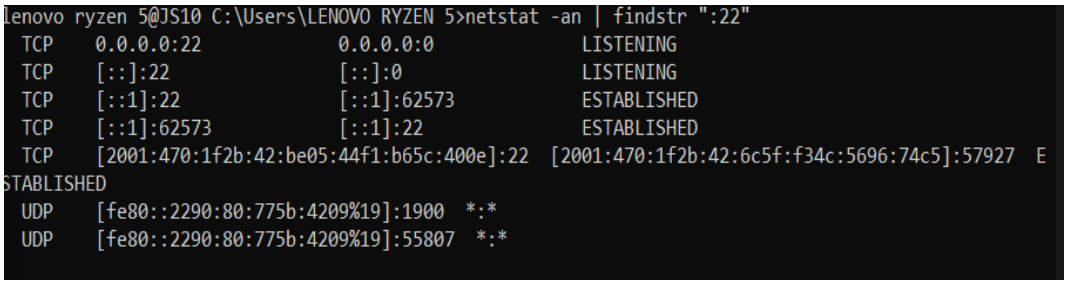


Figura 40 Conexión SSH

3.5 Fase de pruebas de funcionalidad ipv6

Con las pruebas realizadas del direccionamiento IPv6 podemos determinar que los dispositivos finales conectados al punto de acceso Mikrotik admiten el nuevo protocolo de red y mantienen una comunicación estable bajo los mecanismos de coexistencia. Las pruebas se realizarán entre equipos del laboratorio utilizando el símbolo del sistema y el comando ping, con el objetivo de comprobar la conectividad entre los nodos de la red IPv6 y verificar la integración con el protocolo IPv4 mediante Dual Stack. De esta manera, se evaluará el comportamiento del Mikrotik al gestionar simultáneamente ambos protocolos, asegurando la correcta configuración del direccionamiento, las reglas de firewall y la respuesta a las solicitudes ICMPv6, lo que evidencia su capacidad para operar eficientemente en un entorno de migración progresiva hacia IPv6.

3.5.1 Funcionalidad IPv4 e IPV6 en el Mikrotik

Para comprobar la funcionalidad se conectará mediante cable ethernet al puerto ether del mikrotik para tener conectividad por este medio y para la inalámbrica a la red llamada Lab_Redes una vez conectada se procede hacer un ipconfig para conocer la ipv4 e ipv6.

```
Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Dirección IPv6 . . . . . . . . . . . . : 2001:470:1f2b:42:be05:44f1:b65c:400e
   Dirección IPv6 temporal. . . . . . . . : 2001:470:1f2b:42:89b9:2401:4316:da98
   Vínculo: dirección IPv6 local. . . . . : fe80::1ea0:e743:5b2:8c82%15
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.88.243
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::f61e:57ff:feaa:f866%15
                                       192.168.88.1
```

Figura 41 Dirección IPv4 e IPv6

La comprobación se va a hacer mediante ping tanto en ipv4 como ipv6 para ello, cada protocolo envía cuatro paquetes de 32, 512 y 8000 como muestra la Figura 40. para comprobar el envío de direcciones se va hacer en tres pc diferentes y así poder comparar el tiempo de respuesta en ipv4 e ipv6 como muestra la figura 41.

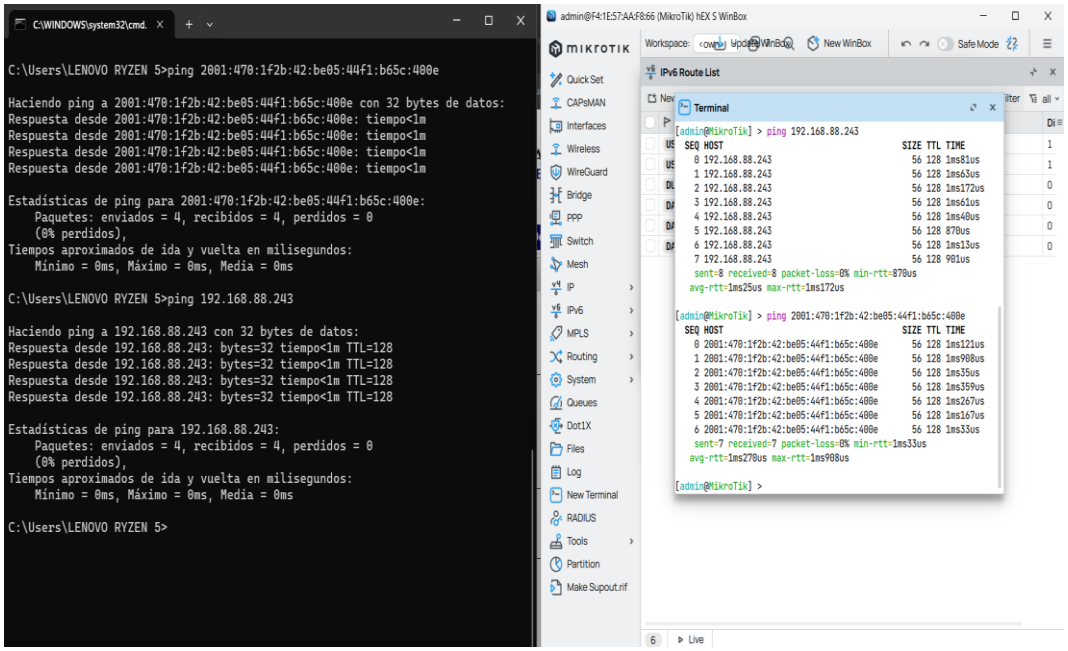


Figura 42 Envió de IPv4 e IPv6 en PC1

En el segundo dispositivo se comprobará el direccionamiento en ipv4 e ipv6 a conectados al cable ethernet como muestra la figura 42.

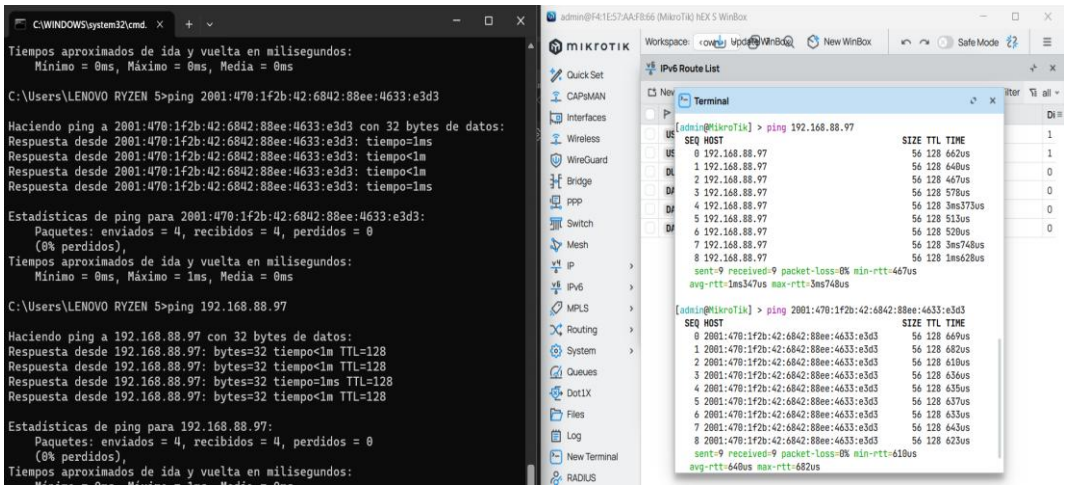


Figura 43 Envió de IPv4 e IPv6 en PC2

Finalmente, se procede a hacer el envío esta vez conectada a una red wifi que a su vez está conectada al equipo mikrotik para segmentar entre los mismos rangos, como muestra la Figura 43.

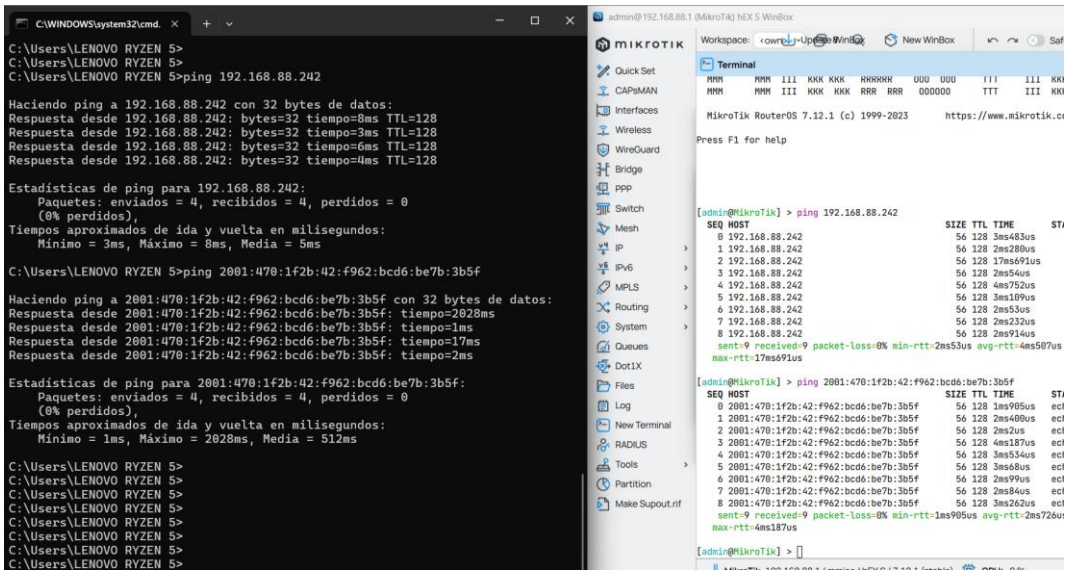


Figura 44 Envió de IPv4 e IPv6 en PC3

La comprobación de la comunicación entre los dispositivos realizada mediante ping entre la PC1, PC2 y PC3, tanto en IPv4 como en IPv6, se envían paquetes de 32, 512 y 8000 bytes, como muestran las Figuras 42, 43 y 44.

3.5.2 Análisis de resultados

En esta sección se va a analizar los resultados obtenidos en la sección 3.5.4 de las pruebas realizadas en la red, además se va a hacer captura con el software Wireshark

para analizar diferentes parámetros. En este caso se va analizar primero los paquetes de IPv4 como muestra la Figura 45.

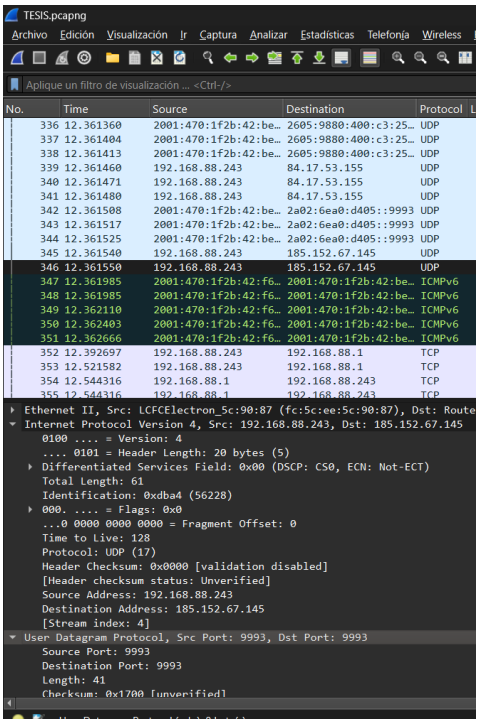


Figura 45 Análisis de ipv4

En este caso se analizaron los mensajes ICMPv6 haciendo ping a las direcciones IPv6 que al mismo tiempo se están capturando en el Wireshark como muestra la Figura 46.

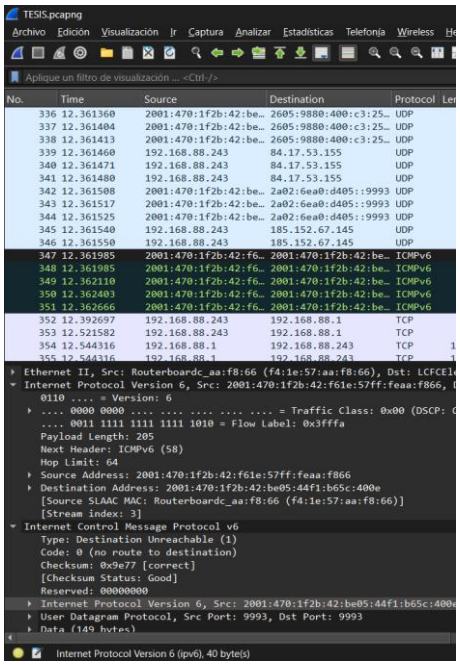


Figura 46 Análisis de IPv6

3.5.3 Análisis de latencia y pérdida de paquetes en la red Mikrotik

Mediante análisis se puede determinar el tiempo en que los paquetes se trasmiten hacia su destino en la red y se podrá determinar si durante la transmisión existe o no perdidas de paquetes, las pruebas se hicieron con el ping con tres pc diferentes con el fin de determinar si hay perdidas o no de paquetes en IPv4 e IPv6.

En la tabla se muestran los datos que fueron obtenidos de las figuras 42, 43 y 44 mencionadas por él en el envío de paquetes.

Latencia de IPv4

PC	Tamaño del paquete (Bytes)	Latencia (us) min-rrt[4] (us) avg-rrt(us) max-rrt(us)			Paquete
PC1	32	870us	125us	1172us	4
PC2	32	467us	1347us	1748us	4
PC3	32	253us	4507us	17691us	4
PC4	32	1905us	2726us	4187us	4
PC5	32	425us	401us	482us	4
PC6	32	418us	394us	458us	4
PC7	32	980us	1430us	2640	4
PC8	32	121us	2250us	9360us	4
TOTAL		6439us	14087us	37238us	
PORCENTAJE		11,15%	24,38%	62,47%	

[4] Tiempo de ruta de enrutamiento rrt (Routing Route Time)

Tabla 18 Latencia del protocolo IPv4

Se pudieron obtener latencias con un promedio mínimo 6439us y máximas de 37238us, además mostrando que no hubo pérdidas de paquetes transmitidos.

Latencia de IPv6

PC	Tamaño del paquete (Bytes)	Latencia (ms) min-rrt[5] (us)	avg-rrt(us)	max-rrt(us)	Paquete
PC1	32	**752us**	**887us**	**1516us**	4
PC2	32	**133us**	1270us	1908us	4
PC3	32	**310us**	640us	682us	4
PC4	32	**124us**	109us	462us	4
PC5	32	**358us**	316us	155us	4
PC6	32	**300us**	280us	420us	4
PC7	32	**650us**	820us	1110us	4
PC8	32	**396us**	360us	438us	4
TOTAL		**3023us**	4682us	5691us	
PORCENTAJE		24,24%	34,22%	41,54%	

Tabla 19 Latencia del protocolo IPv6

En las pruebas realizadas se emplearon en el protocolo IPv4, los tiempos de respuesta fueron de 6439us (mínimo), 14087us (promedio) y 37238us (máximo), representando aproximadamente 11,15%, 24,38% y 62,47% del total de latencias, respectivamente. En contraste, bajo IPv6, los tiempos disminuyeron a 4373us ,

[5] Tiempo de ruta de enrutamiento rrt (Routing Route Time)

6,6172us y 7491us, con proporciones más equilibradas de 24,24 %, 34,22 % y 41,54 %, evidenciando una mayor consistencia y estabilidad en la transmisión de paquetes.

3.5.4 Prueba de bloqueo de conexión

Las PC que se conectan por cable Ethernet no tendrán conexión a internet hasta que se autentifiquen con las credenciales. Una vez logueados podrán navegar sin interrupciones y el portal se activará una vez que la PC muestre 1 minuto sin uso o se desconecte el cable por el mismo tiempo, para poder tener conexión deben volver a autenticarse como muestra la figura 47.

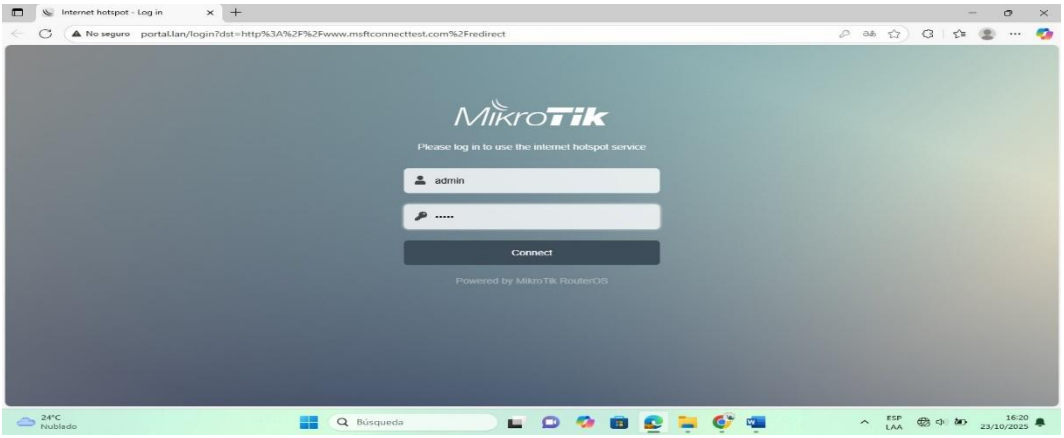


Figura 47 Bloque de hotspot

3.5.5 Compartir archivos por SHH en IPv6

Primero, se va a abrir Putty como un medio de compartir archivos. Ubicamos la dirección en ipv6 del pc a la que deseamos compartir el archivo. En este caso, se va a compartir en una NAS y se va a acceder de forma remota. Por aquello se accede a la interfaz y se ubica en la carpeta Tesis, como muestra la Figura 47.

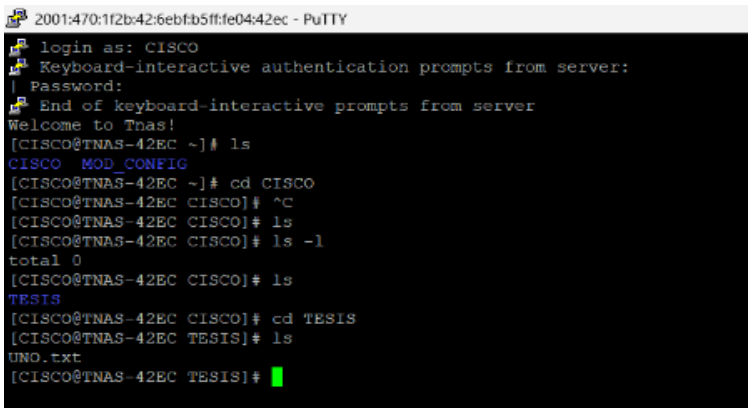


Figura 48 Interfaz Putty

Se abre una terminal por el comando CMD y se procede a compartir el archivo que desea. En este caso, el archivo se llamará uno y dos desde la PC Windows al NAS, como muestra la Figura 48.

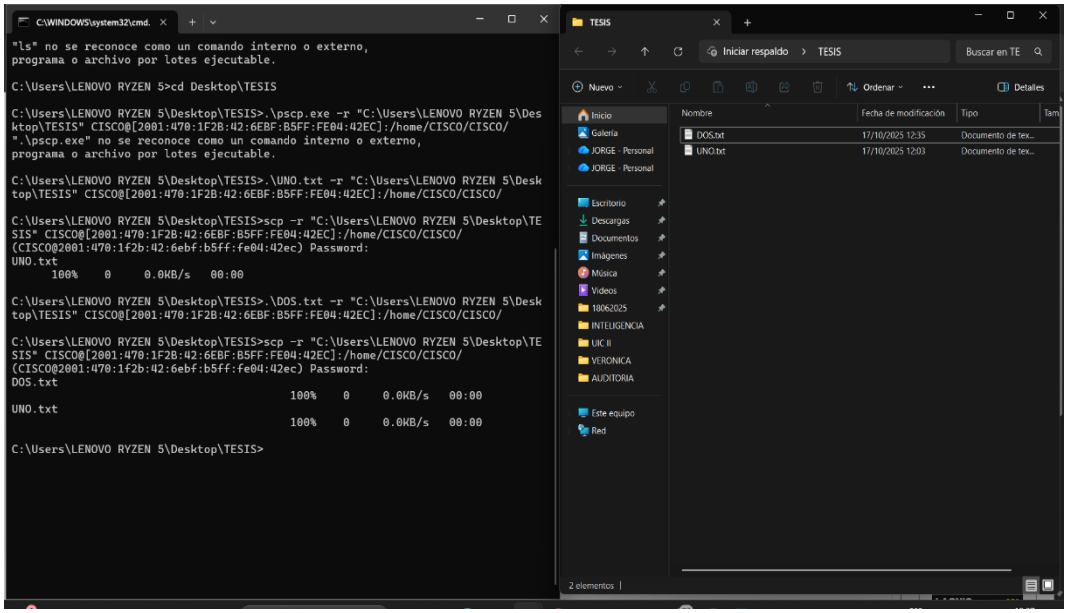


Figura 49 Compartir archivo al NAS

Finalmente, se abre el administrador de archivos donde se procede a comprobar que los archivos llegueN al NAS a través de la dirección IPv6 Figura 49.

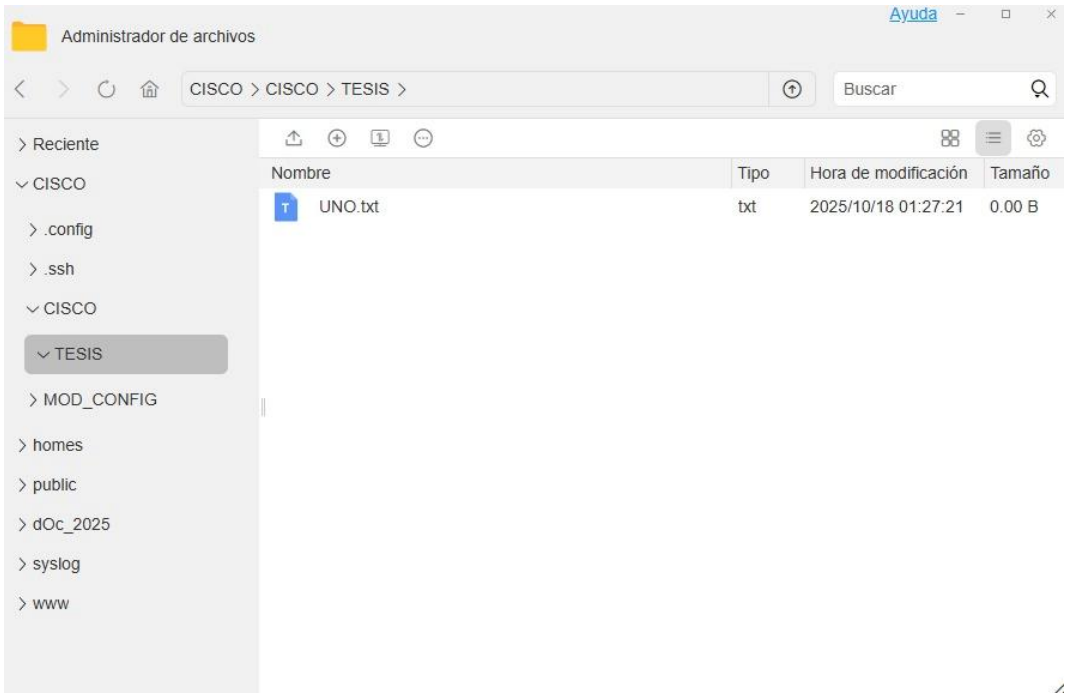


Figura 50 Documentos recibidos en el NAS.

CONCLUSIÓN

- El desarrollo del modelo experimental me permitió evidenciar que la migración progresiva del protocolo IPv4 a IPv6 es factible en el laboratorio de redes de la UPSE mediante la implementación de mecanismos de transición. La configuración de Dual Stack y túneles IPIPv6 demostró la posibilidad de coexistencia entre ambos protocolos, garantizando la comunicación entre dispositivos y sirviendo como base práctica para futuras implementaciones y actividades académicas orientadas al direccionamiento IPv6.
- La configuración del esquema Dual Stack fue exitosa, permitiendo la coexistencia de ambos protocolos en el entorno de laboratorio y comprobando la coexistencia entre los equipos. En cuanto al túnel IPIPv6 su funcionamiento fue correcto en la red interna, sin embargo, no se obtuvo salida a Internet debido a la falta de soporte nativo IPv6 por parte del proveedor del servicio (ISP). Esta limitación no afecta la validez del modelo experimental ya que se comprobó su operación local.
- Las reglas de firewall implementadas cumplieron con su propósito de restringir el tráfico no autorizado proveniente del Hotspot en las que se garantiza un mayor control y seguridad dentro del entorno de pruebas. Se verificó que, al activar las reglas, las conexiones por cable se bloquean correctamente, cumpliendo el objetivo de control de acceso y aislamiento de tráfico.
- Las pruebas de latencia realizadas con ping y el análisis de tráfico en Wireshark muestran que la red bajo IPv6 es más eficiente y estable que IPv4, con tiempos de respuesta máximo de promedio de 62,47% del total de latencias en IPv4, mientras que en IPv6 alcanza un 41,54%, evidenciando una mayor consistencia de manera similar, los valores promedio y máximo muestran proporciones más equilibradas en IPv6 que en IPv4. Estos resultados indican que IPv6 permite la transmisión de paquetes de manera más confiable.

- Se elaboró un manual técnico que documenta detalladamente los procedimientos de instalación, configuración y validación del modelo experimental, el cual servirá como guía de referencia para estudiantes y docentes interesados en replicar o ampliar el proceso de migración hacia IPv6 en futuros proyectos académicos.

RECOMENDACIÓN

- Mejorar la infraestructura de red del laboratorio de FACSISTEL, asegurando que los equipos de comunicación, routers y switches sean completamente compatibles con IPv6. Además, se sugiere liberar las restricciones del protocolo 41 y de los puertos asociados a IPv6 para permitir una conectividad completa con túneles y servicios externos.
- Verificar la compatibilidad del proveedor de Internet (ISP) con el protocolo IPv6. En caso de que no tenga de soporte nativo, se recomienda gestionar un prefijo IPv6 propio o continuar utilizando túneles de proveedores gratuitos como Hurricane Electric y ajustar la configuración para mantener estabilidad en las pruebas.
- Diseñar una red de pruebas independiente (VLAN) para la implementación de IPv6. Esto permitirá realizar configuraciones experimentales sin afectar la red operativa del laboratorio y garantizar una segmentación segura durante la migración.

REFERENCIAS

[1] D. F. NUÑEZ LARA, «ESTUDIO PARA LA MIGRACIÓN DE IPV4 A IPV6 PARA LA EMPRESA PROVEEDORA DE INTERNET MILLTEC S.A.,» 08 2009. [En línea]. Available: https://bibdigital.epn.edu.ec/bitstream/15000/1871/1/CD-2447.pdf.

[2] FEBRABAN, «LOGICALIS Architects of Change,» CIAB FEBRABAN, 04 06 2014. [En línea]. Available: https://www.la.logicalis.com/es/article/la-migracion-ipv6-es-un-tema-obligatorio-para-las-instituciones-financieras.

[3] Vélez Varela, Fernado; Gutiérrez Rancruel, Liliana, «IPV6, una realidad,» de *IPV6, una realidad*, Bogota, Ediciones de la U, 2016, p. 206.

[4] L. C. Lituma Briones, «LABORATORIO VIRTUAL DE ANÁLISIS Y COMPORTAMIENTO DE MALWARE BASADO EN TÉCNICAS Y MÉTODOS DE SEGURIDAD INFORMÁTICA PARA LOS LABORATORIOS EN LA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES,» 11 02 2020. [En línea]. Available: https://repositorio.upse.edu.ec/bitstream/46000/5332/1/UPSE-TIN-2020-0009.pdf.

[5] J. P. Montañez Prieto, «PROPUESTA PARA LA MIGRACIÓN DEL PROTOCOLO IPV4 A PROTOCOLO IPV6 PARA LA SECRETARIA DEL SISBEN DE LA ALCANDIA DE TUNJA,» 2018. [En línea]. Available: https://repository.unad.edu.co/bitstream/handle/10596/19074/7169456.pdf;jses.

[6] L. Salgado Gutierrez, «PROPUESTA PARA LA MIGRACIÓN DEL PROTOCOLO IPV4 A IPV6 EN LA INFRAESTRUCTURA TECNOLÓGICVA DE UNA ORGANIZACIÓN CASO DE ESTUDIO,»

2019. [En línea]. Available: https://repository.unad.edu.co/jspui/bitstream/10596/28471/1/29818267.pdf .

[7] J. E. Plazas Tarache, «Diseño y análisis de infraestructura tecnológica de la alcaldía del municipio de Támara Casanare Colombia que permita la migración del protocolo IPv4 a IPv6,» 2025. [En línea]. Available: https://repository.unad.edu.co/bitstream/handle/10596/73582/jeplazasta.pdf?sequence=1&isAllowed=y.

[8] Gerard, «La evolución de las Direcciones IP:,» FactoríaDigital, 14 10 2014. [En línea]. Available: https://www.factoriadigital.com/la-evolucion-de-las-direcciones-ip-ipv4-vs-ipv6/.

[9] «Cisco,» Academy, 2022. [En línea]. Available: https://www.netacad.com/es/courses/networking-basics?courseLang=en-US.

[10] Nobia Azín, Diana Ramirez,Cybthia Gellibert, Andrea Hemerejildo, Deysi Terán, Harold Burbano, «PLAN NACIONAL DE DESARROLLO ECUADOR NO SE DETIENE 2025-2029,» 21 08 2025. [En línea]. Available: https://www.planificacion.gob.ec/wp-content/uploads/2025/08/PlanNacionalDeDesarrollo25-29_EcuadorNoSeDetiene.pdf.

[11] «¿Qué es el Protocolo de Internet?,» CLOUDFLARE, 2025. [En línea]. Available: https://www.cloudflare.com/es-es/learning/network-layer/internet-protocol/.

[12] C. Valdivia Miranda, «Sistema de telecomunicacuones e Informaticos ELECTRICIDAD Y ELECTRÓNICA,» de *Redes telemáticas*, Madrid-ESPAÑA, Paraninfo, 2015, p. 23.

[13] E. Ariganello, «REDES CISCO,» de *Guia de estudio para la certificación CCNA 200-301*, Madrid, Ra-Ma, 2024, p. 63.

[14] «¿Qué es una broadcast IP?,» IONOS, 13 05 2022. [En línea]. Available: https://www.ionos.com/es-us/digitalguide/servidores/know-how/broadcast-ip/.

[15] Raúl Hernández Palacios, Gonzalo Hernández Hernández , «Comunicaciones multicast,» UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO, 12 2016. [En línea]. Available: https://www.uaeh.edu.mx/scige/boletin/huejutla/n9/r1.html.

[16] A. Barbieri, «Modelo extendido de QoS sobre IPv6,» 11 2015. [En línea]. Available: https://sedici.unlp.edu.ar/bitstream/handle/10915/53028/Documento_completo__.pdf-PDFA.pdf?sequence=3&isAllowed=y.

[17] N. N. O. VILLÓN, *DISEÑO E IMPLEMENTACIÓN DE MECANISMOS DE CONVERGENCIA BRINDANDO CONEXIONES GPON PARA LA COMPARATIVA IPV4 E IPV6 EN EL LABORATORIO DE TELECOMUNICACIONES.,* LA LIBERTAD, 2022.

[18] Alejandro Acosta, Santiago Aggio, Guilllermo Cicileo, Tomas Lynch, Antonio M. Moreira, Mariela Rocha, Arturo Servin, Sofía Silva Berenguer, «Interner Society,» de *[::] IPv6 para operadores de Red*, Buenos Aire - Argentina, ISCO-Ar, 2014, p. 21.

[19] «Direcciones de Red IPv6,» Institut Sa Palomera, 2020. [En línea]. Available: https://www.sapalomera.cat/moodlecf/RS/1/course/module8/8.2.3.3/8.2.3.3.html.

[20] Microsoft, «Configuración 2: Tráfico IPv6 entre nodos en diferentes subredes de un trabajo de Internetwork IPv4 (6to4),» Microsoft Ignite, 12 006 2023. [En línea]. Available: https://learn.microsoft.com/es-es/windows/win32/winsock/configuration-2-ipv6-traffic-between-nodes-on-different-subnets-of-an-ipv4-internetwork-6to4--2.

[21] «¿Qué es una IPv6 Gateway?,» F5, 2025. [En línea]. Available: https://www.f5.com/es_es/glossary/ipv6-gateway.

[22] I. i, «Tipos de direcciones IPv6,» IBM, 07 10 2024. [En línea]. Available: https://www.ibm.com/docs/en/i/7.4.0?topic=concepts-ipv6-address-types.

[23] «Puente de red,» VAS Experts, 26 10 2022. [En línea]. Available: https://vasexperts.com/es/resources/glossary/bridge/.

[24] S. M. B. Fernando, «Monitoreo centralizado de las redes LAN y WAN de las sedes y matrices de la Universidad Regional Autonoma de los Andes Uniandes, para identificar oportunamente problemas.,» 2015. [En línea]. Available: https://dspace.uniandes.edu.ec/bitstream/123456789/3338/1/TUAMEIE004-2014.pdf.

[25] Ma Carmen MEdina Parreño, Jorge Mata, Franciscoj. Merino, Transición IPv4/IPv6, 2021.

[26] M. D. Katz, «IP Versión 6,» de *REDES Y SEGURIDAD*, Buenos Aires, Alfaomega, 2013, p. 115.

[27] C. A. M. ELIZABETH, «ESTUDIO COMPARATIVO DE LOS PROTOCOLOS IPV4, IPV6 Y SU APLICACIÓN EN VIDEO COMFERENCIA,» 10 2018. [En línea]. Available: https://dspace.utb.edu.ec/bitstream/handle/49000/4722/-E-UTB-FAFI-SIST-000110.pdf?sequence=1&isAllowed=y.

[28] MSc. Yesica Maria Pérez Pérez, MSc Andrés Mauricio Puentes Velásquez, «TRANSICIÓN DE IPv4 A IPv6: REVISION,» *Revista Colombiana de Tecnología avanzada,* vol. 2, nº 32-2018, p. 22, 2018.

[29] S. A. Hidrobo Mafla, «Metodología de transición del protocolo de inernet versión 4 a versión 6 en el gobierno provincial de Imbabura,» lacnic, 1 03

2016. [En línea]. Available: https://repositorio.utn.edu.ec/bitstream/123456789/7081/8/04%20RED%20091%20TRABAJO%20GRADO.pdf.txt.

[30] J. S. &. NAT64, «Introducción a la traducción de IPv4/IPv6,» TECNOLÓGICO DE MONTERREY, 2022. [En línea]. Available: https://www.jool.mx/en/intro-xlat.html.

[31] S.A, «Prefijos IPv6,» Oracle Homeage, 2010. [En línea]. Available: https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-170/index.html.

[32] IETF, «Acerca de las RFC,» IETF LLC, [En línea]. Available: https://www.ietf.org/process/rfcs/.

[33] «Guía de configuración basada en CLI del controlador de acceso inalámbrico (AC y Fit AP) V200R019C00,» HUAWEI, [En línea]. Available: https://support.huawei.com/enterprise/en/doc/EDOC1100096325/42f555dd/understanding-dhcpv6.

[34] FAQ, «[Firewall] ¿Cómo configurar Firewall IPv6?,» ASUS, 22 07 2024. [En línea]. Available: https://www.asus.com/es/support/faq/1013638/.

[35] Jeison Jair González Vargas, Jhon Edizon Cruz Hernández, «Diseño e implementación de una red corporativa en DUAL STACK (IPv4 e IPv6), para el fortalecimiento de la infraestructura tecnológica de las telecomunicaciones internas y externas de la CAR Cundinamarca,» 04 2021. [En línea]. Available: https://repository.unad.edu.co/bitstream/handle/10596/40253/jecruzhe.pdf?sequence=3&isAllowed=y.

[36] H. M. B. Palma, «EVALUACIÓN DE LOS MECANISMOS SEGURIDAD DE DNS EN REDES IPV4 E IPV6,» 07 2022. [En línea]. Available:

https://repositorio.puce.edu.ec/server/api/core/bitstreams/eb559611-7211-4d37-8c57-39e86bab0238/content.

[37] E. Sanchez, « Un estudio comparativo en Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNS),» 30 11 2017. [En línea]. Available: https://sedici.unlp.edu.ar/bitstream/handle/10915/63910/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y.

[38] F. Gont, «Network Security IPv6 Security for IPv4 Engineers,» 03 2019. [En línea]. Available: https://internetsociety.org/wp-content/uploads/2019/03/deploy360-ipv6-security-v1.0.pdf?utm_source=chatgpt.com.

[39] D. Doumun, «IPv6 and IPv4 Threat reviews with Automatic Tunneling and Configuration Tunneling Considerations Transitional Model:A Case Study for University of Mysore Network,» 04 08 2018. [En línea]. Available: https://arxiv.org/abs/0908.0548.

[40] «mikrotik,» Aplicación Mikrotik, [En línea]. Available: https://mikrotik.com/product/hex_s.

[41] Jairo José Bacusoy, Edwin Antonio Mero Lino, María Mercedes Ortiz Hernándes, Yenny Beatriz Mero Lino, Winbox ¿Qué es?, Ecuador: 3Ciencias, 2018.

[42] R. C. Z. Martinez, «Analisis y captura de paquete de datos en una red mediante Wireshark,» 2018. [En línea]. Available: http://repositorio.uisrael.edu.ec/bitstream/47000/168/1/UISRAEL-EC-SIS-378.242-404.pdf.

[43] Eva M. Castro, Jesús Gonzalez, Gregorio Robles, Tomás de Miguel, «Interoperidad de aplicaciones IPv4 e IPv6,» *Universidad Rey Juan Carlos de Madrid,* nº 28933, p. 2.

[44] J.R. Gomez-Rodriguez, R. Sandoval-Aréchiga, S. Ibarra-Delgado, J. Flores-Troncoso, «IpV6 El tiempi ha llegado,» *Universidad Autónoma de Zacatecas, Unidad Académica de Ingeniería Eléctrica,* vol. 10, nº 2, p. 5, 2017.

[45] K. Shashidhar, A. Mukta, C. Saurabh, B. Banish y G. Shailender, «Marco de asistencia para la migración de IPv4 a IPv6 basado en reglas,» vol. 01, p. 08, 2019.

[46] Nobia Azín , S. Moya Angulo y Z. Rovira Jurado, «PLAN DE DESARROLLO PARA EL NUEVO ECUADOR 2024-2025,» Secretaria Nacional de Planificación, 16 02 2024. [En línea]. Available: https://www.planificacion.gob.ec/wp-content/uploads/2024/02/PND2024 2025.pdf.

[47] A. F. Aldaz Corrales, «Análisis y diseño para la instalación del protocolo IPv6 en la red LAN de la Universidad de Granma,» 2007. [En línea]. Available: https://repositorio.utc.edu.ec/server/api/core/bitstreams/4e521454-43c6-4259-9ee7-230218b51f48/content.

ANEXOS

Anexo 1 Encuesta dirigidas a estudiantes de Facsistel

<table>
<tr><td colspan="3">Modelo experimental de migración progresiva de IPv4 a IPv6 utilizando mecanismos de túnel y traducción aplicado al laboratorio de redes de FACSISTEL.</td></tr>
<tr><td>Dirigida a:</td><td colspan="2">Estudiantes que utilizan el laboratorio de redes en la Facultad de Sistemas y Telecomunicaciones, perteneciente a la Universidad Estatal de la Península de Santa Elena.</td></tr>
<tr><td>Objetivo:</td><td colspan="2">Obtener datos importantes acerca de su nivel de entendimiento, así como de los requerimientos en relación con el cambio del protocolo IPv4 al protocolo IPv6 en el laboratorio de redes.</td></tr>
<tr><td>Sección 1:</td><td colspan="2">Información general</td></tr>
<tr><td colspan="2">Nivel de experiencia con redes:</td><td>¿Ha trabajado o estudiado alguna vez con el protocolo IPv6?</td></tr>
<tr><td colspan="2">o Básico
o Intermedio
o Avanzado</td><td>o Sí
o No
o Tal vez</td></tr>
<tr><td>Sección 2:</td><td colspan="2">Estado actual del laboratorio y conocimientos sobre IPv6</td></tr>
<tr><td colspan="2">¿Está al tanto de que el laboratorio de redes solo opera actualmente con protocolo IPv4?</td><td>¿Considera importante que el laboratorio implemente soporte completo para IPv6?</td></tr>
<tr><td colspan="2">o Sí
o No
o No estoy seguro/a</td><td>o Sí
o No
o No estoy seguro/a</td></tr>
<tr><td colspan="2">¿Crees que el uso de IPv6 mejoraría la calidad del aprendizaje en redes?</td><td>¿Consideras que aprender IPv6 es necesario para tu formación</td></tr>
</table>

	profesional en telecomunicaciones y sistemas?
o Sí o No o Tal vez	o Sí o No o No lo sé
Sección 3:	**Opinión sobre la implementación del prototipo**
Con relación a la migración a IPv6, ¿considera que las condiciones técnicas del laboratorio permiten mantener un desempeño óptimo en términos de control de acceso y velocidad de transferencia de datos?	¿Cree que sería beneficioso implementar un modelo de prueba para la transición de IPv4 a IPv6 en el entorno del laboratorio de forma controlada?
a. Sí b. No c. No lo sé	o Sí o No o Depende del presupuesto

Anexo 2 Permiso de uso de laboratorio de Redes

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECANATO

Oficio nº. UPSE-FST-2025-421-OF

La Libertad, agosto 26 de 2025

Asunto: Uso de laboratorios

Señor Licenciado
Daniel Quirumbay Yagual, MSIA.
DOCENTE DE LA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
En su despacho.

De mi consideración:

En atención al oficio sin número suscrito por su digna persona, me permito comunicar que se autoriza el uso del Laboratorio de Redes, debiendo coordinar las actividades prácticas del trabajo de titulación de los siguientes estudiantes con el Ing. Enrique Montenegro Romero, en función al horario de clases correspondientes al período académico 2025-2, donde el Laboratorio es usado por los estudiantes de las Carreras de la Facultad.

TRABAJO DE TITULACIÓN	ESTUDIANTES
Modelo de almacenamiento distribuido seguro mediante miniNAS y conexión VPN para entornos de protección de información crítica.	James Carvajal Núñez
Diseño de un entorno controlado para el análisis y monitoreo de tráfico de red en el laboratorio de redes de FACSISTEL.	Miguel Carcelén Tomalá
Modelo experimental de migración progresiva de IPv4 a IPv6 utilizando mecanismos de túnel y traducción aplicado al laboratorio de redes de FACSISTEL	Jorge Soledispa Saltos

Cabe destacar, que el uso de los equipos debe ser bajo responsabilidad exclusiva del Docente Tutor.

Particular que comunico a usted para los fines consiguientes.

Atentamente

WASHINGTON DANIEL TORRES GUIN

Ing. Washington Torres Guin, Mgt.
DECANO DE LA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

cc Ing. Enrique Montenegro Romero

WTG/lquimi

Anexo 3 Permiso de uso de laboratorio y uso de equipo

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECANATO

Oficio n°. UPSE-FST-2025-302-OF

La Libertad, junio 20 de 2025

Asunto: Uso de laboratorio

Señor Licenciado
Daniel Quirumbay Yagual, MSIA.
DOCENTE DE LA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
En su despacho.

De mi consideración:

En atención al oficio sin número suscrito por su digna persona, me permito comunicar que se autoriza el uso del Laboratorio de Redes, debiendo coordinar las actividades prácticas del trabajo de titulación de los estudiantes James Carvajal Núñez, Miguel Carcelén Tomalá y Jorge Soledispa Saltos, en función al horario de clases correspondientes al período académico 2025-1, donde el Laboratorio es usado por los estudiantes de las Carreras de la Facultad.

Cabe destacar, que el uso de los equipos debe ser bajo responsabilidad exclusiva del Docente Tutor.

Particular que comunico a usted para los fines consiguientes.

Atentamente

WASHINGTON DANIEL TORRES GUIN

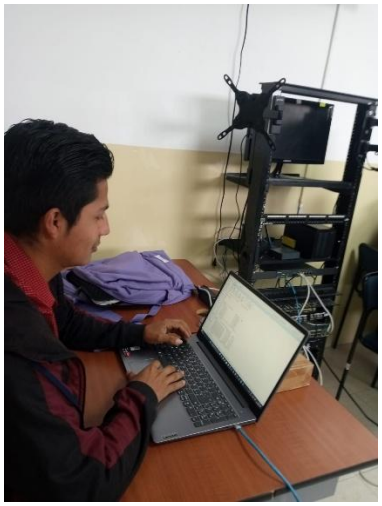
Ing. Washington Torres Guin, Mgt.
DECANO DE LA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

WTG/kjuimi

Anexo 4 Configuración del Mikrotik

Anexo 5 Armado final del RAD

Anexo 6 Configuración del túnel



MANUAL DE MIGRACIÓN DEL PROTOCOLO IPV4 A IPV6 UTILIZANDO MIKROTIK HEX S

Autor:

Jorge Joel Soledispa Saltos

Tutor:

Msia. Daniel Iván Quirumbay Yagual

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMA Y TELECOMUNICACIONES

SANTA ELENA

2025

MIKROTIK HEX S RB760IGS

Es un router gigabit ethernet que cuenta con cinco puertos y no requiere específicamente una conectividad inalámbrica, tiene un CPU de doble núcleo 880MHz, consta de una salida USB 2.0, un puerto POE y cinco puertos ethernet, además cuenta con una salida SFP de 1,25Gbit/s como se muestra en la Figura 51.

Figura 51 Equipo Mikrotik RB760IGS

Reset para el equipo mikrotik

Para aplicar el RESET tenemos dos modos en el equipo Mikrotik hEX S RB760IGS:

- Modo físico presionar el botón RESET por 10 segundos, esta opción permite restablecer al modo de fábrica como se muestra en la Figura 55.

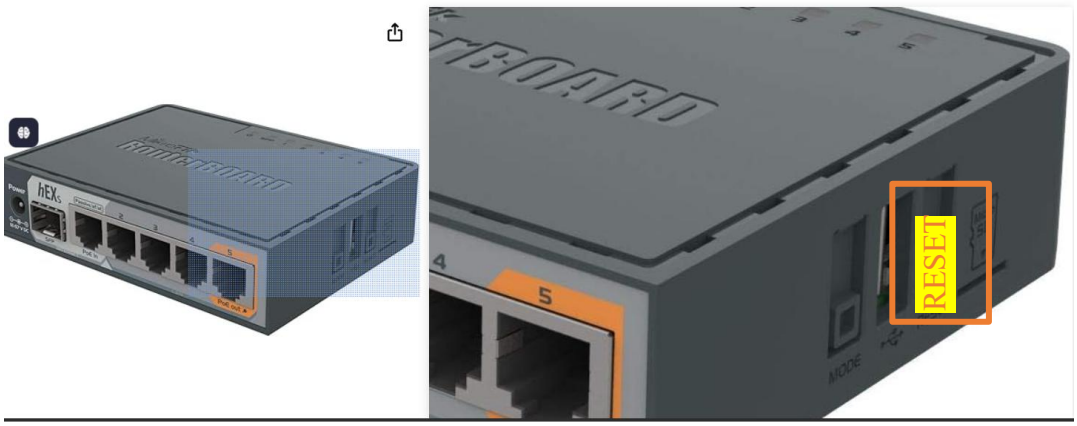


Figura 52 Botón RESET

- Ingresar a la interfaz mikrotik por el CLI en el Winbox donde se ingresa con las credenciales dados por el equipo en la parte posterior, una vez ingresado nos dirigimos a SYSTEM luego a RESET CONFIGURATION,

una vez ingresado se abre una venta con cinco opciones en la que se pueda mantener los usuarios creados o los paquetes adicionales instalados como se muestra en la Figura 56 y 57.

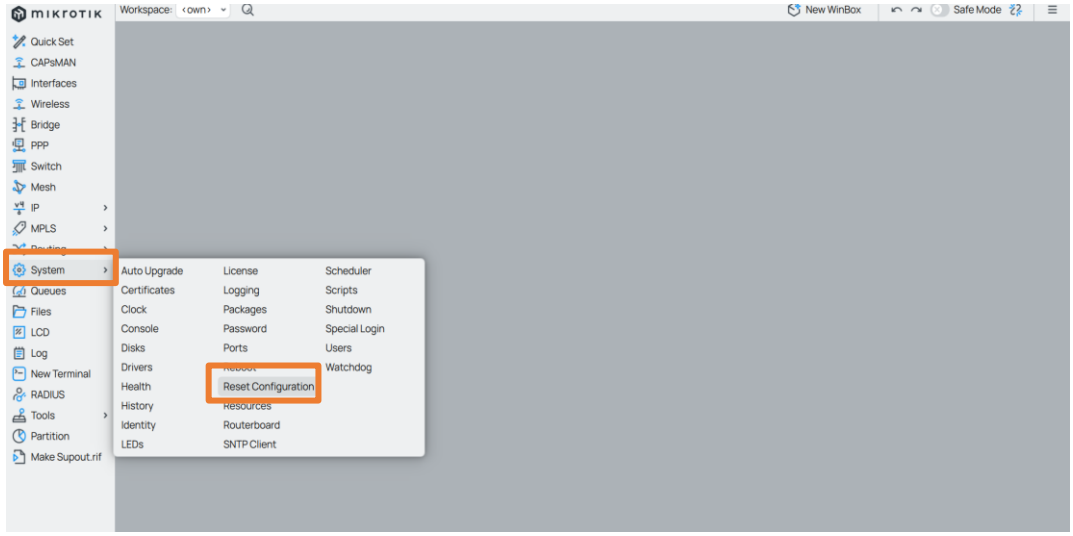


Figura 53 Modo reset configuration

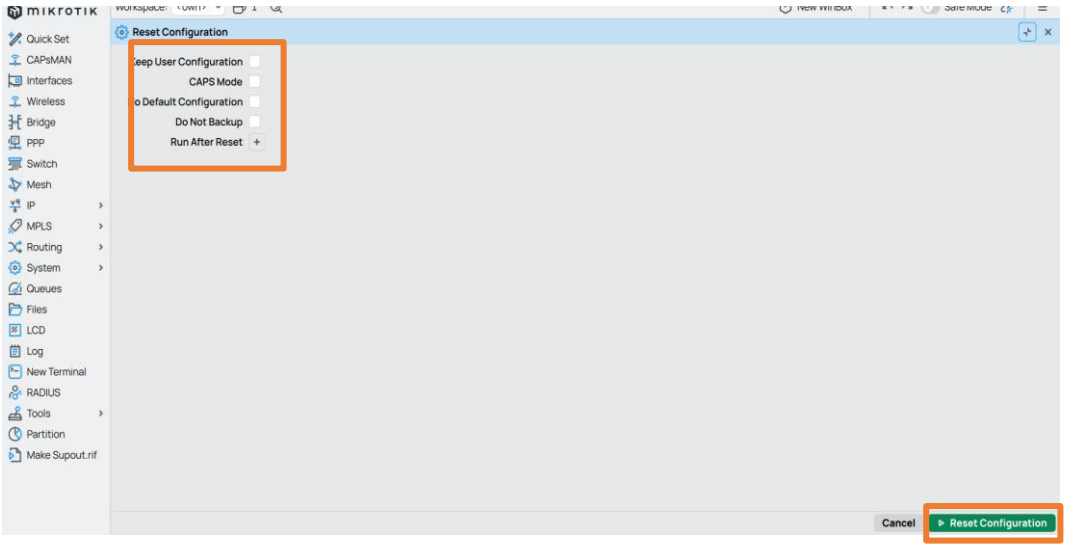


Figura 54 Opciones de RESET

ACTIVAR PAQUETE IPV6

Primero se verifica si el paquete viene activo y si no es así se procede con la activación, entonces se dirige a la opción de SYSTEM, luego a PACKAGES (Figura 58) una vez que se logra acceder se dirige a la pestaña con todos los paquetes disponibles y se selecciona IPv6 y luego se reinicia el dispositivo.

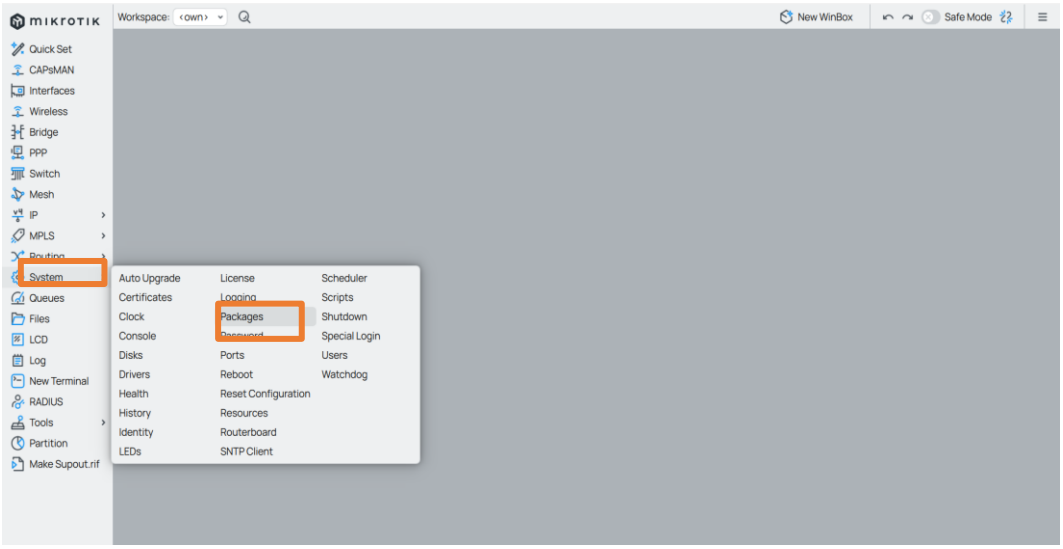


Figura 55 Activar paquete IPv6

Una vez obtenido IPv6 procedemos a hacer la configuración para poder tener la transición por aquello se aplicarán distintos métodos, pero llevando al mismo destino como primer método tenemos el DUAL STACK y el TUNNEL BROKER

Dual Stack

Se empieza verificando que en el Windows esté activado el paquete IPv6 ya que sin esto no se puede avanzar, una vez activado verificamos en el cable ethernet si está obteniendo DHCP de ambos protocolos como muestra la Figura 50.

Figura 56 Verificación de DHCP

Configurar la dirección IPv6 al puerto ether y luego se lo asigne al bridge para poder tener salida a través de la LAN como muestra la Figura 60.

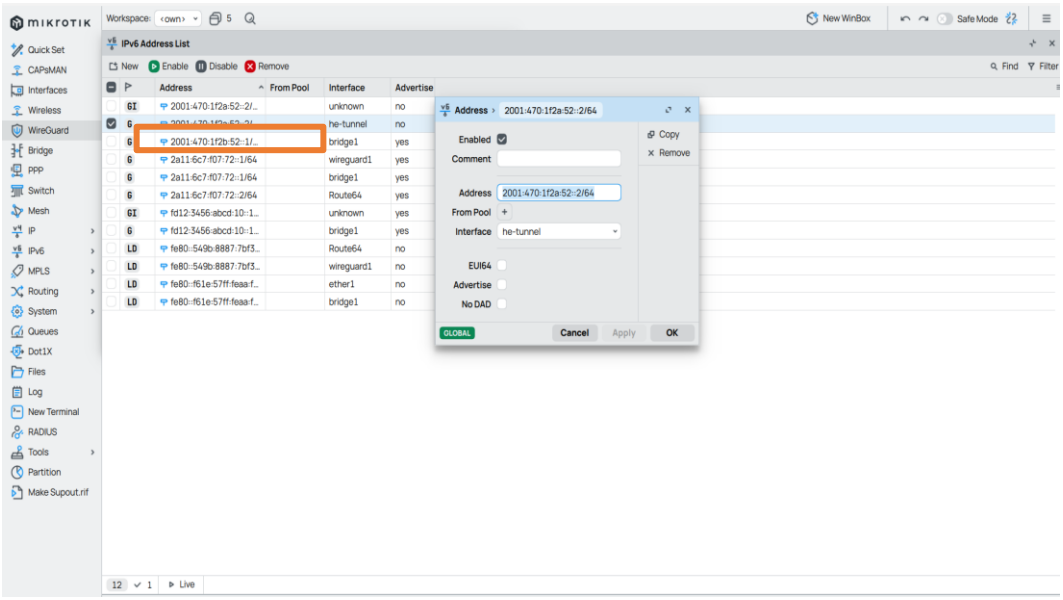


Figura 57 Asignar IPv6 al puerto Ether y Bridge

Una vez configurada se puede apreciar que la conexión está hecha correctamente y se hace ping desde el mikrotik a la PC con la dirección IPv6 que se le asignó por el DHCP como se muestra en la Figura 61.

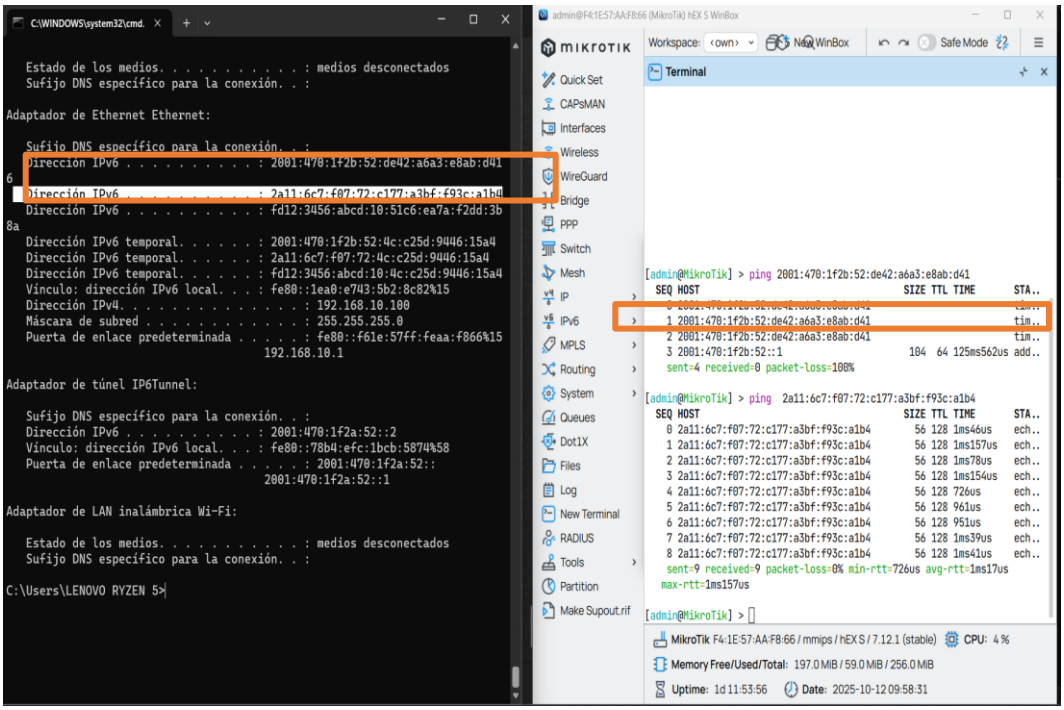


Figura 58 Conexión entre mikrotik y pc dual Stack

Túnel Hurricane Electric

Para crear el túnel IPIPv6 vamos a necesitar enlazar a un servidor remoto del IPv6 en este caso túnel hurricane (Figura 62) que permite obtener ipv6 de forma remota cuando el IP público del proveedor en este caso universitario no lo es de forma nativa, entonces se procede por utilizar esta aplicación.

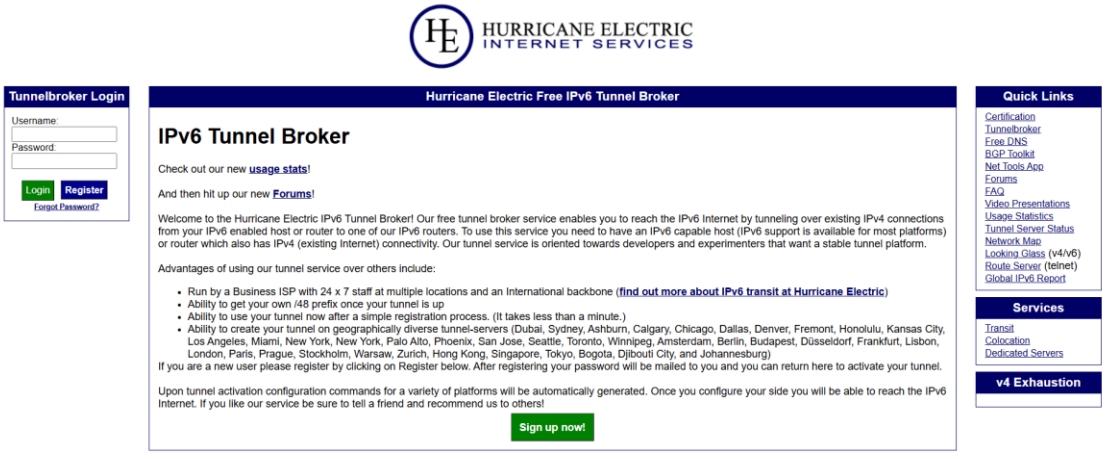


Figura 59 Túnel Hurricane Electric

Una vez creado el usuario por los diferentes métodos procedemos a crear el túnel con la IP pública del proveedor del internet y así poder tener el servicio IPv6

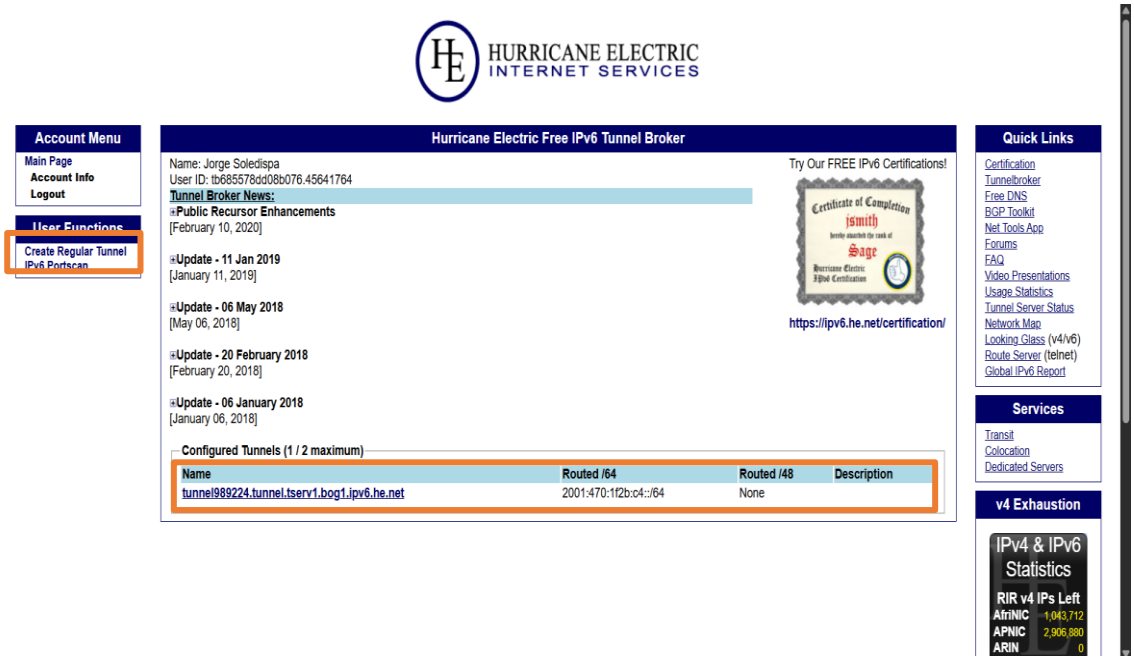


Figura 60 Crear el túnel con la IP pública

Con el IPv6 túnel creado ya podemos obtener el acceso remoto y hacer el enlace con el túnel desde el mikrotik aquí podemos ver el servidor remoto ipv6 y dns6 que nos servirá para asegurar la conexión como muestra la Figura 64.

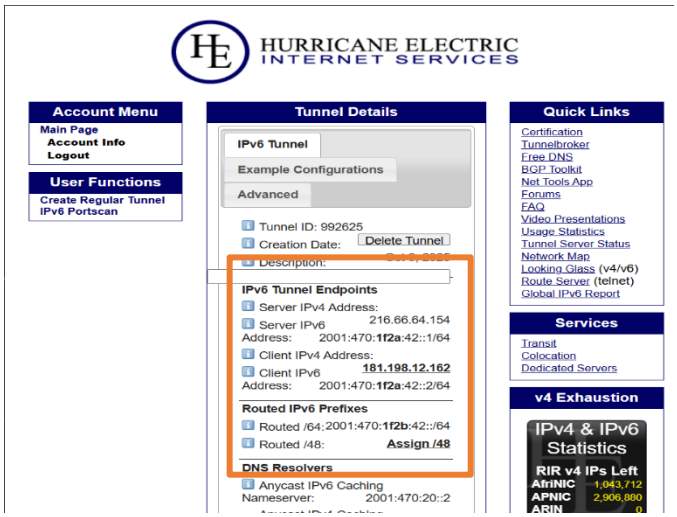


Figura 61 Dirección IP asignada por el túnel sobre IPv4

TUNEL IPIPV6

Este túnel se crea desde la interfaz mikrotik, dentro de la interface tenemos las opciones de túneles disponibles en este caso aplicamos el túnel IPIPV6 y le asignamos un nombre en este caso he-tunel y procedemos a darle la LOCAL ADDRESS y REMOTE ADDRESS (Figura 65) generadas por el servidor remoto HURRICANE.

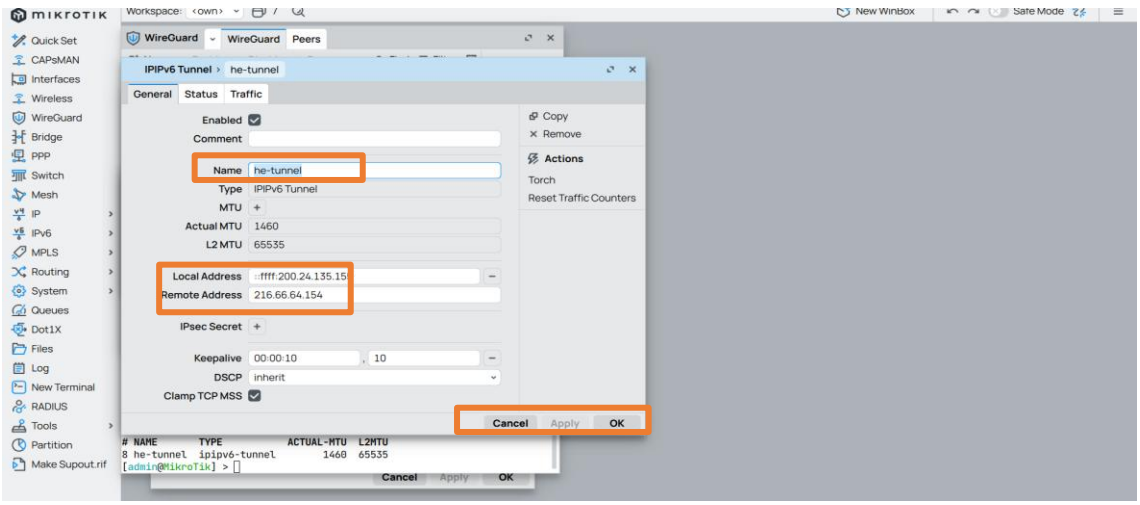


Figura 62 Crear túnel IPIPV6

Se procede a crear la dirección en ipv6 en la opción address luego le asignamos la dirección a la interface he-tunnel, con la advertise yes como muestra la Figura 66.

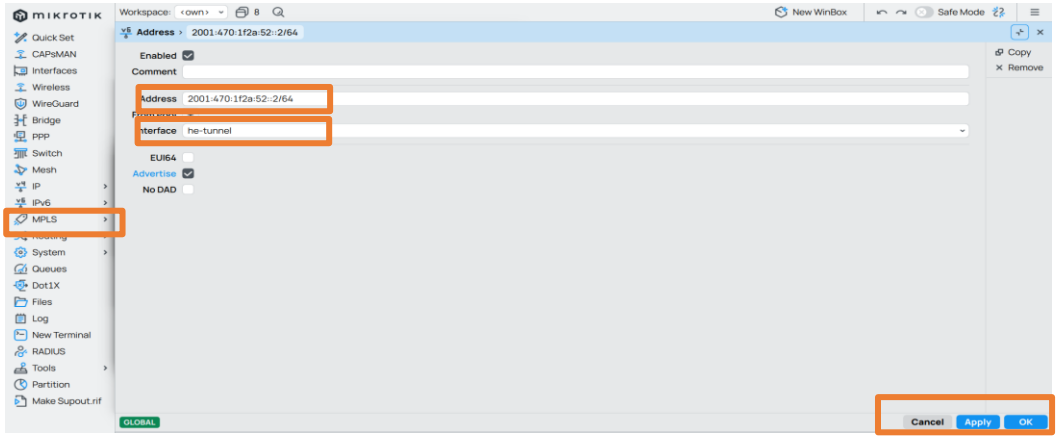


Figura 63 Asignar la dirección al túnel

Se aplica la asignación de la ruta del túnel creado para que permita pasar por los diferentes protocolos o restricciones, como muestra la Figura 67, y en la Figura 68 podemos comprobar la dirección, la ruta y la interfaz.

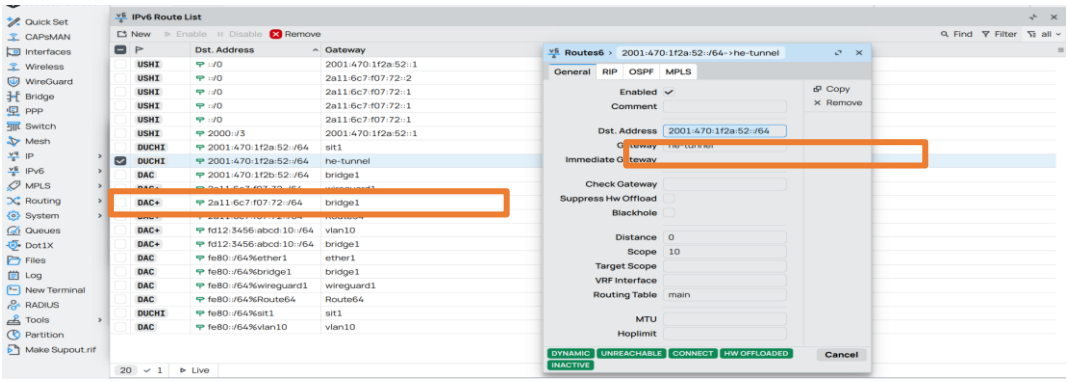


Figura 64 Asignación de rutas

Figura 65 Regla de firewall