Universidad de la Amazonia

TRANSICIÓN IPv4 – IPv6

FASE II IMPLEMENTACIÓN

Tabla de Contenido

Tabla de Gráficos

Introducción

Una vez concluida la fase de planeación estratégica y validado el diseño de implementación, se inicia formalmente la Fase II del proyecto de adopción del protocolo IPv6 en la Universidad de la Amazonia, correspondiente a la etapa de ejecución técnica y validación operativa. Esta fase materializa el plan previamente estructurado, mediante la intervención directa sobre la infraestructura tecnológica institucional, contemplando la configuración del nuevo esquema de direccionamiento, la actualización de parámetros en los dispositivos de red y la verificación integral de su funcionamiento en entornos controlados y productivos.

En el ámbito técnico, se realizaron ajustes y configuraciones en los equipos de enrutamiento y conmutación de la red institucional, habilitando el soporte para IPv6 tanto en el segmento WAN —encargado de la conectividad con el proveedor de servicios de Internet— como en las redes LAN internas. Se implementó el esquema de direccionamiento definido, aplicando segmentación con prefijos /64 para cada dominio de broadcast, en concordancia con las recomendaciones del estándar IPv6. Asimismo, se configuraron los mecanismos de Neighbor Discovery (ND) y Stateless Address Autoconfiguration (SLAAC), permitiendo la autoconfiguración de direcciones IPv6 en los dispositivos finales y garantizando la correcta resolución de vecinos, detección de routers y mantenimiento de tablas de vecindad a nivel de capa 3.

De manera paralela, se desarrolló una documentación técnica exhaustiva de todas las configuraciones efectuadas sobre plataformas de hardware, sistemas operativos, servicios de red y canales de comunicación con acceso a Internet. Esta

documentación incluye parámetros de direccionamiento, políticas de enrutamiento, configuraciones de interfaces, VLAN de prueba y validaciones de conectividad interna y externa. Como parte del aseguramiento de calidad y gestión del riesgo, se habilitó una VLAN independiente destinada exclusivamente a pruebas piloto, lo que permitió evaluar el comportamiento del protocolo en un entorno aislado, verificando la conectividad inter-VLAN, la resolución de rutas, la estabilidad del enrutamiento y la compatibilidad de aplicaciones críticas y sistemas de almacenamiento, sin comprometer la operación del entorno productivo.

En términos estratégicos, esta fase tiene como finalidad garantizar que la adopción de IPv6 se realice bajo criterios de seguridad, estabilidad y continuidad del servicio, minimizando riesgos operativos y asegurando la interoperabilidad con la infraestructura existente bajo un esquema de doble pila (Dual Stack). De esta manera, se consolida una transición técnica controlada y progresiva, alineada con las mejores prácticas internacionales y con los lineamientos de modernización tecnológica del sector público, fortaleciendo la capacidad institucional para enfrentar los desafíos de crecimiento, escalabilidad y sostenibilidad de la red a mediano y largo plazo.

Objetivos

Objetivo General

Implementar la configuración del protocolo IPv6 en la infraestructura tecnológica de la Universidad de la Amazonia, garantizando su correcta integración en los entornos WAN y LAN, la interoperabilidad con IPv4 bajo un esquema de doble pila y la continuidad operativa de los servicios institucionales.

Objetivos Específicos

- Configurar el direccionamiento IPv6 en los entornos WAN y LAN institucionales.
- Validar la conectividad y el funcionamiento de los servicios mediante pruebas piloto y definitivas.
- Documentar las configuraciones realizadas en los equipos, servicios y canales de comunicación intervenidos.

Plan Implementación

Protocolo Seleccionado

Para la configuración interna del direccionamiento IPv6 en la red institucional, se adoptó el protocolo Neighbor Discovery (ND) como mecanismo principal de autoconfiguración y gestión de conectividad en la red LAN. Esta decisión se fundamenta en que ND constituye un componente nativo del protocolo IPv6, diseñado específicamente para reemplazar funciones tradicionales de IPv4 como ARP, ICMP Router Discovery y ciertos procesos dependientes de DHCP.

Neighbor Discovery opera sobre ICMPv6 y permite que los dispositivos dentro de una red local puedan:

- Descubrir automáticamente la presencia de routers.
- Obtener información del prefijo de red.
- Configurar su propia dirección IPv6 de manera autónoma.
- Resolver direcciones MAC mediante Neighbor Solicitation (NS) y Neighbor Advertisement (NA).
- Verificar la unicidad de direcciones a través del proceso Duplicate Address Detection (DAD).

Mecanismo de Asignación de Direcciones IPv6

Dentro del marco de Neighbor Discovery, se implementó el mecanismo SLAAC (Stateless Address Autoconfiguration) para la asignación automática de direcciones IPv6 en las redes LAN institucionales. El uso de SLAAC permitió:

- Reducir la complejidad operativa al no depender exclusivamente de un servidor DHCPv6 para la asignación de direcciones.
- Facilitar la escalabilidad de la red, especialmente considerando la segmentación por VLAN con prefijos /64.
- Permitir que cada dispositivo genere su dirección IPv6 combinando el prefijo anunciado por el router con su identificador de interfaz.
- Minimizar puntos únicos de falla en la asignación de direccionamiento interno.

Este enfoque es particularmente adecuado en entornos con múltiples segmentos de red, como la Universidad, donde cada VLAN institucional dispone de su propio prefijo /64.

Implementación en la Infraestructura MikroTik

La Ilustración 1 corresponde a la sección IPv6 → Neighbor Discovery → Prefixes del enrutador MikroTik, donde se visualiza la configuración de los prefijos IPv6 anunciados en las diferentes interfaces de la red institucional. En esta vista se observan varios prefijos con longitud /64, cada uno asociado a una interfaz específica, lo que indica que el equipo está realizando anuncios de enrutador (Router Advertisements – RA) para permitir la autoconfiguración automática de direcciones en los dispositivos conectados a cada segmento.

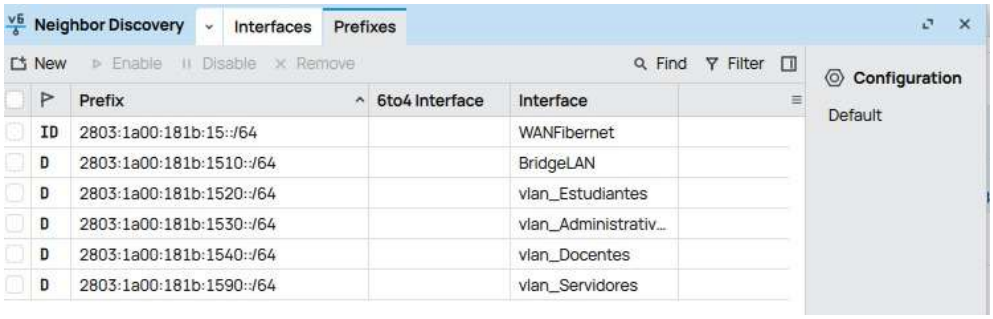

Ilustración 1. Configuración Prefijos Neighbor Discovery – IPv6.

El prefijo configurado sobre la interfaz WANFibernet aparece identificado con la etiqueta ID, lo que indica que corresponde a una configuración estática definida manualmente para la red WAN. Por su parte, los demás prefijos asociados a BridgeLAN, vlan_Estudiantes, vlan_Administrativos, vlan_Docentes y vlan_Servidores aparecen marcados con la letra D, lo que señala que son prefijos dinámicos, generalmente derivados del bloque principal asignado y gestionados automáticamente por el sistema. Esta distribución evidencia una correcta segmentación de la red mediante VLAN, donde cada dominio lógico dispone de su propio prefijo /64 para garantizar orden, aislamiento y escalabilidad.

La configuración mostrada confirma que el MikroTik está operando como router IPv6 y como generador de anuncios ND en cada interfaz interna, habilitando el mecanismo SLAAC para que los equipos finales obtengan su dirección IPv6 sin intervención manual. De esta manera, la infraestructura mantiene una administración eficiente del direccionamiento, optimiza la distribución de recursos y asegura el cumplimiento de las mejores prácticas en la implementación del protocolo IPv6 dentro de la red institucional.

Ventajas Operativas

La implementación basada en Neighbor Discovery y SLAAC proporciona múltiples beneficios:

- Alta escalabilidad: Cada nueva VLAN o segmento puede configurarse simplemente asignando un nuevo prefijo /64.
- Eficiencia administrativa: Se reduce la carga de gestión al no requerir asignaciones manuales por dispositivo.
- Compatibilidad estándar: Todos los sistemas operativos modernos soportan SLAAC de forma nativa.
- Reducción de dependencia de servicios adicionales: Aunque se puede integrar DHCPv6 para parámetros complementarios (como DNS), la asignación de direcciones no depende exclusivamente de este servicio.
- Alineación con buenas prácticas IPv6: El uso de /64 por segmento y autoconfiguración mediante RA es el modelo recomendado internacionalmente.

La adopción del protocolo Neighbor Discovery como mecanismo principal para la configuración interna IPv6 representa una decisión técnica estratégica, ya que permite una red moderna, escalable y acorde con la evolución del estándar IPv6. La implementación mediante SLAAC garantiza automatización, estabilidad y reducción de complejidad operativa, mientras mantiene la posibilidad de integrar DHCPv6 para configuraciones complementarias.

Este modelo asegura que la infraestructura de la Universidad de la Amazonia esté preparada para soportar el crecimiento institucional, la expansión de servicios

digitales y la transición progresiva hacia un entorno plenamente compatible con IPv6.

Pruebas Piloto

Con el propósito de realizar las pruebas piloto para la implementación del protocolo IPv6, se creó una VLAN específica identificada como VLAN 511 – IPV6, como se observa en la Ilustración 2. Esta segmentación permitió aislar el entorno de pruebas del resto de la infraestructura productiva, minimizando riesgos sobre los servicios institucionales activos.

```
Status and Counters - VLAN Information

 Maximum VLANs to support : 256
 Primary VLAN : DEFAULT_VLAN
 Management VLAN :

 VLAN ID Name                             | Status     Voice Jumbo
 ------- -------------------------------- + ---------- ----- -----
 1       DEFAULT_VLAN                     | Port-based No    No
 2       Hearbeat                         | Port-based No    No
 501     Wifi-Publica                     | Port-based No    No
 502     Estudiantes                      | Port-based No    No
 503     Administrativos                  | Port-based No    No
 504     Docentes                         | Port-based No    No
 505     Gestion                          | Port-based No    No
 506     VoIP                             | Port-based Yes   No
 507     CCTV                             | Port-based No    No
 508     Disp-Impresoras                  | Port-based No    No
 509     Servidores                       | Port-based No    No
 510     Biometrico                       | Port-based No    No
 511     IPV6                             | Port-based No    No
```

Ilustración 2. Creación VLAN Para Prueba Piloto.

Tal como se observa en la configuración del switch, la VLAN 511 fue definida bajo un esquema Port-based, al igual que las demás VLAN institucionales (Estudiantes, Administrativos, Docentes, Servidores, entre otras), garantizando

coherencia en la estructura de segmentación de red. Esta VLAN fue utilizada para validar la asignación de direccionamiento IPv6, el funcionamiento de Neighbor Discovery, la autoconfiguración mediante SLAAC y las pruebas de conectividad interna y externa antes de su despliegue definitivo en las redes LAN oficiales.

La creación de esta VLAN de laboratorio permitió verificar el comportamiento del nuevo protocolo en condiciones controladas, asegurando compatibilidad con los equipos de red, servicios y aplicaciones institucionales, y reduciendo el impacto operativo durante la fase de transición.

Prueba Asignación IPv6 vía Ethernet

En la Ilustración 3 se evidencia la correcta asignación de direccionamiento IPv6 en un equipo servidor dentro de la red institucional. A través del comando ipconfig ejecutado en el símbolo del sistema, se observan direcciones IPv6 globales asignadas al adaptador Ethernet, específicamente dentro de los prefijos 2803:1a00:181b:1510::/64 y 2803:1a00:181b:1590::/64, lo que confirma la correcta propagación de los prefijos configurados en el enrutador mediante Neighbor Discovery y SLAAC.

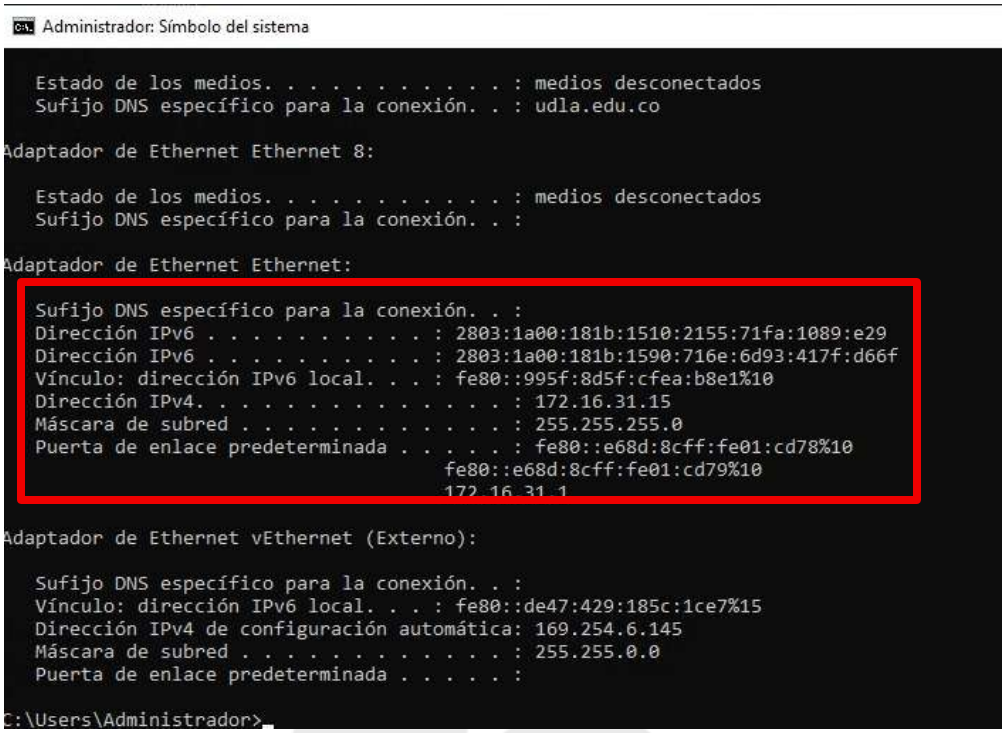

Ilustración 3. Asignación Automática IPv6 vía Ethernet.

Asimismo, se visualiza la dirección IPv6 local de enlace (fe80::/10) y la puerta de enlace predeterminada configurada también en formato IPv6, lo que demuestra que el equipo no solo recibió una dirección válida, sino que además estableció comunicación con el router IPv6 de la red.

Esta evidencia técnica valida el funcionamiento adecuado del esquema de direccionamiento implementado y confirma que el proceso de configuración interna de IPv6 se encuentra operativo a nivel de host, permitiendo la coexistencia con IPv4 en un entorno de doble pila (Dual Stack).

Prueba Asignación IPv6 vía Inalámbrica

La información presentada en la ilustración 4 refleja la correcta asignación de direccionamiento IPv6 a través del medio inalámbrico (Wi-Fi). En la salida del comando ipconfig se observa que el adaptador de LAN inalámbrica posee direcciones IPv6 globales pertenecientes al prefijo institucional 2803:1a00:181b:1510::/64, así como una dirección local de enlace (fe80::/10), lo cual confirma la recepción de mensajes de anuncio de router (RA) y el funcionamiento adecuado del mecanismo de autoconfiguración.

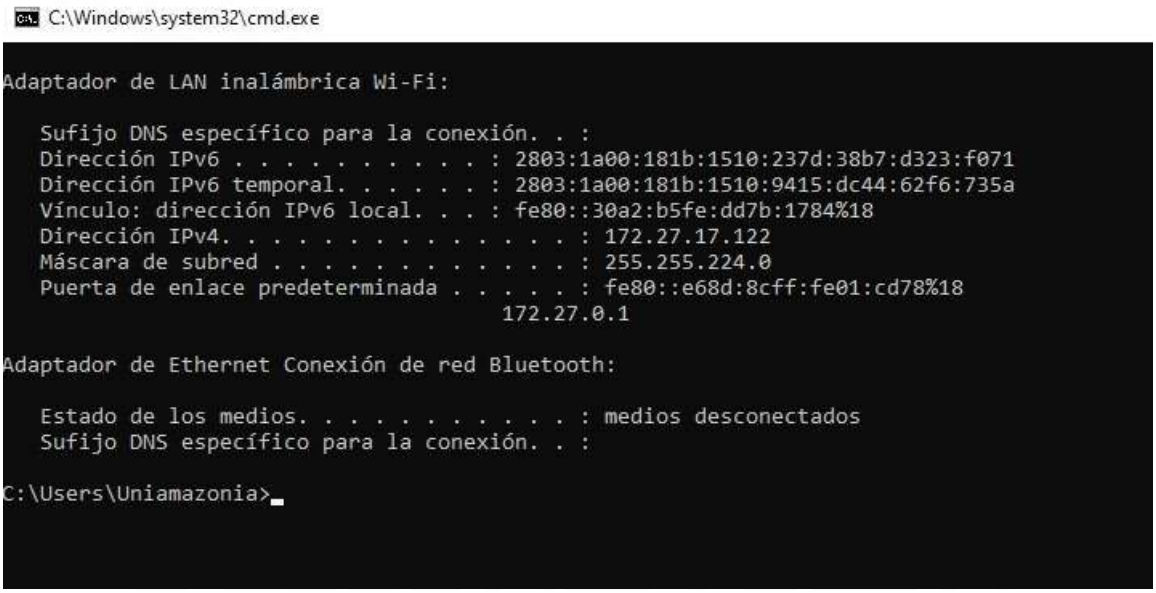

Ilustración 4. Asignación Automática IPv6 vía Inalámbrica

Adicionalmente, el equipo mantiene simultáneamente una dirección IPv4 (172.27.17.122) con su respectiva puerta de enlace, evidenciando un entorno de doble pila (Dual Stack) también en el segmento inalámbrico. Esto demuestra que la infraestructura Wi-Fi institucional soporta correctamente la implementación de IPv6

sin afectar la operatividad de IPv4, garantizando conectividad, interoperabilidad y continuidad del servicio en la red inalámbrica.

Pruebas de Comunicaciones

Verificación de Conectividad IPv6 mediante Ping

Con el fin de validar el correcto funcionamiento del direccionamiento IPv6 y el enrutamiento inter-VLAN, se realizó una prueba de conectividad desde un equipo cliente conectado a la red inalámbrica institucional hacia un equipo ubicado en una VLAN diferente, ambos con direcciones IPv6 globales asignadas, tal como se observa en la Ilustración 5.

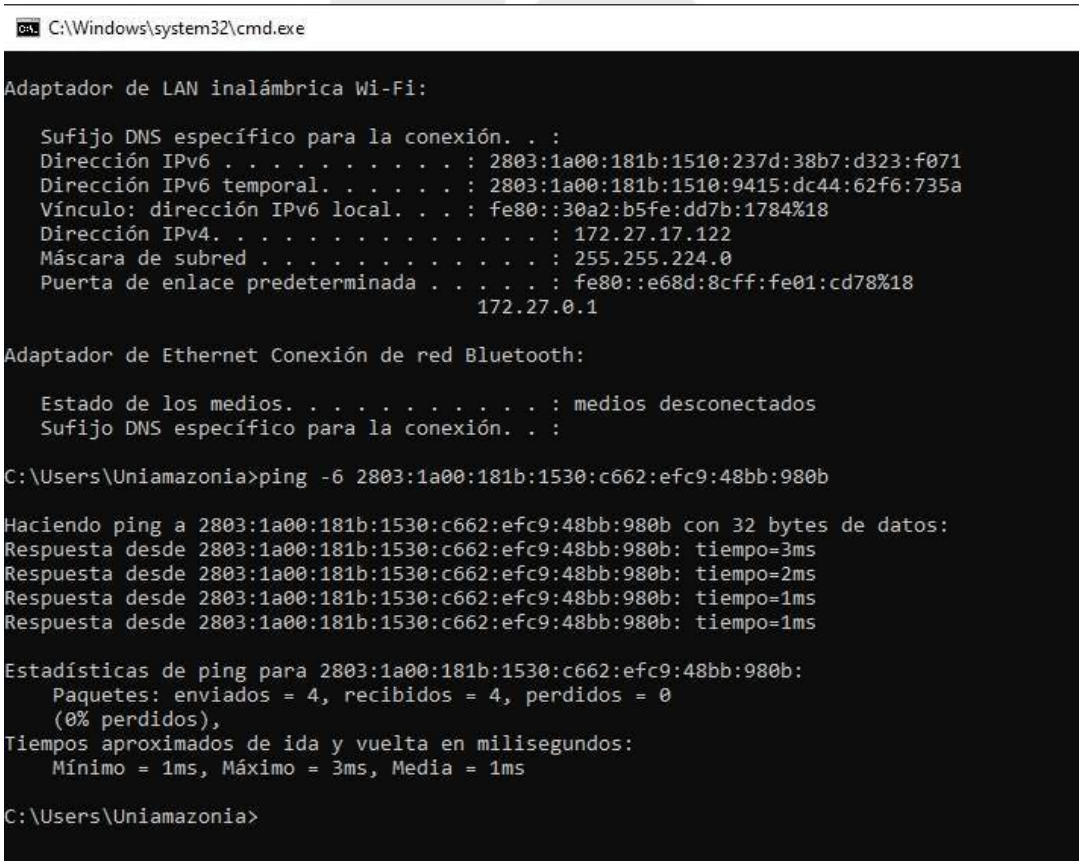

Ilustración 5. Ping Interno Entre Equipos de Distintas VLAN.

El equipo origen presentaba una dirección IPv6 perteneciente al prefijo 2803:1a00:181b:1510::/64, mientras que el equipo destino se encontraba en la subred 2803:1a00:181b:1530::/64, lo que confirma que ambos dispositivos pertenecen a segmentos de red distintos. Esta condición implica que la comunicación debía atravesar el enrutador principal (MikroTik), encargado de realizar el enrutamiento entre VLANs.

La prueba se ejecutó mediante el comando ping -6, obteniendo como resultado la recepción del 100% de los paquetes enviados, sin pérdidas y con tiempos de respuesta promedio entre 1 ms y 3 ms. Estos resultados evidencian que:

- El direccionamiento IPv6 fue correctamente asignado a los equipos.
- El protocolo Neighbor Discovery se encuentra funcionando adecuadamente.
- El enrutamiento IPv6 entre VLANs está correctamente configurado.
- No existen restricciones de firewall que bloqueen tráfico ICMPv6 interno.

En consecuencia, se valida que la segmentación lógica de la red mediante VLANs mantiene su aislamiento estructural sin afectar la comunicación entre redes, garantizando conectividad eficiente y estable dentro del entorno institucional bajo el nuevo esquema de direccionamiento IPv6.

Verificación de Enrutamiento mediante Tracert

Para validar el correcto funcionamiento del enrutamiento IPv6 dentro de la red institucional, se realizó una prueba de trazabilidad utilizando el comando tracert -6 desde un equipo cliente hacia un host ubicado en una VLAN diferente. Esta

prueba permitió verificar no solo la conectividad entre subredes, sino también el comportamiento del router principal como dispositivo de enrutamiento inter-VLAN en el entorno IPv6.

En la Ilustración 6 se observa que la comunicación se estableció en únicamente dos saltos. El primer salto correspondió a la dirección IPv6 2803:1a00:181b:1520::1, identificada como la puerta de enlace configurada en el router MikroTik para la VLAN de origen. Este equipo actúa como nodo central de enrutamiento, permitiendo la interconexión entre las distintas subredes /64 asignadas a cada segmento lógico de la red.

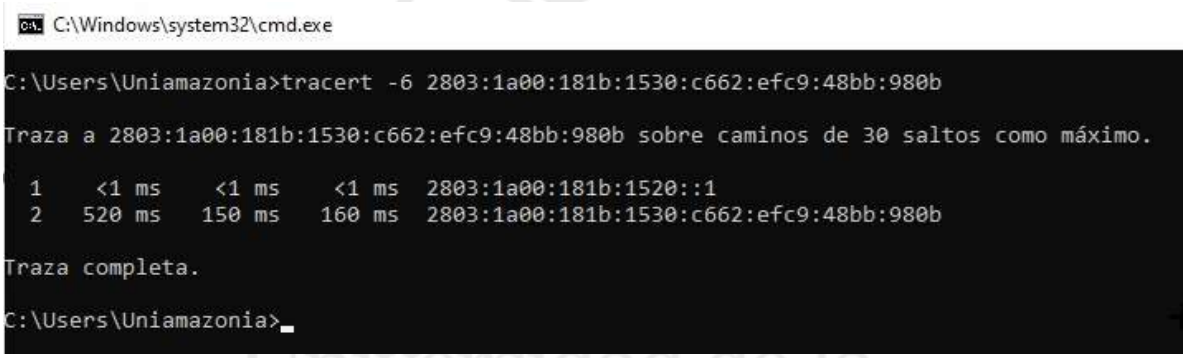

Ilustración 6. Prueba de Traza Entre Equipos de Distintas VLAN.

El segundo salto correspondió directamente a la dirección IPv6 del equipo destino (2803:1a00:181b:1530:c662:efc9:48bb:980b), lo que confirma que el tráfico fue correctamente encaminado hacia la VLAN objetivo sin rutas intermedias adicionales. La traza se completó satisfactoriamente, evidenciando que no existen bloqueos de ICMPv6 ni inconsistencias en la tabla de enrutamiento.

Cronograma de Actividades

Cronograma de Actividades – Fase II: IMPLEMENTACIÓN		Año 2025												Año 2026							
N°	Actividad	Octubre				Noviembre				Diciembre				Enero				Febrero			
		Sem. 1	Sem. 2	Sem. 3	Sem. 4	Sem. 1	Sem. 2	Sem. 3	Sem. 4	Sem. 1	Sem. 2	Sem. 3	Sem. 4	Sem. 1	Sem. 2	Sem. 3	Sem. 4	Sem. 1	Sem. 2	Sem. 3	Sem. 4
1	Habilitación direccionamiento IPv6 (plan de numeración) para cada uno de los componentes de hardware y software de acuerdo con el plan de diagnóstico de la Primera Fase.																				
2	Configuración de servicios de DNS, DHCP, Seguridad, VPN, servicios WEB, entre otros.																				
3	Configuración del protocolo IPv6 en aplicativos, sistemas de Comunicaciones, sistemas de almacenamiento y en general de los equipos susceptibles a emplear direccionamiento IP.																				
4	Activación de políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea cada entidad de acuerdo con los RFC de seguridad en IPv6																				
5	Coordinación con el (los) proveedor (es) de servicios de Internet ISP, para establecer el enrutamiento y la conectividad integral en IPv6 nativo hacia el exterior.																				

Ilustración 7. Cronograma de Actividades Fase II – Implementación.

JAIRO ANDRES DURANGO HERNANDEZ
Coordinador
Oficina Asesora de Tecnologías de la Información
Universidad de la Amazonia

Proyectó. Juan Manuel Claros Guevara.
Revisó. Yhefferson Esneider Huaca Nuñez.