Memoria Técnica

Documento que contiene las especificaciones y requerimientos técnicos del bien o servicio de TIC.

Proyecto: Memoria Técnica que deriva del Piloto de Transición a un Ambiente Operacional de sólo IPv6

V1.1 27/12/2022

Fecha:	Elaboró:	Revisó:	Autorizó:
31/08/2022	Ing. Donato Lucio Lopez Lopez	Ing. Omar Mercado Pedraza	Mtra. Maria de Lourdes Zaldivar Martínez
Puesto	*Coordinador de la Red de Datos*	*Jefe del Departamento de Gestión de Arquitectura e Infraestructura Tecnológica*	*Subdirectora de Tecnologías de la Información y Comunicaciones*
Firma			

CONTENIDO

OBJETIVO DEL DOCUMENTO

El documento tiene como objetivo describir y definir los escenarios y requerimientos que cada uno implica para la implementación de la infraestructura y aplicaciones que formaran parte del escenario de prueba piloto de transición a un ambiente operacional de solo IPv6.

ABREVIATURAS Y DEFINICIONES

Abreviación o acrónimo	Descripción
INRLGII	Instituto Nacional de Rehabilitación Luis Guillermo Ibarra Ibarra
ADTI	Administración para las contrataciones de TIC
APBS	Administración de proveedores de bienes y servicios de TIC
DGE	Departamento de Gestión Estratégica
DGAIT	Departamento de Gestión de la Arquitectura e Infraestructura Tecnológica
IPv6	Protocolo Internet versión 6
issues	Problemas o reglas de seguridad
Routing	la capacidad de buscar la ruta correcta para mover o transferir paquetes de información entre una o varias redes de Internet.
CEDN	Coordinación de la Estrategia Digital Nacional

REFERENCIAS

Nombre del documento	Descripción y ubicación del documento
Manual Administrativo de Aplicación General en materia de Tecnologías de Información y Comunicaciones y Seguridad de la Información.	www.normateca.gob.mx
	https://hgptic.presidencia.gob.mx/hgptic/

OBJETIVO

Realizar Prueba piloto de solo IPV para una transición planificada y de manera gradual al protocolo de internet versión 6 (IPV6) en el Instituto Nacional de Rehabilitación Luis Guillermo Ibarra Ibarra en los equipos de comunicaciones que ven hacia la parte WAN y la Nube de Internet de alta criticidad que conforman la infraestructura de Tecnologías de la Información y Comunicaciones dentro del INR LGII procurando en todo momento la no interrupción o la menor interrupción posible de los servicios.

GENERALES DEL ALCANCE.

El presente documento describe las opciones para la realización de la prueba piloto de IPv6 conforme a las condiciones de existencia del bloque de direcciones asignado a la institución a través de un ISP, así como el respectivo enlace de acceso a Internet, a través del uso del esquema de direccionamiento IPv6.

ANTECEDENTES.

Con fecha 06 de septiembre de 2021 fue publicado en el Diario Oficial de la Federación el ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal, el cual establece en su ARTÍCULO DÉCIMO transitorio que la Coordinación de la Estrategia Digital Nacional (CEDN) emitirá la Guía para la migración al Protocolo de Internet versión 6; dentro de los tres meses posteriores a la publicación de este Acuerdo, a partir de esa fecha, las Instituciones contarán con un plazo de 2 años para concretar la migración de sus servicios de telecomunicaciones.

Con fecha 7 de diciembre de 2021, la CEDN emite la "Guía para la Transición al Protocolo de internet versión 6 (IPv6) en la Administración Pública Federal", en la cual se establecen las disposiciones de carácter general para orientar a las Instituciones Federales, en las acciones técnicas a desarrollar, con la finalidad de que la transición al Protocolo de Internet versión 6 se lleve a cabo de forma expedita y coordinada, con un mínimo de interrupciones y trastornos de carácter técnico u operativo, y en observancia de los controles mínimos de Seguridad de la Información, y su cumplimiento es de carácter general y obligatorio para todas las instituciones de la Administración Pública Federal.

A fin de dar cumplimiento al Artículo 52 del Acuerdo publicado en el Diario Oficial de la Federación el día 06 de septiembre de 2021, la STIC debe notificar a la CEDN al 31 de diciembre de 2022:

- Piloto de transición a un ambiente operacional de solo IPv6.
- Memoria técnica que derive del Piloto de transición a un ambiente operacional de solo IPv6

Derivado de dichos acuerdos y a la demanda de direccionamientos en el mercado actual, lo cual resulta insuficiente el rango de direcciones IPv4, La Subdirección de Tecnologías de la información y comunicaciones del Instituto Nacional de Rehabilitación Luis Guillermo Ibarra Ibarra, se dio a la tarea de realizar esta Memoria Técnica que deriva del Piloto de Transición a un Ambiente Operacional de sólo IPv6, llevando a cabo las acciones que a continuación se mencionan:

ESTRUCTURA DE ASIGNACIÓN DE UNA DIRECCIÓN IPV6

- La dirección IPv6 tiene formato hexadecimal de 128 bits (de "0" hasta "9", de "A" hasta "F")
- La dirección IPv6 consta de 8 cuartetos = 8 grupos de cuatro dígitos hexadecimales
- Cada cuarteto de la dirección IPv6 está separados por dos puntos (:)

2001:0DB8:0001:5276:0127:00AB:CAFE:0E1F

0101 0010 0111 0110 = 16 bits

- Se pueden omitir los ceros iniciales en cualquier cuarteto. Ojo que esta regla se aplica a los ceros iniciales.

Dirección antes de la omisión:
2003:0DB8:0001:5270:0127:00AB:CABE:0E1F
Dirección después de la omisión:
2003:DB8:1:5270:127:AB:CABE:E1F

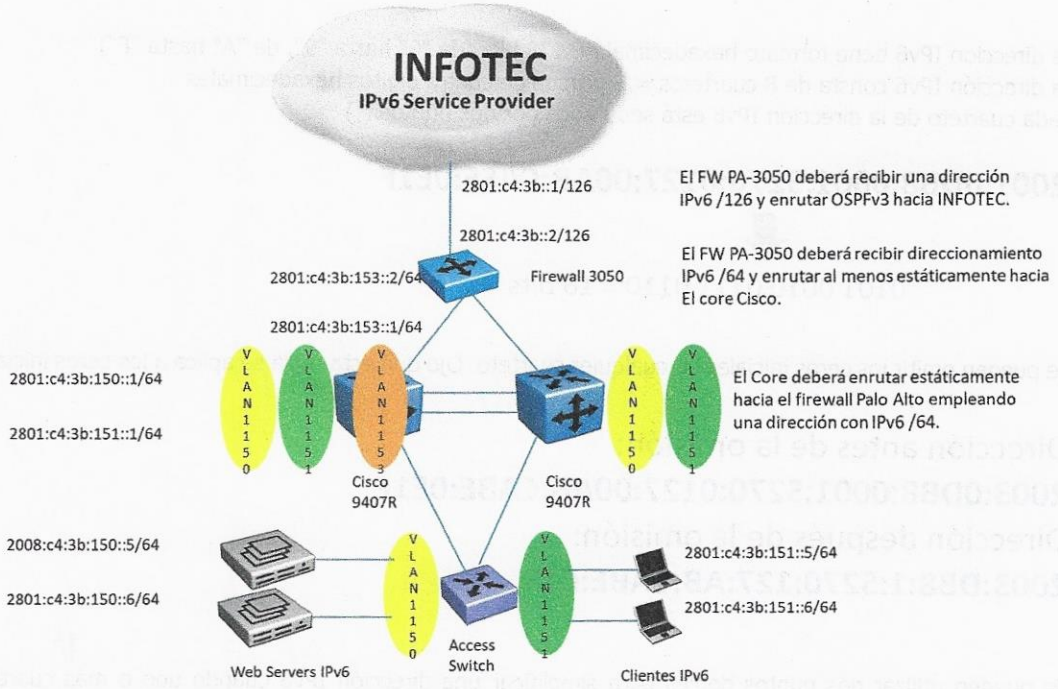
- Se pueden utilizar dos puntos dobles para simplificar una dirección IPv6 cuando uno o más cuartetos consisten solo de ceros. Éstos cuartetos deben ser consecutivos y solo puede usarse una única vez en una dirección IPv6

2003:ABCD:0000:0000:3456:0000:0000:1234
Puede usar una de estas dos direcciones IPv6 simplificadas:
Op 1: **2003:ABCD::3456:0:0:1234**
Op 2: **2003:ABCD:0:0:3456::1234**

Comúnmente se tiene los siguientes prefijos de formato predefinidos:

- Dirección IPv6 no especificada (::/128)
- Dirección IPv6 Loopback (::1/128)
- Dirección IPv6 Global Unicast (2000::/3)
- Dirección IPv6 Link-Local (FE80::/10)
- Dirección IPv6 Multicast (FF00::/8)

ESCENARIO DE PRUEBAS.



CONSIDERACIONES.

- Bloque de Direcciones IPv6 2801:c4:3b::0/48 (obtenido a través de IAR México)
- Enlace Activo de IPv6 con un ISP (Se cuenta con INFOTEC)
- Planear las direcciones que emplearan a partir del bloque obtenido. Partiendo del bloque con prefijo /48 se generar subnets de IPv6 con prefijo /64.
- El contexto de routing para IPv6 deberá ser realizado tanto en el Firewall como en el equipo de Core. El ruteo de la subnets IPv6 con prefijo /64 será realizado a través de la infraestructura de Core, en tanto el enrutamiento hacia Internet a través del ISP será desempeñado por el Firewall.
- Extender las VLANs desde el core hasta el switch de Acceso, pasando por Distribución en un contexto L2.

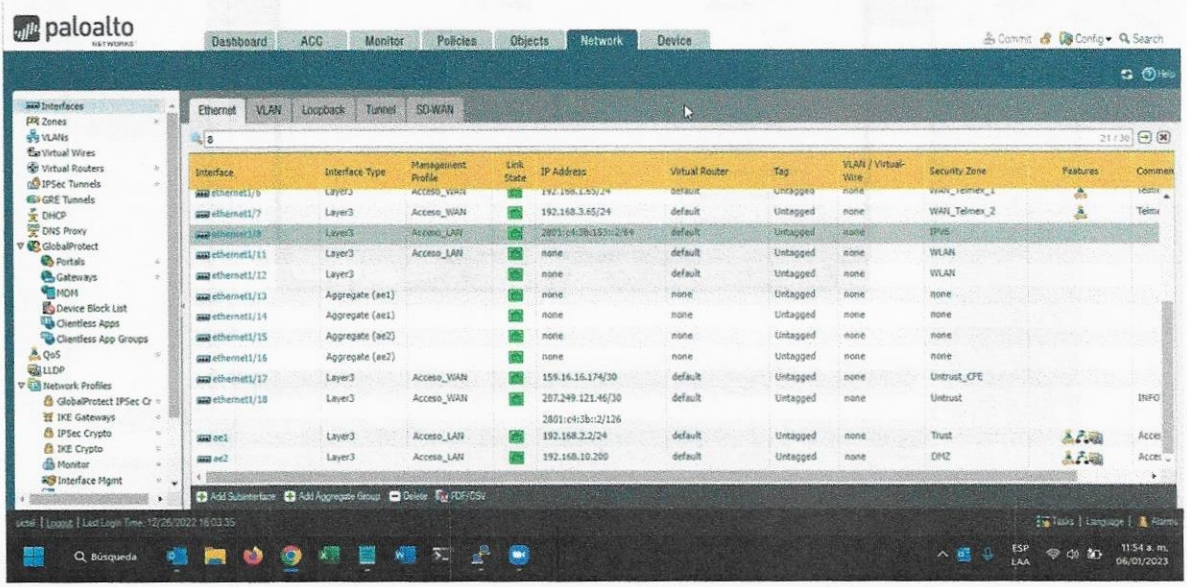
Nota: IAR México también entrega un **ASN 270191**

ACTIVIDADES GENERALES.

CONFIGURACIÓN EN EL FIREWAL

El Firewall 3050 recibe el enlace IPv6 proveniente del proveedor INFOTEC, siendo la interfaz de conexión la 1/18.

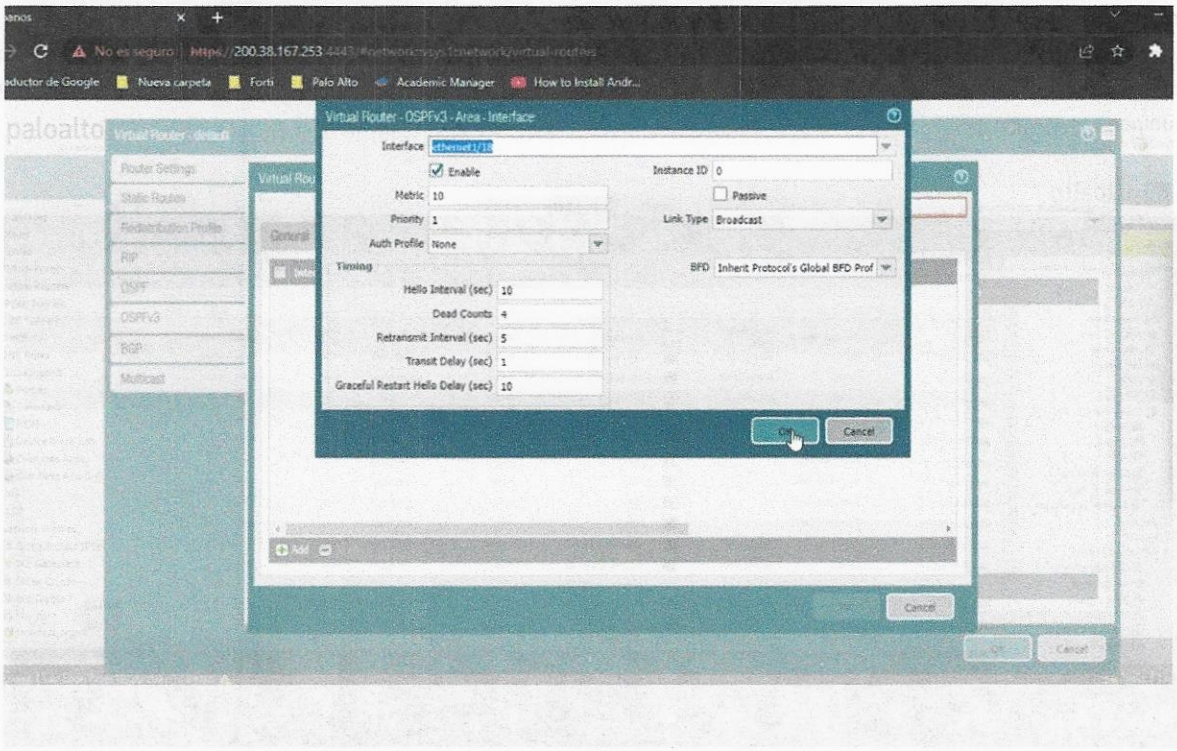
A través del análisis de direccionamiento determina que en la interfaz WAN del Firewall Palo Alto y la interfaz del router Juniper de INFOTEC se debe asignar una dirección IPv6 con Prefijo /126 a fin de evitar overlapping de direcciones, por lo que queda para la interfaz WAN del Firewall Palo Alto la dirección 2801:c4:3b::2/126 y la dirección 2801:c4:3b::1/126 en el Juniper.



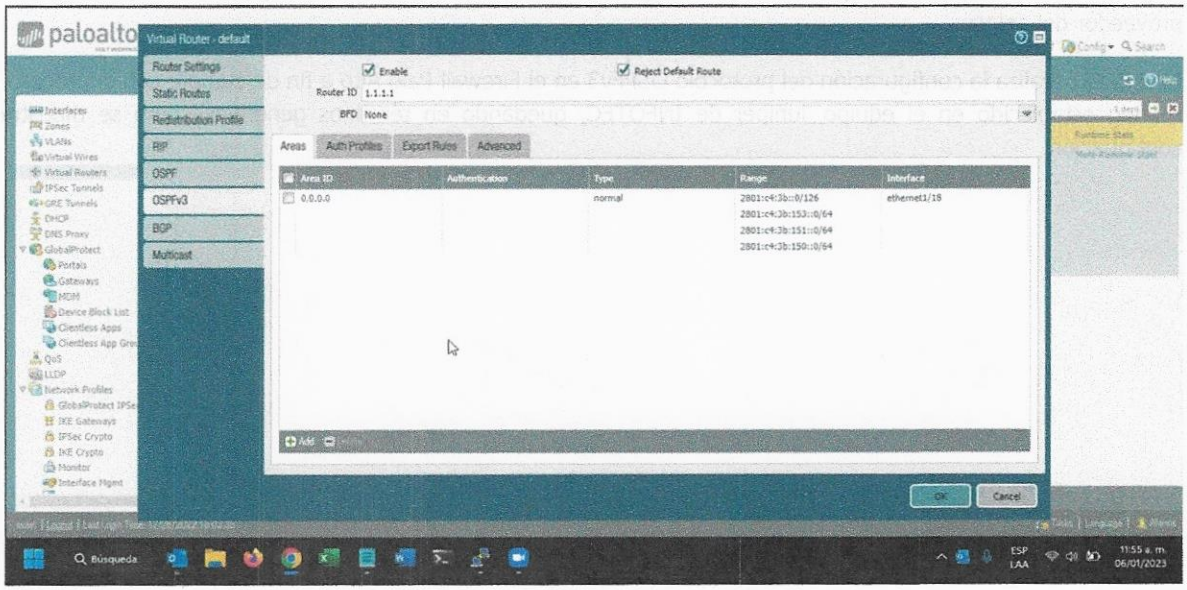
Esta imagen muestra en el puerto 18 la configuración de la dirección 2801:c4:3b::2/126 en el Firewall Palo Alto.

El protocolo de enrutamiento que debe ser configurado contra INFOTEC es OSPFv3, por ser requerimiento del proveedor del enlace.

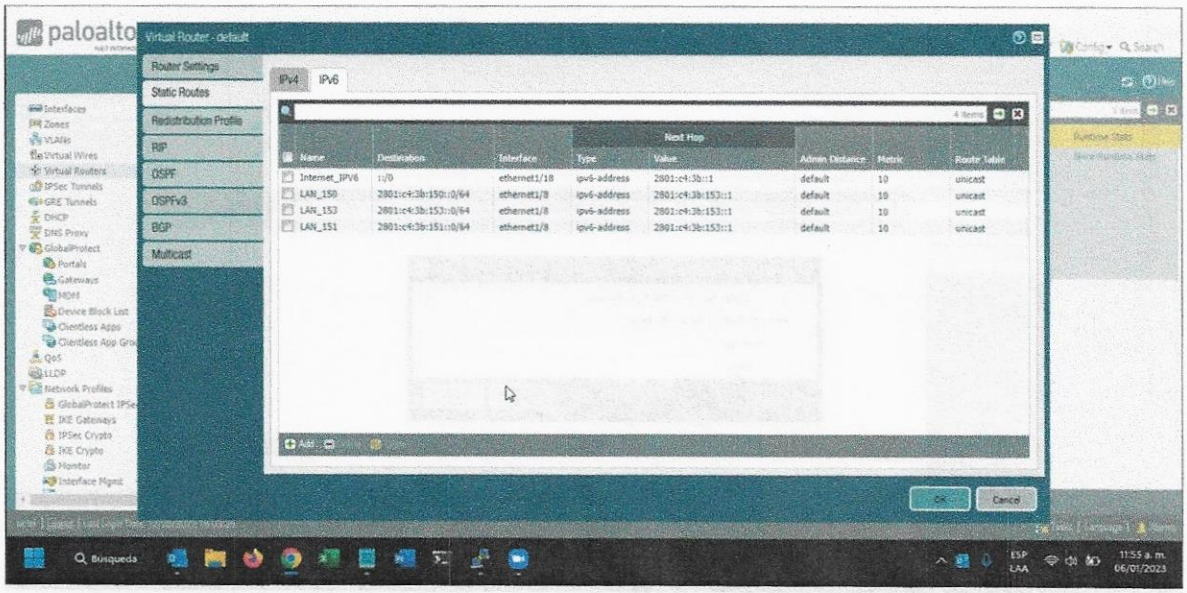
El INRLGII realiza la configuración del protocolo OSPFv3 en el Firewall Palo Alto a fin de cumplir con el proceso de routing establecido en el equipo Juniper de INFOTEC, quedando en términos generales como se muestra a continuación.



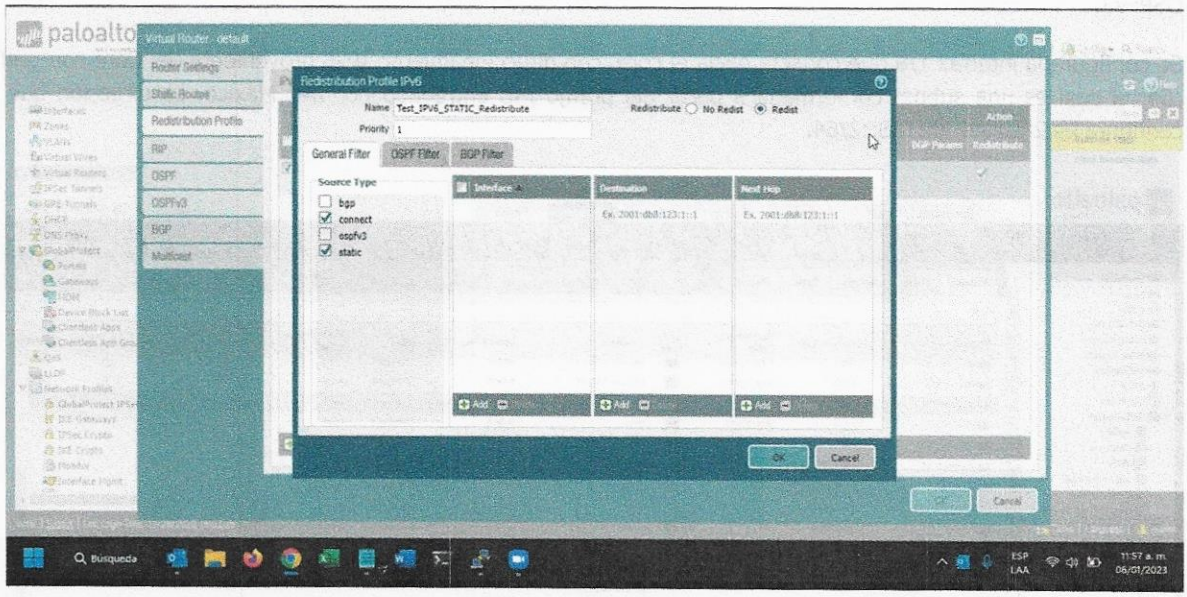
Habilitación de OSPFv3 específicamente sobre la interfaz WAN 1/18 a través de la cual se recibe el enlace IPv6 proveniente de INFOTEC.

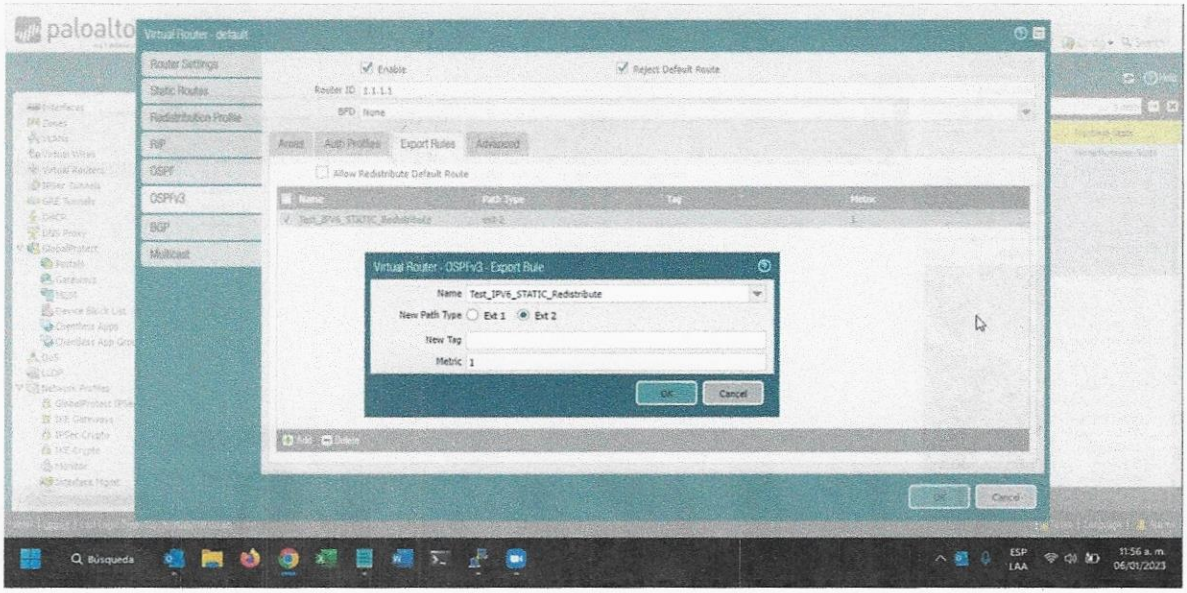


Asignación del Área 0 para la OSPFv3 y la asignación del router ID 1.1.1.1



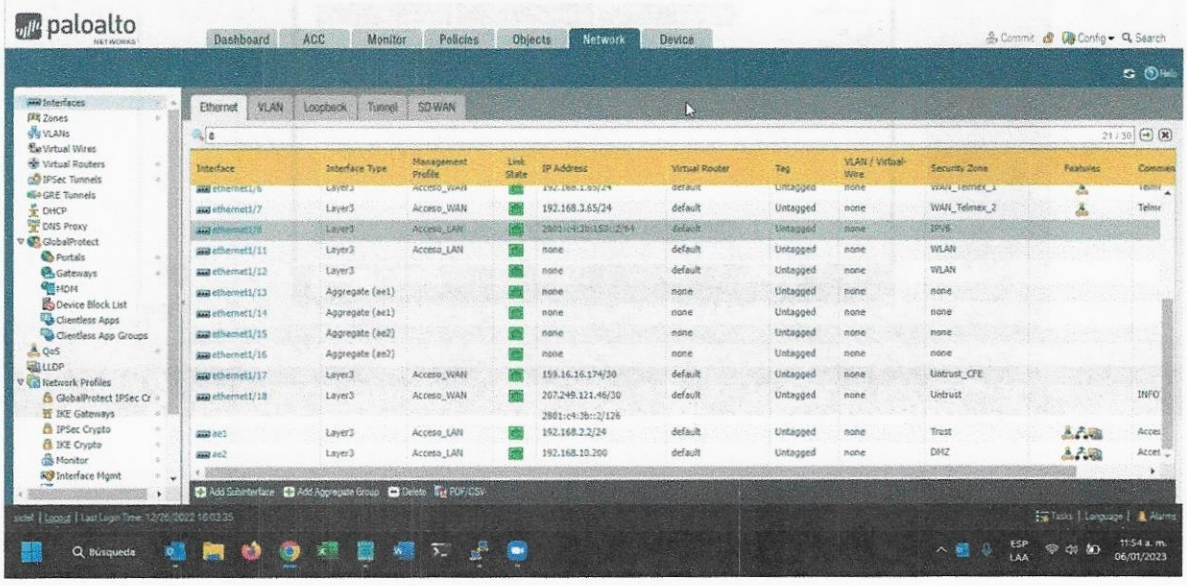
Configuración de las rutas estáticas entre el Firewall y el Core Cisco 4507R





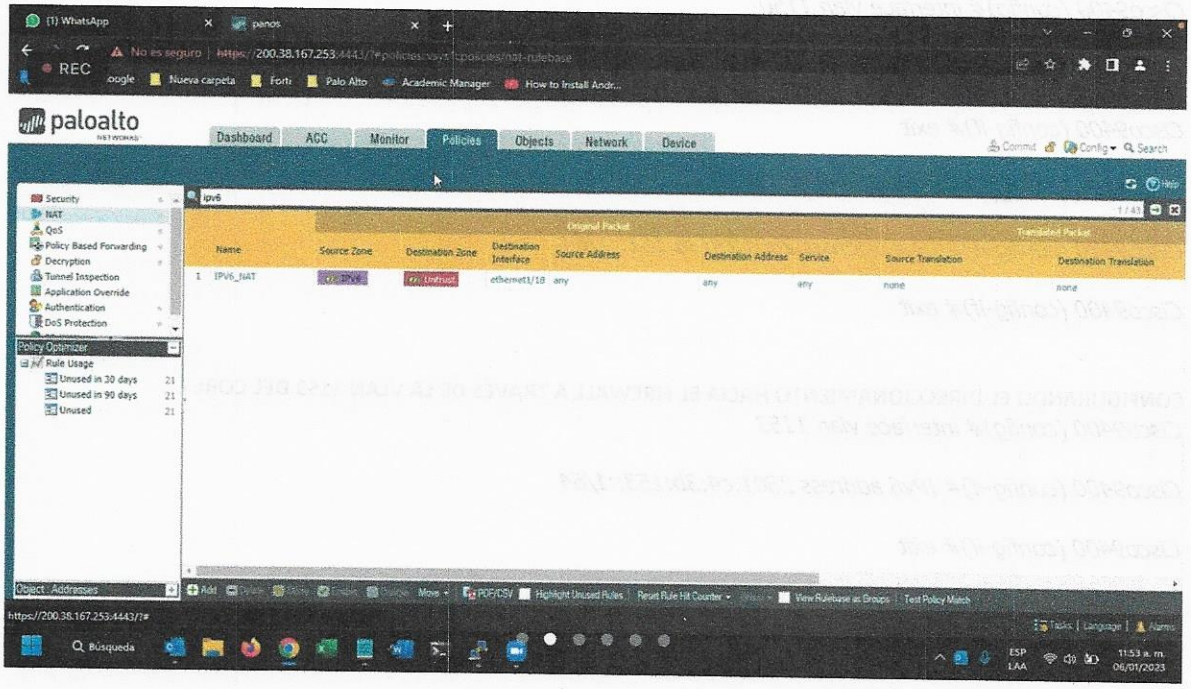
Estas dos últimas imágenes muestran el perfil de redistribución de rutas estáticas y directamente conectadas sobre OSPFv3.

Se configura la interfaz 1/8 que conecta hacia el core, con direccionamiento IPv6 proveniente del Core con prefijo /64, el cual es una subnet conformada a partir del prefijo /48 entregado por IAR México. La dirección que se configura es 2801:c4:3b:153::2/64.



Aquí se muestra para la interfaz 1/8 el direccionamiento 2801:c4:3b:153::264

INRLGII determina a través del análisis de Enrutamiento y generación de políticas en el equipo Palo Alto que debe ser deshabilitado el proceso de NAT que originalmente se estaba aplicando en la política de la Interfaz WAN



En la imagen puede observarse que el campo de **Source Translation** se encuentra en **none** lo cual concluye que se ha deshabilitado.

A través de estos cambios en las políticas y configuración de OSPFv3 el personal operativo del Instituto Nacional de Rehabilitación Luis Guillermo Ibarra Ibarra, concluye el proceso adecuado routing y la navegación en Internet con IPv6.

Nota: *a través de este análisis y pruebas se determina issues de seguridad a tener en consideración para el momento de establecer aplicaciones o dispositivos IPv6 en estatus de producción. Indicando al personal de Expertos en Cómputo que empiecen a planificar y probar sus políticas de IPv6 para cuando sean requeridas.*

CONFIGURACIÓN EN EL CORE

El Core cuenta con dos VLANs con ID´s 1150 y 1151 que serán empleadas para la prueba piloto de IPv6.

Estas VLAN´s son aprovisionadas con direcciones IPv6 con prefijo /64. Estas direcciones proporcionadas a las VLANs serán empleadas por los servidores o clientes IPv6 como su respectivo Default Gateway.

Se debe crear un direccionamiento IPv6 con prefijo /64, que se compartirá entre el core y el Firewall para efectos de routing, creando una ruta estática del Core hacia el firewall.

CONFIGURACIÓN DE IPV6 EN VLANS 1150 Y 1151

Cisco9400 (config)# ipv6 unicast-routing

Cisco9400 (config)# interface vlan 1150

Cisco9400 (config-if)# IPv6 address 2801:c4:3b:150::1/64

Cisco9400 (config-if)# exit

Cisco9400 (config)# interface vlan 1151

Cisco9400 (config-if)# IPv6 address 2801:c4:3b:151::1/64

Cisco9400 (config-if)# exit

CONFIGURANDO EL DIRECCIONAMIENTO HACIA EL FIREWALL A TRAVÉS DE LA VLAN 1153 DEL CORE

Cisco9400 (config)# interface vlan 1153

Cisco9400 (config-if)# IPv6 address 2801:c4:3b:153::1/64

Cisco9400 (config-if)# exit

CONFIGURANDO UNA RUTA ESTÁTICA IPV6 HACIA EL FIREWALL

Cisco9400 (config-if)# ipv6 route ::/0 2801:c4:3b:153::2

Cisco9400 (config)# save config

CONFIGURACIÓN EN EL ACCESO

En este caso solo se deberán extender las VLAN´s 150 y 151 desde el core hacia el o los Switches de acceso involucrados.

Login: admin

Password: (enter)

ExtremeSW # create vlan "name x"

ExtremeSW # create vlan "name y"

ExtremeSW #configure vlan "name x" tag 150

ExtremeSW #configure vlan "name y" tag 151

ExtremeSW # configure vlan "name x" add ports b,c tagged (agregar el o los puertos trunk a través de los cuales se reciben estas VLANs desde el core o distribución)

ExtremeSW #configure vlan name x" add ports c,d untagged

ExtremeSW # configure vlan "name y" add ports b,c tagged (agregar el o los puertos trunk a través de los cuales se reciben estas VLANs desde el core o distribución)

ExtremeSW #configure vlan name y" add ports c,d untagged

ExtremeSW # save config

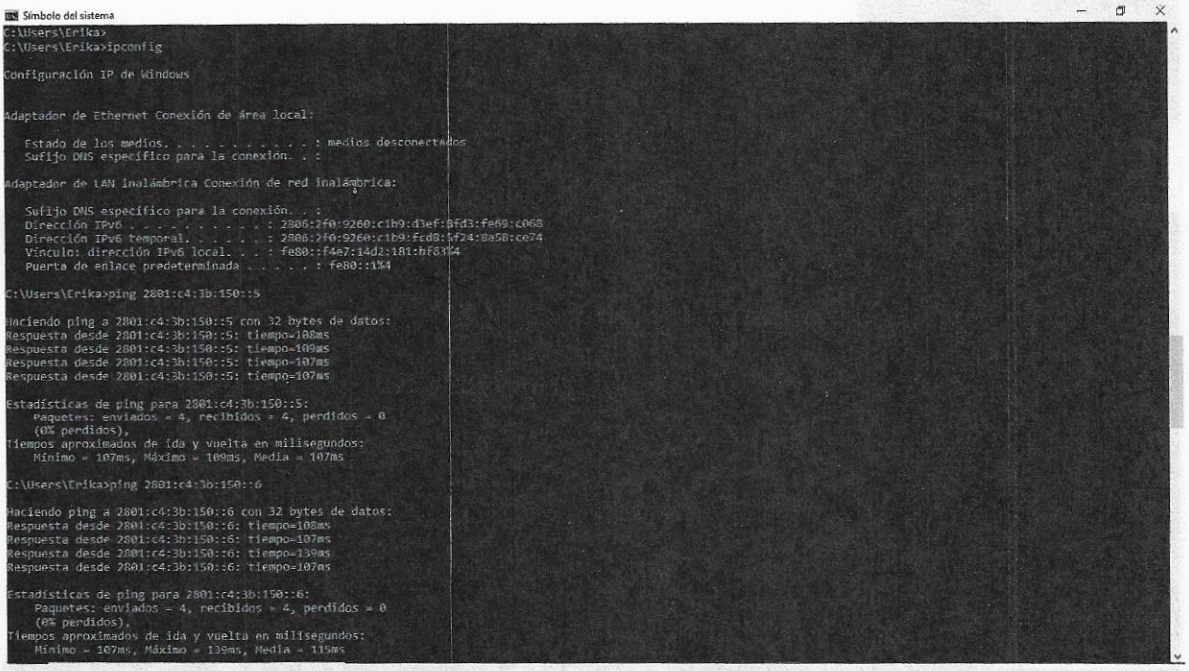
PROTOCOLOS DE PRUEBAS.

A fin de cumplir con las necesidades operativas de comunicación y administración en un ámbito de IPv6, se considera el siguiente conjunto de pruebas.

PRUEBAS DE IPV6

1. Verificar que los servidores y clientes se encuentren con direcciones IPv6

Satisfactoria: **SÍ** No satisfactoria:

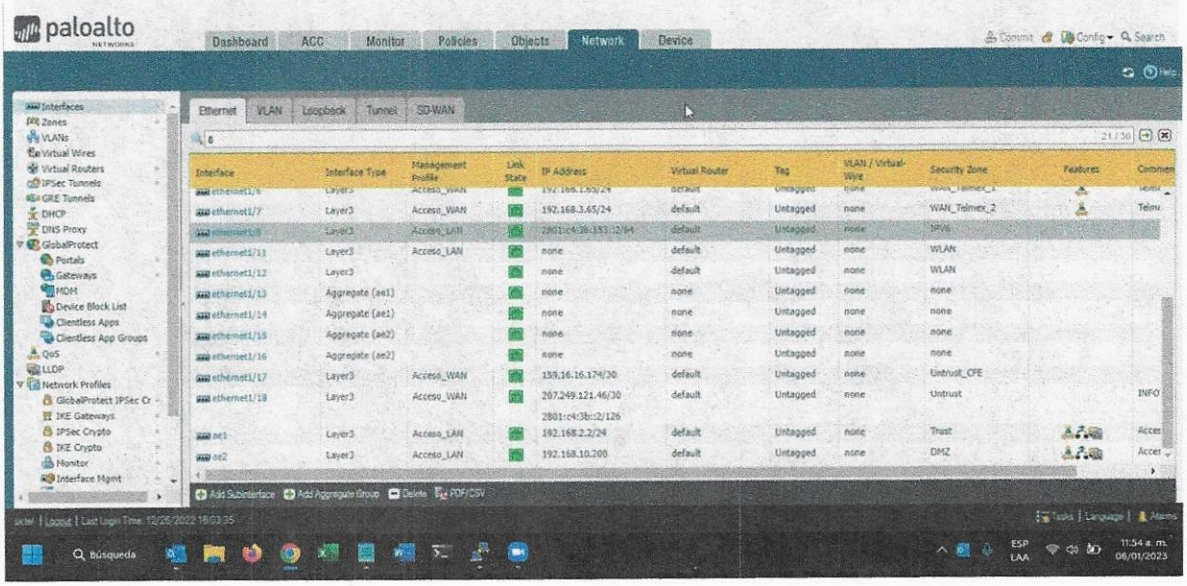


Nota: Las pruebas de conectividad con Ping validan el direccionamiento que aquí se indica para los servers

2. Verificar que los elementos de red operando en el ámbito de IPv6 cuenten con el direccionamiento correspondiente (Switch de Core, Firewall)

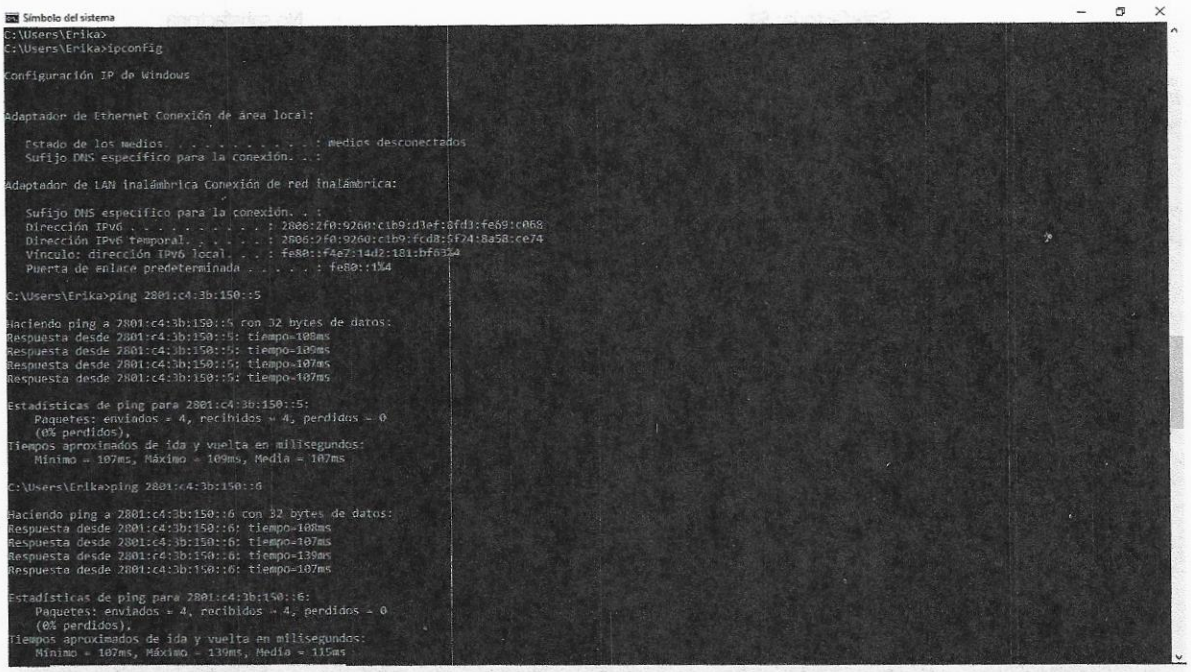
Satisfactoria: **SÍ** No satisfactoria:

```
INR_CORE#
INR_CORE#sh run interface GigabitEthernet1/7/0/7
Building configuration...

Current configuration : 93 bytes
!
interface GigabitEthernet1/7/0/7
 switchport access vlan 1153
 switchport mode access
end

INR_CORE#sh run interface Vlan1150
Building configuration...

Current configuration : 101 bytes
!
interface Vlan1150
 ip address 192.168.150.1 255.255.255.0
 ipv6 address 2001:C4:3B:150::1/64
end

INR_CORE#sh run interface Vlan1151
Building configuration...

Current configuration : 101 bytes
!
interface Vlan1151
 ip address 192.168.151.1 255.255.255.0
 ipv6 address 2001:C4:3B:151::1/64
end

INR_CORE#sh run interface Vlan1153
Building configuration...

Current configuration : 101 bytes
!
interface Vlan1153
 ip address 192.168.153.1 255.255.255.0
 ipv6 address 2001:C4:3B:153::1/64
end

INR_CORE#sh run | inc ipv6 route
ipv6 route ::/0 2001:C4:3B:153::2
INR_CORE#
```



3. Verificar la visibilidad entre clientes IPv6 mediante Ping

Satisfactoria: **SÍ** No satisfactoria:

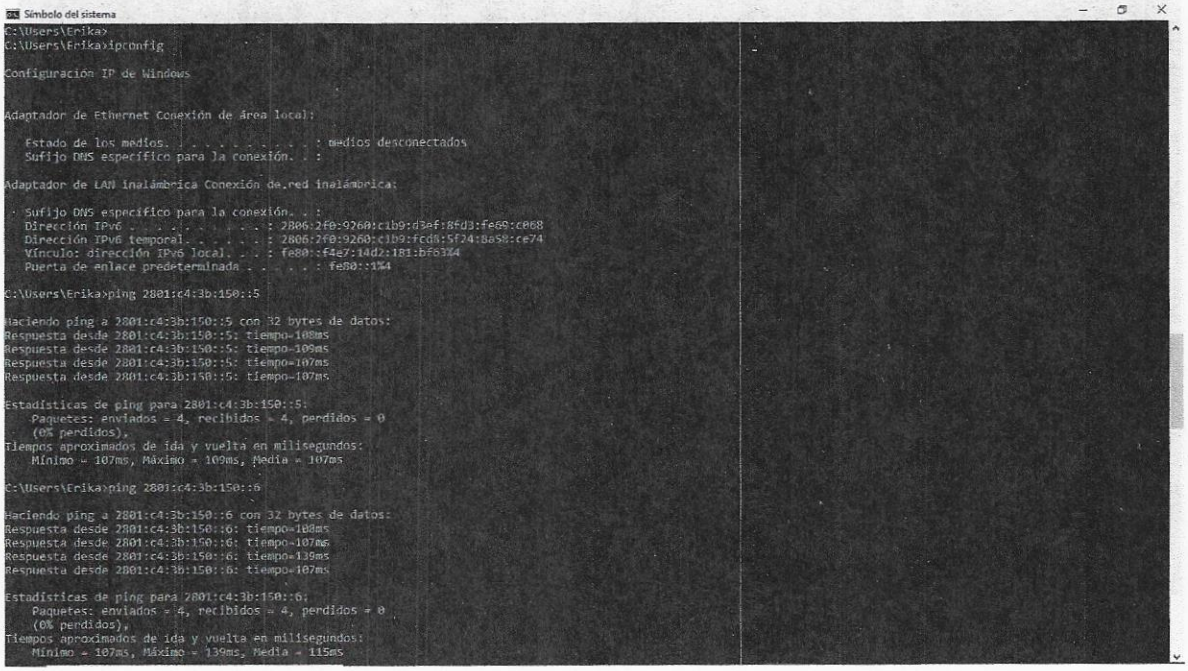


Nota: La prueba va desde el host 2806:2f0:9260:c1b9:d3ef:8fd3:fe69:c068

hacia el Server 2801:c4:3b:150::5 y ::6 ambas con prefijo /64.

4. Verificar la visibilidad entre servidores y clientes IPv6 empleando Ping

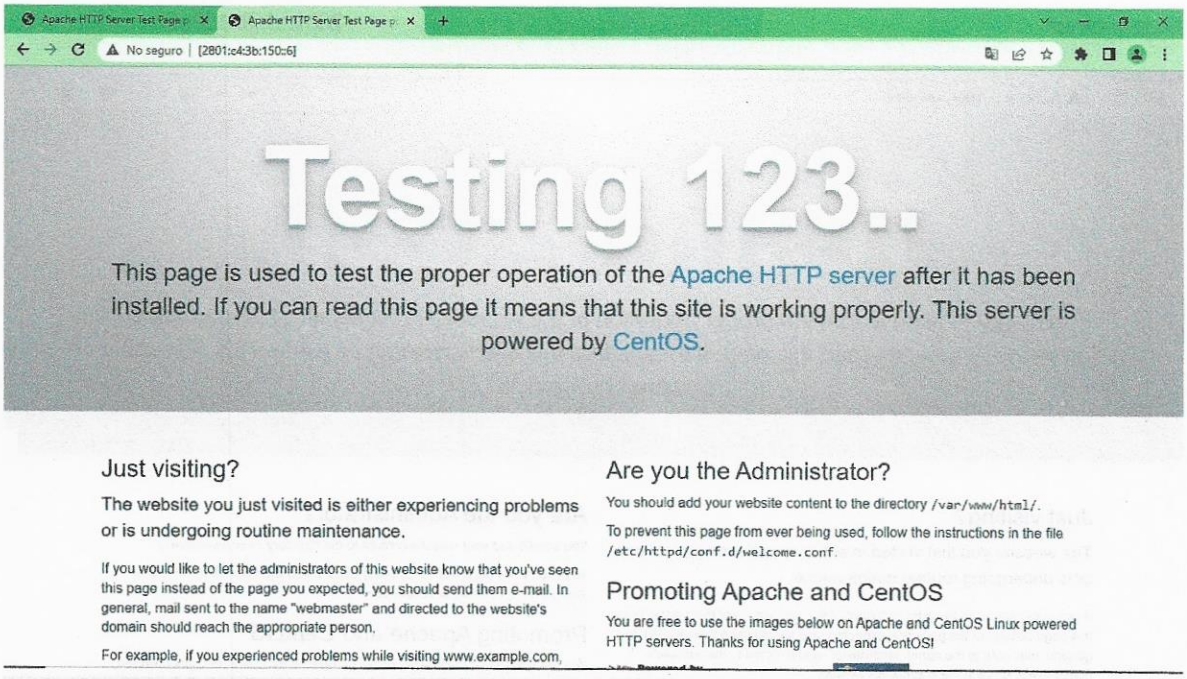
Satisfactoria: **SÍ** No satisfactoria:

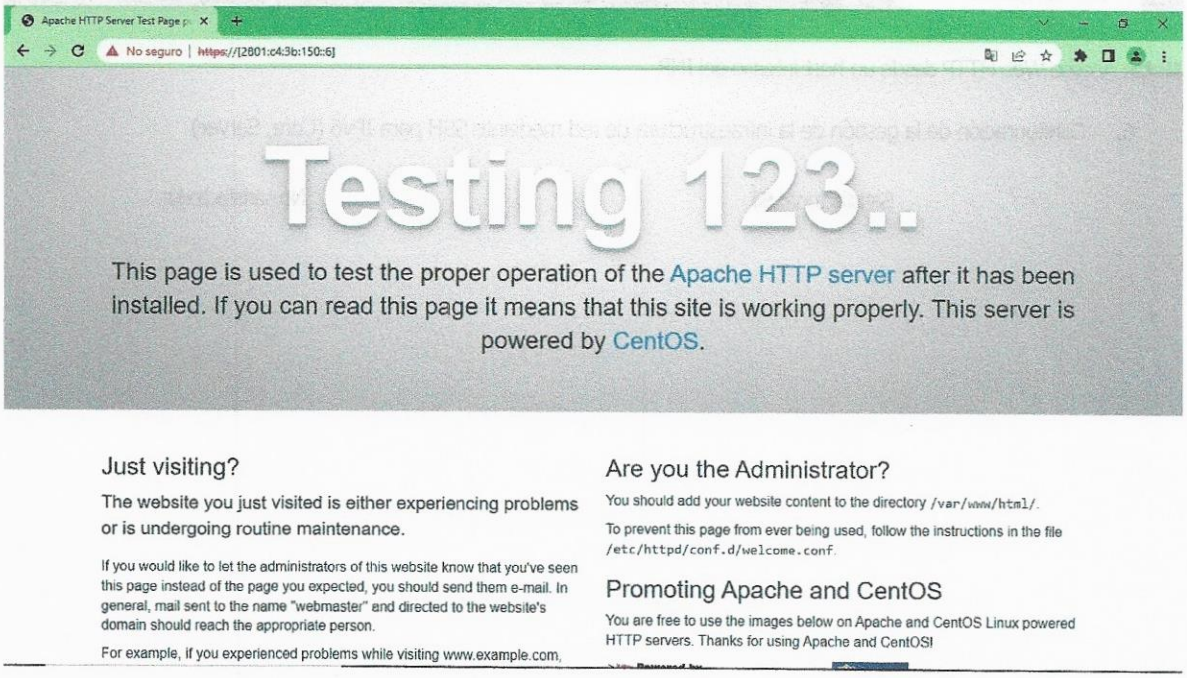


Nota: se realizaron pruebas desde el host 2806:2f0:9260:c1b9:d3ef:8fd3:fe69:c068 hacia el server 2801:c4:3b:150::6 y ::5.

5. Verificar el funcionamiento de las aplicaciones web de los servidores, acensando las desde un cliente IPv6

Satisfactoria: **SÍ** No satisfactoria:

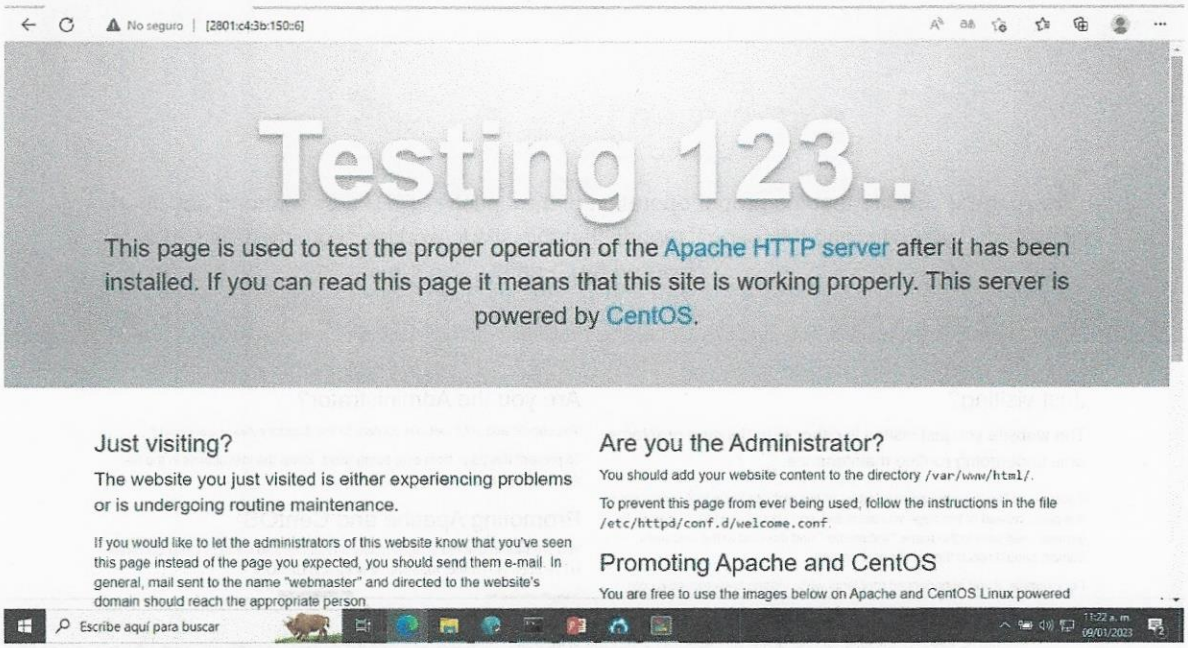




Nota: Las pruebas de acceso WEB http y https se realizaron desde:

el host 2806:2f0:9260:c1b9:d3ef:8fd3:fe69:c068

hacia el server 2801:c4:3b:150::6.

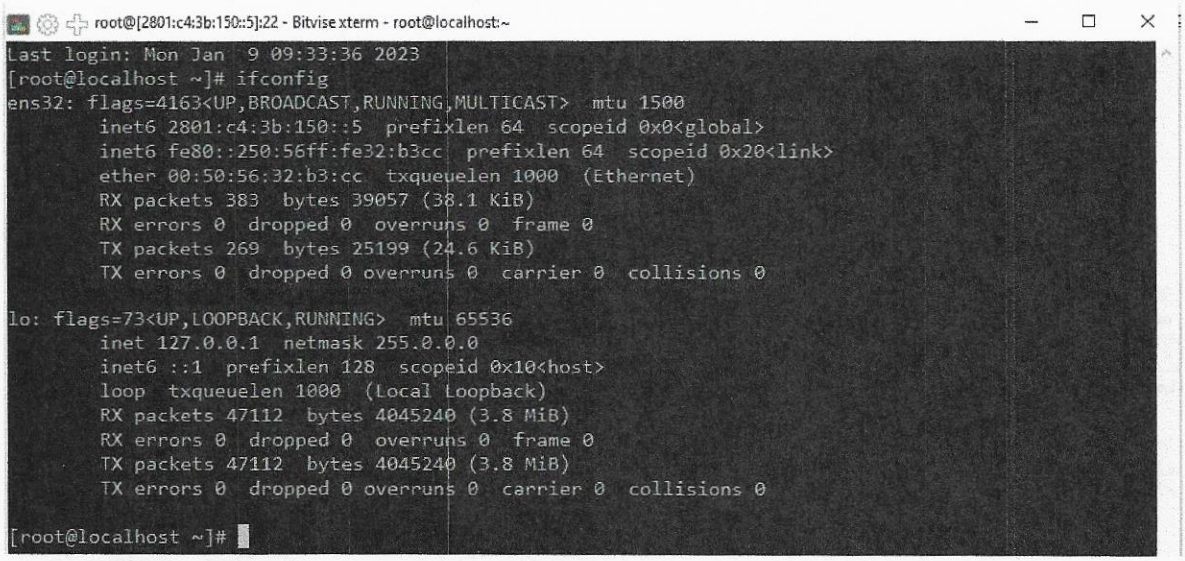


Nota: Acceso Web HTTP desde un host interno del INR

6. Configuración de la gestión de la infraestructura de red mediante SSH para IPv6 (Core, Server)

Satisfactoria: **SÍ** No satisfactoria:

Nota: Se realiza la prueba de SSH hacia el core a través de un host externo.



Nota: Acceso SSH al servidor

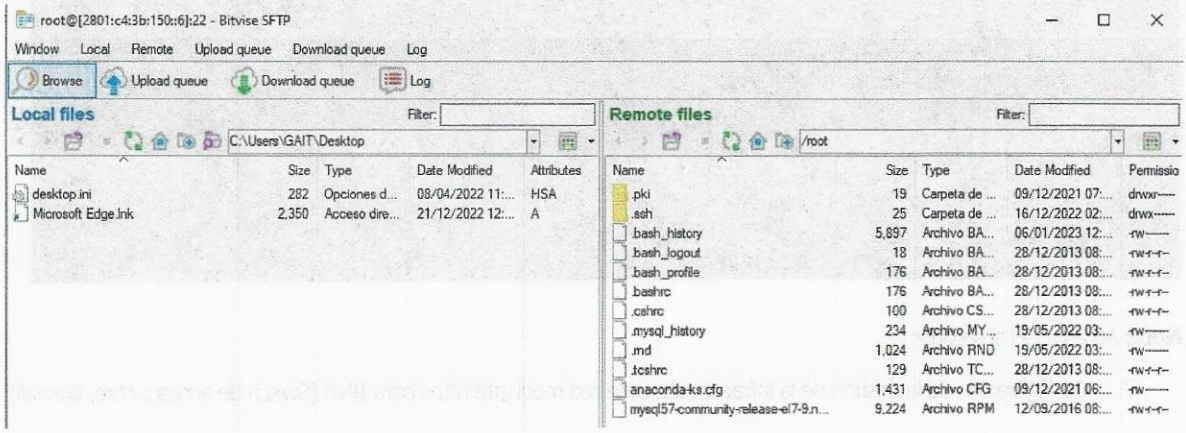
7. Configuración de la gestión de la infraestructura de red mediante https para IPv6 (Switch de acceso, core, firewall)

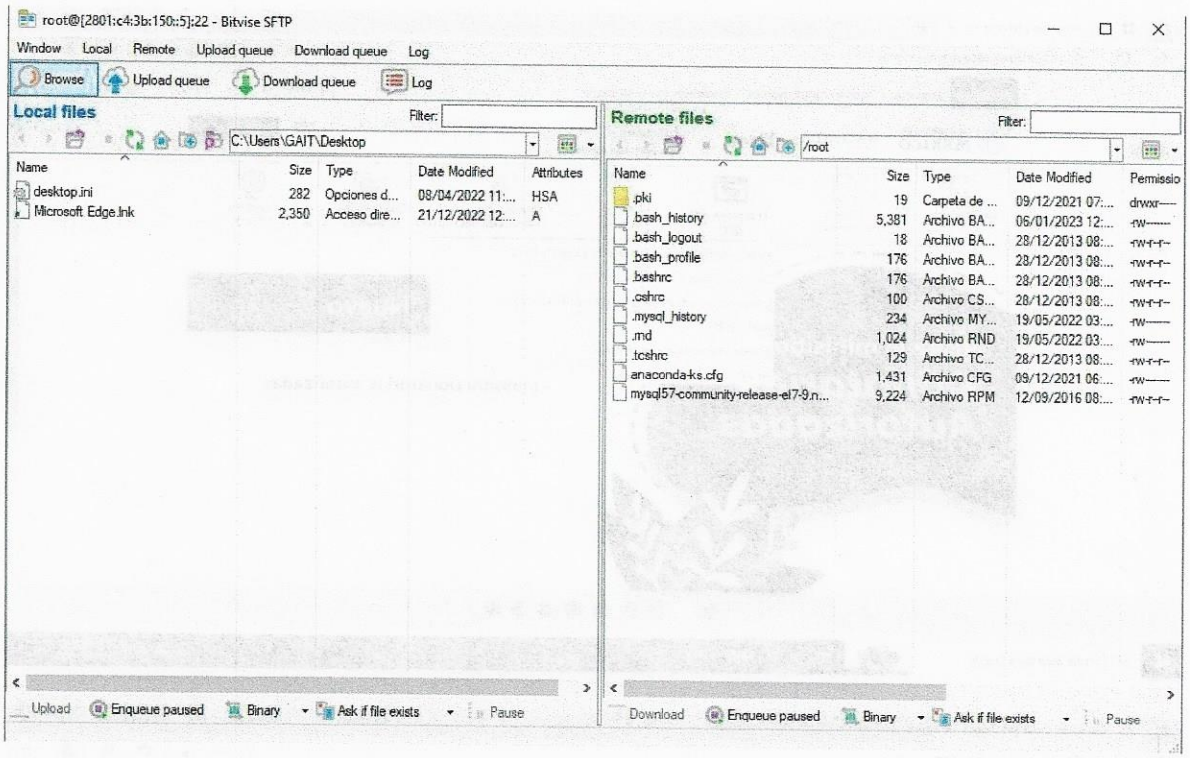
Satisfactoria: **SÍ** No satisfactoria:

Nota: La prueba se realizó con SSH desde un host externo para no continuar aperturando puertos lógicos en el core.

8. Operatividad del servicio FTP en alguno de los servidores, realizando una descarga desde un cliente de IPv6

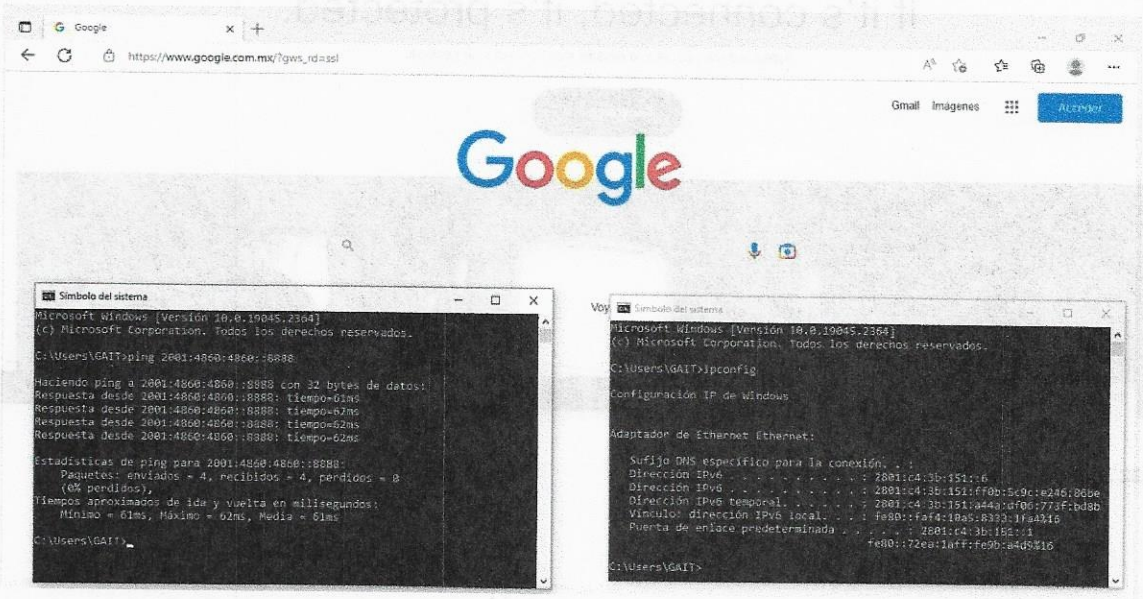
Satisfactoria: **SÍ** No satisfactoria:

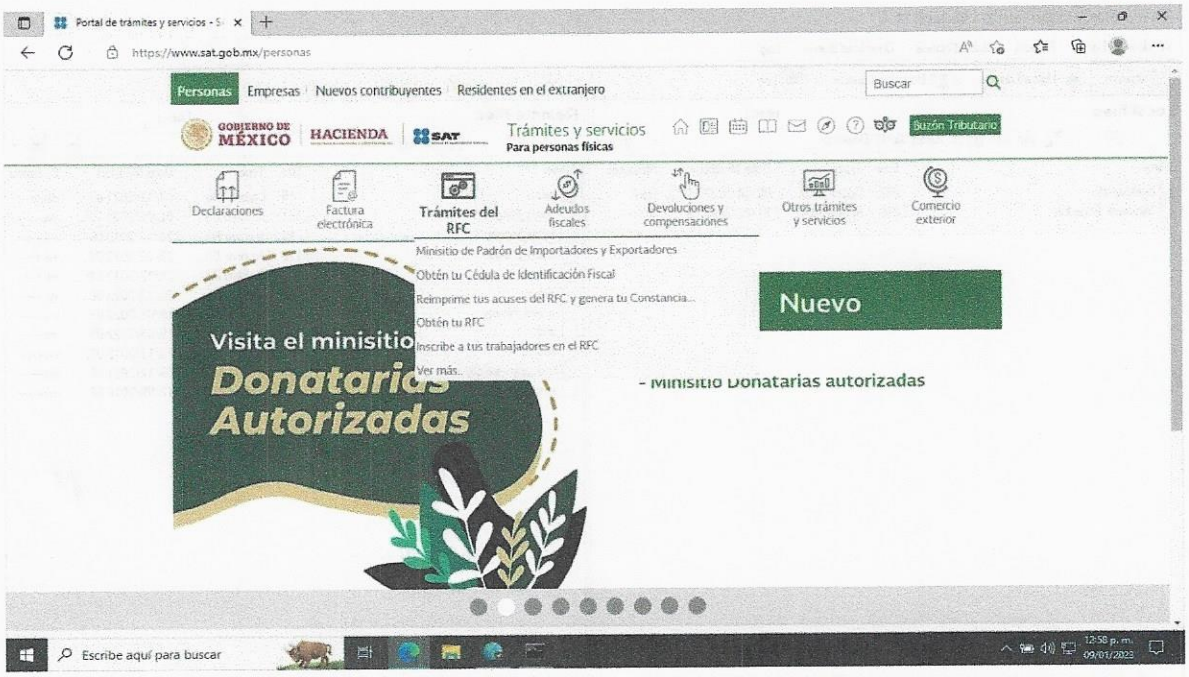


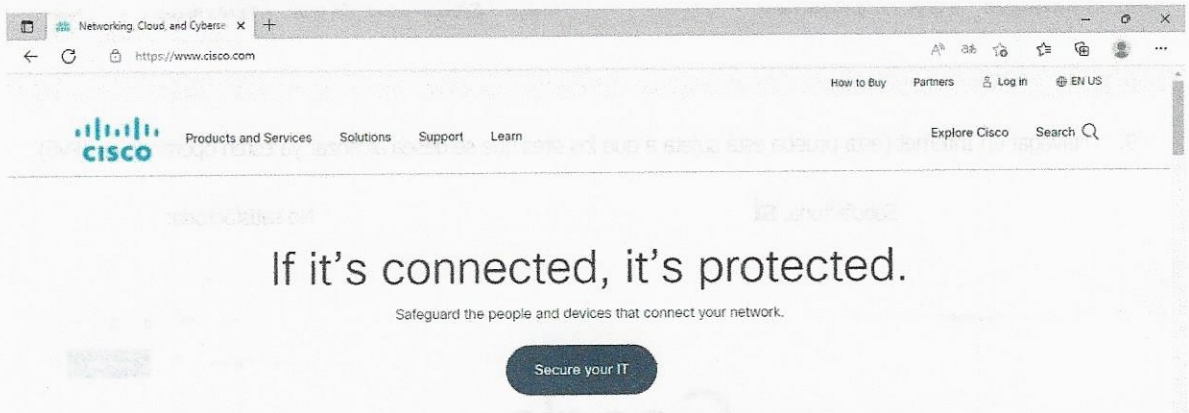


9. Navegar en Internet (esta prueba está sujeta a que los sites que se desea alcanzar ya estén operando en IPv6)

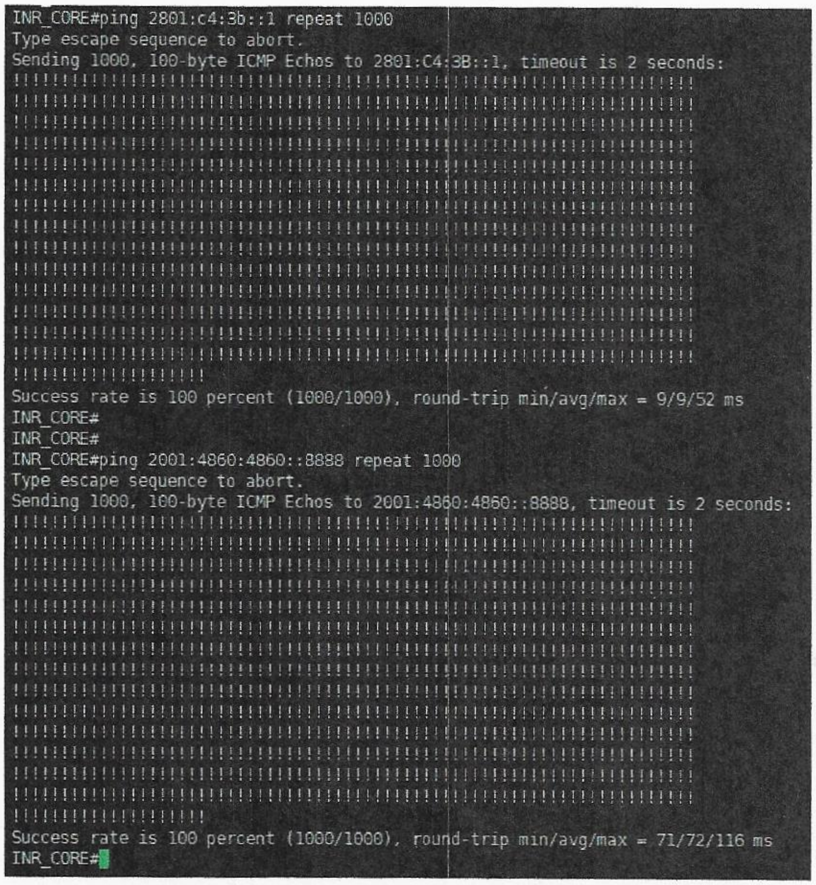
Satisfactoria: **SÍ** No satisfactoria:







Nota: Accesando a Google desde un Host Interno



```
INR_CORE#ping 2801:c4:3b::1 repeat 1000
Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 2801:C4:3B::1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 9/9/52 ms
INR_CORE#
INR_CORE#
INR_CORE#ping 2001:4860:4860::8888 repeat 1000
Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 2001:4860:4860::8888, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 71/72/116 ms
INR_CORE#
```

Nota: probando la conectividad hacia Internet desde core, en este caso hacia el DNS de Google 2001:4860:4860::8888

EQUIPOS INVOLUCRADOS:

Core

Cisco 9407R

Distribución y Acceso

Switch Extreme

WAN

Firewall Palo Alto 3050

Servidores

Servidores con Centos y Apache

Clientes

Laptop Dell con Microsoft Windows

Carrier (INFOTEC)

Router Juniper

CONCLUSIONES

- La infraestructura principal de la red del Instituto Nacional de Rehabilitación Luis Guillermo Ibarra Ibarra que consiste en los Equipos Cisco 4507R tienen capacidad para poder llevar a cabo un despliegue de IPv6 de manera centralizada.
- Los equipos que se encuentran en el Acceso de la red están en un estatus de End of Life o fin de vida, por lo que es importante considerar un próximo remplazo, ya que el riesgo por hardware o software durante la operación es Alto, toda vez que ya no existen procesos de soporte y atención a fallas para estos.
- Debido a la naturaleza operativa del protocolo IPv6 es crítico el contexto de seguridad, por lo que a pesar de que la infraestructura de Firewall cuenta con las funcionalidades de IPv6 para desempeñar la conectividad WAN y LAN, es conveniente que se verifique con el prestador del servicio:
    - El desarrollo de políticas de seguridad que permitan una operación con mínimos riesgos.
    - Que las políticas sean desarrolladas en función de las necesidades analizadas en conjunto con el equipo de la STIC del INR LGII. A fin de determinar que las políticas realmente respondan a las necesidades de la institución.

- Que el contexto de las políticas sea documentado y entregado al personal de la STIC a fin de contar con antecedentes de las estrategias de seguridad.
- La factibilidad de operar con un esquema en HA

- Con el proveedor de enlaces en términos de IPv6 actualmente se cuenta con un único enlace, por lo que cabe la perspectiva de empezar a analizar la factibilidad de poder contar en un término de corto o mediano plazo con la capacidad de contar con enlaces redundantes que garanticen una operación activo-activo y por consecuencia la continuidad del servicio.

- Si bien partiendo de la infraestructura de servidores y el tipo de cliente empleado para las pruebas se verifica que existe factibilidad y capacidad de migración a IPv6. Es importante que el análisis de inventario de dispositivos considere todo elemento que vaya a tener conectividad a la red como teléfonos IP, cámaras de videovigilancia, dispositivos médicos, etc. y así poder dar pie al proceso de transición a IPv6.

- Es importante para darle continuidad al proceso de transición o migración se lleven a cabo los análisis de red pertinentes para garantizar la transición con la menor cantidad de contratiempos.