CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS



Plan de Pruebas del Proceso de Transición IPv4 a IPv6

Relación de Versiones

Versión	Fecha	Revisó	Aprobó
1	Diciembre 23 de 2023	Yorguin Gómez	

Tabla de contenido

1. INTRODUCCIÓN 7

2. OBJETIVOS 8

2.1 Objetivo general 8

2.2 Objetivos específicos 8

3. EVALUACIÓN DE PROTOCOLO IPV6 9

3.1 Evaluación del protocolo IPv6 en red WAN 9

3.1.1 Equipos de comunicaciones 9

3.2 Evaluación del Protocolo IPV6 en red LAN 14

3.2.1 Equipos de comunicaciones 14

3.2.2 Equipos de cómputo 19

3.3 Evaluación de servicios sobre el protocolo IPV6 23

3.3.1 Servicio de DHCPv6 23

3.3.2 Sistema de vigilancia 25

3.4 Evaluación de aplicaciones sobre el protocolo IPV6 27

3.4.1 Aplicativos terceros 27

4. TERMINOLOGÍA 31

REFERENCIAS 37

Tabla de figuras

Figura 1. Ingreso a CLI en equipo Firewall 10

Figura 2. Ejemplo de visualización de tabla de enrutamiento 11

Figura 3. Ejemplo ejecución de comando ping 11

Figura 4. Visualizacion de estado de VPN-SSL 12

Figura 5. Ejemplo visualizacion comando get vpn 12

Figura 6. Visualización de políticas 13

Figura 7. Visualización de logs & report. 14

Figura 8. CLI del equipo Mikrotik 15

Figura 9. Consulta permitidas con comando Ping. 16

Figura 10. Prueba Ping en segmento de red de la CORPORACIÓN AUTÓNOMA REGIONAL DEL ORIENTE - CAS 16

Figura 11. Interfaz de IPv6 Address List en equipo Mikrotik 17

Figura 12. Pruebas ejecutas en navegador equipo tesorería 22

Figura 13. Interfaz de servidor DHCPv6 24

Figura 14. Interfaz de IPv6 NeigHbor List 24

Figura 15. Equipos vistos por equipo Mikrotik con IPv6 25

Figura 16. Configuración de IPv6 de equipo de cómputo en red del NVR 26

Figura 17. Verificación de IPv6 en equipo de cómputo 26

Figura 18. Prueba de comunicación con comando Ping 27

Figura 24. Interfaz de ingreso a plataforma seguros bolívar 28

Figura 25. Ingreso a Plataforma de Seguros bolivar 28

Figura 26. Interfaz de ingreso a plataforma banco agrario de Colombia 29

Figura 27. Ingreso a Plataforma de banco agrario de Colombia..... 30

1. INTRODUCCIÓN

La Corporación Autónoma Regional del Oriente - CAS dando cumplimiento a lo estipulado por el Ministerio de tecnologías de Información y las Comunicaciones (MINTIC) en la resolución 2710 de 2017 y la Resolución 1126 de 2021, y tomando como guía el documento: "Guía de Transición de IPv4 a IPv6 para Colombia", ha desarrollado el proyecto transición de protocolo IPv4 a IPv6 en la entidad. Lo anterior con el fin de incentivar el desarrollo de las TICs dentro de la organización y cumplir con la normatividad establecida para la vigencia actual.

Al terminar la puesta en marcha de cualquier implementación se hace necesario la realización de pruebas o test para corroborar que el sistema o en este caso la implementación del protocolo IPv6 funciona correctamente con los lineamientos establecidos, es por tal motivo que el presente documento recopila cada una de las pruebas que se deben considerar en el sistema de comunicaciones dispuesto en la red de la Corporación Autónoma Regional del Oriente - CAS

Dentro de las pruebas desarrolladas en el presente documento se pueden observar los pasos a seguir para la verificación de las configuraciones hechas en los equipos de comunicación, además de las consideraciones propuestas para determinar el cómo se desarrolla el tráfico de datos en IPv6 por la red de comunicaciones de la CORPORACIÓN AUTÓNOMA REGIONAL DEL ORIENTE - CAS, igualmente propone herramientas web o aplicativos que permiten realizar pruebas para el protocolo IPv6.

Este tipo de documentación donde se hace mención al cómo se deberían desarrollar las pruebas en un sistema, son de gran ayuda para determinar posibles errores cometidos durante la etapa de implementación, igualmente se genera un documento base para resolución de problemas que se puedan presentar a futuro, ya sea por el crecimiento de la red o la adecuación de nuevos servicios en la Corporación Autónoma Regional del Oriente - CAS

2. OBJETIVOS

2.1 Objetivo general

Realizar las pruebas de verificación de la puesta en marcha de los activos de tecnología de información configurados en IPv6 en la Corporación Autónoma Regional del Oriente - CAS

2.2 Objetivos específicos

- Dar a conocer los métodos con los cuales se puede comprobar la comunicación bajo el protocolo IPv6.
- Exponer los resultados obtenidos en las pruebas de adopción bajo el protocolo IPv6.

3. EVALUACIÓN DE PROTOCOLO IPV6

3.1 Evaluación del protocolo IPv6 en red WAN

La red WAN hace referencia a todas las conexiones que se generan de la red interna de la CORPORACIÓN AUTÓNOMA REGIONAL DEL ORIENTE - CAS con la red de internet, esto con ayuda de los servicios de conectividad suministrados por el proveedor de servicios de internet (ISP) local, las conexiones generadas pueden tener diversas características según los protocolos utilizados o los niveles de seguridad que se requieran aplicar, en este caso se analiza el funcionamiento del protocolo IPv6 en el equipo de comunicaciones dispuesto en la Corporación Autónoma Regional del Oriente - CAS para las conexiones entre las redes WAN y LAN, además de mencionar criterios para las pruebas de seguridad informática en el equipo.

3.1.1 Equipos de comunicaciones

Actualmente la Corporación Autónoma Regional del Oriente - CAS está en un proceso de implementación para la adecuación de un equipo firewall, el cual brindara la seguridad y las comunicaciones necesarias para la red interna de la CORPORACIÓN AUTÓNOMA REGIONAL DEL ORIENTE - CAS, en esta sección se señalan las consideraciones más relevantes para realizar las pruebas bajo el protocolo IPv6 en el equipo firewall una vez realizada la adecuación de este.

3.1.1.1 Firewall

En el equipo firewall que en este caso es un equipo fortinet, se debe analizar tres puntos fundamentales referentes al protocolo IPV6, el enrutamiento, el servicio de red privada virtual (VPN) y las políticas de seguridad, una vez implementadas las configuraciones en el equipo, se deben realizar las siguientes pruebas para confirmar su funcionamiento, las pruebas señaladas pueden variar un poco según la interfaz utilizada y la referencia del equipo firewall, igualmente para todas las pruebas se debe verificar que el protocolo IPv6 este activo.

Prueba para enrutamiento Estático

I. Inicialmente se verifica la adopción por parte del sistemas de las rutas configuradas, para este tarea se puede utilizar la interfaz gráfica o la interfaz de línea de comandos (CLI) del equipo fortinet, en esta prueba se utiliza la CLI, para ingresar se selecciona en el menú el símbolo de CLI (ver figura 1.)

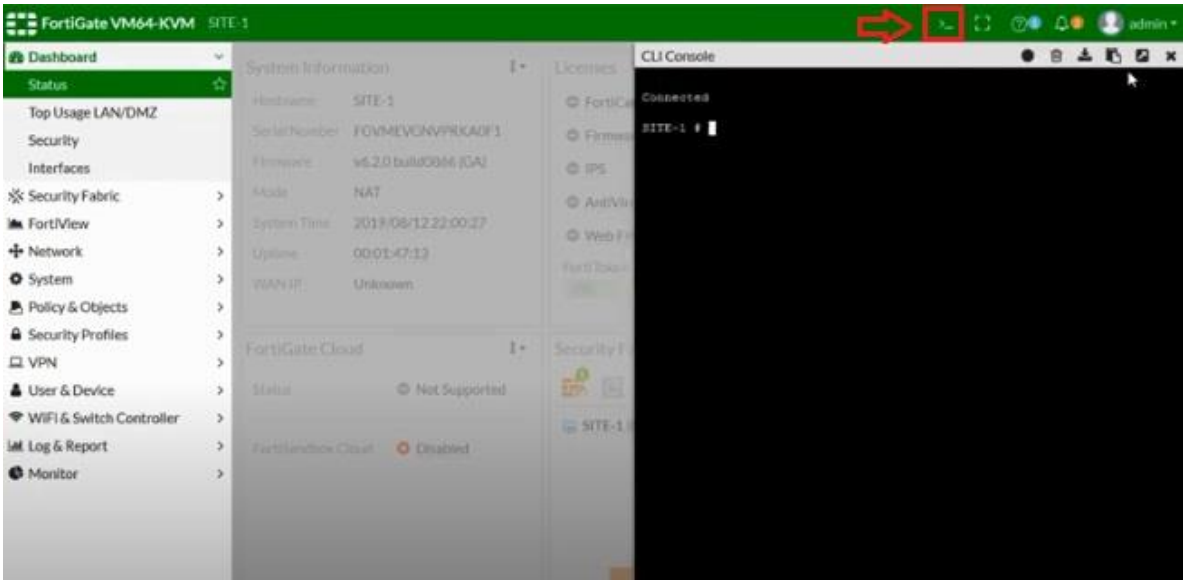


Figura 1. Ingreso a CLI en equipo Firewall

Fuente: Elaboración propia

II. Una vez en la interfaz de línea de comando se ingresa alguna de las siguientes sentencias: get *router info routing-table all* o *get router info6 routing-table database,* aplicada la sentencia se obtiene la tabla de enrutamiento y con esta información se puede comprobar la adicción de las rutas estáticas configuradas al equipo.

```
CABA # get router info routing-table all

Routing table for VRF=0
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [15/0] via 190.210.40.2, port1
C       172.16.10.0/24 is directly connected, port2
C       190.210.40.0/30 is directly connected, port1
S       192.168.0.0/24 [10/0] via 190.210.40.2, port1
```

Figura 2. Ejemplo de visualización de tabla de enrutamiento

Fuente: Elaboración propia

III. Ahora se realiza una prueba de conectividad de cada una de las interfaces configuradas, además del funcionamiento del enrutamiento utilizando el comando: *exec ping [IPv4/IPv6/DNS]*

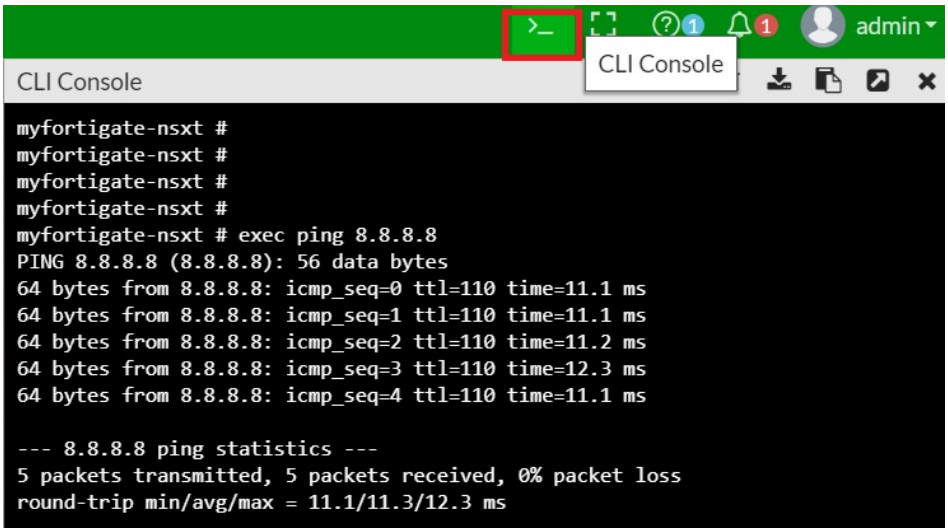


Figura 3. Ejemplo ejecución de comando ping

Fuente: Elaboración propia

Prueba para red privada virtual (VPN)

I. para verificar la conexión del servicio VPN-SSL realizado en la etapa de instalación, se ingresa al menú del equipo fortinet y se selecciona la opción *panel de control* > *red*, ya en esta área se puede ver la actividad generada por la conexión del servicio.



Figura 4. Visualizacion de estado de VPN-SSL

Fuente: https://tinyurl.com/2p8tdy7e

II. Si se desea verificar el funcionamiento de otras características de la VPN se puede utilizar la CLI, los siguientes comandos se hacen relevantes para realizar las pruebas.

- *get vpn ssl monitor*
- *get router info routing-table database*
- *get router info6 routing-table database*

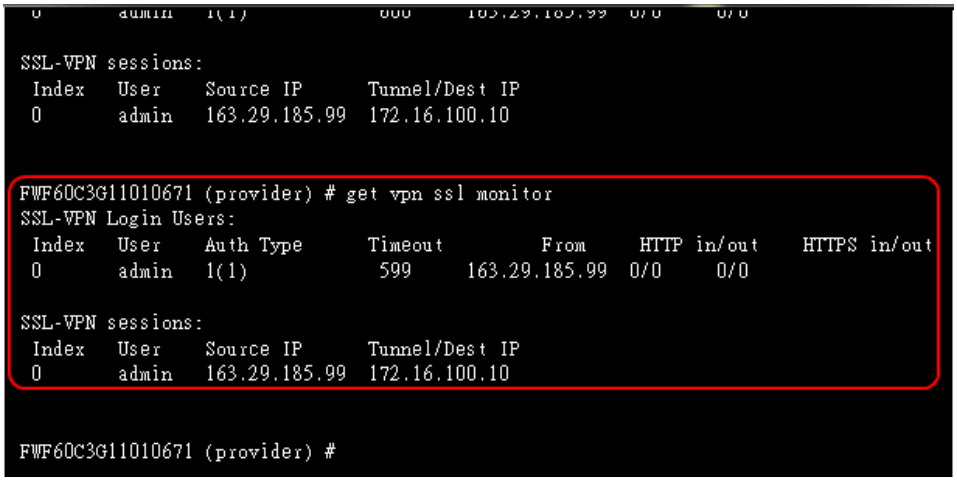


Figura 5. Ejemplo visualizacion comando get vpn

Fuente: https://tinyurl.com/2p8tdy7e

Prueba de políticas de seguridad

I. Como primera medida se verifica la aplicación de la política de seguridad ejecutada en el equipo firewall, para esto se ingresa al menú de configuración en la opción *firewall policy.*

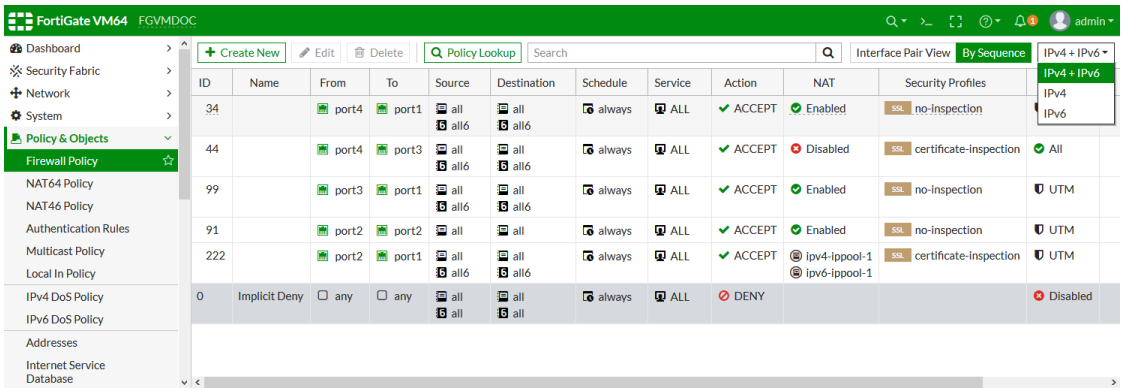


Figura 6. Visualización de políticas

Fuente: Elaboración propia

II. Una vez verificada cada una de las políticas de seguridad, se realizan simulaciones de tráfico de datos en la red de la CORPORACIÓN AUTÓNOMA REGIONAL DEL ORIENTE - CAS, donde se pueda observar el comportamiento de dichas políticas y así comprobar su funcionamiento, el trafico puede ser generado por medio de la CLI o utilizando herramientas de los equipos finales como los navegadores, para visualizar el tráfico y comprobar el cumplimiento de las políticas se debe ingresar al menú de configuraciones de firewall y seleccionar el ítem *logs & report.*

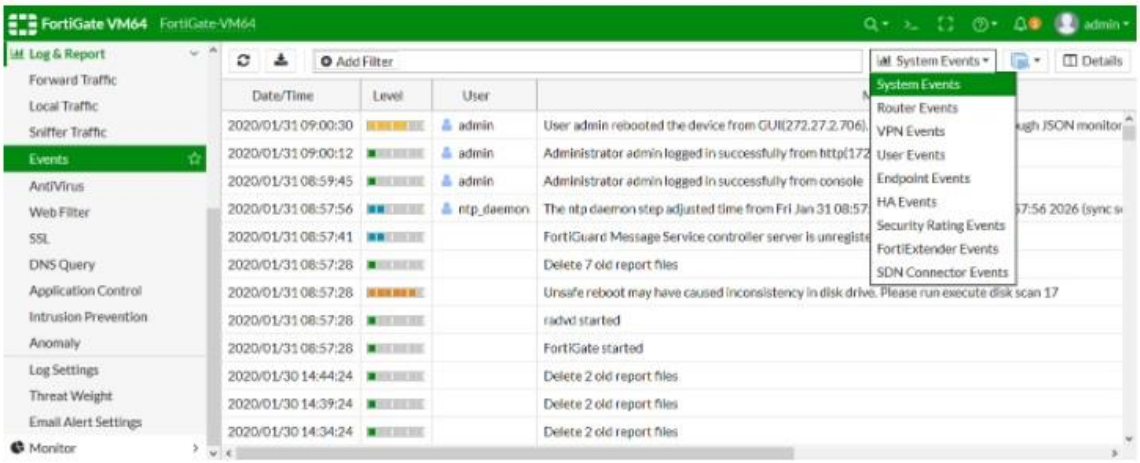


Figura 7. Visualización de logs & report.

Fuente: Elaboración propia

3.2 Evaluación del Protocolo IPV6 en red LAN

En esta sección se menciona las diferentes pruebas que se realizan para validar la implementación de protocolo IPv6 en los dispositivos o programas que están dispuestos en la red de área local (LAN) de la Corporación Autónoma Regional del Oriente - CAS

3.2.1 Equipos de comunicaciones

Los equipos de comunicaciones que permiten la comunicación de datos en la red LAN están conformados básicamente por RouterBoard y conmutadores de capa dos, la conectividad entre estos elementos se muestra en los documentos del plan de diagnóstico del presente proyecto.

3.2.1.1 Routerboard

Se realizan diversas pruebas al equipo RouterBoard-Mirotik pues este cumple diferentes funciones esenciales para comunicación entre equipos y redes, las pruebas a tener en cuenta son las de conectividad y revisión de tablas de enrutamiento.

Prueba de Conectividad

La prueba de conectividad hace referencia a la verificación de que los puertos y enlaces de comunicación que utiliza el equipo RouterBoard-Mirotik están funcionando, es decir que se debe comprobar que dichos enlaces de comunicaciones están activos, enviando y recibiendo paquetes de datos bajo el protocolo IPV6. A continuación como se realizó la prueba de conectividad

I. Inicialmente se ingresa al menú de configuración del equipo RouterBoard-Mirotik, una vez adentro se puede observar las diferentes opciones de configuración para este caso se ingresa al terminar donde se puede utilizar la línea de comandos.

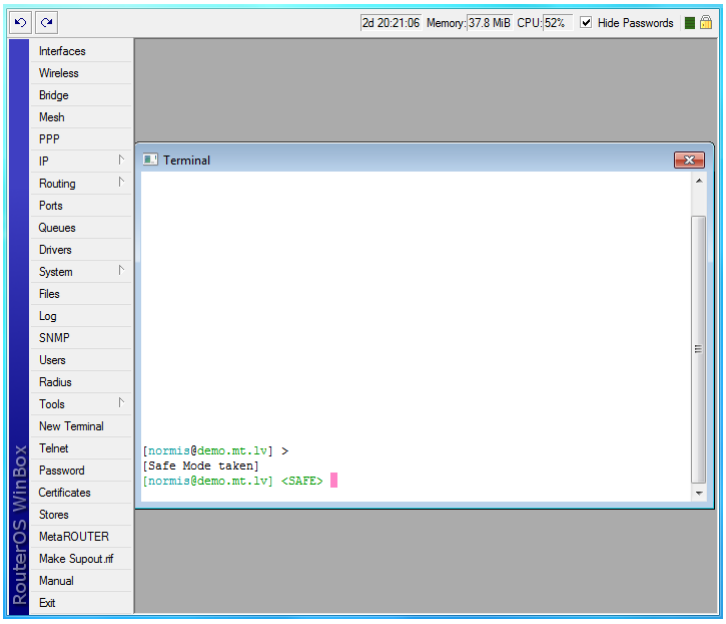


Figura 8. CLI del equipo Mikrotik

Fuente: Elaboración propia

II. En la línea de comandos se utiliza el comando *ping* para comprobar la conectividad de cada una de las interfaces activas bajo el protocolo IPv6 en el equipo, al igual que verificar él envió de paquetes de datos.

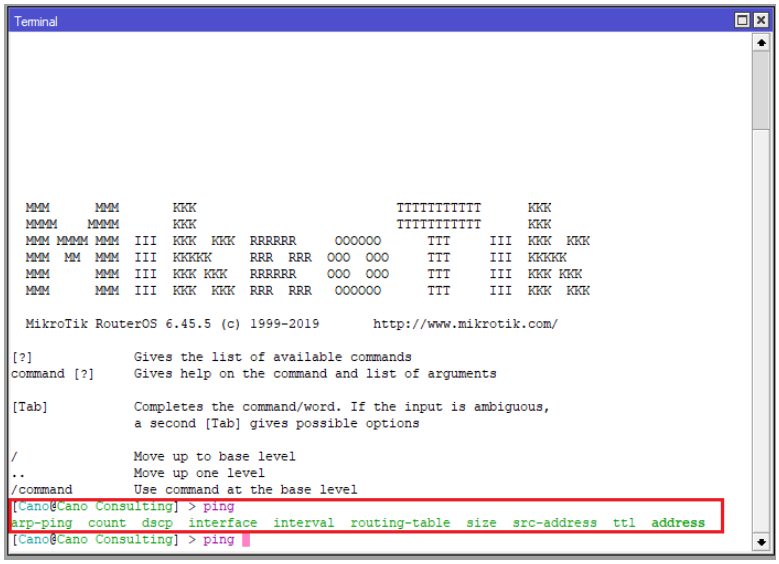


Figura 9. Consulta permitidas con comando Ping.

Fuente: Elaboración propia

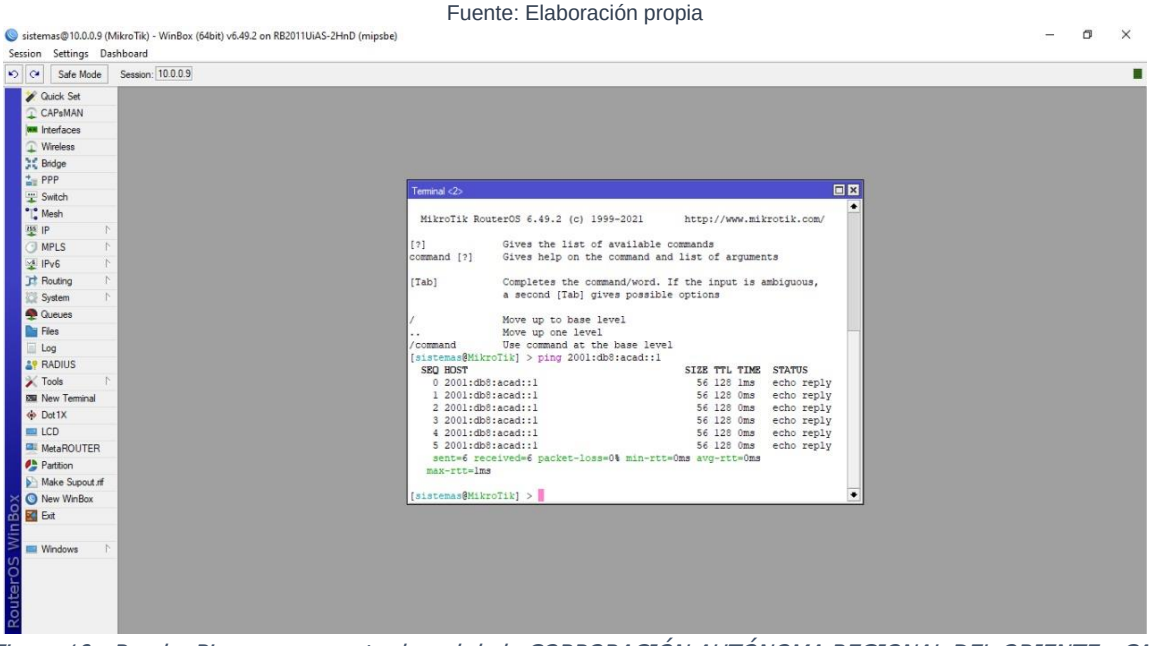


Figura 10. Prueba Ping en segmento de red de la CORPORACIÓN AUTÓNOMA REGIONAL DEL ORIENTE - CAS

Fuente: Elaboración propia

Como el proceso de comprobar la conectividad con el comando *ping* desde la interfaz del equipo Mikrotik es exitoso, se puede corroborar que el protocolo IPv6 esta adoptado.

Revisión de tablas de enrutamiento

Una vez realizada las configuraciones necesarias que permitan al enrutador (RouerBoard) conocer las redes o rutas por donde enviar los paquetes de información, se debe comprobar en el dispositivo que dichas rutas agregadas fueron añadidas por el sistema correctamente, también se ha de confirmar que las direcciones en IPv6 provistas para el enrutamiento son las deseadas

I. Se Ingresa al menú del equipo Mikrotik y se selecciona la pestaña IPV6, donde se ingresa al ítem *Addresses*

II. Después de ingresar se despliega una ventana donde se pueden observar las IPv6 con las rutas que toma cada una de las direcciones, con esta información se puede corroborar que las direcciones son añadidas correctamente por el sistema.

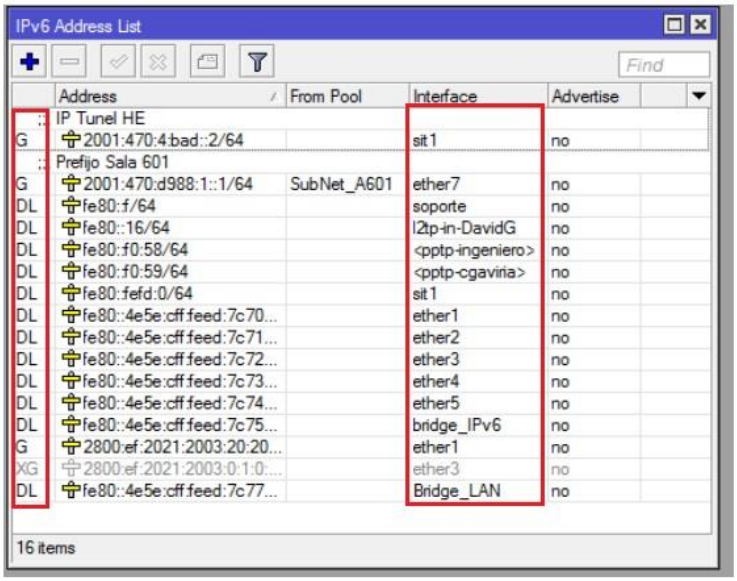


Figura 11. Interfaz de IPv6 Address List en equipo Mikrotik

Fuente: Academy Xpert. IPv6 con Mikrotik. Libro de estudio (p. 25)

Nota: La prueba de revisión de tablas de enrutamiento no fueron desarrolladas puesto que se necesita habilitar por parte del proveedor de servicios (ISP), los canales de comunicación o rutas hacia internet bajo el protocolo IPv6.

3.2.1.2 Switches(Conmutador)

Estos equipos son la base de la conexión de todos los dispositivos de usuario final por lo que son tan importantes en un esquema de redes de datos, para la implementación del protocolo IPv6 en la red de la CORPORACIÓN AUTÓNOMA REGIONAL DEL ORIENTE - CAS se hace igualmente relevante, pero según se ha comentado en otros documentos del presente proyecto como lo son el plan de diagnóstico y el plan de configuración, este tipo de dispositivos que tiene actualmente la Corporación Autónoma Regional del Oriente - CAS no permiten ningún tipo de administración o configuración, lo cual limita las pruebas que se puedan realizar o visualizar en el equipo, las pruebas a realizar se basan en la conectividad que genera el equipo de comunicaciones switch entre los dispositivos del usuario final. A continuación la prueba desarrollada para que confirma la funcionalidad del switch bajo el protocolo IPv6

I. Inicialmente se ingresa al símbolo del sistema desde un computador dentro de la red LAN, para esto se utiliza la ventana *Ejecutar de* Windows con el comando *CMD* se como se muestra a continuación:

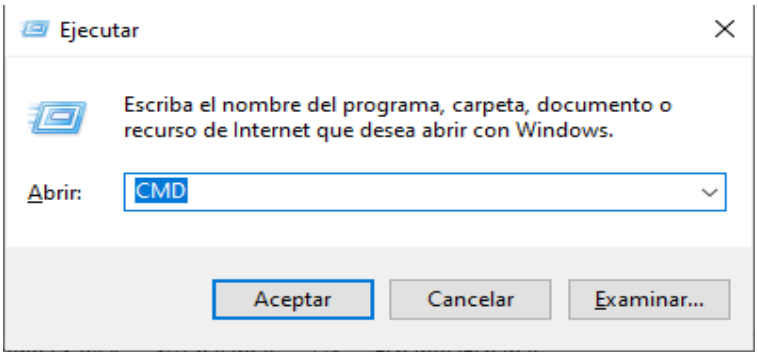


Figura 7. Ingreso de comando para ingreso al símbolo del sistema

Fuente: Elaboración propia

II. En el símbolo del sistema se hace *ping* a una de las direcciones IPv6 desplegadas en la red de datos de la CORPORACIÓN AUTÓNOMA REGIONAL DEL ORIENTE - CAS, como se observa en la siguiente figura el *ping* responde al llamado y con esto se verifica que el equipo Smith está cumpliendo su función de conmutador.

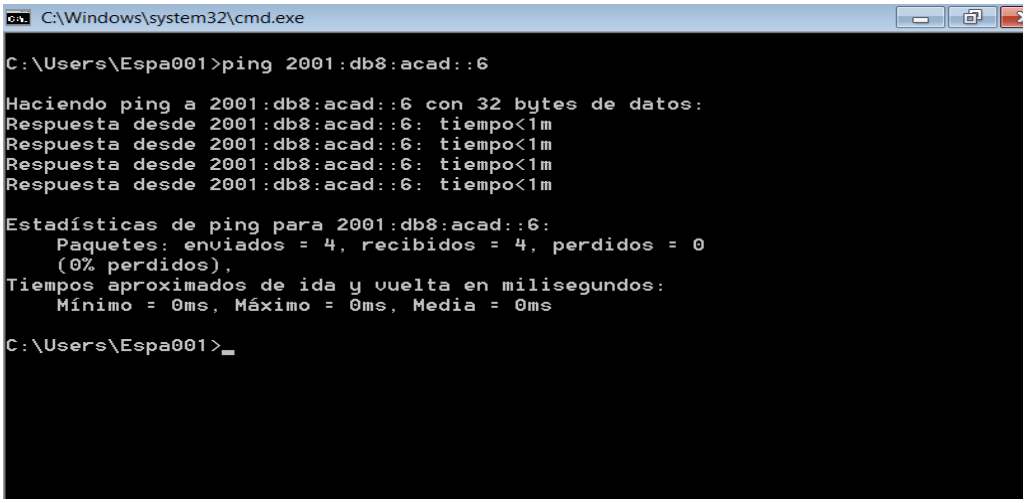


Figura 8. Ping a dirección IPv6 en red de la CORPORACIÓN AUTÓNOMA REGIONAL DEL ORIENTE - CAS

Fuente: Elaboración propia

3.2.2 Equipos de cómputo

En las pruebas para los equipos de cómputo dispuestos en la CORPORACIÓN AUTÓNOMA REGIONAL DEL ORIENTE - CAS, inicialmente se muestra el paso a paso que se realiza para la verificación de las configuraciones realizadas bajo IPv6 en un equipo dispuesto en el área de tesorería.

I. Inicialmente desde el equipo de tesorería de referencia CPU 4 EN 1 Lenovo 0004ls, se ingresa al símbolo del sistema, para esto se utiliza la ventana *Ejecutar de* Windows con el comando *CMD.*

II. Una vez en el símbolo del sistema del computador se requiere ver las direcciones IPv6 que han sido asignadas a nuestro equipo de cómputo en la tarjeta de red de forma dinámica desde la Mikrotik a través de un DHCP, para esto se utiliza el comando *ipconfig* como se muestra a continuación:

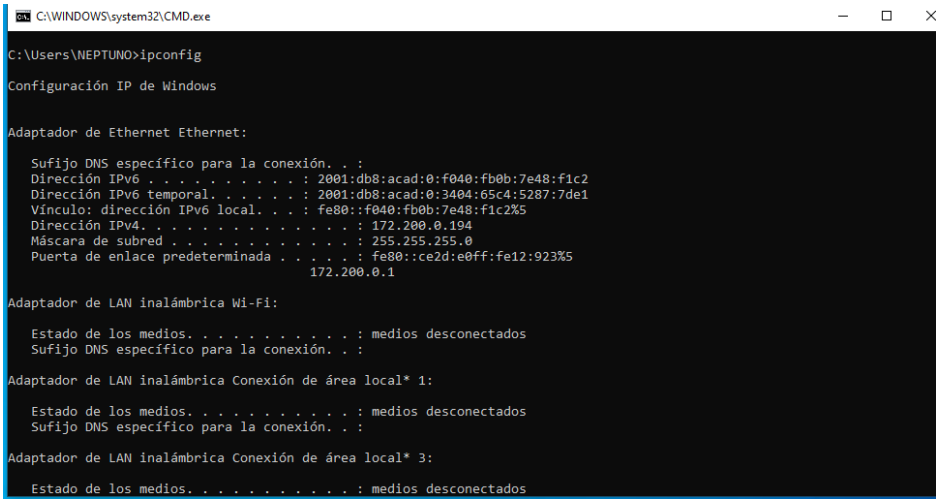


Figura 2. ipconfig en la tarjeta de red en equipo de tesorería

Fuente: Elaboración propia

III. Ahora el siguiente paso a seguir es hacer *ping a la dirección DNS 8.8.8.8* para verificar que la red tenga salida a internet como se muestra a continuación:

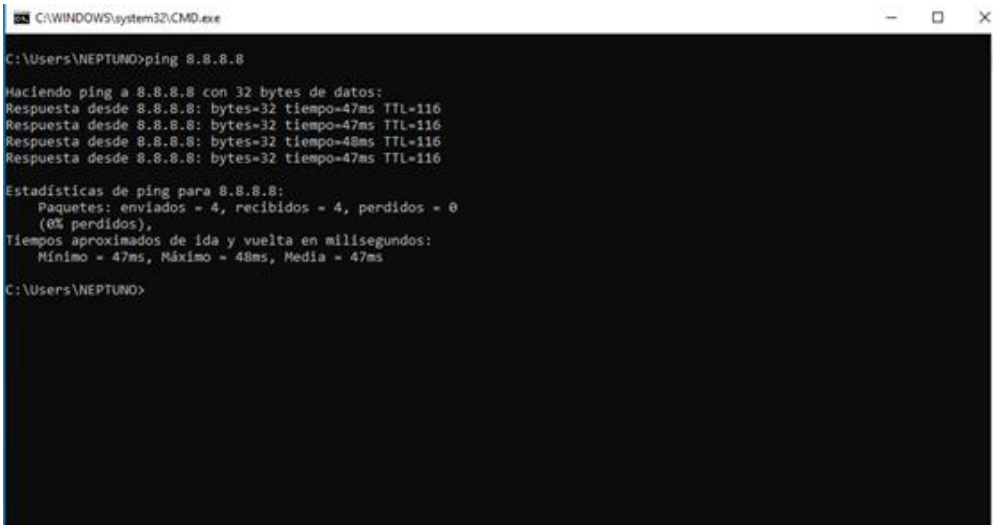


Figura 3. Verificación de salida a internet equipo tesorería

Fuente: Elaboración propia

IV. Luego de verificar que el equipo de cómputo tiene asignada su dirección IPv6 de forma dinámica y se haya comprobado que hay salida a internet, se realiza un test de prueba IPv6 desde el navegador, para esto se utiliza el navegador que se tenga predeterminado,

en este caso se realizara el test de prueba desde el navegador de *Google Chrome,* para realizar las pruebas se busca *test IPv6* y se da clic en la primera búsqueda que aparece como se muestra a continuación:

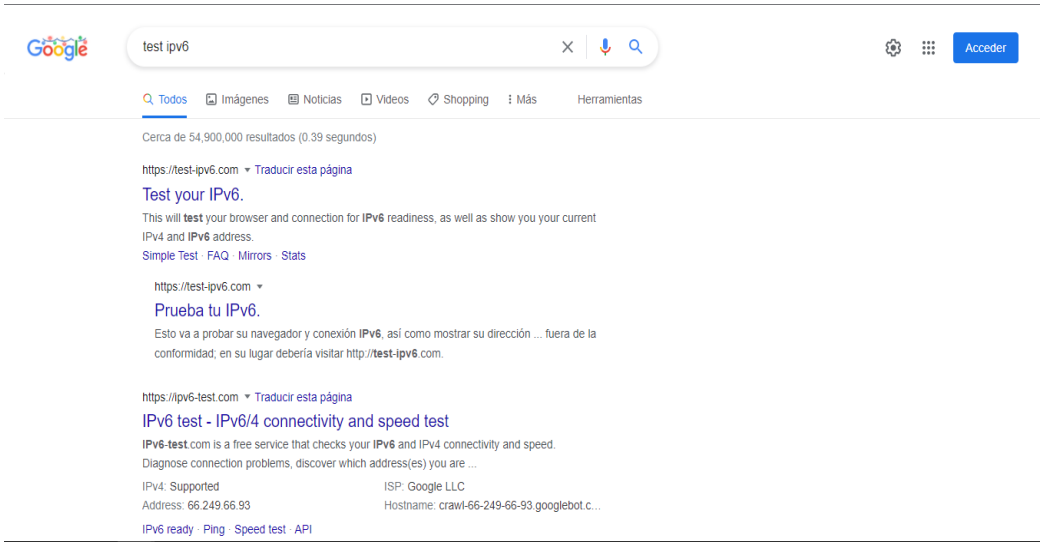


Figura 4. Búsqueda del test de IPv6 en el navegador de Google

Fuente: Elaboración propia

V. Una vez de haber ingresado al test de prueba IPv6, se verá una ventana informando que el test de conectividad IPv6 del equipo de cómputo está comenzando como se muestra a continuación:



Figura 5. Comienzo de test de prueba IPv6

Fuente: Elaboración propia

VI. Después de haber cargado todo el test de prueba IPv6 como resultado se obtiene la siguiente información:

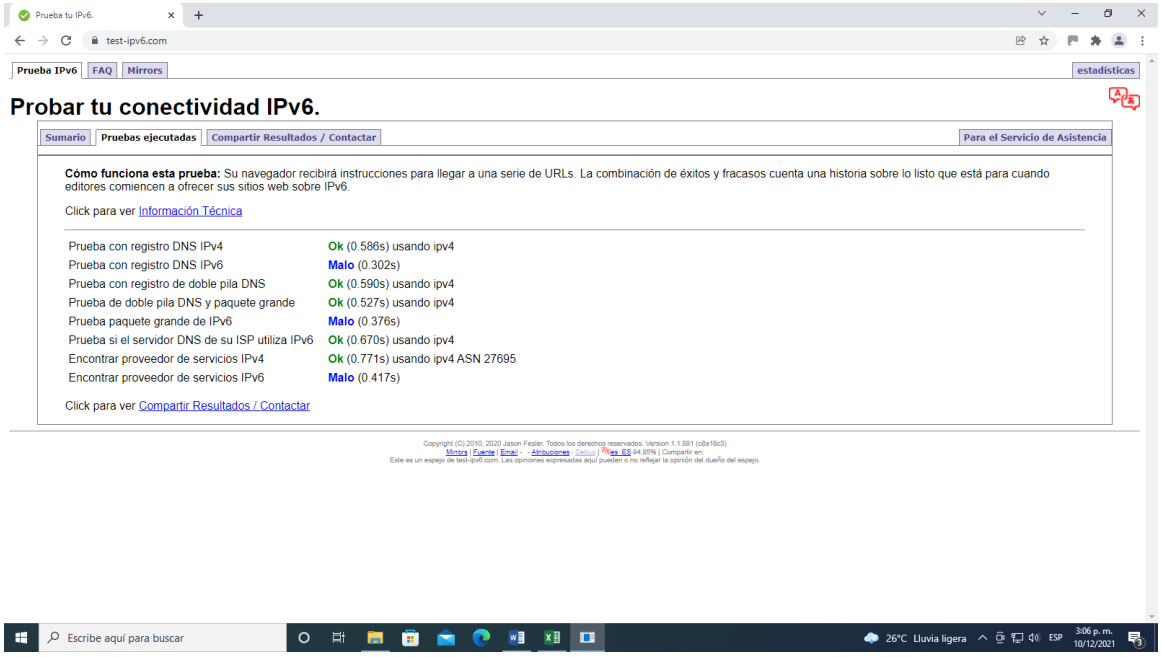


Figura 12. Pruebas ejecutas en navegador equipo tesorería

Fuente: Elaboración propia

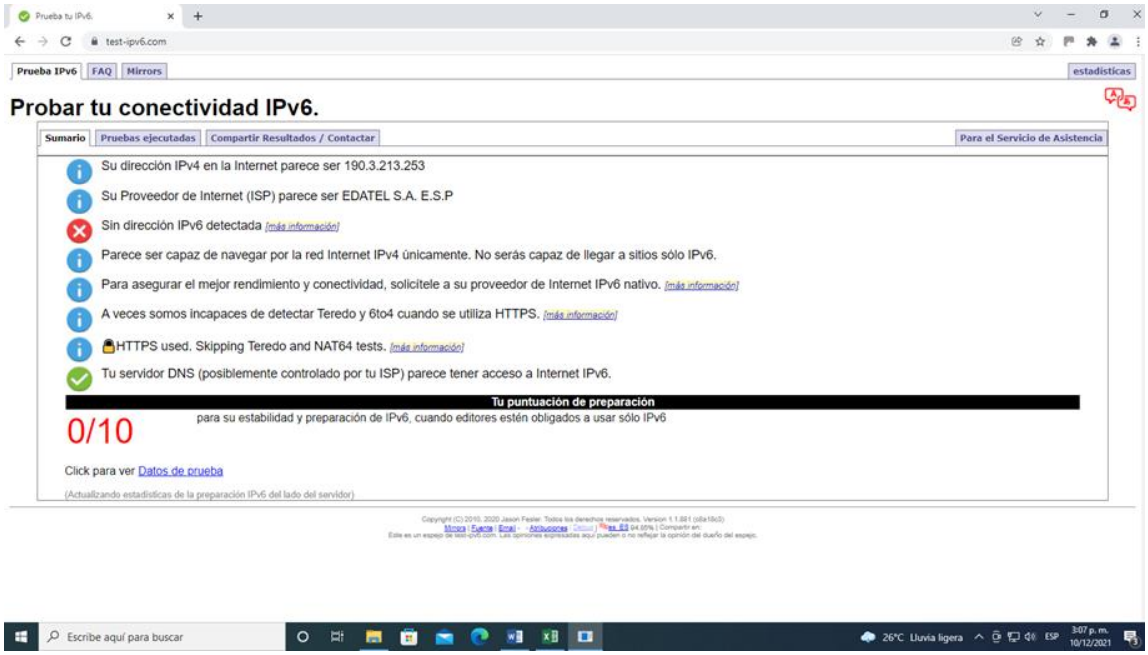


Figura 6. Resumen de test de prueba IPv6 en equipo tesorería

Fuente: Elaboración propia

Nota: Todas las pruebas del test de IPv6 ejecutadas en el navegador mostraran una no adopción de protocolo, debido a que se requiere la implementación de IPv6 por parte del proveedor de servicios (ISP), puesto que a través de estos canales se generan las consultas o conexiones hacia internet.

3.3 Evaluación de servicios sobre el protocolo IPV6

3.3.1 Servicio de DHCPv6

Para comprobar el servicio de DHCPv6, se revisa que el equipo Routerboard-Mikrotik añadió los cambios hechos en la fase configuración y que equipos en la red de la Corporación Autónoma Regional del Oriente - CAS adquieran una IP del servicio DHCPv6. A continuación se muestran los resultados obtenidos.

- Para verificar la adicción del servicio de DHCPv6 en el equipo Mikortik se ingresa al menú de configuración y se selecciona la opción *DHCPv6 Server*, en esta área se observa los diferentes servidores DHCP en el protocolo IPv6 creados.

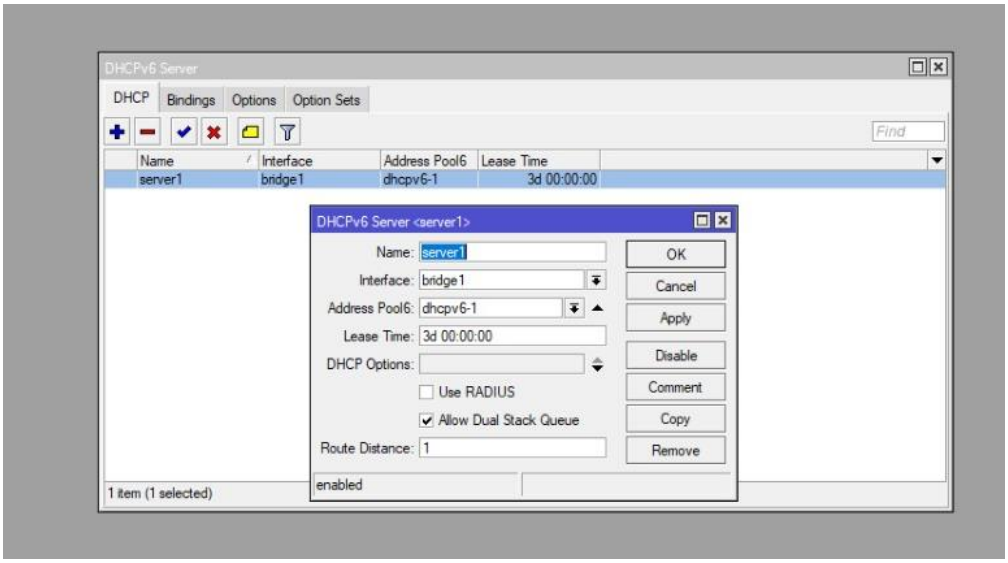


Figura 13. Interfaz de servidor DHCPv6

Fuente: Elaboración propia

- Una vez el servidor DHCPv6 entregue las direcciones IP, el equipo mikrotik guarda información sobre que dispositivos adquieren una Dirección en IPv6 en la red de la CORPORACIÓN AUTÓNOMA REGIONAL DEL ORIENTE - CAS, esto se observa al seleccionar la opción *IPv6 neighbor list*.

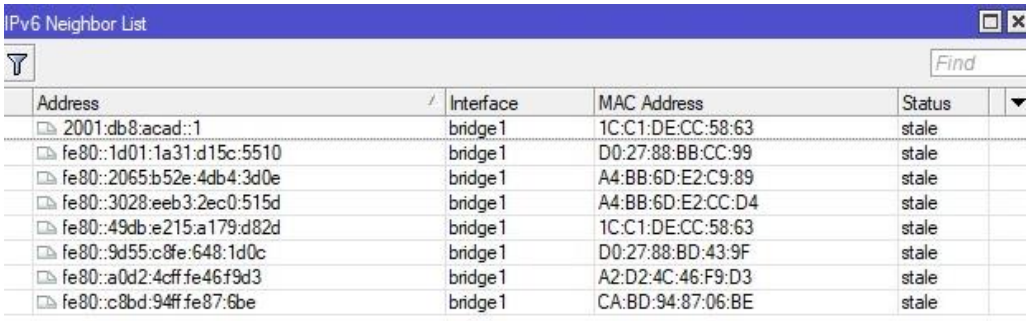


Figura 14. Interfaz de IPv6 NeigHbor List

Fuente: Elaboración propia

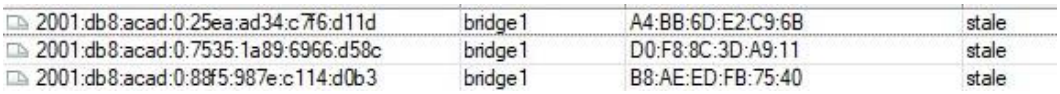


Figura 15. Equipos vistos por equipo Mikrotik con IPv6

Fuente: Elaboración propia

3.3.2 Sistema de vigilancia

Al sistema de vigilancia el cual está conformado por las cámaras IP y el Grabador de Video de Red (NVR) se les realiza diferentes pruebas para determinar el funcionamiento del protocolo IPv6, una de las pruebas está enfocada en confirmar la adopción de las direcciones IPv6 en las cámaras y la otra prueba para confirmar que le NVR permite el ingreso a su sistema bajo el protocolo IPv6, en el caso de las cámaras se confirmó en la fase de configuración se confirmó que no soportan el protocolo IPv6, Por lo cual no hay pruebas de adopción que realizar, en el caso de las pruebas para el equipos NVR estas fueron las evidencias tomadas ante la pruebas realizadas.

- Inicialmente para realizar las pruebas de adopción de IPv6, se ingresa a un equipo de cómputo con el mismo segmento de red que el NVR.

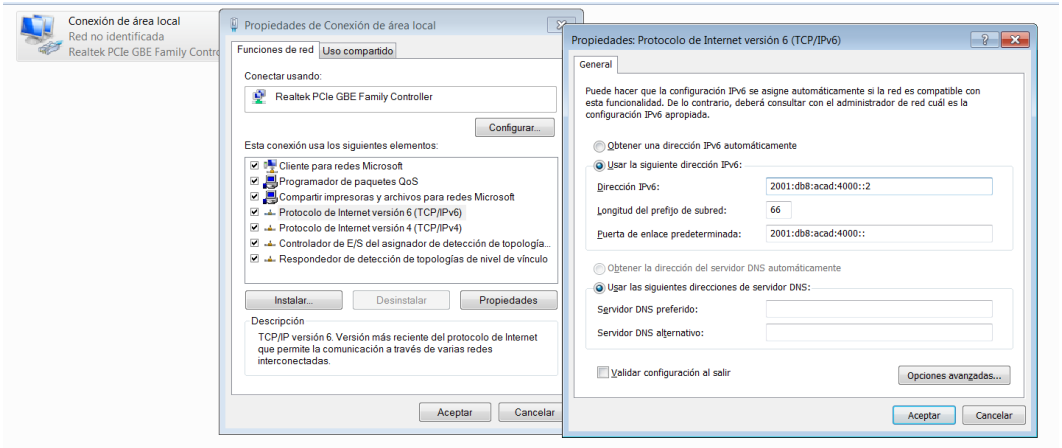


Figura 16. Configuración de IPv6 de equipo de cómputo en red del NVR

Fuente: Elaboración propia

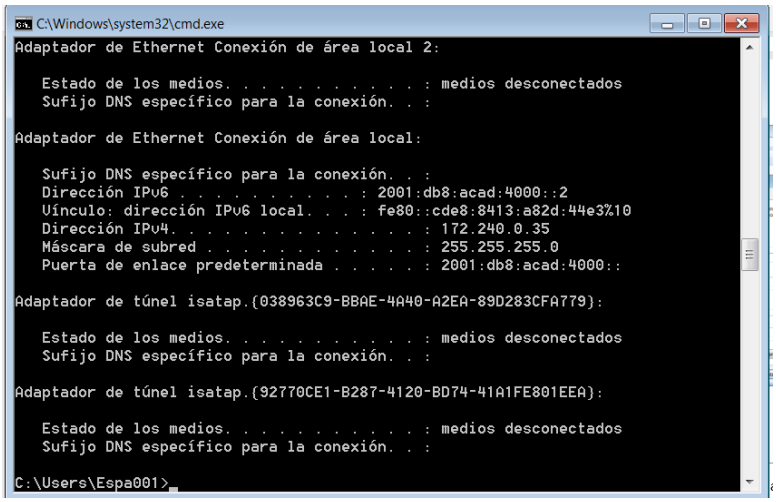


Figura 17. Verificación de IPv6 en equipo de cómputo.

Fuente: Elaboración propia

- Una vez con los equipos en el mismo segmento de red, desde el equipo de cómputo en red ,se utiliza el comando *Ping* para comprobar la conectividad

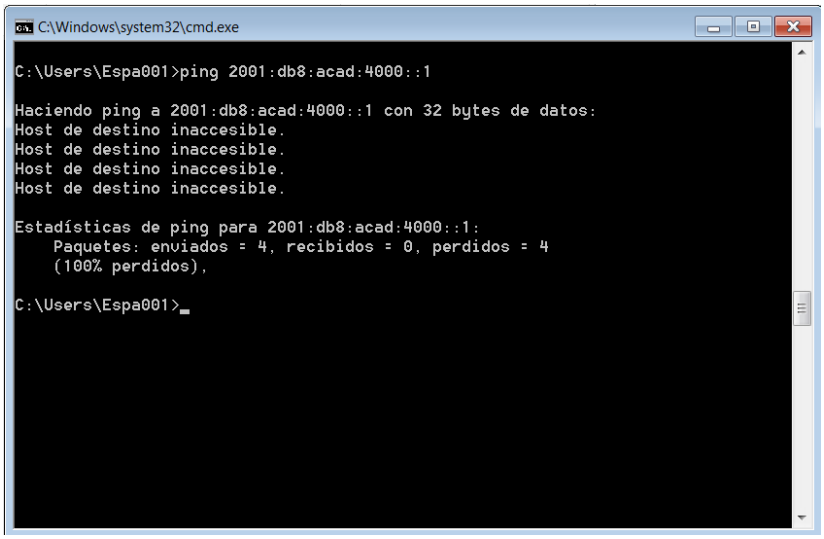


Figura 18. Prueba de comunicación con comando Ping

Fuente: Elaboración propia

3.4 Evaluación de aplicaciones sobre el protocolo IPV6

Para cada aplicación utilizada en la CORPORACIÓN AUTÓNOMA REGIONAL DEL ORIENTE - CAS, se prueba el ingreso al sistema desde los equipos de usuario final configurados con el protocolo IPv6, confirmando de esta forma que las plataformas, paginas o aplicativos funcionan correctamente, validando la convivencia de los 2 protocolos (Dual Stack). Cabe señalar que las pruebas hechas a los aplicativos confirman el funcionamiento de todos los elementos que la conforman como: servidores, base de datos, lenguaje de programación e interface de usuario.

3.4.1 Aplicativos terceros

Todos aquellos sistemas de información que utiliza la Corporación Autónoma Regional del Oriente - CAS pero que no son de su propiedad, se denominan aplicativos de terceros, estos son evaluados de la misma forma que los aplicativos propios con el fin de demostrar la operatividad dual de los protocolos IPv4 e IPv6, entre los aplicativos que se verificaron en

esta etapa están ARL y Seguridad Social. A continuación la evidencia de los ingresos a dichas plataformas

ARL

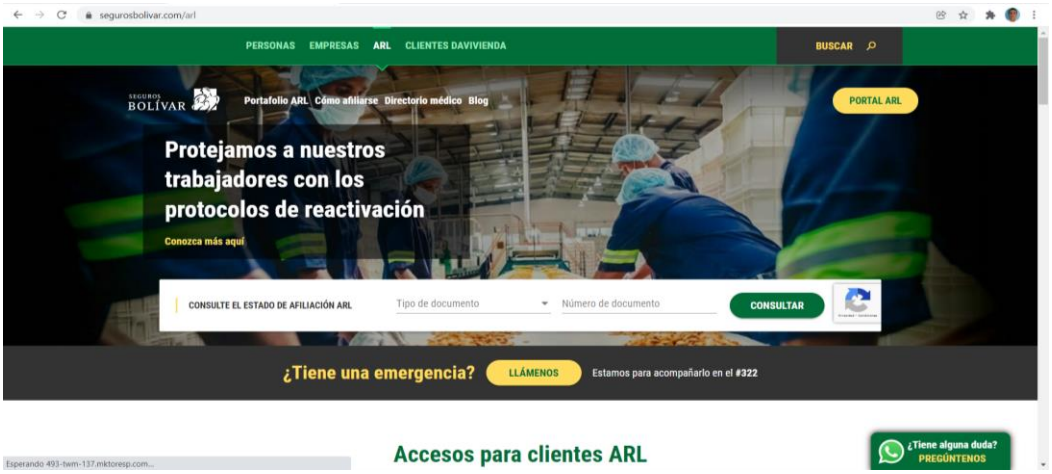


Figura 19. Interfaz de ingreso a plataforma seguros bolívar

Fuente: Elaboración propia

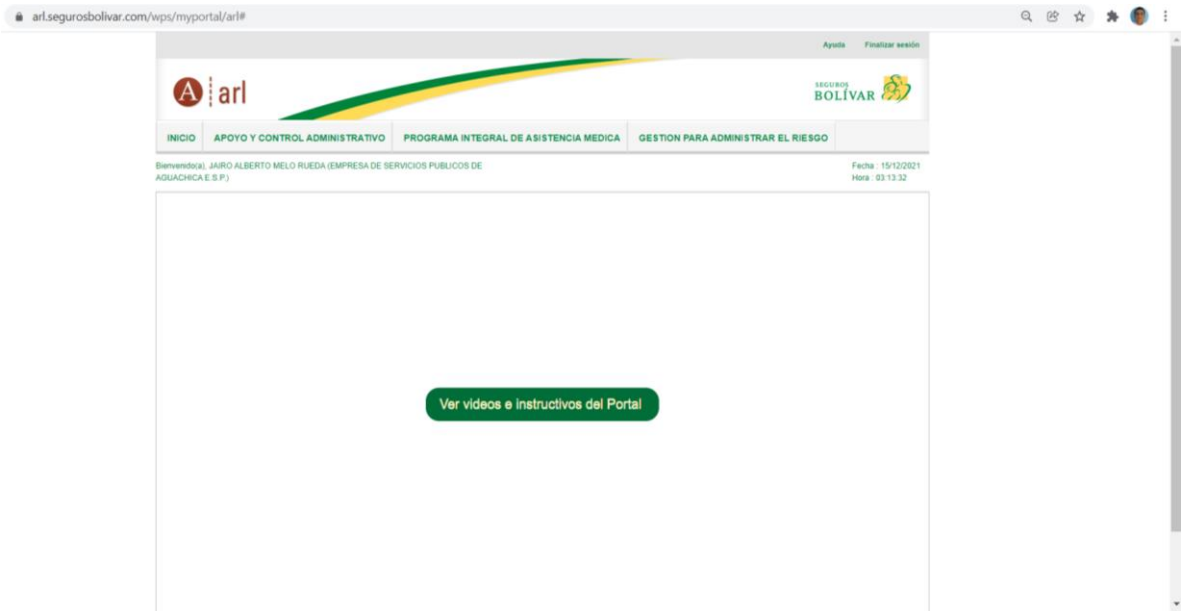


Figura 20. Ingreso a Plataforma de Seguros bolivar

Fuente: Elaboración propia

Seguridad social



Figura 21. Interfaz de ingreso a plataforma banco agrario de Colombia

Fuente: Elaboración propia



Figura 22. Ingreso a Plataforma de banco agrario de Colombia

Fuente: Elaboración propia

4. TERMINOLOGÍA

AUDITORÍA: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.

AUTENTICACIÓN: Provisión de una garantía de que una característica afirmada por una Entidad es correcta.

BASE DE DATOS: Tecnología de la información que permite la estructuración de forma adecuada de los datos a través de la construcción de relaciones de sus elementos.

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, Entidades o procesos no autorizados.

DIRECCIÓN IP: Representación numérica que identifica una interfaz en particular de manera exclusiva en una red de datos.

DIRECCIONAMIENTO IPV6: Es una etiqueta numérica del paquete usada para identificar una interfaz de red que provee una conexión entre nodos de una red sobre IPv6, esto facilita el enrutamiento de los paquetes entre distintos hosts.

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una Entidad autorizada.

DHCPv6 (Protocolo Dinámico de Configuración de nodos)[1]: Protocolo de configuración con estado ("stateful") que proporciona direcciones IP, direcciones de los servidores DNS y otros parámetros de configuración.

[1] Las definiciones (g) a (m) Tomadas de http://www.IPv6.es/es-ES/Glosario/

DIRECCIÓN: Identificador único asignado a nivel de la capa de red a una interfaz o conjunto de ellas, que puede ser empleado como campo de origen o destino en datagramas IPv6.

DNS (Sistema de nombres de dominio, Domain Name System): Sistema jerárquico de almacenamiento y el protocolo asociado para almacenar y recuperar información que permite vincular nombres y direcciones IP.

DOBLE-PILA (DUAL-STACK): Mecanismo de coexistencia IPv4/IPv6, mediante el cual un nodo incorpora tanto la pila IPv4 como la pila IPv6.

INFRAESTRUCTURA TECNOLÓGICA: Conjunto de elementos de hardware y software sobre el que se asientan los servicios de una organización.

IP: Protocolo Internet

IPsec (IP Security): Protocolo de seguridad definido por el estándar IETF desde 1999 y basado inicialmente en los RFC 2401 y 2412, pero en la tercera generación de documentos nacieron los RFC 4301 y 4309, que le dieron la abreviatura IPsec como hoy en día se conoce; ofrece integración a nivel de red, brindando seguridad de IP a los protocolos de capas superiores, actúa como un componente embebido dentro de IPv6 que suministra control de acceso, autenticación de origen de datos, confidencialidad, integridad es un esquema no orientado a la conexión, con independencia en los algoritmos de cifrado y negociación de compresión IP.

IPv4: Protocolo de Internet versión 4.

IPv6: Protocolo de Internet versión 6.

ISP – INTERNET SERVICE PROVIDER[2]: Un Proveedor de Servicios de Internet asigna principalmente Corporación Autónoma Regional del Oriente - CAScio de direcciones IP a los usuarios finales de los servicios de red que éste provee. Sus clientes pueden ser otros ISPs. Los ISPs no tienen restricciones geográficas como lo tienen los NIRs.

LACNIC: Organización internacional no gubernamental con sede en Uruguay cuya función es la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), números autónomos y resolución inversa para la región de América Latina y el Caribe.

LENGUAJE DE CONSULTA ESTÁNDAR (SQL): Lenguaje de programación dentro del cual se establecen las reglas para la estructura, consulta y presentación de datos e información.

LENGUAJE DE PROGRAMACIÓN: Conjunto de reglas sintácticas que permiten la construcción de aplicaciones y/o Sistemas de Información

MECANISMOS DE TRANSICIÓN A IPV6: Los protocolos IPv4 e IPv6 no son compatibles y para la migración a IPv6 debe mantenerse la coexistencia de ambos protocolos por un tiempo determinado en lo que se logra la total migración a IPv6. La clave para una migración exitosa consiste en poder utilizar ambos protocolos en la red hasta que todos los servicios sean migrados a IPv6. La mayoría de los nodos de Internet van a necesitar utilizar ambos protocolos por mucho tiempo, lo que requiere la definición e implementación de mecanismos de transición a IPv6. Esos mecanismos de transición pueden agruparse en tres grandes categorías: (Doble Pila, Traductores, Tunneling).

A pesar de las ventajas que ofrecen cada uno de estos mecanismos, la esencia principal de todos ellos es el mecanismo de Doble Pila.

De acuerdo a las recomendaciones de MinTIC (Ministerio de Tecnologías de la Información y las Comunicaciones) y organismos internacionales como LACNIC el mecanismo que

[2] Tomado de http://www.lacnic.net/web/lacnic/manual-1

garantiza con eficiencia la coexistencia de ambos protocolos (IPv4 e IPv6) es el de Doble Pila. Este será por tanto el mecanismo que se considerará para la implementación del Protocolo Internet Versión 6 (IPv6) al interior de la institución.

MOTOR DE BASE DE DATOS: Herramienta tecnológica que permita la gestión de la información a través de la implementación de las reglas establecidas por el lenguaje SQL y la relación de entidades

NOTACIÓN HEXADECIMAL[3]: Notación empleada para expresar direcciones IPv6 en forma literal. La dirección de 128 bits es dividida en 8 bloques de 16 bits cada uno. Cada bloque se expresa como un número hexadecimal y éstos están separados del siguiente por medio del ":". Los ceros situados a la izquierda de cada bloque pueden ser omitidos. Ejemplo de una dirección IPv6 unicast: 2001:DB8:1234:ABCD:789:EF01:0:1.

POLÍTICAS DE SEGURIDAD: Son aquellas reglas y procedimientos definidos por una organización con el propósito de preservar la confidencialidad, la integridad y la disponibilidad de los sistemas y la información.

POLÍTICAS DE ENRUTAMIENTO: El enrutamiento basado en políticas proporciona una herramienta para reenviar y enrutar paquetes de datos basados en las políticas definidas por los administradores de red. En efecto, es una manera de que la política invalide las decisiones del protocolo de enrutamiento. El enrutamiento basado en políticas incluye un mecanismo para aplicar selectivamente políticas basadas en la lista de acceso, el tamaño de los paquetes u otros criterios. Las medidas que se toman pueden incluir el enrutamiento de paquetes en rutas definidas por el usuario, el establecimiento de la precedencia, el tipo de bits de servicio, etc.

PREFIJOS IPV6: Representan un rango o bloque de direcciones IP consecutivas. Que deberán solicitarse formalmente ante organismos autorizados para su asignación en cuyo caso la organización será propietaria indefinidamente de tal bloque de direcciones o podrá

[3] Las definiciones (o) a (s) Tomadas de http://www.IPv6.es/es-ES/Glosario/

recibirse de un Proveedor de Servicios de Internet con la diferencia de que tal direccionamiento no pertenecerá a la organización.

PROTOCOLO DE PRUEBAS: Programa sistemático de verificación e inspección diseñado y ejecutado para el control de calidad de la tecnología y operación de un equipo, proceso o servicio. Así como condiciones de seguridad y fiabilidad.

PROTOCOLO DE INTERNET: Conjunto de reglas para el emisión y recepción de datos a través de un canal de internet.

PROTOCOLO IPV4: Es la cuarta versión del Protocolo de Internet, es un protocolo de interconexión de redes. Utiliza direcciones de 32 bits que limitan el Corporación Autónoma Regional del Oriente - CAScio de direcciones a 42.934.967.296 direcciones.

PROTOCOLO IPV6: es la nueva versión del Protocolo de Internet (Internet Protocol -IP) en el cual se sustenta la operación de Internet. Las especificaciones técnicas básicas de IPv6 se desarrollaron en la década de los 90s con el IETF (Internet Engineering Task Force). Destinado a sustituir al Protocolo Internet Versión 4. IPv6 amplía el número máximo de direcciones de Internet al manejar un tamaño de dirección IP de 128 bits a diferencia de su antecesor IPv4 que maneja un tamaño de dirección IP de 32 bits.

PROVEEDOR DE SERVICIOS INTERNET: Empresas que proporcionan servicios de conexión a Internet y temas relacionados.

PRUEBAS DE FUNCIONALIDAD: Proceso mediante el cual se valida la funcionalidad de un sistema.

REDES PRIVADAS VIRTUALES – VPN: (Virtual Private Network): Es una tecnología de acceso que permite una extensión segura de la red local sobre una red pública o no controlada como Internet.

RESOLUCIÓN DE NOMBRES: Obtención de una dirección a partir de un nombre.

RFC: Petición de Comentarios, Request For Comments. Paso previo de un documento estándar de Internet (STD), aunque en la actualidad, los fabricantes implementan en sus productos RFC, sin esperar a que sean STD.

RIR: Regional Internet Registry: Los Registros de Internet Regionales (RIRs) son establecidos y autorizados por las comunidades regionales respectivas, y reconocidos por el IANA para servir y representar grandes regiones geográficas. El rol principal de los RIRs es administrar y distribuir los recursos de Internet dentro de las respectivas regiones.

SEGMENTOS DE RED: Resultado de dividir una red de datos con el propósito de aumentar el número de nodos conectados a ella.

SERVICIO WEB: Herramienta de software que permite la interoperabilidad entre sistemas o herramientas tecnológicas, de forma que garanticen la comunicación de escritura o lectura de datos.

SISTEMAS DE INFORMACIÓN: Conjunto de mecanismos ordenados como lenguaje de programación, base de datos, interfaz, servicio web, que tienen como fin la administración de datos e información para su procesamiento y entrega.

SISTEMAS DE COMUNICACIÓN: Conjunto de dispositivos interconectados para el transporte y entrega de información.

SUBRED: Uno o más enlaces que utilizan el mismo prefijo de 64 bits.

TOPOLOGÍA DE RED: Es el arreglo físico o lógico en el cual los dispositivos o nodos de una red (ejemplo: computadores, impresoras, servidores, switches, enrutadores, etc.) se interconectan entre si sobre un medio de comunicación.

a). Topología física: Se refiere al diseño actual del medio de transmisión de la red.

b). Topología lógica: Se refiere a la trayectoria lógica de una señal a su paso por los nodos de la red.

REFERENCIAS

- Ministerio de Tecnologías de la Información y las Comunicaciones (2016). Transición de IPv4 a IPv6 para Colombia. Bogotá: Ministerio de Tecnologías de la Información y las Comunicaciones. Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf
- Ministerio de Tecnologías de la Información y las Comunicaciones (2016). Aseguramiento del Protocolo IPv6. Bogotá: Ministerio de Tecnologías de la Información y las Comunicaciones. Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf
- Resolución del MINTIC 2710 de 2017. Fuente:https://www.mintic.gov.co/portal/inicio/61000:Resolucion-2710-de- 2017.
- Academy Xpert. IPv6 con Mikrotik. Libro de estudio. p. 94
- Fortinet. Consolidated IPv4 and IPv6 policy configuration. Fuente: https://docs.fortinet.com/document/fortigate/6.4.0/new-features/815846/consolidated-ipv4-and-ipv6-policy-configuration
- Fortinet. Dual stack IPv4 and IPv6 support for SSL VPN. Fuente: https://docs.fortinet.com/document/fortigate/7.0.0/new-features/766455/dual-stack-ipv4-and-ipv6-support-for-ssl-vpn