CONACYT
Consejo Nacional de Ciencia y Tecnología

CIMAT

2023
AÑO DE
Francisco
VILLA
EL REVOLUCIONARIO DEL PUEBLO

Memoria Técnica
IPv6

CIMAT

Guanajuato, Gto.

Versión	Fecha
1.0	28/02/2023

CONACYT
Consejo Nacional de Ciencia y Tecnología

CIMAT

2023 AÑO DE Francisco VILLA
EL REVOLUCIONARIO DEL PUEBLO

Índice General

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

Índice de Tablas

Índice de Figuras

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

1. DEFINICIONES

Prefijo: Número de bits contados de izquierda a derecha de una dirección IPv6, equivalente a la porción de red utilizada en las direcciones IPv4.

GRP: Global Routing Prefix o prefijo de enrutamiento global, diseñado para hacer una estructura jerárquica desde una perspectiva de enrutamiento global.

IID: Interface ID o identificador de interface equivalente a la porción de Host de una dirección IPv4, también conocido como sufijo.

RIR: Regional Internet Registry o Registro Regional de Internet, es una organización que supervisa la asignación y registro de recursos de internet en una región especifica.

NIBBLE: Digito hexadecimal (0-F) de 4 bits de una dirección IPv6.

SEGMENTO: Porción de 16 bits de una dirección IPv6 compuesta por 4 nibbles, cada uno de los segmentos debe estar delimitado por ¨: ¨ los valores de cada segmento oscilan entre :0000: y :FFFF:, es decir 65,536 combinaciones.

SLAAC: Stateless Address Autoconfiguration, Auto configuración de direcciones IPV6 sin estado.

DHCPv6: Dinamic Host Configuration Protocol, protocolo de configuración dinámica de direcciones o prefijos IPv6.

Disrupción: Interrupción brusca o trastorno en la operación de redes o sistemas.

Dual stack: Técnica de transición a IPv6 que implica que todo dispositivo conectado a una red cuente con direcciones IPv4 e IPv6 asignadas de forma simultánea.

Estrategia Digital Nacional: El plan de acción del Ejecutivo Federal para aprovechar el potencial de las tecnologías de la información y comunicación, incluidos los servicios de banda ancha e Internet, como elemento catalizador del desarrollo del país, mediante su incorporación a la vida cotidiana de las personas, y a la Administración Pública Federal, mediante el uso de la informática y el desarrollo del gobierno digital.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

Grupo de Trabajo para IPv6: el conformado en cada Institución de la Administración Pública Federal para establecer las acciones de planeación y ejecución necesarias para la transición a IPv6. Instituciones: las dependencias y entidades integrantes de la Administración Pública Federal.

Riesgo: la probabilidad de que una amenaza pueda explotar una vulnerabilidad, generando un impacto sobre la infraestructura de TIC y los activos de información de la Institución.

Seguridad de la Información: la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.

Tecnologías de la Información y Comunicación: el equipo de cómputo, software, dispositivos de impresión, infraestructura y servicios que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.

Translation: técnica de transición a IPv6 que implica la transformación de IPv4 en IPv6, o viceversa; no se recomienda la utilización de esta técnica como enfoque primario de la transición.

Tunneling: técnica de transición a IPv6 que implica la encapsulación de IPv4 en IPv6, o viceversa.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

2. ACRÓNIMOS

APF: Administración Pública Federal.

ASN: (Autonomous System Number): Número de Sistema Autónomo.

CEDN: Coordinación de Estrategia Digital Nacional de la Oficina de la Presidencia de la República;

DNS: (Domain Name Service): Sistema de nombres de dominio

IAR México: Organización encargada de prestar el servicio de distribución y administración de Recursos de Numeración de Internet, esto es, direcciones IP en sus versiones 4 y 6, así como los ASN y de la delegación de DNS inverso, para entidades establecidas en el territorio mexicano.

IPv4 o IPv6 (Internet Protocol version 4 or 6): Protocolo de Internet versión 4 o 6.

MGSI: Marco de Gestión de Seguridad de la Información.

OCF: Órgano de Control y Fiscalización de las Instituciones, el cual considera a los Órganos Internos de Control y/o análogos dependientes de la Secretaría de la Función Pública.

TIC: Tecnologías de la Información y Comunicación.

UAF: Unidad de Administración y Finanzas.

UTIC: Unidad de Tecnologías de Información y Comunicaciones o área responsable de las TIC en cada Institución.

IETF: Internet Engineering Task Force

Protocolo: es un conjunto formal de estándares y normas. Estos rigen tanto el formato como el control de la interacción entre los distintos dispositivos dentro de una red o sistema de comunicación.

DOF: Diario Oficial de la Federación.

LACNIC: Latín American and Caribbean Network Information Center, es el registro regional de internet para la zona de Latino América y el Caribe.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

3. RESUMEN

El proyecto de transición al protocolo de internet versión 6, surge como iniciativa de la Coordinación de Estrategia Digital Nacional (CEDN) en común acuerdo con la Administración Pública Federal en el acuerdo de TIC´s (Tecnologías de la Información y Comunicación) en el Título Cuarto sobre las Políticas Tecnológicas aplicables a los Proyectos de TIC y SI en su capítulo 2 referente a las redes de datos y servicios de internet, publicado en el diario oficial de la federación el 6 de septiembre de 2021, en el que se pide a las instituciones federales solicitar a la autoridad NIC México, el ASN y direccionamiento de IPv6 para un mejor aprovechamiento de la informática por parte del gobierno digital y de las tecnologías de la información, apegándose a los estándares técnicos definidos por la CEDN.

CAPÍTULO II

REDES DE DATOS Y SERVICIOS DE INTERNET

Artículo 50.- Los servicios de internet corporativo o de internet de oficinas remotas que contraten las Instituciones deberán cumplir con los Estándares Técnicos de la CEDN.

Artículo 51.- Las instituciones deberán adoptar las medidas para migrar sus servicios de telecomunicaciones hacia el protocolo de internet IPV6, de conformidad con la guía que para tal efecto emita la CEDN; mientras tanto, podrán utilizar el Protocolo de Internet IPv4 en aquellos servicios que sean expuestos tales como correo electrónico, transferencia de archivos, conexiones seguras y aplicaciones web.

Artículo 52.- Todas las Instituciones deberán solicitar ante la autoridad NIC México el número de ASN de IPv6; y deberán solicitar a sus proveedores de servicios la capacidad de ruteo de ASN. La gestión de la solicitud deberá notificarse a la CEDN a través de la Herramienta, adicionalmente, registrarán la solicitud de los nombres en el dominio gob.mx especificando su vigencia y propósito.

Artículo 53.- Las Instituciones deberán privilegiar la implementación de servicios de redes de telecomunicaciones proporcionados por otras Instituciones que cuenten con la capacidad técnica para hacerlo, con apego a los Estándares Técnicos de la CEDN.

Artículo 54 .- Las instituciones deberán, ante el uso compartido de redes de comunicaciones, considerar al menos los siguientes elementos:

a) Mecanismos y políticas de seguridad;

b) Protocolos de actuación en contingencias;

---

c) Niveles de servicios;

d) Identificación de vulnerabilidades; así como

e) Requisitos de gestión de todos los servicios de red.

Los cuales deberán estar contemplados en los Instrumentos de colaboración y contratos de servicios de red que se celebren.

Figura 1 ***DOF****.: Políticas Tecnológicas aplicables a los Proyectos de TIC.*

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

En relación a este acuerdo, se difundió igualmente por parte de la CEDN, la Guía para la Transición al Protocolo de Internet versión 6 (IPv6) en la Administración Pública Federal. En dicho documento se establecen las fechas en las cuales se debe desarrollar esta transición tecnológica y el porcentaje mínimo de avance en las mismas de acuerdo a la siguiente tabla:

1. Grupos de Trabajo para IPv6 integrados en un plazo no mayor a 45 días Hábiles.	A más tardar al 8 de febrero de 2022
2. Solicitud de Bloques de direcciones IP y el ANS ante IAR México.	A más tardar el 30 de junio de 2022
3. Piloto de transición a un ambiente operacional de sólo IPv6	A más tardar el 31 de diciembre 2022
4. Memoria técnica que derive del piloto de transición a un ambiente operacional de solo IPv6.	A más tardar el 31 de diciembre de 2022
5 .20% de los activos en las redes de la institución operando en un ambiente IPV6 y e informe de la conclusión de la transición a IPv6 de todos los sistemas que brindan servicios a la ciudadanía	A más tardar el 31 de diciembre de 2023
6. 50% de los activos en las redes de la institución operando en un ambiente IPv6.	A más tardar 31 de diciembre de 2024
7. 80% de los activos en las redes de la institución operando en un ambiente IPv6.	A más tardar 31 de diciembre de 2025

Tabla 1 Guía para la transición a IPv6.

Los puntos que se abordarán en el presente documento es el 3 y 4 de acuerdo a la guía.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

4. INTRODUCCIÓN

Como parte de la adaptación tecnológica de los Centros Públicos de Investigación, el proceso de transición al protocolo IPv6 forma parte medular de la arquitectura tecnológica que han de adoptar todas las entidades en el mundo. Si bien los conceptos del Internet de las Cosas (IoT) e inteligencia artificial, entre otros, requieren recursos de direccionamiento más efectivos y que involucren procesos más cortos para la entrega de información, la incorporación de un protocolo con un espectro más amplio de direccionamiento aportará un sinnúmero de posibilidades de experimentación e integración de servicios de tecnologías de información y comunicaciones, mejorando aún más los servicios y los tiempos de respuesta involucrados en ellos.

El Centro de Investigación en Matemáticas, A.C., a través del Grupo de Transición al Protocolo IPv6, presenta este piloto de transición que contempla una base fundamental para la experimentación en un entorno simple ya en IPv6, cuyo objetivo, además de la integración de elementos tecnológicos conviviendo en este entorno y configurados en IPv6, el sustento de las primeras pruebas de convivencia en dual-stack con elementos IPv4 versus elementos IPv6. Las notas y observaciones derivadas de este piloto, permitirán la planeación, análisis y contención de posibles riesgos, hallazgos e incidentes relacionados con el intercambio de información entre ambos protocolos.

El resultado esperado es lograr una planeación en etapas desarrolladas en el periodo comprendido entre enero 2023 y diciembre 2025, contemplando las necesidades inmediatas en cuanto a arquitectura tecnológica y la configuración final de los elementos tecnológicos que la conforman.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

5. OBJETIVOS

1. Obtener una infraestructura piloto donde se puedan detectar las necesidades en términos de infraestructura, configuración y adaptación a los cambios implícitos en una transición al protocolo IPv6, mediante un laboratorio de equipos que permitan evaluar todos los factores involucrados sin afectar la operación de los servicios de telecomunicaciones y seguridad de la información, para que una vez que se inicie en modo producción ya se tengan previstos la mayor cantidad de variables involucradas en este proceso y contener la afectación de las mismas, considerando los factores externos que pudieran afectar o beneficiar la arquitectura institucional, para la implementación de los mismos.

2. Dar cumplimiento a las etapas que especifica la Guía para la Transición al Protocolo de Internet versión 6 (IPv6) en la Administración Pública Federal.

3. Establecer la base de conocimiento necesaria para la transición de la infraestructura completa de la red del Centro en todas sus unidades.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

6. PLAN DE TRABAJO

Como parte de las actividades realizadas para la preparación del laboratorio de la prueba piloto solicitada por la CEDN para el plan de transición a IPv6, el personal del CIMAT responsable de esta actividad planteó el laboratorio en base a los siguientes elementos:

1. Definir los segmentos IPv6 a usar en la sede Guanajuato tanto para la parte de LAN como para la WAN, para su publicación a través del protocolo BGP con el apoyo del ISP.
2. Configuración de un Router para la publicación de los segmentos IPv6 y uso del Sistema Autónomo.
3. Configuración de un Firewall de prueba para el uso del nuevo esquema de IPv6.
4. Configuración de servidores DNS Autoritativos y Recursivos basados en el esquema de IPv6 e IPv4.
5. Configuración de un servidor de prueba para la página web del CIMAT con direccionamiento IPv6.

Los puntos definidos anteriormente son en base a un ambiente similar a lo que se tiene actualmente en producción en el Centro, con el objetivo de gradualmente integrar cada elemento en nuestra infraestructura a manera de evitar situaciones que puedan afectar el desempeño en los servicios que se brindan en el CIMAT.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

6.1 Plan de direccionamiento IPv6 independiente del prefijo

El plan de direccionamiento significa básicamente la segmentación de un prefijo inicial, el prefijo inicial puede ser de documentación o el prefijo que asignó IAR. La CEDN en su guía sugiere la generación de un plan de direccionamiento para la fase de planeación con un prefijo de documentación, comenzando con plan de direccionamiento para la fase de pruebas de funcionamiento. Para este documento se usará un prefijo asignado por IAR ajustado a las necesidades de dirección de la entidad.

Mediante el uso de una sola red sumarizada, esta situación facilita el tráfico IPv6 debido a que se disminuye el tamaño de las tablas de enrutamiento de los equipos de capa 3. Para realizar una segmentación exitosa que garantice la implementación, la buena práctica es establecer la cantidad de segmentos IPv4 que actualmente funcionan en la infraestructura de la entidad, esta práctica indica el número exacto de LANs o VLANs que se van a cubrir con direccionamiento IPv6, además de establecer el número exacto de LANs o VLANs nuevas para usos específicos y las reservas que se necesiten en el proceso de implementación.

Para el caso del Centro, que cuenta con 6 sedes conectadas a internet y a un DATACENTER central, se definió prefijos /48. Las razones por las cuales se eligió este prefijo son las siguientes:

- *Escalabilidad*: Debido a la posible demanda de estudiantes a lo largo del territorio nacional, el subnetting del prefijo /44 a prefijos /48, estos darán la posibilidad de conectar 65,536 subredes /64 para cada uno.

- *Asignación de recursos*: Cada digito hexadecimal de una dirección IPv6 contiene 4 bits y se denomina NIBBLE, LACNIC recomienda que la solicitud del prefijo se realice en limites binarios, esto significa que se deben solicitar prefijos múltiplos de 4 para garantizar NIBBLES completos y facilitar la segmentación del prefijo, por esta razón se asignó un prefijo /44 por parte IAR.

La red del CIMAT se define como una gran estrella lógica cuyo punto central es un DATA CENTER. Todas las sedes pueden comunicarse a internet de manera independiente y a este DATA CENTER para solicitar servicios y recursos. El prefijo /44 permite entregar direccionamiento a todas las sedes del Centro con un enfoque escalable, este prefijo permite la construcción de nuevas sedes y la configuración de más LANs o VLANs en cada sitio.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

Verificando las necesidades actuales del Centro, en donde se detecta la existencia de por lo menos 6 redes, segmentadas mediante LANs o VLANs, con direccionamiento IPv4 y máscara de Subred de 24 y 28 Bits, es necesario replicar un modelo adaptable en el protocolo IPv6.

Como primera medida y como parte del proyecto actual se realizó la solicitud formal ante el NIR (National Internet Registry - para el caso de México IAR, dependiente de LACNIC) del direccionamiento IPv6 global de acuerdo con la guía dada por CEDN.

Después de realizar un proceso exitoso de solicitud de recursos ante IAR, el Centro cuenta ahora con un prefijo IPv6 propio y una dirección de sistema autónomo. El prefijo que fue asignado por IAR es: **2801:** [redacted][1] notación abreviada de 2801: [redacted]

Un ejemplo de asignación de direccionamiento IPv6 completo partiendo del prefijo asignado por IAR puede ser:

2801: [redacted]

Rojo**:** Direccionamiento otorgado por el ISP (/32).
Azul: Direccionamiento de la organización otorgado por IAR a CIMAT (/44).
Verde: Subred de la organización (/48 ó /64).
Negro**:** ID (Interface ID) Dirección individual del host (/128).

De acuerdo con el ejemplo y teniendo en cuenta los aspectos sobre IPv4 enumerados anteriormente, es recomendable hacer una asignación de red de la organización basados en /64 para redes IPv6, en donde tienen cabida las redes actuales y permite una amplia proyección a nuevas redes. (En el ejemplo esto corresponde al segmento de color **verde**, 1,048,576 subred /64).

La asignación del direccionamiento propio de la red, para el caso actual del Centro, cuyo direccionamiento IPv4 puede ser por ejemplo 172.22.XX.XX, 10.105.X.X, 172.29.XX.XX y 192.168.XX.XX, entre otros, de acuerdo al RFC 1918 de la IETF, para IPv6 en el ejemplo corresponde al segmento Azul, donde se hace la definición de la red; cabe anotar que esta dirección, así como en IPv4, es un identificador único y particular dentro de las redes y su asignación es definitiva, porque nombra la red y si es cambiado posteriormente puede generar incidentes de conectividad.

[1] Representa una cadena continua de segmentos IPv6 que contienen únicamente cero (0).

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

En el segmento Negro se denota el direccionamiento propio de cada o host IID (Interface ID).

Por último, el segmento Rojo es asignado por el ente regulador (LACNIC) o el ISP y NO es modificable ya que representa las direcciones globales.

6.1.1 Definición del direccionamiento IPv6.

La definición del direccionamiento propio en IPv6 para al Centro se realiza en el segmento de color Azul como en el ejemplo. Cabe recordar que estas direcciones son asignadas en hexadecimal con dígitos del 0 – 9 y caracteres A, B, C, D, E, F.

Aquí se puede colocar el direccionamiento a consideración propia de la entidad cuyo valor debe ser único, por ejemplo: ::1234. Es importante considerar que después de nombrado este debería ser un direccionamiento definitivo, ya que su modificación afecta equipos de comunicaciones, aplicaciones, bases de datos y demás activos de información en la red.

Tomando como base el prefijo asignado por IAR se selecciona un prefijo que cumpla con las necesidades de direccionamiento del Centro. Las condiciones que debe cumplir el prefijo son las siguientes: Número suficiente de Direcciones IPv6 y que sea múltiplo de cuatro para que esté en limite binario y facilite la segmentación. Para el caso de la entidad se selecciona el prefijo /44

2801:[redacted]

Para asignar direccionamiento a cada una de las sedes, data center y segmentos de WAN se usarán prefijos /48

2801:[redacted]

Para asignar direccionamiento a cada una de las WANs, LANs o VLANs se usarán prefijos /64

2801:[redacted]

Definidos estos segmentos se pueden definir direcciones IPv6 de este tipo:
2801:[redacted]
2801:[redacted]

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

Azul Prefijo /48 y Verde Subred desde /48 hasta /64

Negro: Corresponde al direccionamiento propio de cada host o IID (interface ID), esta porción de la dirección IPv6 se puede configurar de forma estática o usando SLAAC (autoconfiguración de direcciones con estado) o DHCPv6 (protocolo de asignación dinámica de direcciones IPv6).

PREFIJO ASIGNADO POR IAR	2801:[redacted]
SISTEMA AUTÓNOMO	[redacted]

6.2 Asignación de prefijo ipv6 /48 en las sedes del CIMAT

Segmentación del direccionamiento Ipv6 en todas las unidades de CIMAT.

2801:[redacted]	CIMAT GUANAJUATO
2801:[redacted]	
2801:[redacted]	
2801:[redacted]	
2801:[redacted]	
2801:[redacted]	CIMAT MONTERREY
2801:[redacted]	
2801:[redacted]	
2801:[redacted]	CIMAT AGUASCALIENTES
2801:[redacted]	
2801:[redacted]	CIMAT ZACATECAS
2801:[redacted]	
2801:[redacted]	CIMAT MERIDA

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

2801:[redacted]	
2801:[redacted]	PUERTO INTERIOR
2801:[redacted]	

Tabla 2 Asignación de prefijos a las sedes.

Se puede observar de manera precisa el prefijo /48 principal de cada una de las sedes; y la segmentación en prefijos /64 suficientes para cubrir todas las LANs o VLANs que se van a usar. Es importante mencionar que se tendrán en cuenta segmentos para LANs o VLANs nuevas de prueba, aplicaciones, equipos de comunicación y servidores, también se dejarán LANs o VLANs disponibles en caso de que la entidad las requiera para desplegar nuevos servicios en cada una de sus sedes.

El plan de direccionamiento también podrá contemplar segmentos /56 de reserva (respaldo) en cada una de las sedes en caso de que en un futuro se requiera direccionamiento adicional o sistemas de contingencia.

6.2.1 Segmentos para DATACENTER y WAN

Guanajuato 2801:[redacted]	
2801:C4:E0::/64	WAN, LOOPBACK Y ENLACES PUNTO A PUNTO
2801[redacted]	
2801:[redacted]	
2801:[redacted]	
2801[redacted]	
2801[redacted]	
2801[redacted]	
…	
2801[redacted] ó 2801[redacted]	
2801[redacted] ó 2801[redacted]	
2801[redacted] ó 2801[redacted]	
2801[redacted] ó 2801:[redacted]	

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

2801:[redacted]	DATACENTER
2801:[redacted]	TELEFONICA
2801:[redacted]	LAN
2801:[redacted]	VLAN
…	…
2801:C4:[redacted]	ETC.

Monterrey 2801:[redacted]	
2801:[redacted]	WAN, LOOPBACK Y ENLACES PUNTO A PUNTO
2801:[redacted]	
2801:[redacted]	
2801:[redacted]	
2801:[redacted]	
2801:[redacted]	
2801:[redacted]	
…	
2801:[redacted] ó 2801:[redacted]	
2801:[redacted] ó 2801:[redacted]	
2801:[redacted] ó 2801:[redacted]	
2801:[redacted] ó 2801:[redacted]	
2801:[redacted]	DATACENTER
2801:[redacted]	TELEFONICA
2801:[redacted]	LAN
2801:[redacted]	VLAN
…	…
2801:[redacted]	ETC.

Tabla 3 Segmentación del direccionamiento.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

Como se puede observar en la tabla anterior, en el caso de los servidores y equipos que poseen IPv4 pública, se hará la asignación en IPv6 en base a su homólogo en IPv4, convirtiendo la IPv4 a hexadecimal para obtener la equivalente en IPv6.

Cada una de las sedes o sitios tiene en promedio 25 a 30 LANs o VLANS para asignar a los diferentes departamentos, dependencias, redes especiales (networking, seguridad, aplicaciones, servidores, etc.), este direccionamiento se va a cubrir con prefijos /64 que parten de cada prefijo /48 del sitio, esto significa que cada sitio va a contar con 65,535 subredes /64, debido a que el primer prefijo /64 se para la definición de la red, la sede y/o la dependencia que usará determinado prefijo /64, esto dependerá exclusivamente del método de asignación de ID que se use en cada uno de los segmentos. (SLAAC, DHCPv6 O DIRECCIONAMIENTO ESTÁTICO).

Para el caso de los equipos servers que se van a configurar con direccionamiento estático, se puede hacer la asignación manual teniendo en cuenta la ubicación física y el direccionamiento IPv4.

6.3 Implementación del laboratorio para las pruebas para el piloto de transición.

A continuación, se muestra el diagrama de conexión usado para el laboratorio de pruebas en el que ya se usan IP's del segmento asignado por IAR para cumplir con el requerimiento de la prueba piloto.

6.3.1 Equipos usados en el laboratorio.

Equipo	Marca	Modelo	Función
Router	Huawei	AR650	Permite la comunicación hacia la red de Internet, anunciando los segmentos de red IPv4 e IPv6 a través del protocolo BGP.
Router ASR	CISCO	ASR1002-X	Anunciar los segmentos IPv4 e IPv6 por medio del protocolo de ruteo BGP usando el sistema autónomo de CIMAT, así como funcionar como puerta de enlace o Gateway para los equipos en la LAN.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

Servidor	HPE	Proliant DL380 G7	Soporta las máquinas virtuales de Firewalls, DNS y la de ambiente web.
Switch	CISCO	WS-C2960X-24TS-L	Interconectar los diferentes dispositivos (ASR, Firewall y servidores) segmentando la red en equipos dentro y fuera de la LAN.

Tabla 4 Equipos que forman parte del laboratorio.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

6.3.2 Esquema de conexión del laboratorio

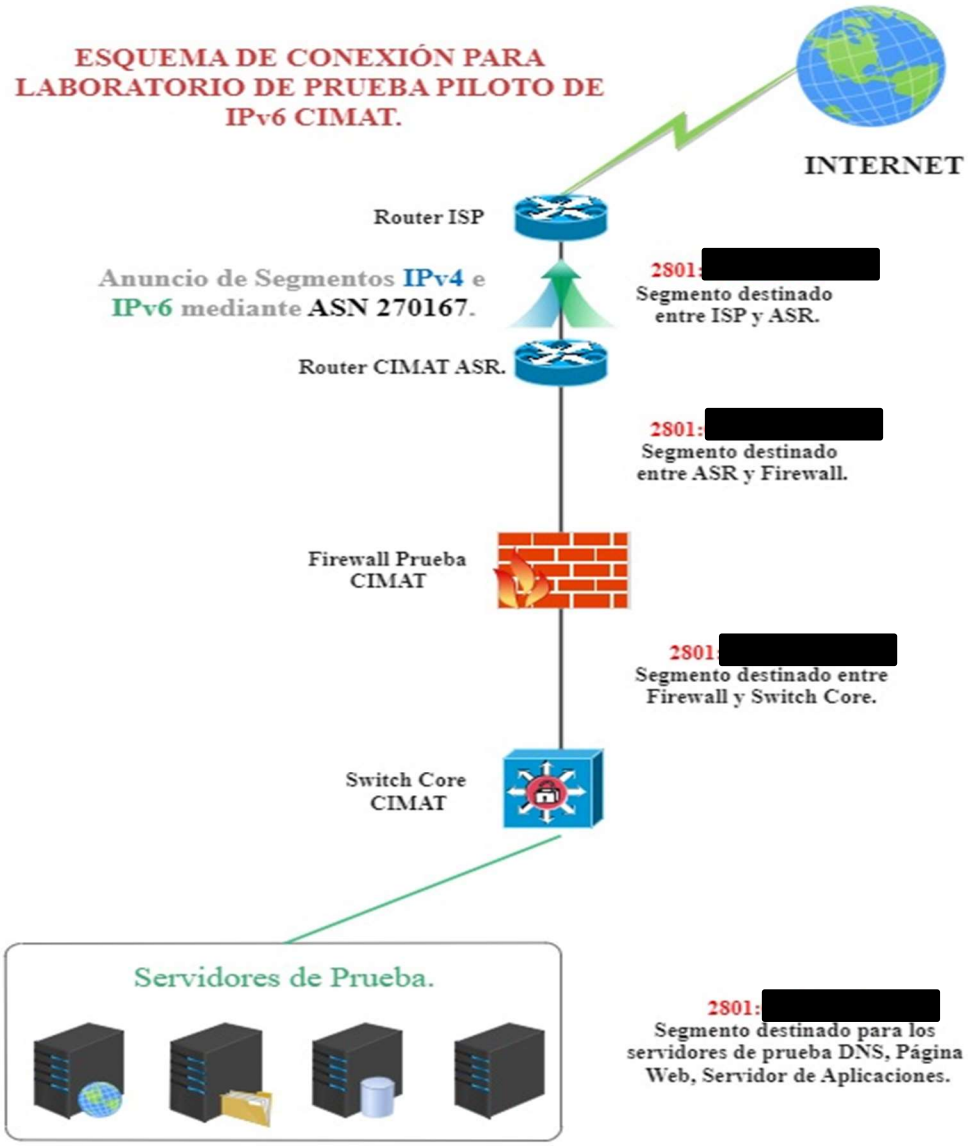


Figura 2 *Diagrama de conexión de red del laboratorio.*

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

6.3.3 Configuración de Router para anuncio de segmentos IPv6 y uso de ASN.

Como parte del proceso de transición a IPv6, que corresponde a la sede en Guanajuato del CIMAT, se solicitó de manera formal al proveedor de servicios de internet ISP, el anuncio de los segmentos IPv6 e IPv4 a través del Sistema Autónomo propios.

Los recursos IPv6 e IPv4 que se ha solicitado sean publicados por medio del protocolo BGP versión 4, además del uso del Sistema Autónomo recién adquirido por el CIMAT: el 2801[redacted] y 2801:[redacted] con el ASN [redacted] (de 32 bits). Se solicitó al ISP que el anuncio de los segmentos IP entrantes sean la ruta por defecto o Default Route, tanto para IPv4 como IPv6, con el objeto de evitar que el Router del CIMAT no sature su capacidad de memoria con la totalidad de prefijos que se reciban por medio de BGP.

El equipo que se usará para el ruteo es un equipo Cisco modelo ASR1002-X, el cual tendrá la dirección IPv6 2801:[redacted] en una conexión punto a punto con el Router del ISP que será la salida a internet como parte de la conexión WAN (o la dirección que indique el proveedor). Para la parte de la conexión LAN será la dirección IP 2801:[redacted] la cual estará conformada en una conexión punto a punto con el firewall de prueba del laboratorio.

```
router bgp 270167
 bgp log-neighbor-changes
 !
 address-family ipv4
  network [redacted] mask 255.255.255.0
 exit-address-family
 !
 address-family ipv6
  network [redacted]
 exit-address-family
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ipv6 route [redacted]
!
!
```

Figura 3 *Configuración del protocolo BGP en el ASR.*

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

Para la conexión entre el firewall y el switch principal o Core del CIMAT, que además funge como Gateway de las subredes del Centro, se ha determinado usar otra conexión punto a punto con ruteo estático, por lo que se usará el segmento de red 2801:[redacted]

Finalmente, para el segmento de LAN donde de momento se usarán servidores de prueba, en una zona simulando la DMZ del Centro se usará el segmento 2801:[redacted]

Para cumplir con lo solicitado por la Función Pública Federal mediante la CEDN, se requirió crear un laboratorio, este tiene la función de ejemplificar un ambiente híbrido (IPv4 e IPv6). Con el que es posible hacer diversas pruebas de funcionamiento sin afectar los servicios productivos, así mismo permite recabar la evidencia necesaria para demostrar que se ha implementado en su primera etapa el protocolo IPv6 en las instalaciones de CIMAT.

En este laboratorio se trabajó con 2 servidores físicos Hp DL380 G7, a estos servidores se les instaló VMware ESXi versión 6.0 para a su vez instalar las máquinas virtuales necesarias y realizar las configuraciones, con esto se podrá recabar la evidencia solicitada.

Las máquinas virtuales instaladas y configuradas en los servidores físicos fueron 6 y se configuraron conforme al avance de las pruebas.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

6.3.4 Configuración de los servidores de Nombre Dominio.

6.3.4.1 Servidor de sistema de nombre de dominio (DNSv6) autoritativo master:

La transición se basa en los DNS, por lo cual se debe tener control de las zonas de autoridad y la recursividad del servicio, para el uso intensivo del DNS para todo. Por ello, se instaló una máquina virtual (MV) basada en Windows server estándar 2019, en esta MV se habilitó y configuró el servicio de DNSv6 maestro, se agregaron los registros A y AAAA para la zona principal cimat.mx y las zonas de resolución inversa para el ambiente de laboratorio, como este servidor es el master autoritativo se le deshabilita la función de recursividad.

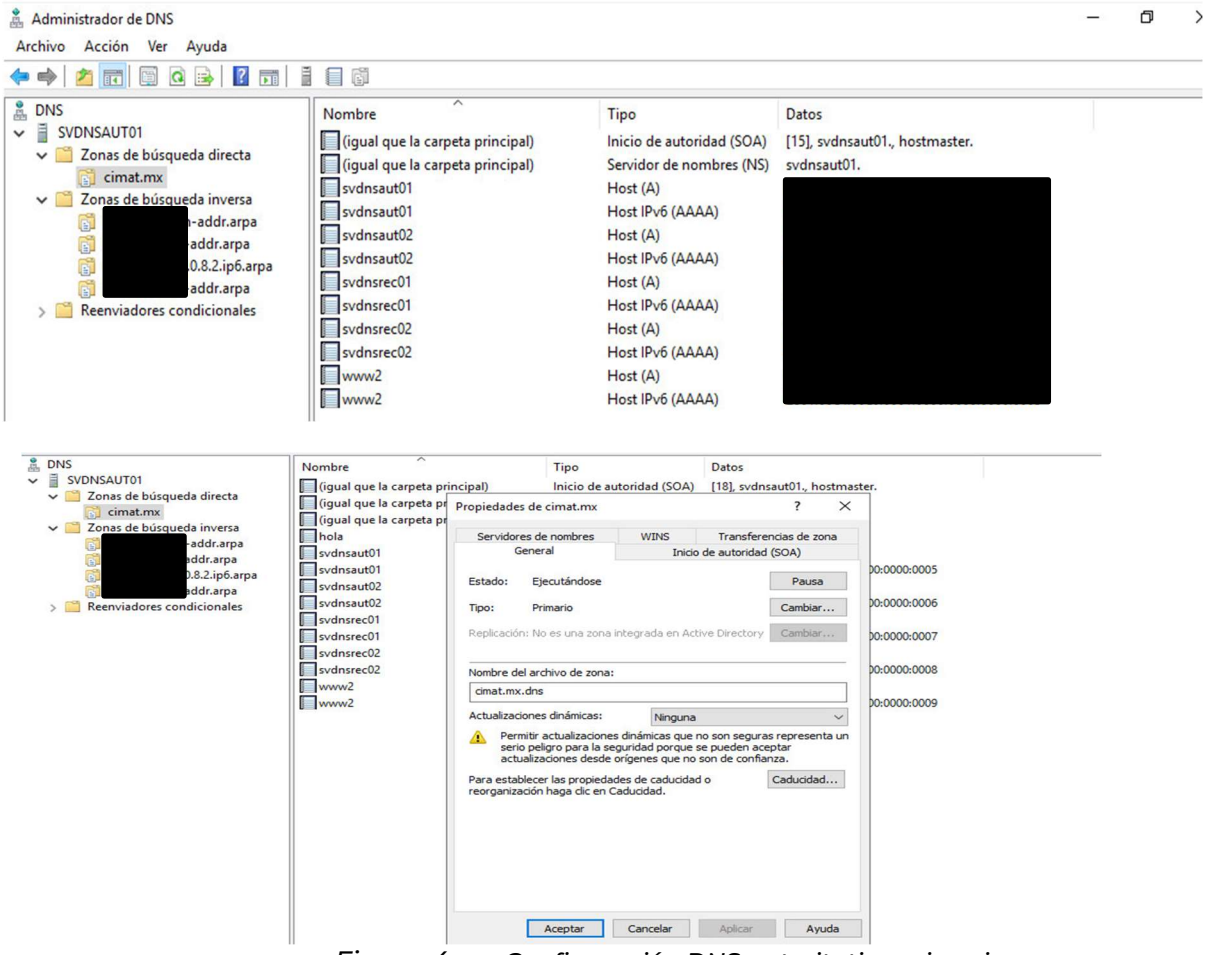


Figura 4 Configuración DNS autoritativo primario.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

6.3.4.2 Servidor de sistema de nombre de dominio (DNSv6) autoritativo esclavo:

De la misma manera se creó la máquina virtual (MV) y se le instaló un Windows server estándar 2019. En esta MV se habilitó y configuró el servicio de DNSv6 esclavo, el cual tendrá una copia de la base de datos del DNS autoritativo maestro tanto de su zona principal como de las zonas de resolución inversa.
Como este servidor es el esclavo autoritativo se le quita también la función de recursividad.

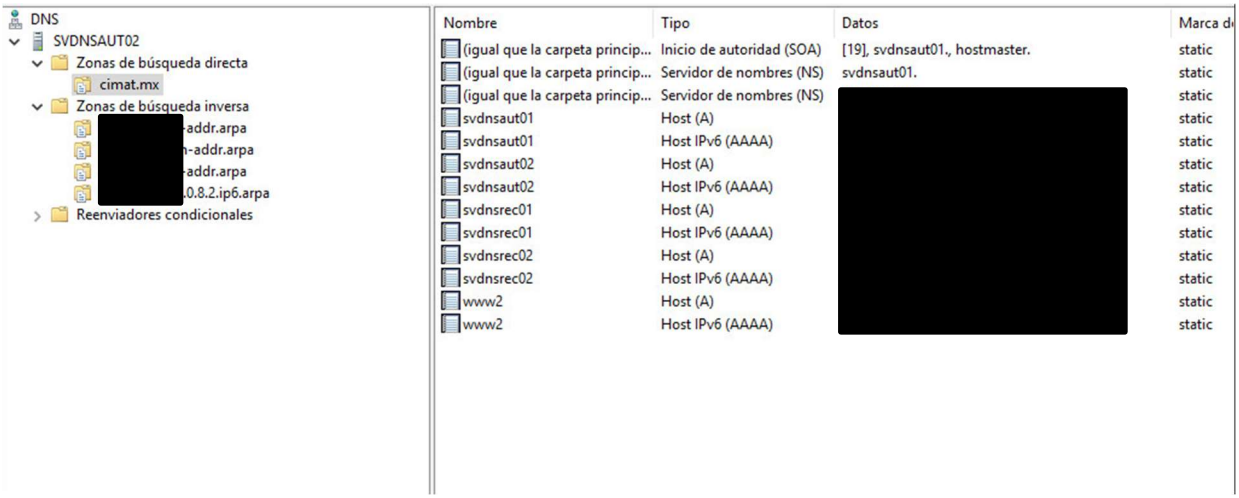


Figura 5 Registros de DNS autoritativo secundario.

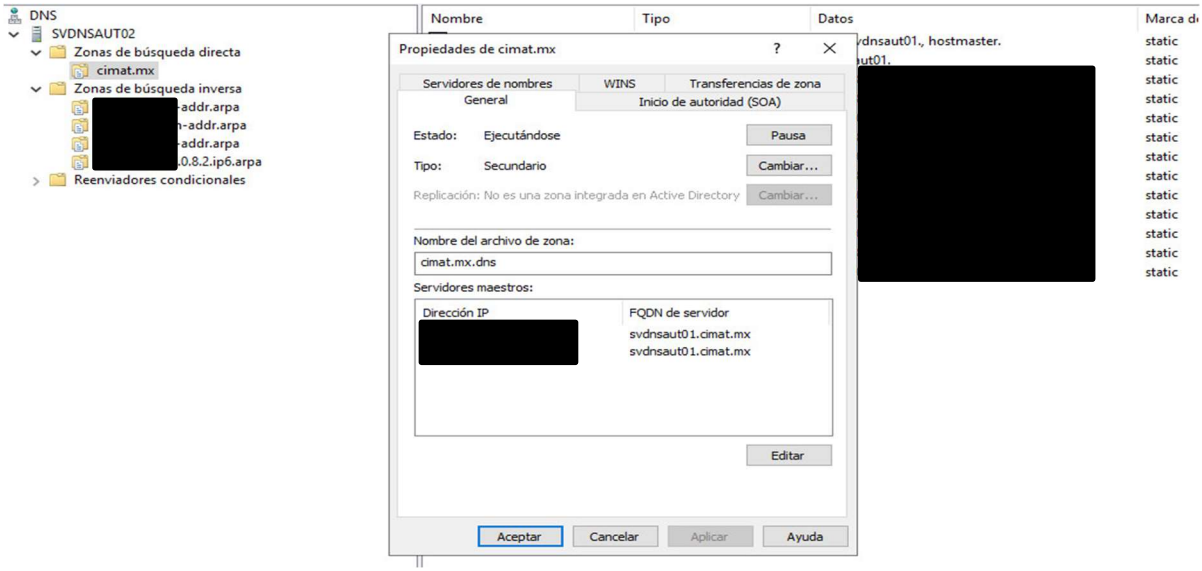


Figura 6 Configuración de DNS autoritativo secundario.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

6.3.4.3 Servidor de sistema de nombre de dominio (DNSv6) recursivo 01:

Los servidores DNS recursivos tienen un papel primordial de comunicación con otros servidores DNS autoridad para búsqueda de una dirección IP y devolverla al cliente. Esto se diferencia de una consulta de DNS iterativa, en la que el cliente se comunica directamente con cada servidor DNS implicado en la búsqueda. Aunque se trata de un proceso muy técnico, una mirada más cercana al sistema DNS y a la diferencia entre recursión e iteración debe ser la mejor práctica hacia la transición. Para ello, se creó una máquina virtual (MV) a la cual se instaló un Windows server estándar 2019. En esta MV a diferencia de los DNSv6 autoritativos solo se habilitó el servicio de DNS, este servidor no tendrá base de datos configurada, ni ninguna zona creada, es decir, este servidor servirá solo como DNSv6 de recursividad.

A este servidor se le habilita la recursividad puesto que esta será su principal funcionalidad, darles salida a los clientes finales de la red del Centro.
Este DNSv6 recursivo será uno de los que envíe nuestro firewall o Router a los usuarios finales para que puedan navegar en internet.

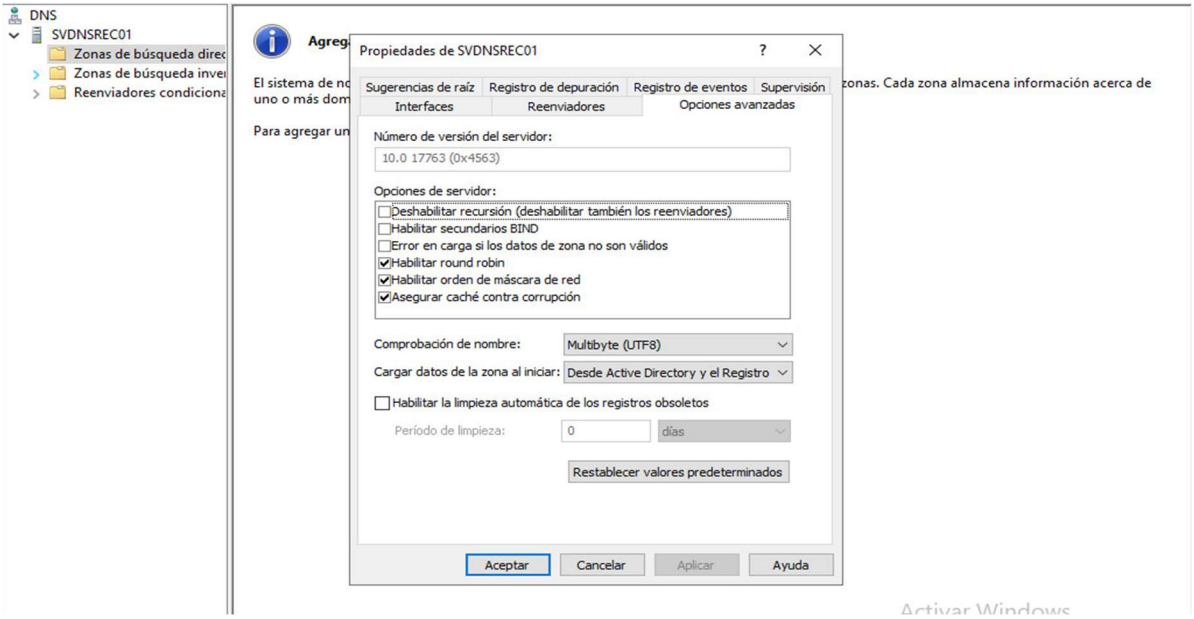


Figura 7 Configuración del DNS recursivo primario.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

6.3.4.4 Servidor de sistema de nombre de dominio (DNSv6) recursivo 02:

Para la redundancia y protección de los servicios de resolución de nombres se creó una máquina virtual (MV) y se le instaló de igual manera otro Windows server estándar 2019, está MV será la segunda con el servicio recursividad la cual será enviada a nuestros usuarios finales mediante nuestro firewall o Router.
A este servidor se le habilita la recursividad puesto que esta será su principal funcionalidad dar salida a los equipos finales de nuestra red.

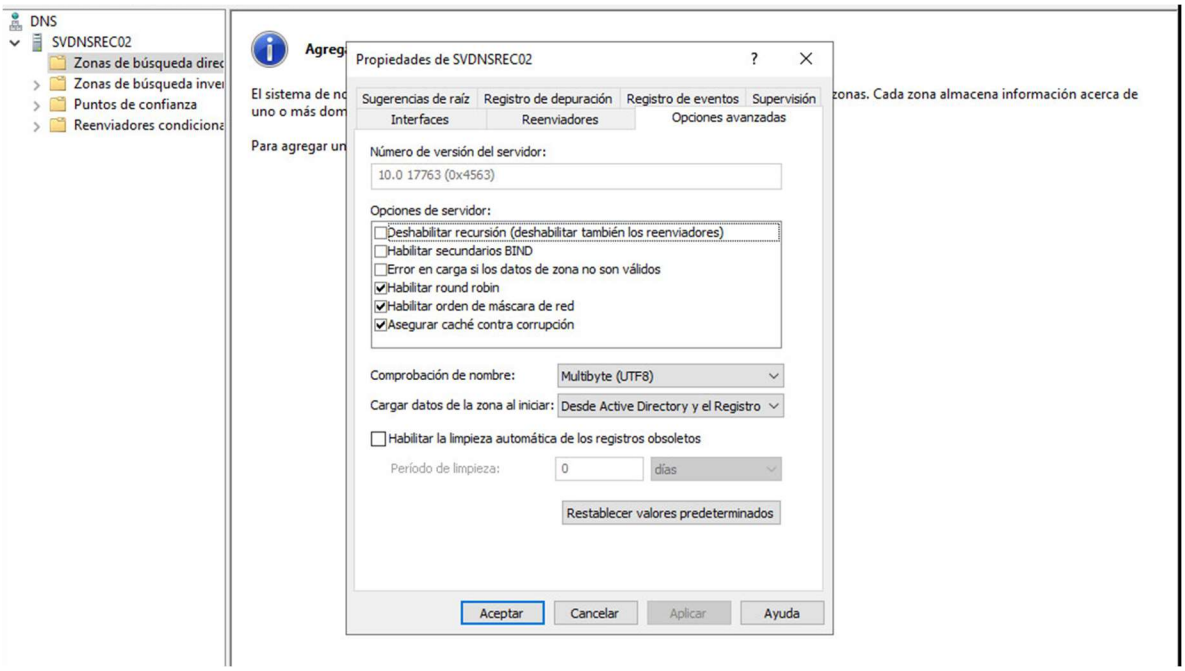


Figura 8 Configuración del DNS recursivo secundario.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

6.3.4.5 Servidor de página web:

Se creó la máquina virtual (MV) y se le instaló un Linux server CentOS versión 8.7, en esta máquina virtual se cargó una de las páginas web que están en producción en CIMAT, a continuación, se muestra la página “BUC” mediante un navegador de internet en el protocolo IPV4 e IPV6, esta página es la que se usará para ejemplificar que ya se está publicando por ambos protocolos.

Protocolo IPv4.

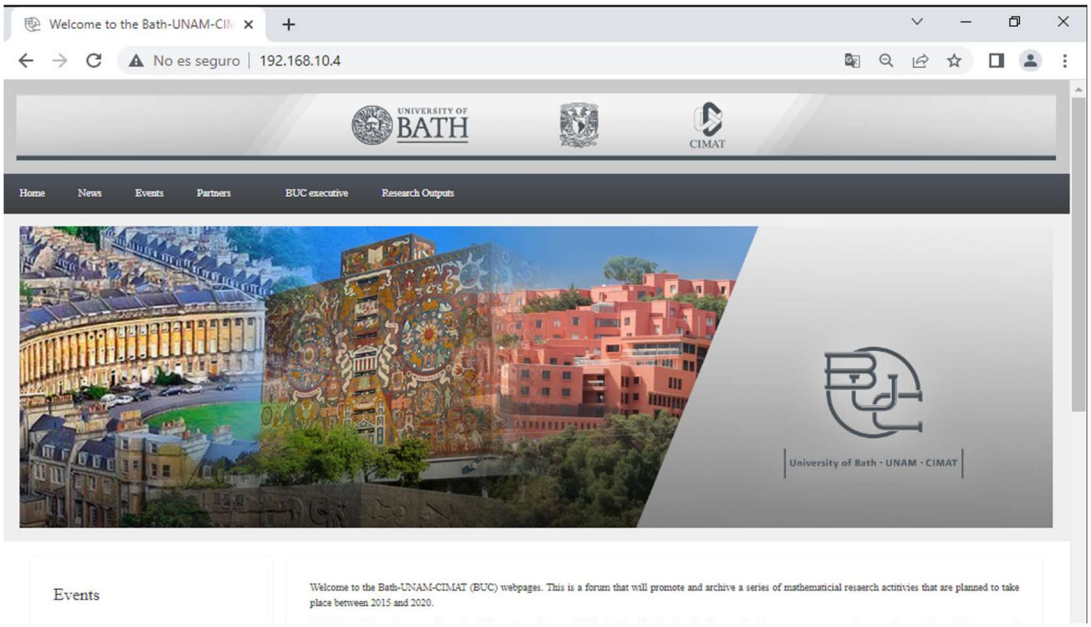


Figura 9 Página de prueba en IPv4.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

Protocolo IPv6.

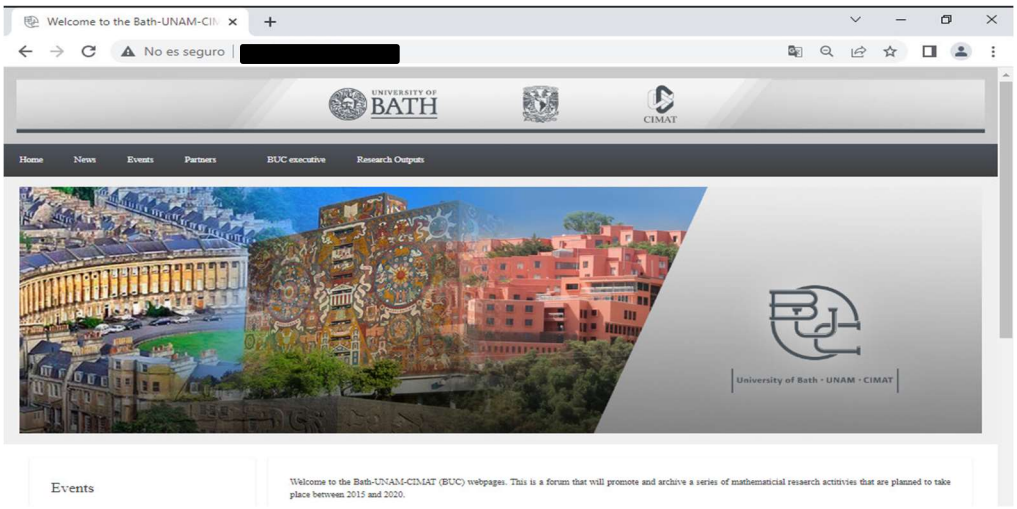


Figura 10 Página de prueba en IPv6.

6.3.5 Configuración del Firewall perimetral.

Después de realizar la instalación de pfSense, se establece el direccionamiento que se utilizó en las interfaces de red WAN y LAN.

Para la interfaz WAN se utilizaron las direcciones IP:

IPv4 (DHCP): [redacted]
Gateway IPv4: [redacted]

Este direccionamiento es temporal debido a que está pendiente habilitar el direccionamiento IPv4 público en el Router y se utilizó un enlace del proveedor Telmex (Infinitum)

IPv6: **2801:**[redacted]
Ruta por defecto IPv6, ::/0 con siguiente brinco a **2801:**[redacted]

Y para la interfaz LAN:

IPv4: [redacted]

Gateway IPv6: 2801:[redacted]

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

6.3.5.1 Asignación de servidores DNS públicos y nombre para pfSense.

Se asignaron servidores de DNS recursivos públicos como parte de la configuración inicial de pfSense, se asignaron los siguientes servidores:

DNS1: 8.8.8.8
DNS2: 9.9.9.9

También se asignó un nombre de equipo para este Firewall de prueba: fwprueba01

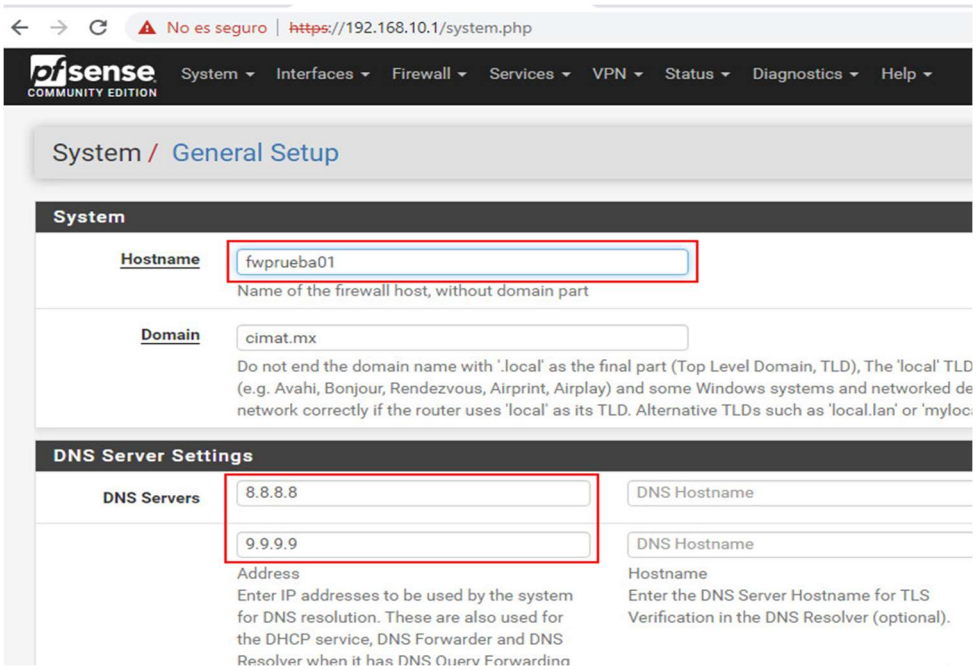


Figura 11 Asignación de servidores DNS y nombre al firewall.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

6.3.5.2 Configuración del servicio RA (Router Advertisements) en el Firewall.

Esto se realiza para que el Firewall propague en la red local, a través de ICMPv6, la información sobre el Router por defecto y los servidores de DNSv6 recursivos a los equipos clientes finales.

En el menú de Servicios, seleccionar la opción (DHCPv6 Server & RA) y en la pestaña correspondiente a la red local (LAN) seleccionar Router Advertisements.

Se configuran los siguientes valores:

Router mode: Stateless DHCP - RA Flags [other statefull], Prefix Flags [onllink, auto, router]
Router priority: Normal
Subnets: **2801:**[redacted]
DNS1: **2801:**[redacted]
DNS2: **2801:**[redacted]

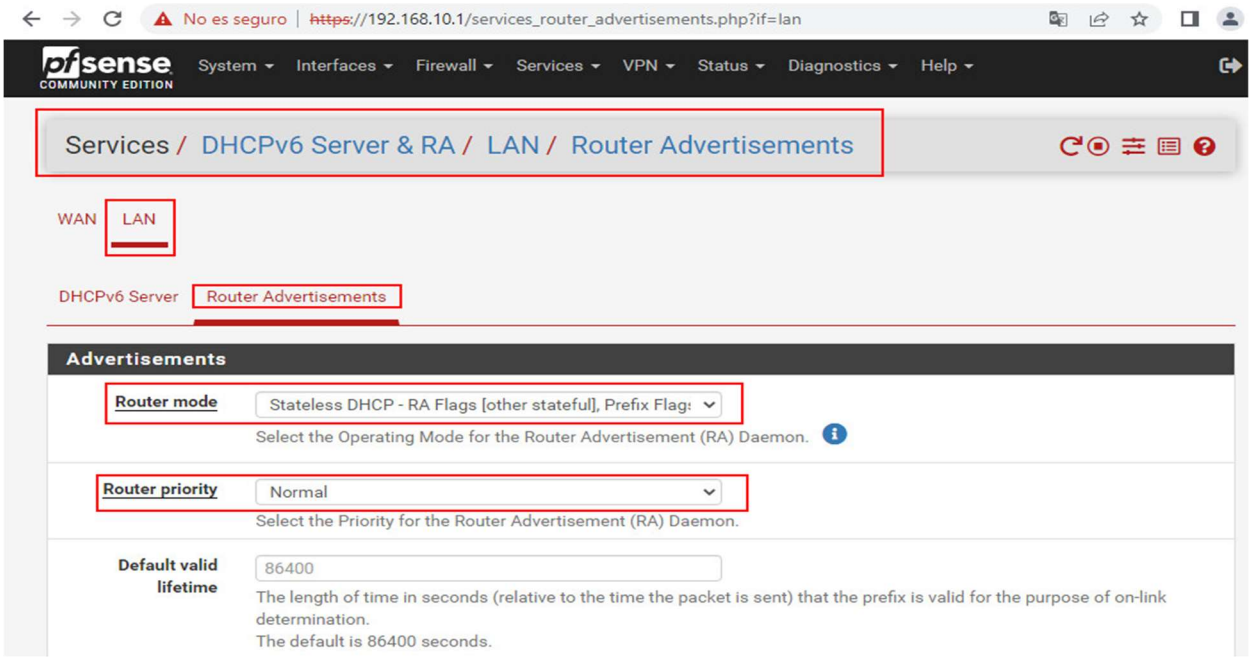


Figura 12 Activación de Router Advertisement.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

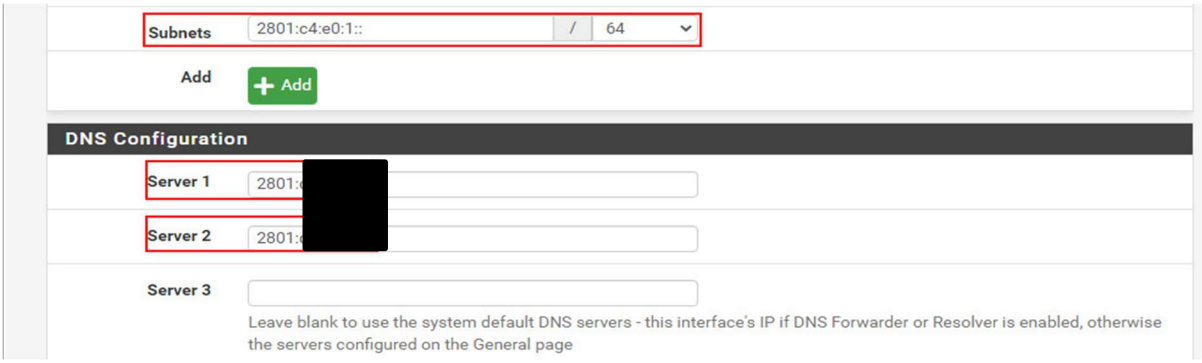


Figura 13 Configuración de DNS's IPv6 en el firewall.

6.3.5.3 Configuración de reglas en el Firewall.

En la sección de reglas de la red local, se agregaron las siguientes:

1. Regla por default de pfSense.
2. Permitir todo el tráfico ICMPv6 necesario para el correcto funcionamiento del protocolo IPv6.
3. Permitir el tráfico desde internet al servidor de prueba de la página web por el puerto TCP/80.
4. Permitir todo el tráfico en la red local (con fines de pruebas únicamente).
5. Bloquear todo el tráfico IPv6 desde internet hacia la red local.

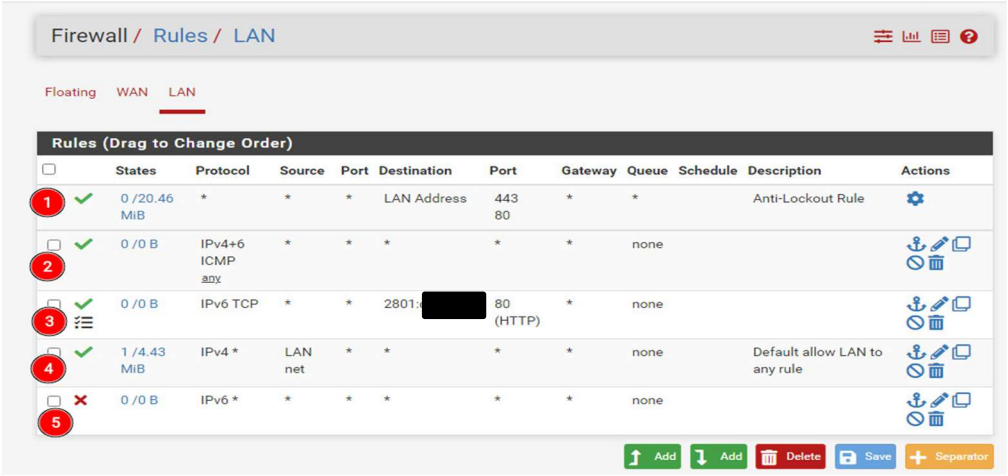


Figura 14 Sección de reglas para la interface LAN (IPv4-IPv6).

Al finalizar la configuración del firewall se realizaron pruebas de la propagación de IPv6 en los equipos de la red local:

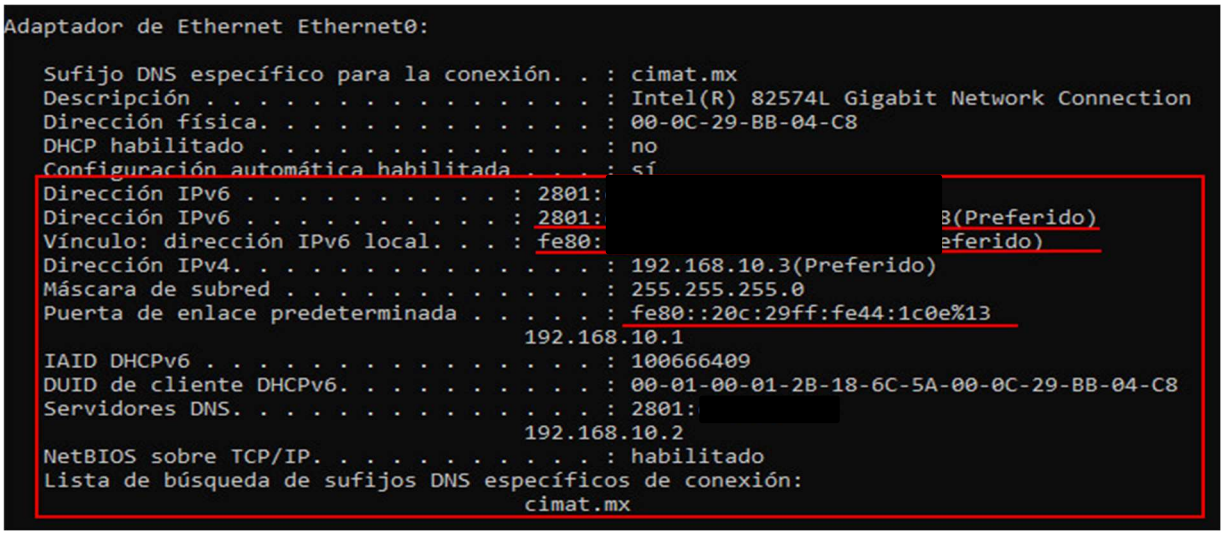


Figura 15 Prueba de la propagación de IPv6 en los equipos de la red local.

6.3.6 Propagación del direccionamiento IPv6 al exterior a través del ISP.

Se solicitó al ISP con el que el CIMAT tiene contratado el servidor de internet que nos apoyara para la propagación y diera salida al equipo de CIMAT a la red de Internet externa. El contrato se tiene con el proveedor B-DRIVE.

6.3.6.1 Configuración de ruteo IPv6.

Como parte del proceso de migración para operar en el esquema IPv6 en Dual-Stack en conjunto con IPv4, se configuró el Router o ASR que tenemos en el CIMAT. Se procedió a configurar la parte de los segmentos que se habían obtenido previamente, para que el proveedor de internet que en este caso es la empresa B-Drive S. A. de C. V. nos apoyara con las configuraciones en sus equipos permitiendo el anuncio de los segmentos antes mencionados hacia la nube de Internet.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

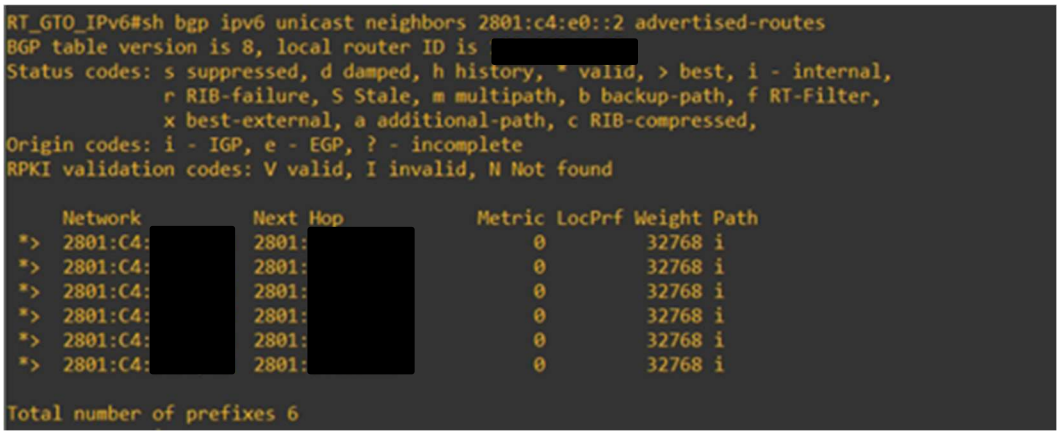


Figura 16 *Segmentos IPv6 anunciados desde el ASR.*

En la imagen se muestra la configuración de los segmentos anunciados desde el Router ASR para que sean vistos por el equipo del proveedor. Se puede observar que se anuncian los segmentos en un tamaño de prefijo /48 el cual es el tamaño mínimo para que sean publicados a través del protocolo BGP y sean publicados en Internet.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

En el diagrama se pueden mostrar los requerimientos que se le solicitaron al proveedor para que el segmento IPv6 en conjunto con el IPv4 quedarán funcionando en un esquema de Dual Stack en el que tanto IPv4 como IPv6 puedan ser anunciados usando el Sistema Autónomo adquirido por el CIMAT mediante el protocolo BGP.

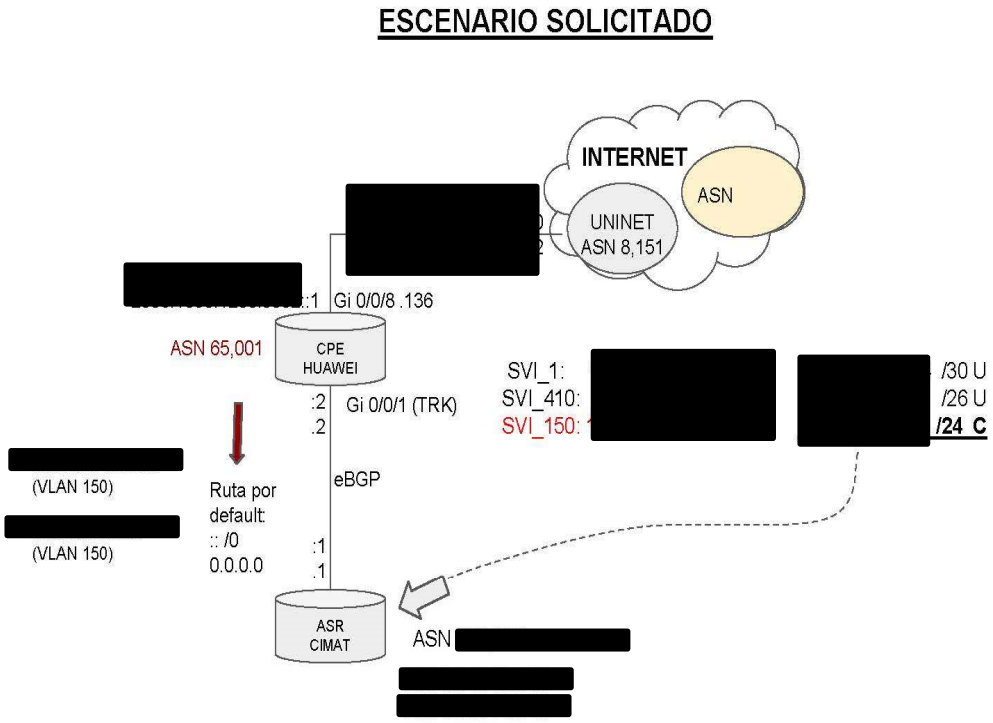


Figura 17 *Diagrama de conexión hacia la WAN de Telmex.*

A continuación, se muestra la configuración del equipo del proveedor para hacer el anuncio de los segmentos IPv6 en tamaños de prefijo /48.

```
<CMAT>displ BGP ipv6 PEER
 Status codes: * - Dynamic
BGP local router ID : 187.237.137.85
Local AS number : 65001
Total number of peers : 2          Peers in established state : 2
Total number of dynamic peers : 0
 Peer        V       AS  MsgRcvd  MsgSent  OutQ  Up/Down      State PrefRcv
 2801[redacted]  4  8023    1304     1184     0 19:41:15 Established     6
 2806:[redacted]
          4     8151    2571     2581     0 0042h32m Established     1
<CMAT>
<CMAT>displ ipv6 routing-table | inc C4
Routing Table : Public
     Destinations : 13      Routes : 13

Destination :[redacted]  PrefixLength : 46
NextHop     :            Preference   : 255
Destination :            PrefixLength : 48
NextHop     :            Preference   : 255
Destination :            PrefixLength : 126
NextHop     :            Preference   : 0
Destination :            PrefixLength : 128
Destination :            PrefixLength : 48
NextHop     :            Preference   : 255
Destination :            PrefixLength : 48
NextHop     :            Preference   : 255
Destination :            PrefixLength : 48
NextHop     :            Preference   : 255
Destination :            PrefixLength : 48
NextHop     :            Preference   : 255
<CMAT>
```

Figura 18 *Configuración de ruteo para el anuncio de segmentos en Router del ISP.*

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

7. RESULTADOS

Dentro de las pruebas realizadas posteriores a las configuraciones hechas en ambos equipos (ASR 1002-X y Router Huawei del proveedor) se procedió a llevar a cabo las pruebas de conexión desde el Router ASR hacia Internet usando ping al DNS IPv6 de Google y por medio de la página Hurricane Electric, que permite visualizar los segmentos de red publicados por el Router del proveedor.

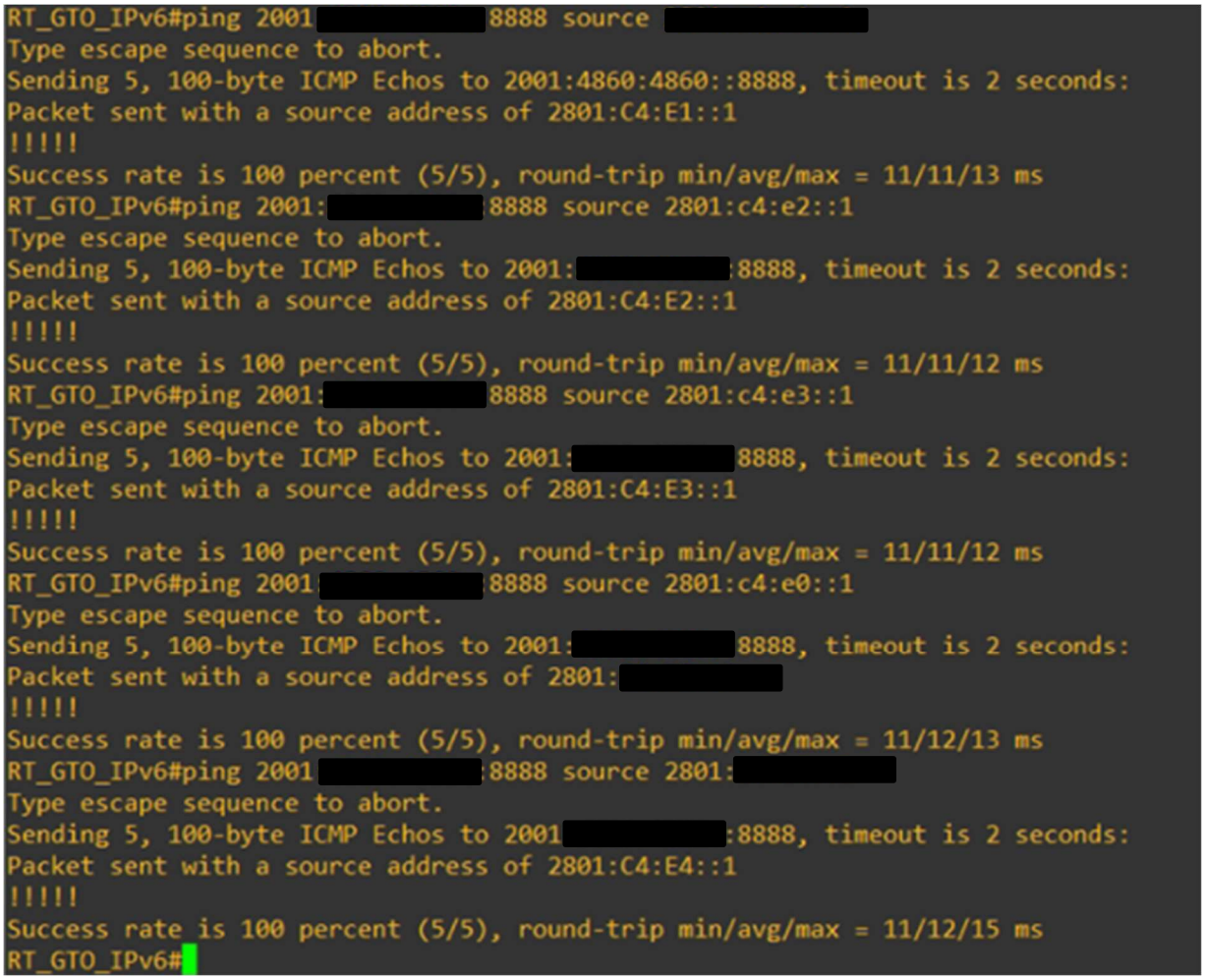


Figura 19 Ping del Router ASR a Google.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

Por otro lado, revisando desde la página Hurricane Electric, se obtuvieron las siguientes capturas:

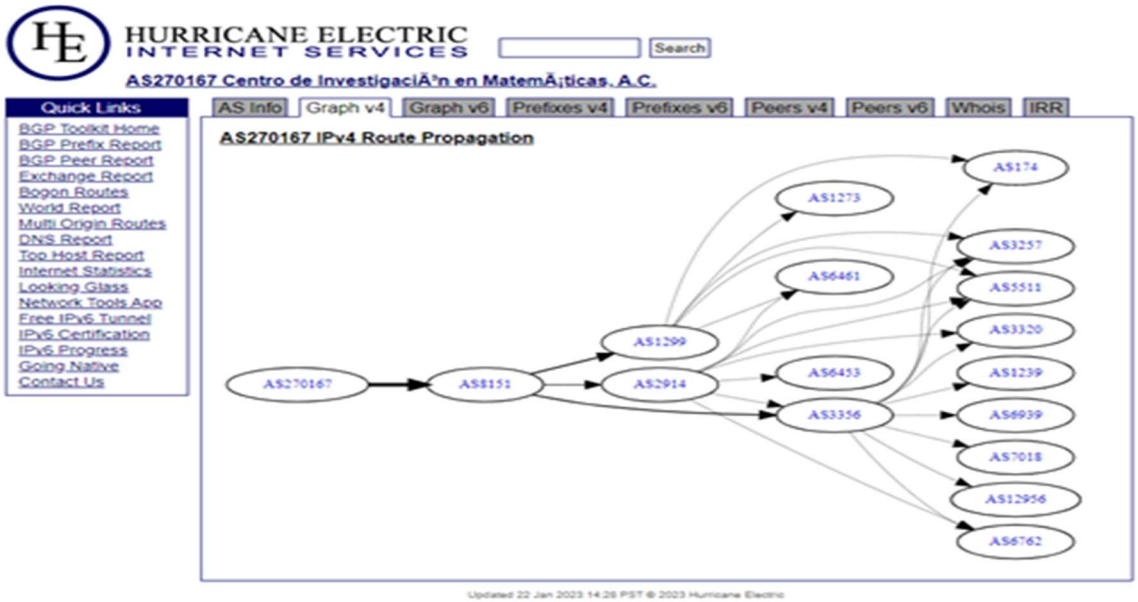


Figura 20 *Secuencia de conexión del sistema autónomo en IPv4.*

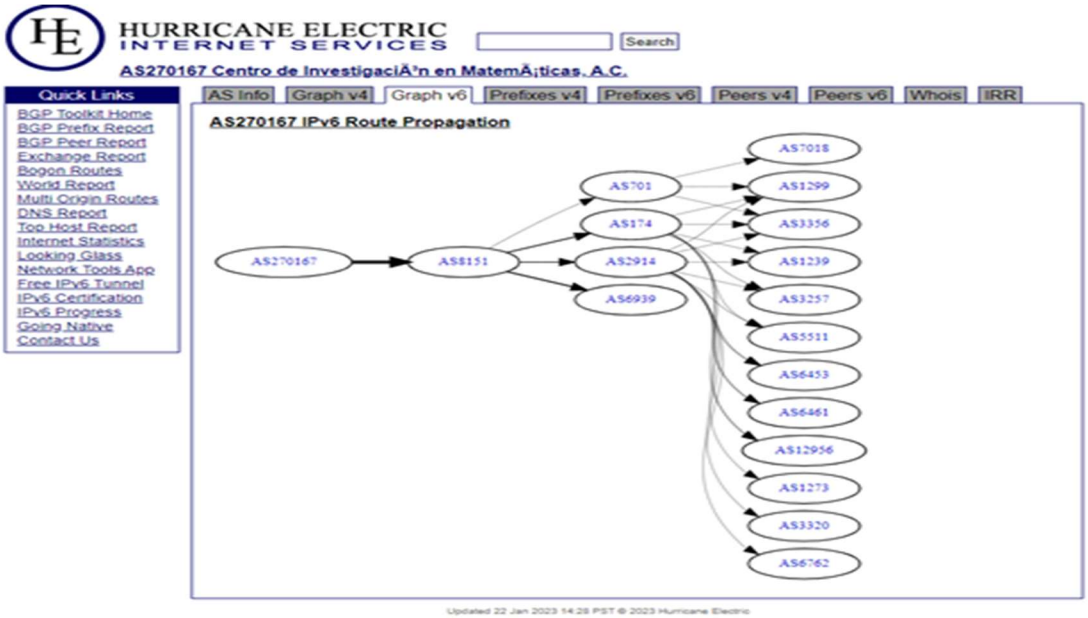


Figura 21 *Secuencia de conexión del sistema autónomo en IPv6.*

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

Figura 22 Información del registro para el Sistema Autónomo contratado por CIMAT.

7.1.1 Segmentación de del direccionamiento público por el ISP.

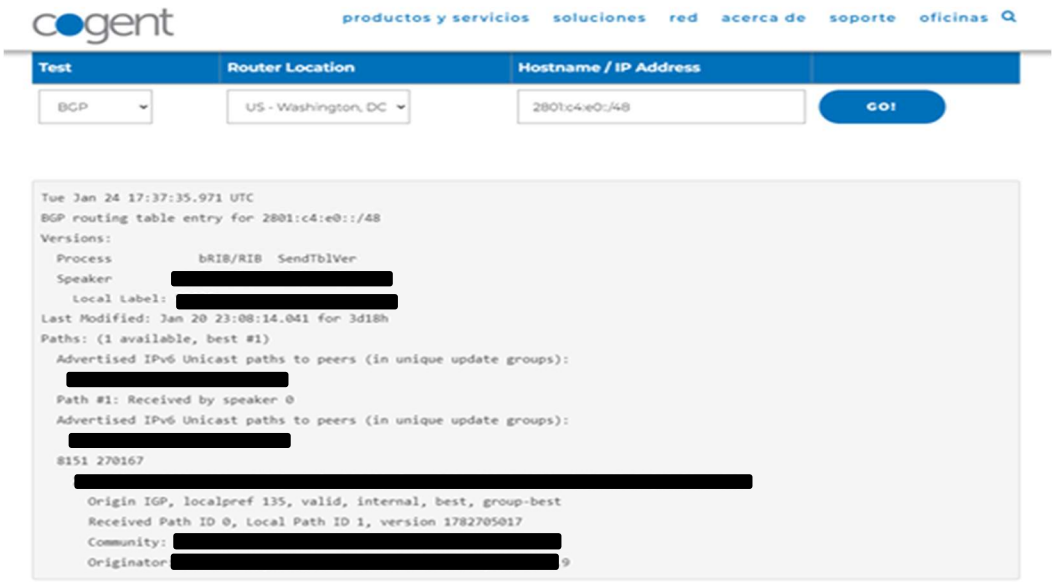


*Figura 23 Tabla de BGP para el segmento **2801:C4:***

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

Figura 24 *Tabla de ruteo BGP para el segmento* ***2801:***[redacted]

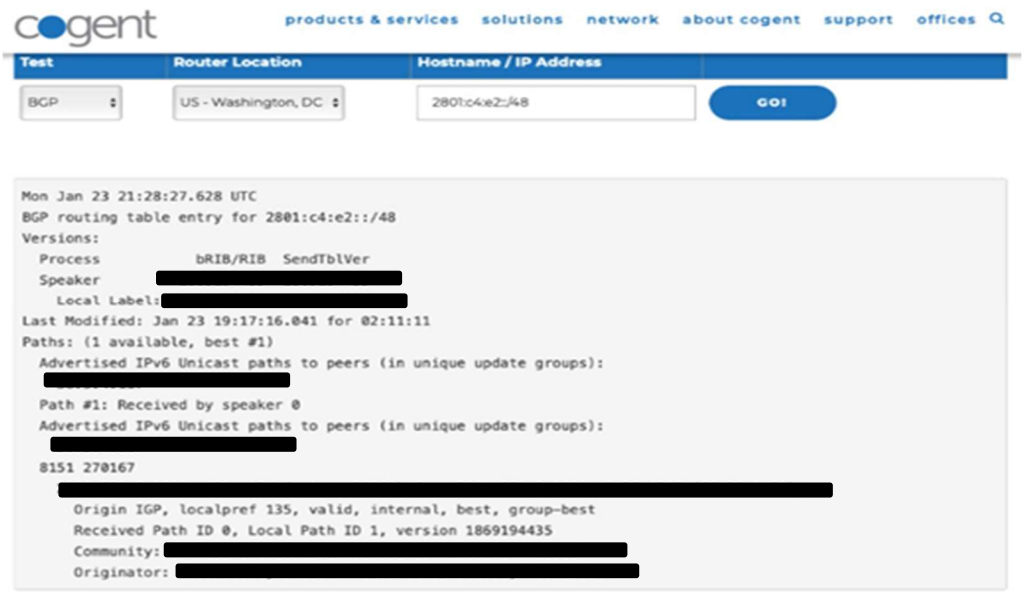


Figura 25 *Tabla de ruteo BGP para el segmento* ***2801:***[redacted]

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

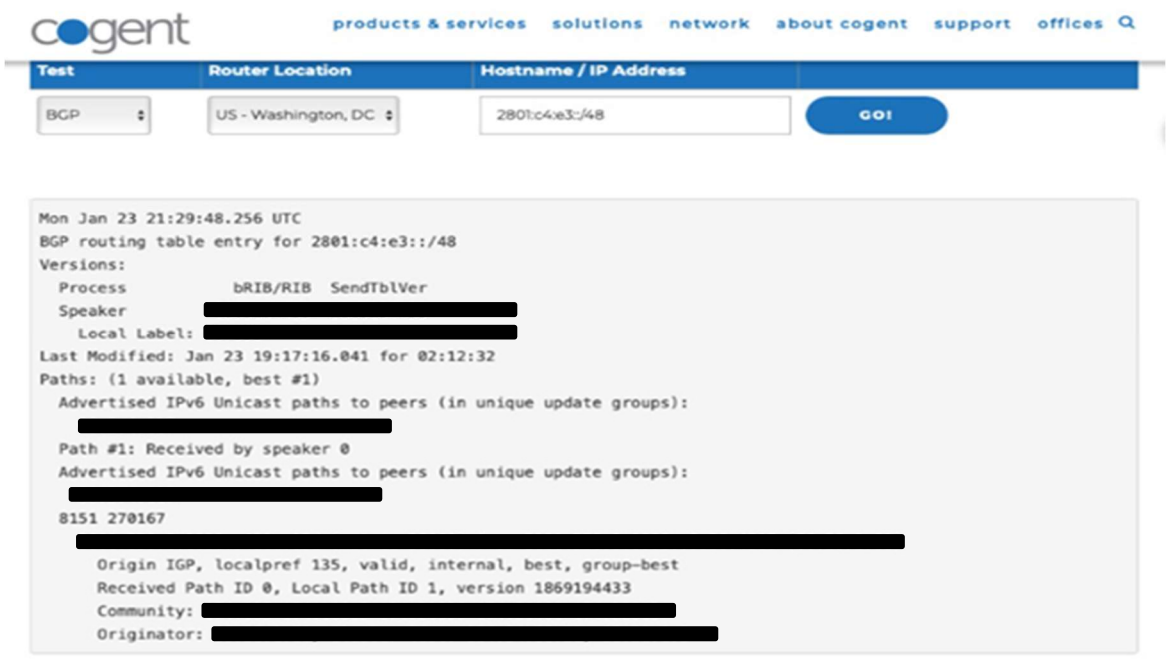


Figura 26 *Tabla de ruteo BGP para el segmento* ***2801:[redacted]***

Figura 27 *Tabla de ruteo BGP para el segmento* ***2801:[redacted]***

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

7.1.1.1 Pruebas de Ruteo por BGP

En las imágenes siguientes se muestra la ruta por la que sale cada segmento, así como la métrica, el peso, los sistemas autónomos para llegar al segmento y el protocolo de ruteo IGP.

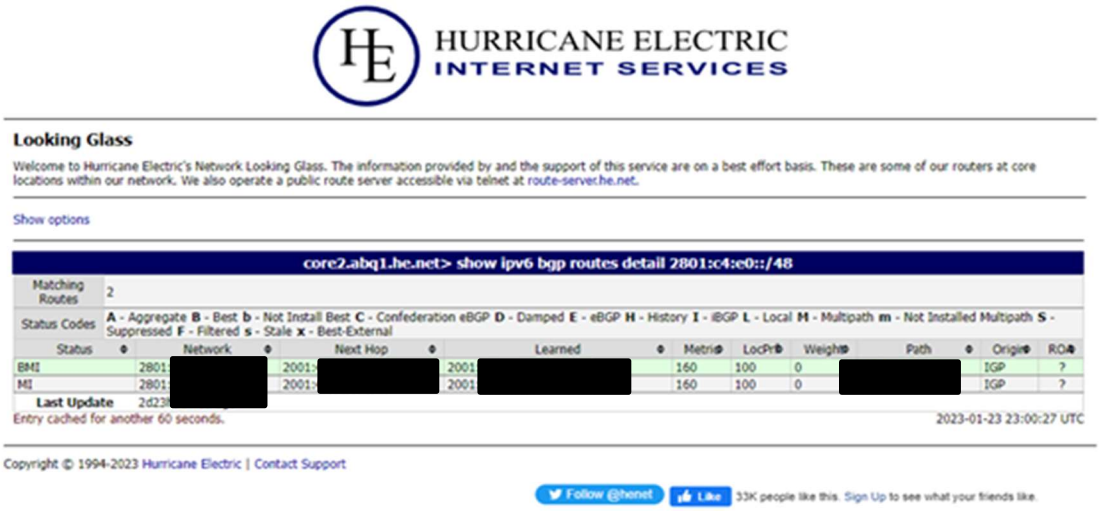


Figura 28 Evidencia de ruteo del segmento 2801:

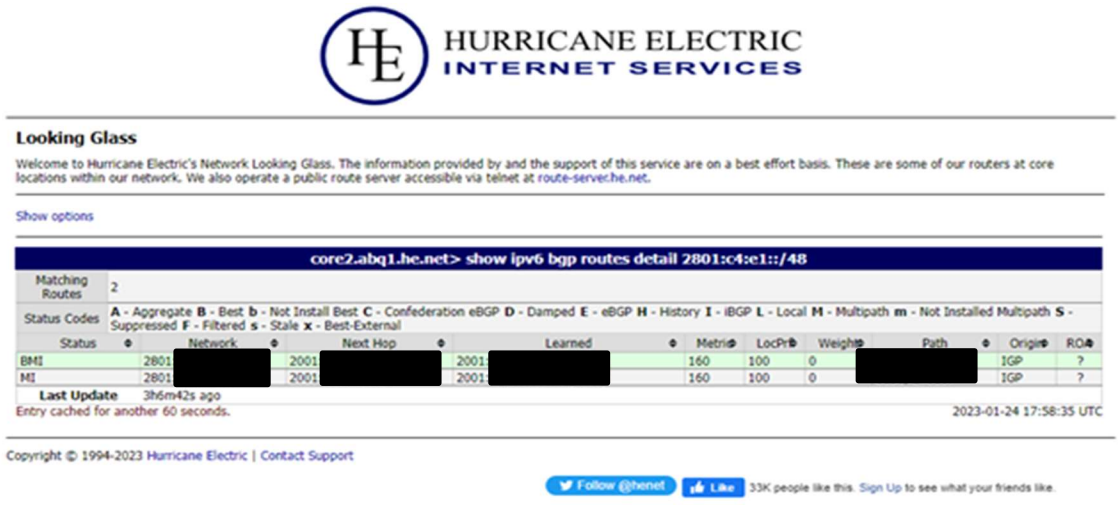
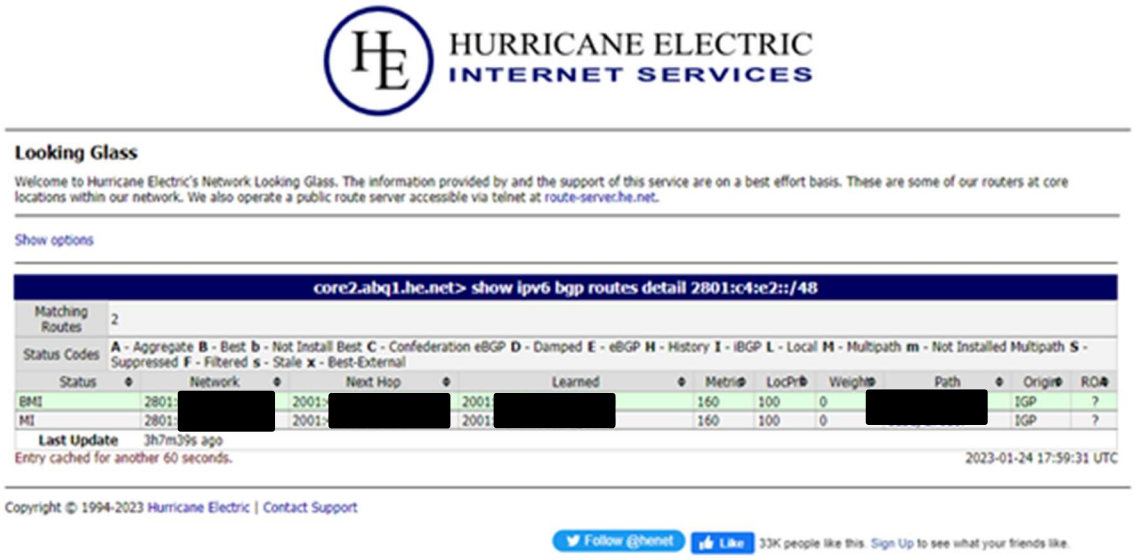


Figura 29 Evidencia de ruteo del segmento 2801:


HURRICANE ELECTRIC INTERNET SERVICES

Looking Glass

Welcome to Hurricane Electric's Network Looking Glass. The information provided by and the support of this service are on a best effort basis. These are some of our routers at core locations within our network. We also operate a public route server accessible via telnet at route-server.he.net.

Show options

core2.abq1.he.net> show ipv6 bgp routes detail 2801:c4:e2::/48

Matching Routes	2
Status Codes	A - Aggregate B - Best b - Not Install Best C - Confederation eBGP D - Damped E - eBGP H - History I - iBGP L - Local M - Multipath m - Not Installed Multipath S - Suppressed F - Filtered s - Stale x - Best-External

Status	Network	Next Hop	Learned	Metric	LocPrf	Weight	Path	Origin	ROA
BMI	2801:[redacted]	2001:[redacted]	2001:[redacted]	160	100	0	[redacted]	IGP	?
MI	2801:[redacted]	2001:[redacted]	2001:[redacted]	160	100	0	[redacted]	IGP	?

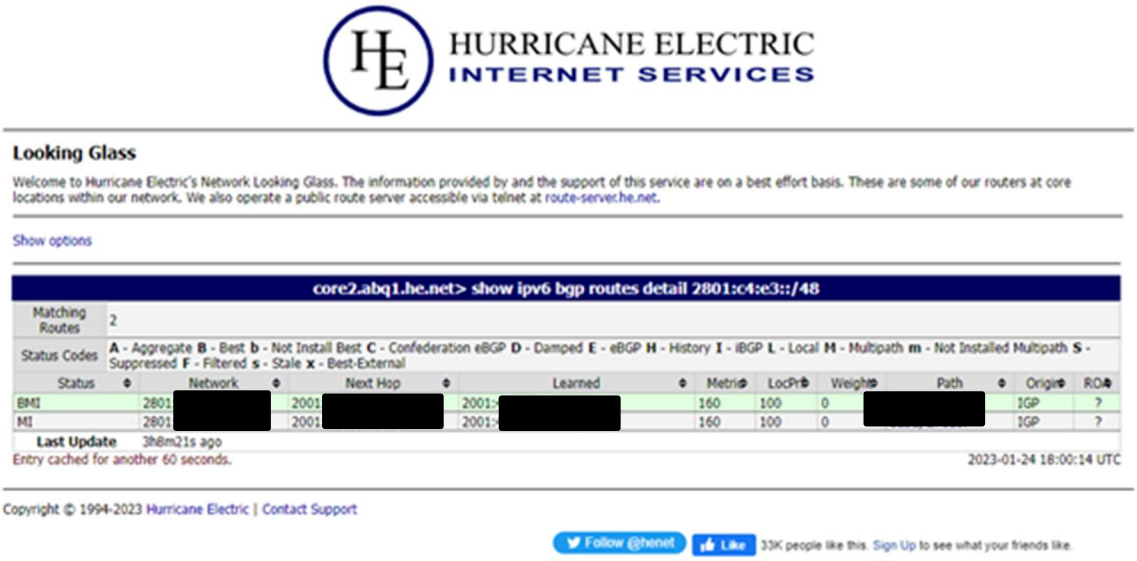
Last Update 3h7m39s ago

Entry cached for another 60 seconds. 2023-01-24 17:59:31 UTC

Copyright © 1994-2023 Hurricane Electric | Contact Support

Follow @henet Like 33K people like this. Sign Up to see what your friends like.

Figura 30 *Evidencia de ruteo del segmento 2801:[redacted].*


HURRICANE ELECTRIC INTERNET SERVICES

Looking Glass

Welcome to Hurricane Electric's Network Looking Glass. The information provided by and the support of this service are on a best effort basis. These are some of our routers at core locations within our network. We also operate a public route server accessible via telnet at route-server.he.net.

Show options

core2.abq1.he.net> show ipv6 bgp routes detail 2801:c4:e3::/48

Matching Routes	2
Status Codes	A - Aggregate B - Best b - Not Install Best C - Confederation eBGP D - Damped E - eBGP H - History I - iBGP L - Local M - Multipath m - Not Installed Multipath S - Suppressed F - Filtered s - Stale x - Best-External

Status	Network	Next Hop	Learned	Metric	LocPrf	Weight	Path	Origin	ROA
BMI	2801[redacted]	2001[redacted]	2001:[redacted]	160	100	0	[redacted]	IGP	?
MI	2801[redacted]	2001[redacted]	2001:[redacted]	160	100	0	[redacted]	IGP	?

Last Update 3h8m21s ago

Entry cached for another 60 seconds. 2023-01-24 18:00:14 UTC

Copyright © 1994-2023 Hurricane Electric | Contact Support

Follow @henet Like 33K people like this. Sign Up to see what your friends like.

Figura 31 *Evidencia de ruteo del segmento 2801:[redacted]*

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

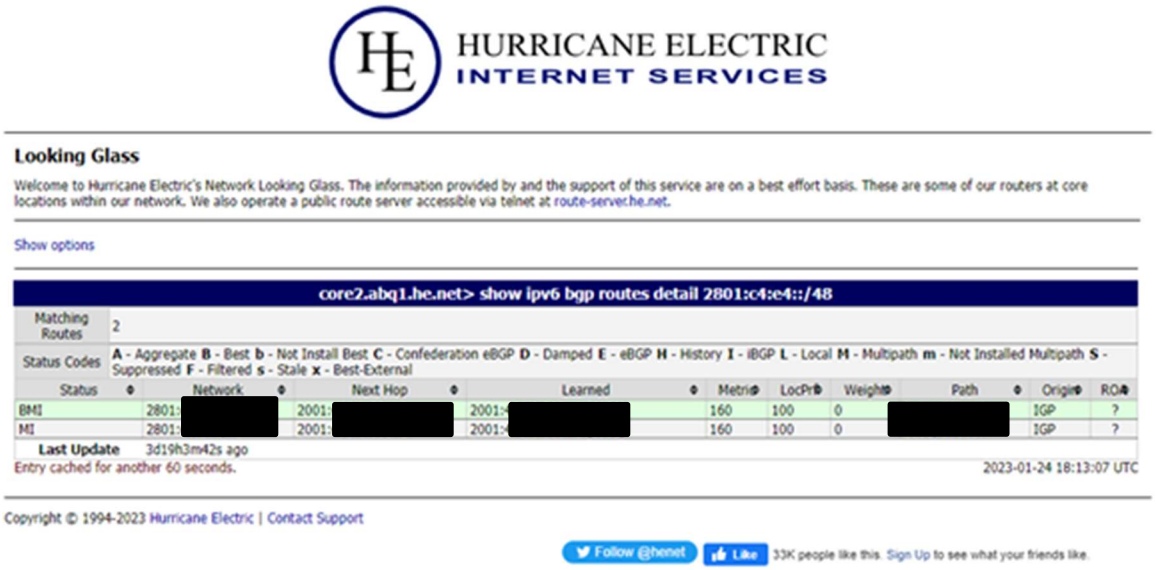


Figura 32 *Evidencia del ruteo del segmento 2801:*[redacted]

El conjunto de imágenes anteriores, se usaron a recomendación del consultor a manera de validar que los segmentos configurados en nuestros equipos de pruebas, fueran visibles desde internet usando estos sitios.

http://he.net/

https://www.cogentco.com/es/

https://www.manrs.org/netops/participants/

https://stats.labs.apnic.net/ipv6/MX

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

7.1.1.2 Pruebas de autoconfiguración de IPv6 con equipos terminales.

Además de las pruebas realizadas desde los servidores. Se realizaron algunas otras pruebas hacia los equipos LAN por medio de la autoconfiguración con el EUI-64.

- Equipo de videoconferencias GRANDSTREAM GVC3212.

Figura 33 Evidencia de autoconfiguración en equipo de videoconferencia.

En la imagen se puede observar que un equipo de Videoconferencia obtuvo la IP una vez que alcanzo al ASR para la autoconfiguración de su IP global.

- Impresora HP LaserJet Pro MFP M521dn.

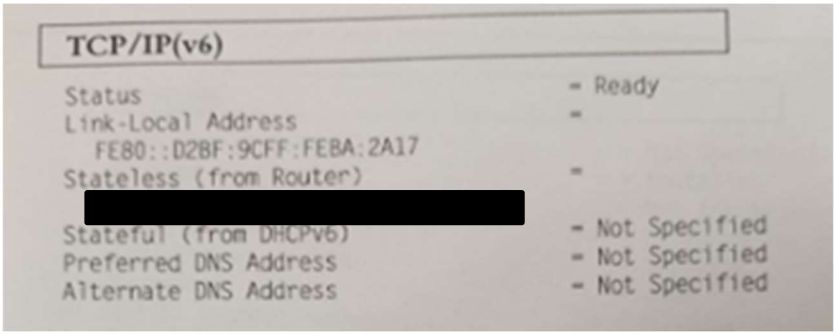


Figura 34 Evidencia de autoconfiguración de impresora Hp

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

- Equipo portátil con sistema operativo Ubuntu 22.04

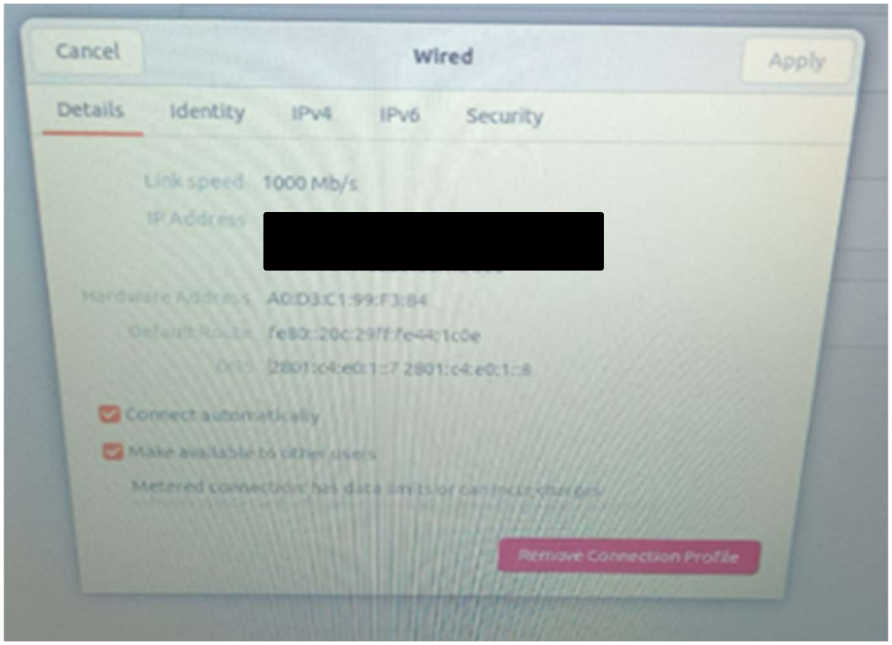


Figura 35 *Evidencia de autoconfiguración en laptops con S.O Ubuntu.*

- Equipo de escritorio con Linux

```
[root@centos network-scripts]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:BA:8C:15
          inet6 addr: 2801:                                 Scope:Global
          inet6 addr: fe80::20c:29ff:feba:8c15/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5211 (5.0 KiB)  TX bytes:2280 (2.2 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:264 (264.0 b)  TX bytes:264 (264.0 b)
```

Figura 36 *Evidencia de autoconfiguración en servidores con Linux.*

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

7.1.2 Firewall perimetral

7.1.2.1 Cambios en la configuración y reglas del Firewall

Se realizaron los ajustes necesarios por parte del ISP (Proveedor de Internet) para que el laboratorio cuente con salida a Internet mediante un Router propio y utilizando direccionamiento IPv6.

7.1.2.2 Pruebas de conexión a internet desde equipos en la red LAN

En este punto ya se logró hacer pruebas reales de conectividad a internet y se realizaron los siguientes cambios:

- Deshabilitar la regla No. 5 que se encontraba activa en la interfaz LAN. Esta regla estaba bloqueando todo el tráfico IPv6 excepto el protocolo ICMP.

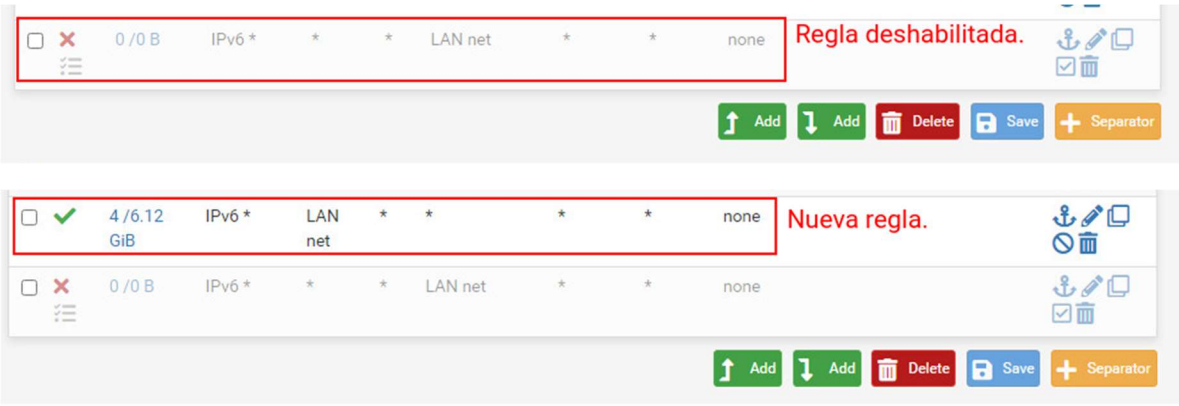


Figura 37 Regla que permite el tráfico IPv6 en la interfaz LAN.

Al realizar estos cambios, los equipos conectados a la red LAN ya lograron salir a Internet mediante el protocolo IPv6.

Nota:

Al realizar pruebas de velocidad a internet, se detectó un problema de velocidad, el enlace tiene una capacidad de 500 Mbps, pero en las pruebas únicamente se alcanzaba la cantidad de 20 Mbps en promedio.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

Figura 38 *Prueba de velocidad con resultados no esperados.*

Se consultó el problema con el asesor de IPv6 y se determinó que al no contar con una salida a internet mediante IPv4 se debe quitar temporalmente los Gateway de IPv4 en los equipos conectados en la red LAN. Al hacer este cambio se mejoró considerablemente la conexión:

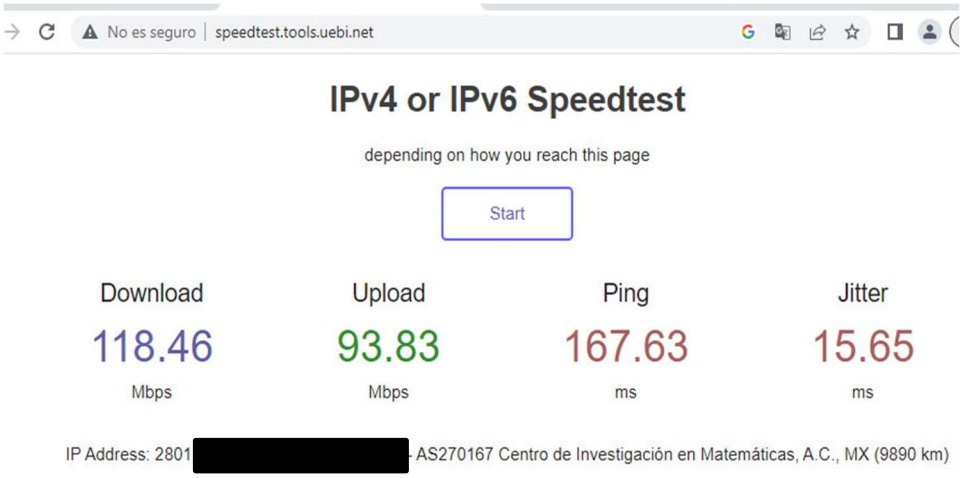


Figura 39 *Prueba de velocidad después de cambio en configuración.*

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

No se obtiene la totalidad de la capacidad del enlace ya que se está utilizando en el ambiente de producción y depende del consumo de ancho de banda por parte de los usuarios.
Adicionalmente se realizó un cambio de servidores DNS utilizados por el Firewall, anteriormente se tenían DNS en IPv4 así que se cambiaron por los DNS públicos de Google en IPV6:

Figura 40 DNS´s de Google en IPv6 utilizados por el FW.

7.1.2.3 Pruebas de publicación de servicios internos hacia el exterior.

Otra de las pruebas realizadas es validar que un servicio interno sea accesible desde Internet. Se cuenta con un servidor de prueba con una página Web con la dirección IPv6: 2801:c4:e0:1::9 en el puerto 80/TCP.

Anteriormente se había creado la regla que permite el tráfico entrante a este servidor en la interfaz LAN, pero no funcionó de esta manera. Para realizar la publicación de servicios internos es necesario crear la regla en la interfaz WAN o en la interfaz que cuente con la conexión del enlace de Internet.

Regla anterior deshabilitada:

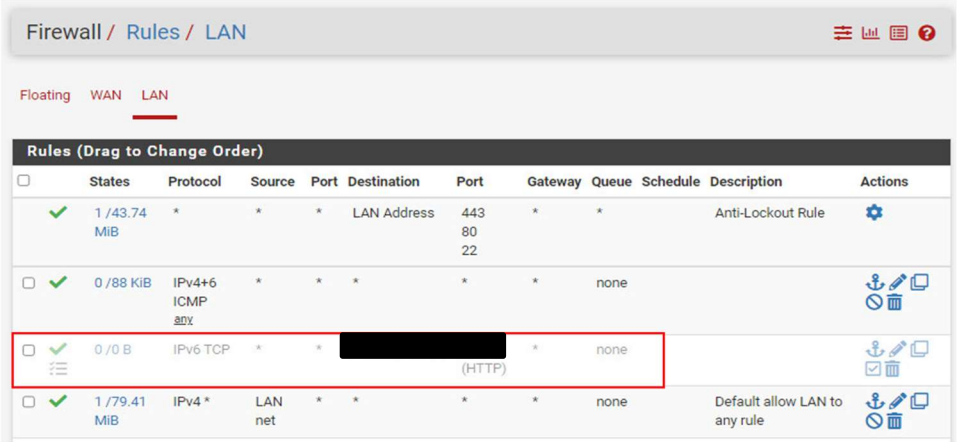


Figura 41 Regla deshabilitada por cambio de interfaz.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

Regla creada en la interface WAN:

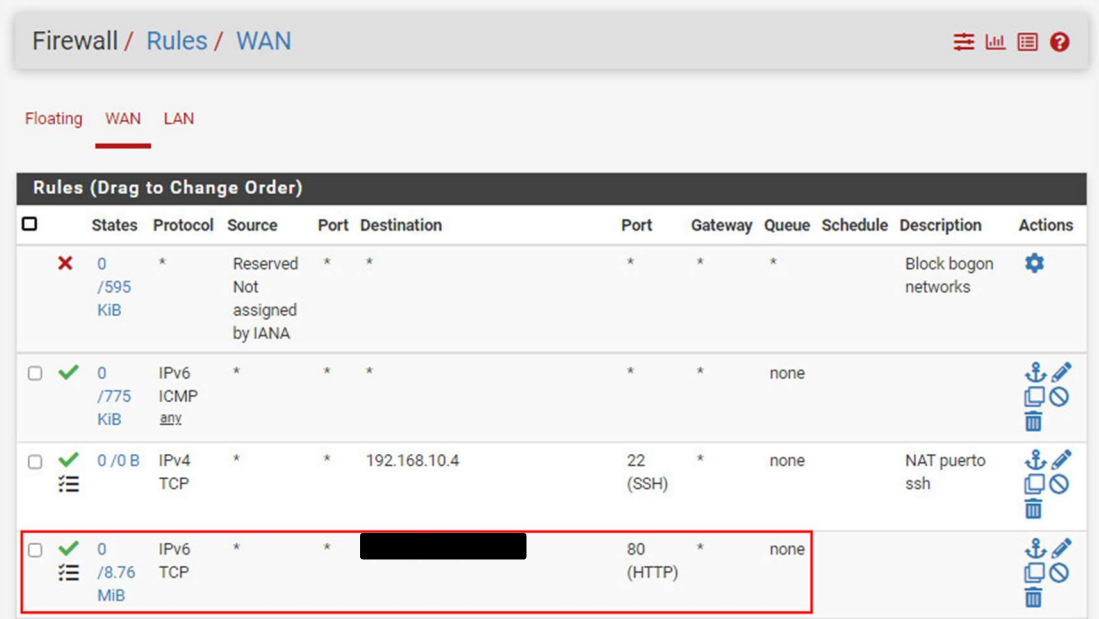


Figura 42 Configuración de regla en la interfaz correcta.

Como resultado, la página web se logró acceder desde una conexión externa:

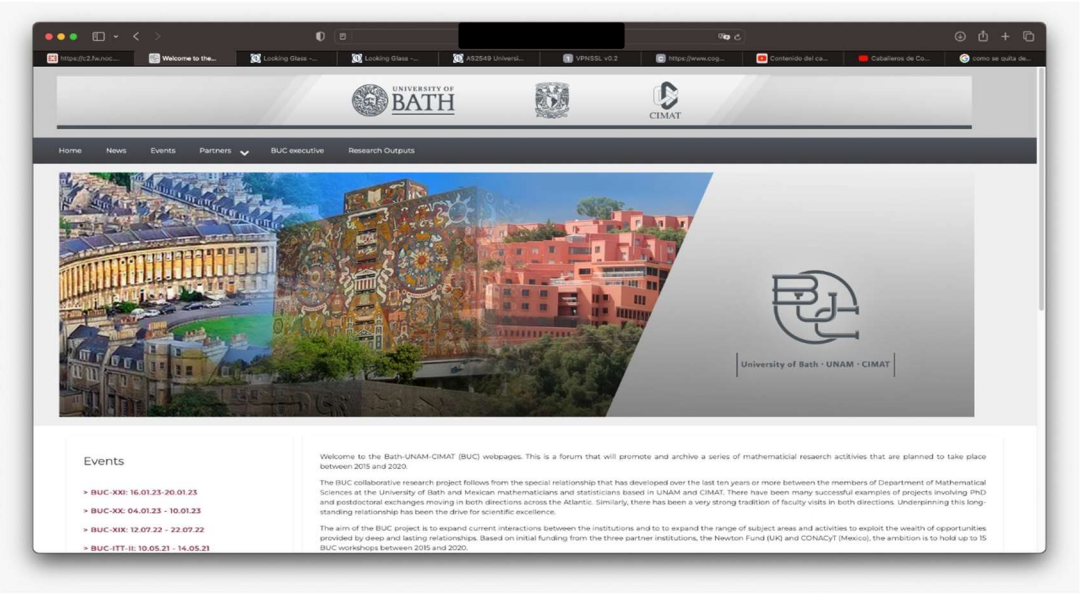


Figura 43 Evidencia de la visibilidad del sitio web en IPv6.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

En este punto todas las pruebas se realizan por IP mediante el protocolo IPv6 y no por nombre de dominio (DNS).

Después de que se realizó la compra y configuración del dominio cyr.org.mx en los servidores de DNS, fue necesario crear la regla que permite el tráfico hacia el servidor autoritativo con dirección **IPv6 2801:**[redacted]

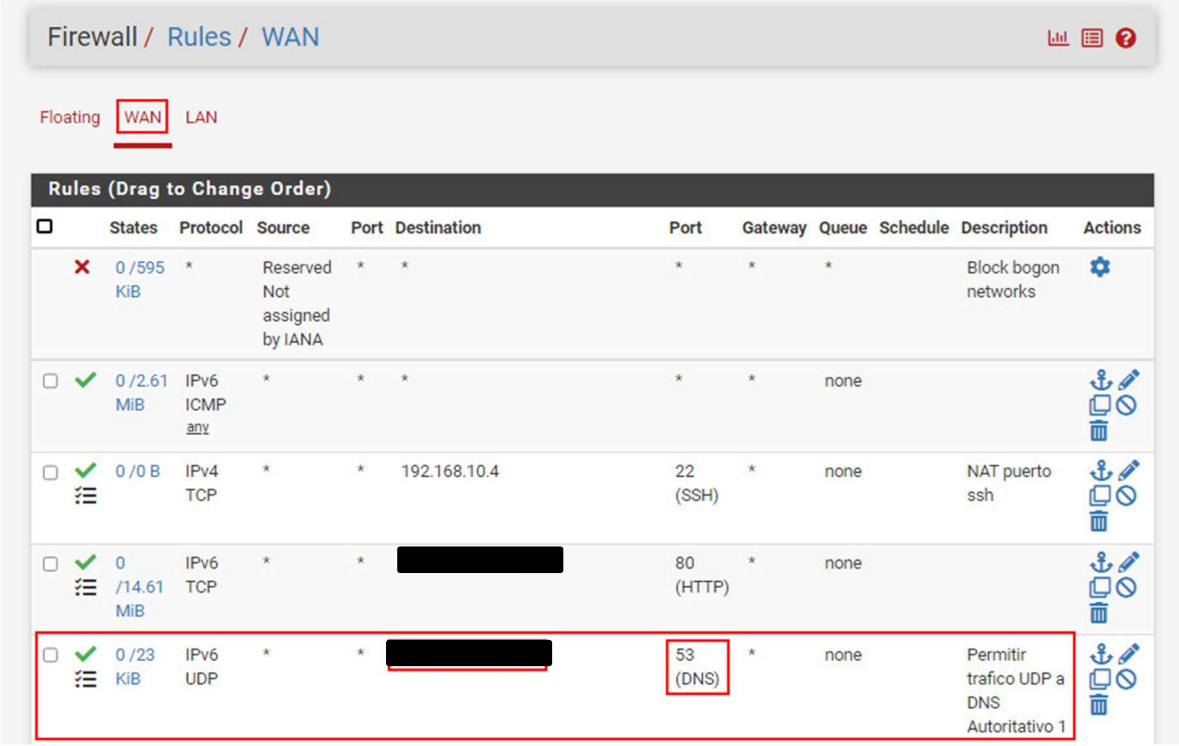


Figura 44 Publicación del servidor DNS autoritativo.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

7.1.3 Sistema de Nombres de Dominio (DNS)

7.1.3.1 Cambios en la configuración del servicio de los DNS. Realizados durante las pruebas

Se requirió hacer algunos cambios en las configuraciones de la interface de red para que los servidores DNS y las máquinas de prueba del ambiente de laboratorio tuvieran acceso a internet mediante el protocolo IPv6.

En primera instancia se configuraron todas las máquinas virtuales con una IP protocolo IPv4 para acceso local y comunicación entre estas. A estas mismas máquinas se les configuró también una IP con el protocolo IPv6.

Nota: En este momento solo tenemos salida a internet mediante el protocolo IPv6 aún no se cuenta con salida a las máquinas por el protocolo IPv4.

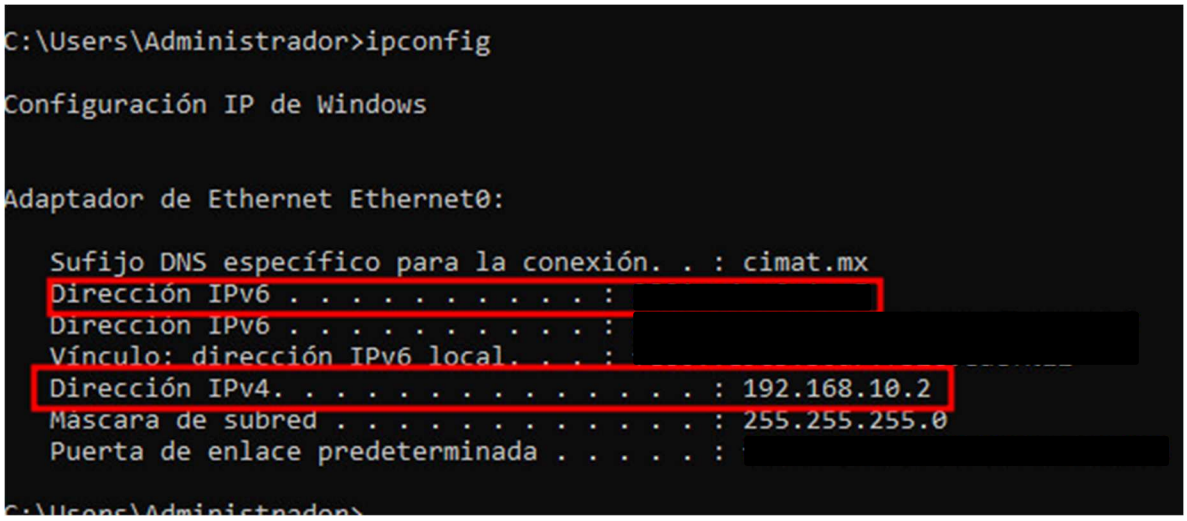


Figura 45 Evidencia de asignación de IP tanto de IPv4 como IPv6.

Una vez que se configuró el Router para dar salida a internet por el protocolo IPv6 a todas las máquinas virtuales del laboratorio, procedimos a realizar pruebas de navegación, estas máquinas tenían navegación limitada incluso nula en algunos de los casos. Platicando con el asesor de IPv6 llegamos a la conclusión de que la intermitencia en la navegación se debía a que las máquinas virtuales tenían configurada la puerta de salida para el protocolo IPv4 y esto causaba la problemática con la navegación, a consecuencia de esto, por el momento las máquinas están sin puerta de enlace en su protocolo IPv4.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

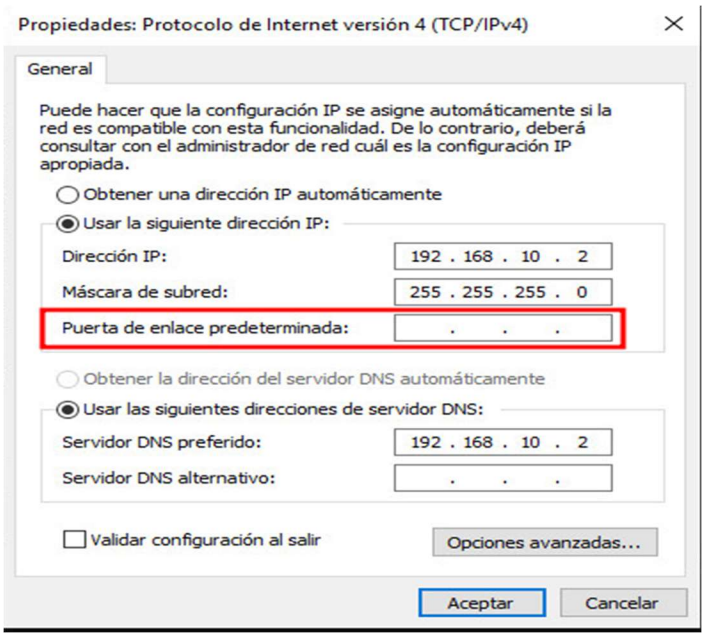


Figura 46 Configuración general de IPv4.

Por el momento las máquinas virtuales de laboratorio tienen salida a internet mediante el protocolo IPv6, como se comentó anteriormente, la interfaz está configurada de la siguiente manera teniendo como DNS principal el recursivo con su IP IPv6: **2801:**[redacted]

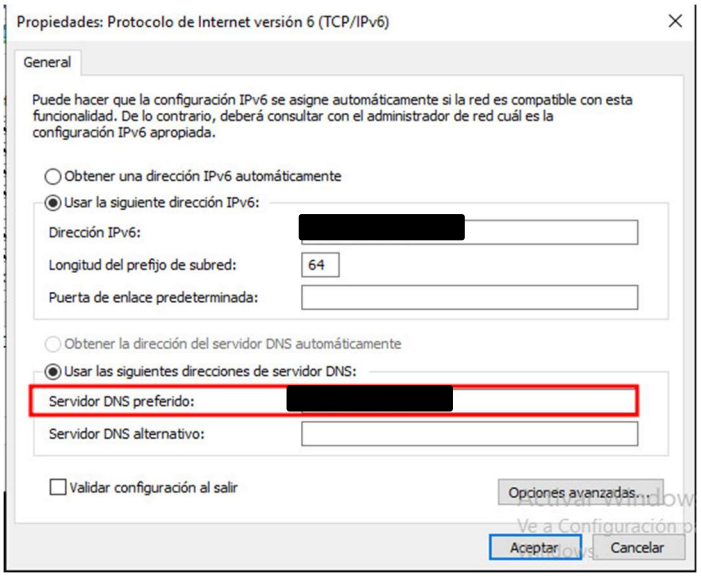


Figura 47 Configuración general IPv6.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

Después de retirar la puerta de enlace de la configuración IPv4 y estar usando los DNS recursivos para la salida en la configuración IPv6 nos percatamos que la navegación (velocidad) estaba bien, pero algunas páginas en internet que responden al protocolo IPv6 no se mostraban.

Después de investigar, integramos los DNS IPv6 de Google en la opción de renviadores (forwarders) en los servidores recursivos. Una vez integrados, las máquinas virtuales del laboratorio mostraban las páginas sin ningún problema.

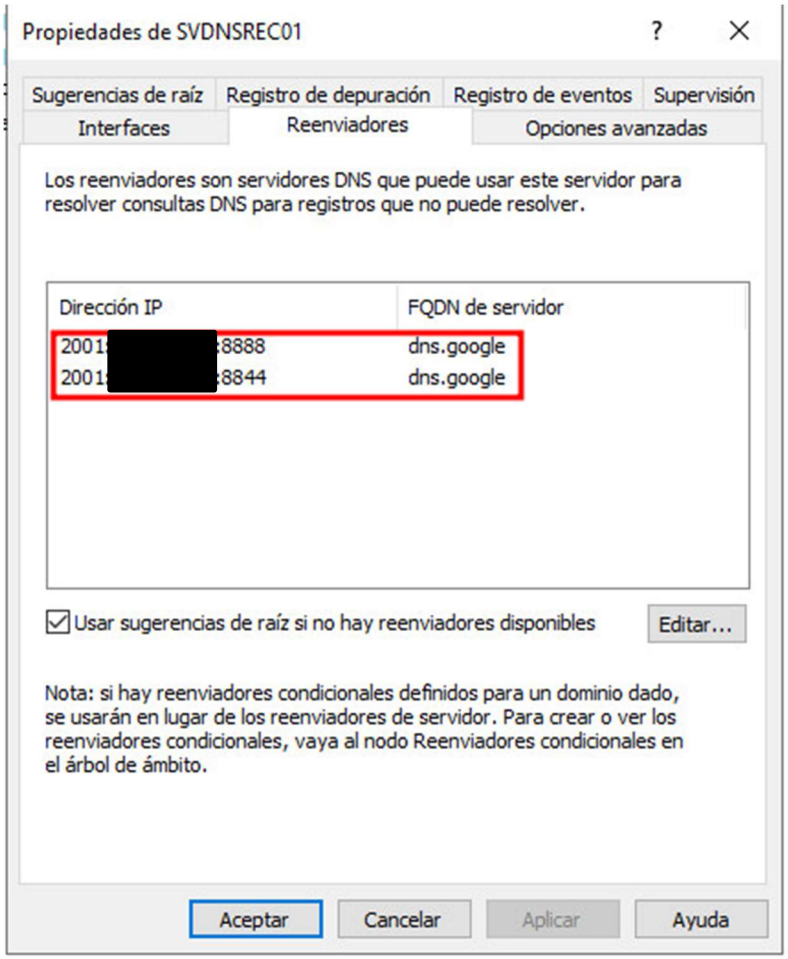


Figura 48 *Configuración DNS recursivo primario.*

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

Como se mencionó con anterioridad, actualmente solo tenemos vista desde fuera del laboratorio a nuestra página web de prueba llamada www2.cimat.mx con IP IPv6: 2801:[redacted] Esto se debe a que aún necesitamos hacer pruebas en el ambiente y no queremos publicar el DNS autoritativo con el dominio cimat.mx que tenemos en producción.

Se revisó con el asesor de IPv6 para identificar cuál era la mejor opción y poder empezar a publicar el DNS autoritativo y realizar pruebas por nombre con el protocolo IPv6. Se llegó a la conclusión de contratar un dominio de prueba y reestructurar la base de datos del DNS autoritativo para que empiece a contestar con el nombre del dominio de prueba.

7.1.3.2 Configuración del dominio de prueba

Se compró el dominio de prueba cyr.org.mx y se configuró una zona más en la base de datos del servidor de DNS autoritativo para que pudiera resolver nuestra página de prueba ahora llamada www.cyr.org.mx.

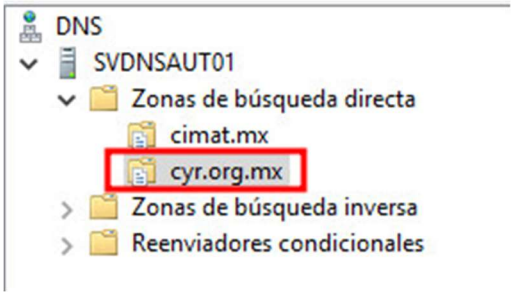


Figura 49 Configuración de una nueva zona en DNS primario.

Terminada la configuración de la nueva zona en el dominio principal procedimos a generar los registros en la base de datos, pero ahora con el dominio nuevo.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

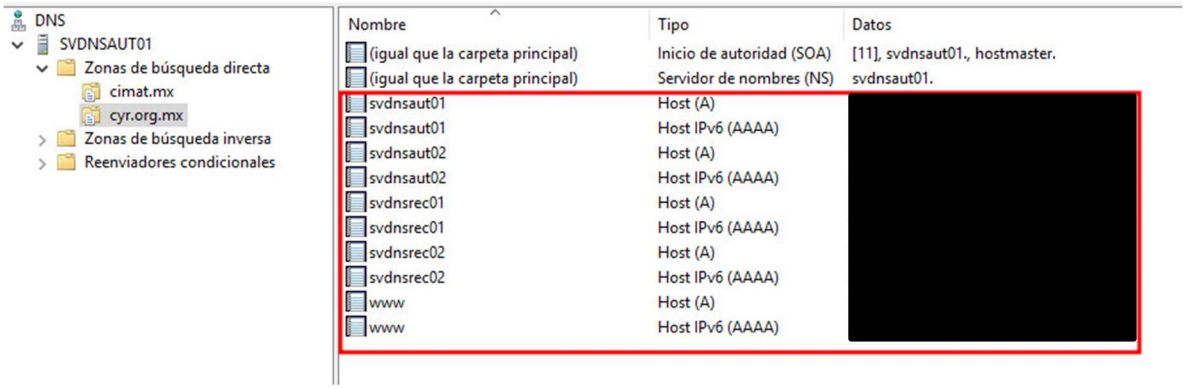


Figura 50 *Registros en nueva zona de DNS primario.*

7.1.3.3 Pruebas de publicación del dominio www.cyr.org.mx

A Continuación, se muestra una serie de imágenes donde podemos ver que nuestra página de prueba ahora renombrada www.cyr.org.mx ya se puede ver desde fuera del ambiente de laboratorio creado para esta primera etapa de la transición.

```
[redacted]@v6 ~ % dig @[redacted]00:1::29 www.cyr.org.mx aaaa

; <<>> DiG 9.10.6 <<>> @[redacted]:1::29 www.cyr.org.mx aaaa
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37505
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.cyr.org.mx.                IN    AAAA

;; ANSWER SECTION:
www.cyr.org.mx.         2796    IN    AAAA    2801:c4:e0:1::9

;; Query time: 46 msec
;; SERVER: 2001:1210:100:1::29#53([redacted]1::29)
;; WHEN: Tue Jan 24 13:55:20 CST 2023
;; MSG SIZE  rcvd: 71
```

Figura 51 *Validación de página web en la nueva zona primaria.*

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

```
$ ping6 www.cyr.org.mx
PING www.cyr.org.mx(2801:          ) 56 data bytes
64 bytes from 2801:c4:e0:1::9: icmp_seq=1 ttl=58 time=23.4 ms
64 bytes from 2801:c4:e0:1::9: icmp_seq=2 ttl=58 time=22.1 ms
64 bytes from 2801:c4:e0:1::9: icmp_seq=3 ttl=58 time=30.7 ms
64 bytes from 2801:c4:e0:1::9: icmp_seq=4 ttl=58 time=40.8 ms
64 bytes from 2801:c4:e0:1::9: icmp_seq=5 ttl=58 time=34.8 ms
```

Figura 52 *Ping a nueva página web, desde el exterior.*

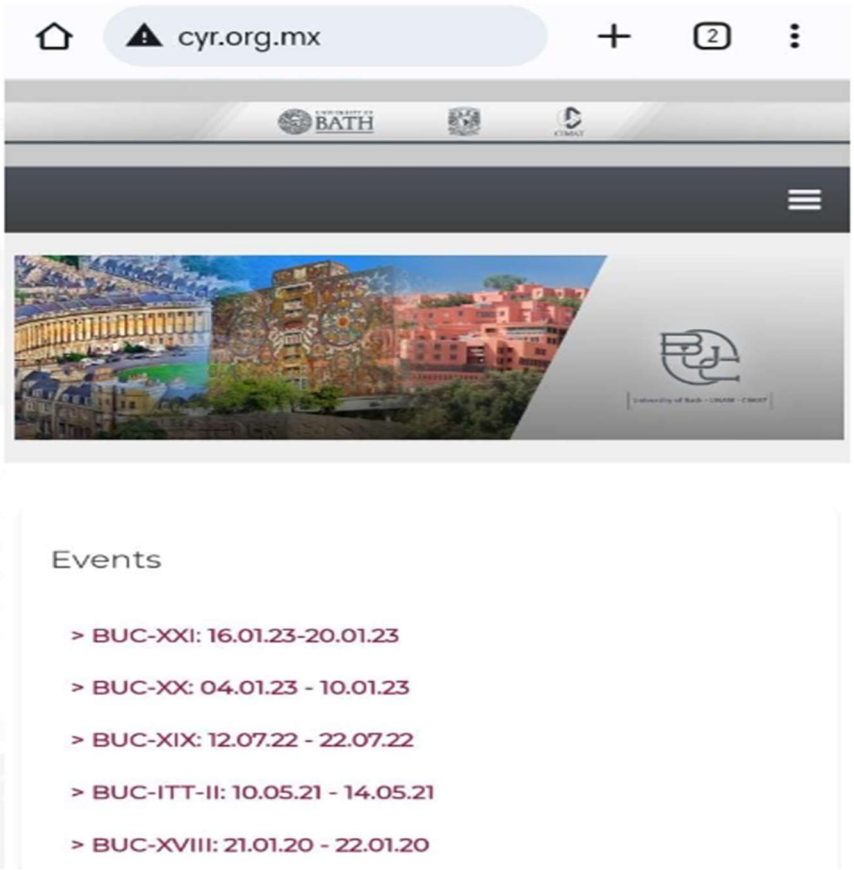


Figura 53 *Validación de página Web por nombre desde el exterior.*

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

7.1.4 Registro de direccionamiento ante LACNIC

Como parte de las responsabilidades al utilizar recursos de internet como lo son IPv4, IPv6 y ASN el CIMAT se apegó al cumplimiento de las Normas de Acuerdo Mutuo para la Seguridad del Enrutamiento (por sus siglas en inglés MANRS) con el fin de aportar a la iniciativa para mejorar en gran medida la seguridad y la resiliencia del sistema de enrutamiento global de internet. Completando algunas de las acciones que tienen como objetivo abordar los principales de problemas, como:

- Información de enrutamiento incorrecta
- Tráfico con direcciones IP de origen falsificadas
- Coordinación y colaboración entre redes

Para lo anterior, se creó la Autorización de Origen de Ruta (por sus siglas en inglés ROA) dentro del portal de Milacnic validando cada prefijo de IPv6 que está legítimamente autorizado que tenga origen de CIMAT.

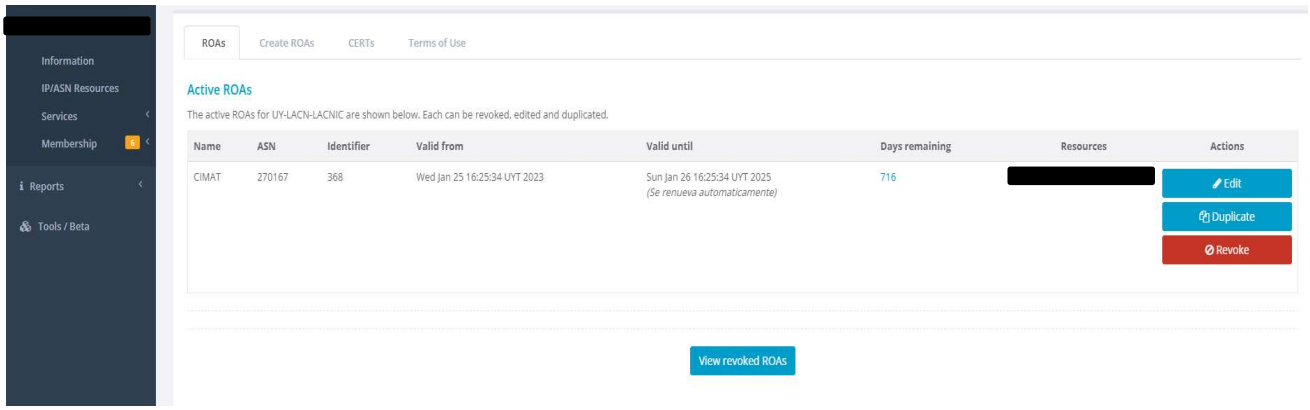


Figura 54 *Evidencia del registro del direccionamiento otorgado al CIMAT en Milacnic.*

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

Figura 55 *Evidencia en Milacnic del registro ROA como público*

Este método es el más seguro para facilitar la validación a escala global a través del sistema RPKI que permite verificar criptográficamente los anuncios de enrutamiento. Con ello, los operadores de red como CIMAT obtienen los certificados RPKI para sus propios prefijos de IPv6 e IPv4 de los LIR/RIR que los asignaron con el fin de generar, publicar y mantener las autorizaciones de ruta de origen (ROA) correspondientes a los prefijos de IPv6 que anuncia CIMAT.

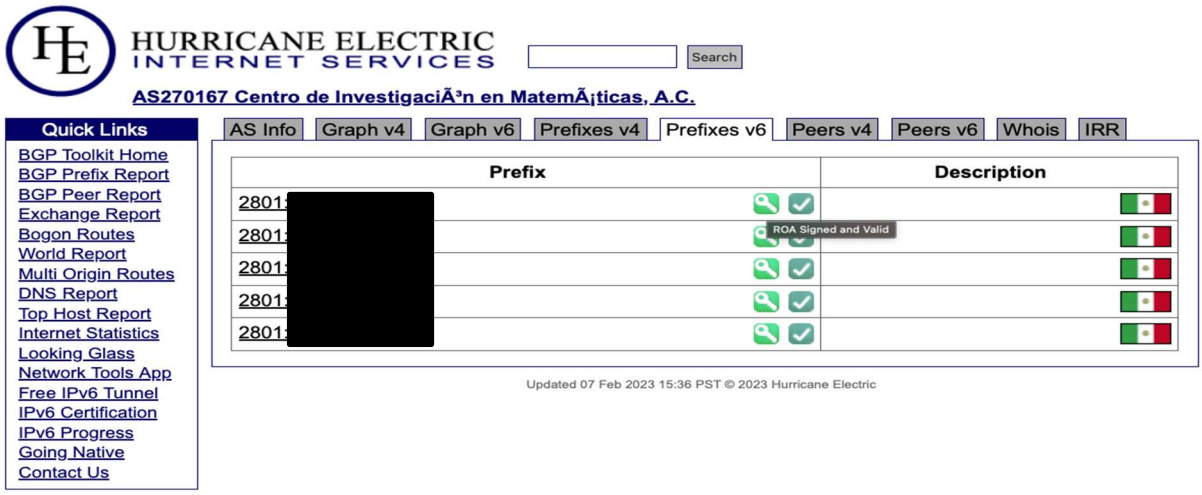


Figura 56 *Firmas de autorización de origen de ruta por BGP.*

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

8. CONCLUSIÓN

El protocolo IPv6 fue diseñado por la IETF Internet Engineering Task Force, para reemplazar y resolver las necesidades actuales de internet, particularmente el agotamiento de direcciones IPv4, con el objetivo entre otros, de garantizar la escalabilidad y disponibilidad de los servicios tecnológicos al corto, mediano y largo plazo.

En este sentido podemos concluir que esta primera etapa realizada por CIMAT establece los cimientos de una coexistencia segura y transparente en el uso de ambos protocolos, y hacia el uso productivo futuro de IPv6 en la institución.

Si bien es cierto para el usuario final institucional este proceso resultará totalmente transparente. Para que esto suceda, esta primera etapa requirió de una estrategia de planeación y capacitación con miras a establecer una red de pruebas con dicho protocolo. Conformando una réplica de todo el equipamiento y servicios actuales con el que cuenta la red institucional. Resultando con ello la adquisición de buenas prácticas relativamente sencilla para el proceso de puesta en producción, que no revistan complejidad y además de la adquisición de experiencia por parte del personal de TI, en el aprovisionamiento de la red con IPv6, de manera que la red no presente problemas de desconexión durante su proceso de transición de las siguientes etapas.

Otros puntos importantes que recalcar en esta primera etapa, es que sirvió para reforzar, así como mejorar las condiciones de la red actual institucional, descubriendo y perfeccionando la publicación y uso de servicios críticos, como lo es el sistema de nombres, preparando al mismo hacia una transición segura. Respecto a las mejoras derivadas de la adquisición de recursos propios, podemos mencionar la incorporación del proveedor de servicios de internet, a través de la interconexión por medio de un protocolo de enrutamiento más robusto (BGP), que permita contar con redundancia en internet, así como la independencia de los recursos IP de terceros, que repercuta en el descenso de los costos en el corto plazo.

Finalmente, esta etapa se considera exitosa debido que los factores de riesgo en la incorporación de una nueva tecnología se redujeron considerablemente.

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx

9. BIBLIOGRAFÍA

9.1.1 Cursos en Línea:

1. Campus.Lacnic.net

- IPv6 Básico
- IPv6 Avanzado

2. 6consultores, S.A de C.V.

- Capacitación para la transición al Protocolo de Internet versión 6

  https://www.gob.mx/cedn/documentos/guia-para-la-transicion-al-protocolo-de-internet-version-6-ipv6-en-la-administracion-publica-federal-que-emite-la-cedn

Jalisco S/N, Col. Valenciana, CP. 36023, Guanajuato, Gto. México. Apartado Postal 402, CP 36000.
Tel: +52 473 732 7155 www.cimat.mx