Diseño e implementación de una red corporativa en DUAL STACK (IPv4 e IPv6), para el fortalecimiento de la infraestructura tecnológica de las telecomunicaciones internas y externas de la CAR Cundinamarca

Jeison Jair González Vargas
Jhon Edizon Cruz Hernández.
Abril 2021

Universidad Nacional Abierta y a Distancia - UNAD
INGENIERÍA DE TELECOMUNICACIONES (Resolución 14518) ECBTI.
Bogotá

Diseño e implementación de una red corporativa en DUAL STACK (IPv4 e IPv6), para el fortalecimiento de la infraestructura tecnológica de las telecomunicaciones internas y externas de la CAR Cundinamarca

Jeison Jair González Vargas
Jhon Edizon Cruz Hernández

Proyecto Aplicado de Grado
Trabajo para optar al título de Ingeniero de Telecomunicaciones

Director
Jairo Luis Gutiérrez
Ingeniero Electrónico

Universidad Nacional Abierta y a Distancia - UNAD
Escuela de ciencias Básicas Tecnología e Ingeniería
Programa Ingeniería De Telecomunicaciones
Bogotá
2021

DEDICATORIA

Jhon E Cruz H: Este trabajo se dedica a cada uno de nuestros familiares que nos han apoyado desde nuestros inicios de carrera quienes nos han inculcado ánimo y esfuerzo cada día para seguir adelante, a nuestros amigos ingenieros que estuvieron ahí dándonos consejos, acalorando nuestras dudas.

De manera personal, doy agradecimiento a mi compañero de proyecto Jeison que se mantuvo firme y muy dispuesto a trabajar en cada detalle, aportando la experiencia que ha adquirido durante su vida laboral.

Jeison J González V: Mi dedicatoria primeramente la presento a Dios, en quien he dispuesto mis anhelos, sueños y triunfos, siendo él quien permite este momento, sujeto a la bendición de poder estar tan cerca de obtener el título como profesional.

Así como el regalo recibido en mi vida, del apoyo incondicional e impulso de ser mejor cada día. Seguidamente a mi familia, por su compañía en este proceso de años y por último a la UNAD, por garantizar el acompañamiento a este proceso y desarrollo profesional.

Agradecimientos

De manera general agradecemos a la universidad UNAD, por garantizar el acompañamiento a este proceso y desarrollo profesional, pero en mayor medida y al tutor Jairo Luis Gutierrez Torres por disponer del tiempo para la guía en el desarrollo y aceptación de este proyecto de grado aplicado.

TABLA DE CONTENIDO

LISTADO DE TABLAS

LISTADO DE ILUSTRACIONES

Resumen

Este proyecto será el resultado del estudio que se hará en el entorno de la Red Corporativa de la CAR Cundinamarca, sujeto a la necesidad de mejorar el rendimiento de las comunicaciones de Red interna y externas reportadas a la mesa de servicio. En el diagnóstico de comunicaciones se podrán encontraran fallas en la estructuración y diseño en la red tecnológica de telecomunicaciones locales; por ejemplo, un diseño de red plana de un dominio de broadcast de mascara de red 21, falta de visión de evolución, adaptabilidad de escalabilidad y adopción del protocolo IPv6 decretado a las entidades públicas por MinTIC en la Resolución 2710 del 03 octubre de 2017 donde se exige que las entidades gubernamentales, como mínimo deben tener en producción un servicio establecido bajo la norma IPv6.

Con base en lo anterior, se desea diseñar e implementar una red corporativa en DUAL STACK (IPv4 - IPv6), donde se mejore la infraestructura tecnológica de las telecomunicaciones internas y externas de la CAR mediante el uso de segmentación en subredes de un dominio de broadcast de 512 usuarios. Metodológicamente se contempla un diseño de investigación no experimental aplicado con enfoque mixto.

En este proyecto se dejarán documentadas las evidencias de cómo se encuentra actualmente la red corporativa de la CAR Cundinamarca, y se detallará el contraste de beneficios de haber restructurado el diseño topológico de la red de comunicaciones en el protocolo IPv4, acompañado de la implementación del nuevo protocolo IPv6, cuyo tráfico de red será protegido a nivel de servicios UTM por un Firewall Perimetral que asumirá el papel de Core de la Red Corporativa (protección de la información), sujeto a la visión de expansión (escalabilidad), y mejoramiento continuo.

Palabras clave: DUAL-STACK, Protocol IP, Topología, IPv6, Red.

ABSTRACT

This project will be the result from the studies that will be carried out to the CAR Cundinamarca Corporate Network, because of the needs to improve the performance from internal and external Networks communications that are reported to the Help Desk. During the diagnostics, maybe, it will be find infrastructure and design failures; for example, a flat network design, a wide broadcast domain, lack of vision, evolution, adaptability to the adoption of the IPv6 protocol that was decreed to public entities by MinTIC in the Resolution 2710 of October 03, 2017, where It is required that government entities, at least, must have in production a service under the IPv6 standard.

Based on the above, it is desired to design and implement a corporate network in DUAL STACK (IPv4 - IPv6), where the technological infrastructure of internal and external Network telecommunications are improved thanks to the use of subnet segmentation. Methodologically, a non-experimental research design approach is contemplated.

Keywords: DUAL-STACK, IP Protocol, Topology, IPv6, Network.

Introducción

La comunicación y transporte de información desde redes de datos locales hacia redes externas, como la Internet, están sujetos a los avances tecnológicos, esto nos permite identificar que en la actualidad se ha producido un aumento de la cantidad de dispositivos interconectados de manera simultánea, provocando un agotamiento de direccionamiento público basado en el estándar IPv4.

Tomando la evidencia publicada en la web de la organización encargada de supervisar la asignación y registro de recursos de números de Internet para Latinoamérica, siendo el RIR (Regional Internet Registry) LACNIC (Latin America and Caribean) vemos que existe un ítem que muestra una disponibilidad de cero direcciones disponibles

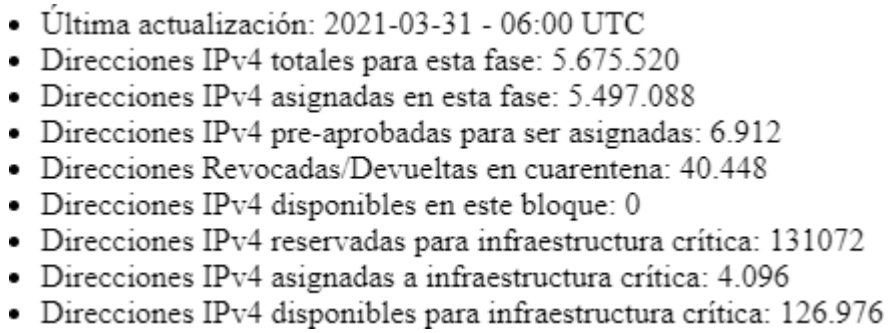

- Última actualización: 2021-03-31 - 06:00 UTC
- Direcciones IPv4 totales para esta fase: 5.675.520
- Direcciones IPv4 asignadas en esta fase: 5.497.088
- Direcciones IPv4 pre-aprobadas para ser asignadas: 6.912
- Direcciones Revocadas/Devueltas en cuarentena: 40.448
- Direcciones IPv4 disponibles en este bloque: 0
- Direcciones IPv4 reservadas para infraestructura crítica: 131072
- Direcciones IPv4 asignadas a infraestructura crítica: 4.096
- Direcciones IPv4 disponibles para infraestructura crítica: 126.976

Ilustración 1. Evidencia Agotamiento marzo 2021

Tomado de LACNIC https://n9.cl/44hn0

Con el propósito de resolver el problema anterior, se han implementado técnicas de sostenibilidad de las comunicaciones como por ejemplo el uso de NAT, pero a pesar de esto se siguen presentando limitaciones de comunicación peer to peer, la no creación de servicios DNS y la publicación de nuevos sitios WEB.

La corporación ICANN en su estudio de la demanda y consumo de recursos de redes WAN (Internet), estableció que es necesario tener recursos que no limiten la conexión de usuarios a la red, por ello se presentó el protocolo IP en versión 6, el cual amplia de manera drástica el tamaño del direccionamiento IP, mediante el uso de numeración hexadecimal y el manejo de una máscara de red de 128 bits.

La implementación del protocolo IPv6 garantizará la conexión sin limitantes de los nuevos dispositivos electrónicos que usarán la tecnología IoT pero sobre todo garantizará la convivencia y transición suave de IPv4 hacia IPv6, proceso conocido como DUAL-STACK, para luego si manejar redes puras en IPv6.

CAPÍTULO 1: GENERALIDADES DEL TRABAJO DE GRADO

ANTECEDENTES

Históricamente la temática del nuevo estándar IP para nuestro país ha tomado gran importancia sólo un par de años atrás, por ello, se ha encontrado una monografía que fue publicada como proyecto de grado por los alumnos ADELAIDA CORREA y MARTHA LUCIA CANDAMIL para la Universidad Libre de Colombia sobre el mecanismo de transición de IPv4 a IPv6, pero sobre todo concebido para mostrar desde el uso de un simulador de red el crecimiento del Internet queriendo permitir que todas las personas puedan hacer uso de él, adicional tratando de encontrar la respuesta de cuál sería el mecanismo para usar sobre plataformas de Windows server 2003.

El desarrollo hizo uso de una investigación exploratoria y documental de fuentes como libros, artículos publicados en la web en el que después de plasmar la parte teórica y conceptual que implicaba esta transición, inicia con el diseño de una topología de red hipotética a las que hace asignación de direccionamiento IPv4 e IPv6.

La monografía de los alumnos tuvo una finalización exitosa en la implementación logrando conectividad, por ello, como conclusión, podemos decir que desde un ambiente interno el problema de agotamiento del direccionamiento puede ser solventado.

Nuestro proyecto tendrá bastantes diferencias debido que hará uso de infraestructura física y estará en convivencia a la par de un ambiente productivo, lo cual hace que todas las variables deben ser previstas y planeadas a mayor detalle como por ejemplo un esquema de topología lógico con previo inventario.

PLANTEAMIENTO DEL PROBLEMA

El avance tecnológico, el auge de nuevas tecnologías y el incremento de conexiones simultaneas a las redes locales y externas con tráfico IP, ha ocasionado que los diseños básicos, obsoletos y no estructurados de la red de

telecomunicaciones de la CAR presenten fallas de transmisión, generando saturación, colisiones, pero sobre todo la percepción de indisponibilidad del servicio ante los usuarios finales.

Las comunicaciones actualmente se encuentran basadas en el protocolo IPv4. Protocolo que, según los estudios presentados por los RIR, IETF e IANA, indican que el agotamiento de las direcciones IPv4 aumentó significativamente, y que, en nuestro caso, LACNIC, siendo el ente que nos regula en Latinoamérica, publicó en su portal web en el año 2020 que ha entregado todo el direccionamiento IPv4 público disponible a los ISP, lo cual genera que en un tiempo inmediatamente cercano ya no se nos permita el uso, publicación de servicios o conexión de un dispositivo en la nube.

Frente a todo lo anterior, ¿cómo se puede superar la necesidad de crecimiento corporativo, inclusión de nuevos servicios, cumplimiento de la norma de migración del MinTIC y sobre todo de seguridad de información en la Red Corporativa de la CAR Cundinamarca? y ¿Con el diseño de implementación de una red escalable en Dual Stack se admitiría la convivencia simultanea de los protocolos IPv4 e IPv6?

JUSTIFICACIÓN

La infraestructura de red de la CAR CUNDINAMARCA, al estar diseñada en una red plana con un dominio de Broadcast tan grande, donde presenta conexiones simultáneas de más de 1800 host o terminales en una red plana, tiende a bajar el desempeño de Switching y Forwarding de comunicaciones de un 100 % a un 75 %, tanto en servicios locales como externos, aclarando que no son perdidas de paquetes ni intermitencias, sino que es algo reflejado en lentitud de las comunicaciones.

Adicional a esto, se debe tener en cuenta que, si se presenta una falla de red todas las comunicaciones se verán afectadas ya que toda la topología de comunicaciones es una red plana, un solo dominio de broadcast, por ende, un único Gateway. Una de las fallas en redes más conocidas y que así mismo es de la más básicas y conocidas dentro de la administración de redes, son los LOOP o bucles físicos. Así mismo, la entidad deberá procurar cumplir la solución 2710 de 2017 del MinTIC, la cual se sujeta a la necesidad de adoptar el protocolo IPv6 en conjunto con la infraestructura de la entidad existente en protocolo IPv4.

El MinTIC dicta guías básicas para que las entidades estatales ejecuten la transición al protocolo IPv6, y adopten de este modo una arquitectura DUAL-STACK.

Los puntos expuestos anteriormente, serán atacados por la entidad, partiendo del diseño de una arquitectura topológica que contemple dominios de Broadcast pequeños, subdividiendo el direccionamiento IP actual cuya red plana de IPv4 está en una máscara de red /21, hacia máscaras de red pequeñas de 24 o 23 bits, por medio de subredes en capa 3 y un ID de VLAN por cada subred.

Este diseño liberará cargas y eliminará la lentitud en la red, así como también permitirá tener fallas no generales sino centralizadas al contar con subredes independientes, así como Gateway y dominio broadcast.

A continuación, se presenta el gráfico que ilustra una lluvia de broadcast.

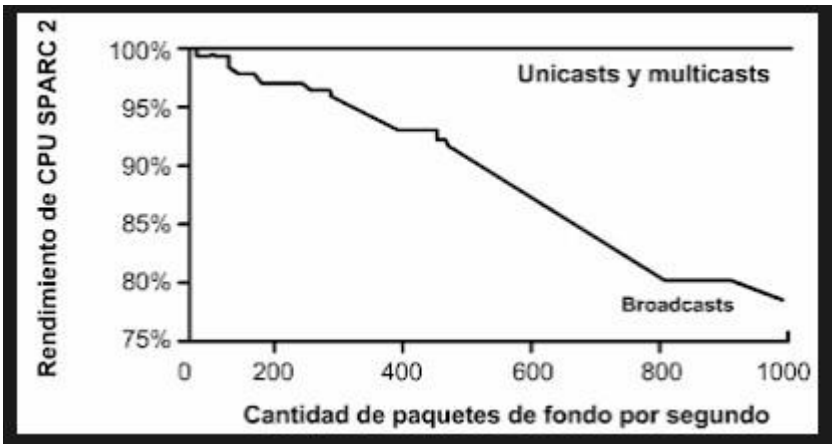


Ilustración 2. Lluvia de Broadcast.

Tomado de ***https://sites.google.com/site/conmutacionredes/problemas-de-broadcast***

Posterior a la restructuración de la red corporativa de la entidad, se confirmará que es viable operativamente para la CAR Cundinamarca realizar la implementación del protocolo IPv6 en modalidad Dual Stack, que adoptará la convivencia de las dos versiones del protocolo IP, a nivel de comunicaciones red, seguridad como servicios.

El agotamiento de las direcciones IPv4, es la principal justificación para la implementación del protocolo IPv6 a nivel global, por ello todas las entidades estatales deben adoptar este protocolo, quizás como ejemplo y pioneros de la actualización tecnológica e integración a las plataformas mundiales que ya convergen en el protocolo IPv6.

A continuación, se muestra el estado de adopción del protocolo IPv6 y fases de adopción IPv6 presentadas por el MinTIC en la resolución 2710 de 2017, así como las indicaciones e información de agotamiento del protocolo IPv4 entregada por LACNIC RIR para Latinoamérica y el caribe.

FASES DE AGOTAMIENTO PRESENTADAS POR LACNIC:

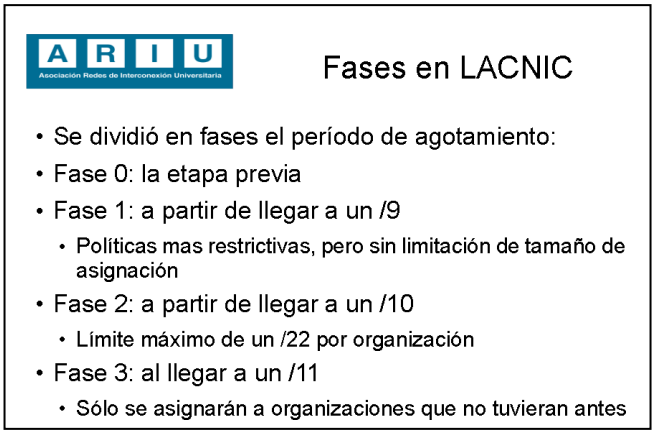


Ilustración 3. Fases de agotamiento IPv4.

Tomado de

https://www.palermo.edu/Archivos_content/2014/ingenieria/agosto/ietf/agotamiento-ipv4-jaiio-Cicileo.pdf

La fase 2 finalizo el 14 de febrero de 2017 dejando el siguiente panorama de asignación:

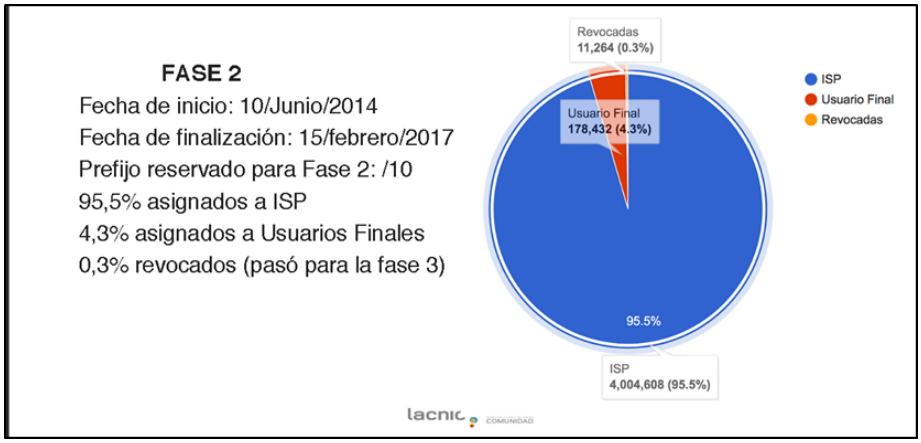


Ilustración 4. Finalización de Fase 2

Tomado de http://slides.lacnic.net/wp-content/uploads/2017/05/sergio-rojas_reporte-agotamiento_ipv4.pdf

A mayo de 2020 nos encontramos en la fase 3.

El inicio de Fase se dio el 15/febrero/2017, a partir de esta fecha la máxima asignación será de un prefijo /22 y la mínima asignación será de un /24, las cuales solo serán asignadas únicamente a los nuevos entrantes (nuevos miembros en LACNIC):

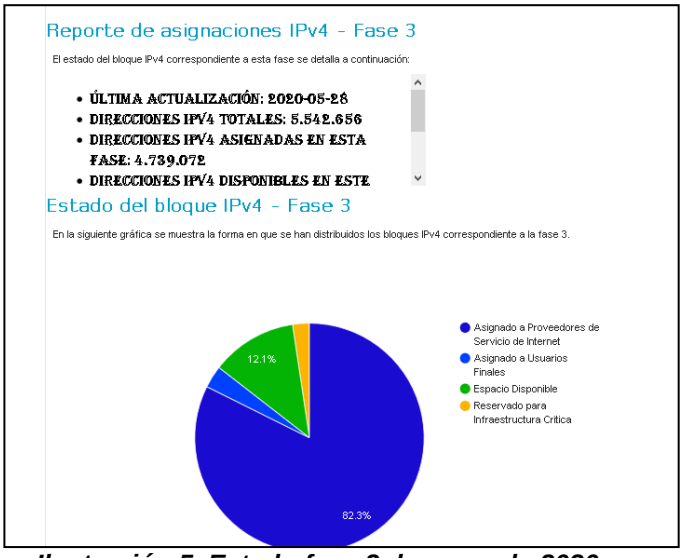


Ilustración 5. Estado fase 3 de mayo de 2020,

Tomado de https://www.lacnic.net/1001/1/lacnic/fases-de-agotamiento-de-ipv4#tabs-1

El MinTIC como pionero en Colombia del protocolo IPv6, ha publicado en su portal WEB el progreso en la adopción y convivencia del protocolo IPv6 con IPv4 siendo ya en un 100 %.

Acompañado a la información de adopción, el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia presenta guías de adopción y en un mayor grado de atención y necesidad de ejecución la resolución 2710 de 2017, documentos que ampara los tiempos límites de adopción.

Así mismo se resalta el proyecto Renata, como uno de los primeros entes que presentan la adopción del protocolo IPv6 en su infraestructura WAN y LAN, para las redes de Internet en las universidades que están en este convenio, y en su documentación se encuentra información valiosa como las fases resultantes luego de acoger el protocolo e implementarlo:

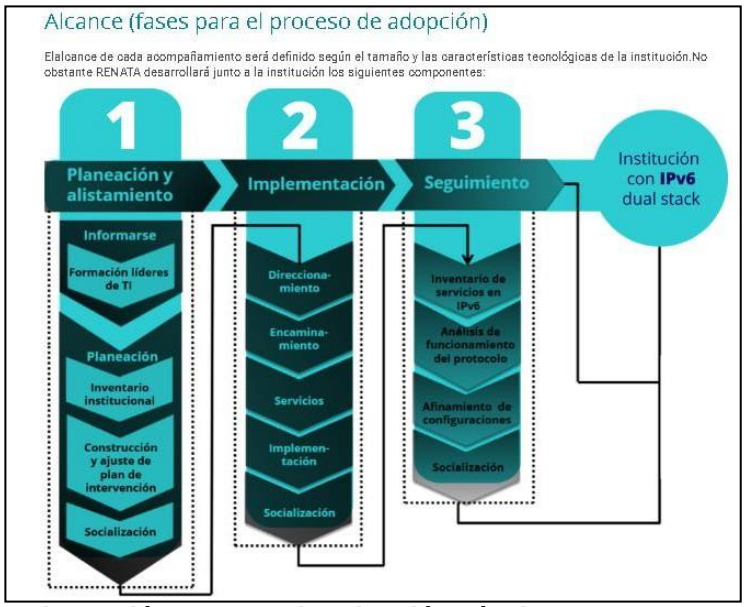


Ilustración 6. Fases de Adopción Técnica RENATA

Tomado de https://www.renata.edu.co/ipv6

OBJETIVO GENERAL

Diseñar e implementar una red corporativa en DUAL STACK (IPv4 - IPv6), para el fortalecimiento de la infraestructura tecnológica de las telecomunicaciones internas y externas de la CAR Cundinamarca.

OBJETIVOS ESPECÍFICOS

1. Realizar el levantamiento de información de los inventarios de red tecnológica de la CAR Cundinamarca, con el fin de elaborar un plan de trabajo de ejecución técnica con el diseño e implementación de los protocolos IPv4 e IPv6.

2. Presentar la propuesta de restructuración y diseño topológico, para la implementación del DUAL STACK en la red tecnológica de telecomunicaciones en la CAR Cundinamarca.

3. Implementar la restructuración en la red de telecomunicaciones en DUAL STACK, garantizando la operatividad de los servicios tecnológicos y acceso a la información de la CAR Cundinamarca, garantizando el correcto cumplimiento de la Resolución 2710 del 2017 del MinTIC, respecto de la generación de tráfico IPv6 de forma local y a Internet de forma segura.

4. Brindar el acompañamiento en la ejecución de pruebas y actividades de afinamiento de la solución implementada en la CAR Cundinamarca en la red de telecomunicaciones.

CAPÍTULO 2: MARCO CONCEPTUAL Y TEÓRICO

¿QUÉ ES IPV6?

Es la versión 6 de IP, diseñado para coexistir con IPv4 durante una fase de transición, hasta que, de forma transparente, IPv4 deje de utilizarse y desaparezca de la red.

ESPECIFICACIONES PROTOCOLO INTERNET VERSION 6

De acuerdo con el estándar brindado por la IETF (Internet Engineering Task Force) en la norma RFC8200, el IPv6 es una actualización al protocolo IPv4, diseñado para resolver el problema de agotamiento de direcciones. Su desarrollo comenzó en diciembre de 1998 cuando Steve Deering y Robert Hinden, empleados de Cisco y Nokia publicaron una especificación formal del protocolo a través de un RFC12.

La sustitución de IPv4 se dio por la no admisión de direcciones y restricción del crecimiento y uso de Internet, especialmente en China, India, y otros países asiáticos densamente poblados. El nuevo estándar busca mejorar el servicio globalmente; por ejemplo, proporcionando a futuras celdas telefónicas y dispositivos móviles con sus direcciones propias y permanentes.

IPv4 posibilita 4.294.967.296 (2^{32}) direcciones de dispositivos diferentes, un número menor a la población mundial, y menor a la cantidad de dispositivos totales. A principios de 2010, quedaban menos del 10 % de IP sin asignar. En la semana del 3 de febrero de 2011,4 la IANA (Agencia Internacional de Asignación de Números de Internet, por sus siglas en inglés) entregó el último bloque de direcciones disponibles (33 millones) a la organización encargada de asignar IPs en Asia, un mercado que está en auge y no tardará en consumirlas todas.

En cambio, IPv6 admite 340.282.366.920.938.463.463.374.607.431.768.211.456 (2^{128} o 340 sextillones de

direcciones), cerca de $6{,}7 \times 10^{17}$ (670 mil billones) de direcciones por cada milímetro cuadrado de la superficie de la Tierra.

RED DE DATOS, TOPOLOGÍA DE RED

Las redes de datos son infraestructuras que han sido creadas para poder transmitir información a través del intercambio de datos. Es decir, son arquitecturas específicas para este fin, cuya base principal es la conmutación de paquetes y que atienden a una clasificación exclusiva, teniendo en cuenta la distancia que es capaz de cubrir su arquitectura física y, por supuesto, el tamaño que presentan.

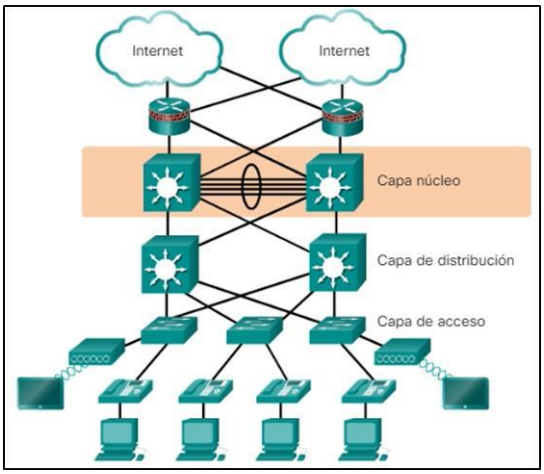


Ilustración 7. Diseño de Topología de red

Tomado de https://ccnadesdecero.es/diseno-jerarquico-de-redes/

CABECERA IPV6.

La longitud total de la cabecera IPv6 es de 40 bytes (en IPv4 eran 20bytes) y dicha cabecera tiene un tamaño fijo, esto ayuda a los equipos a conmutar tráfico lo que se traduce en mayores prestaciones.

Además, hay que tener en cuenta que los campos van alineados a 64bits lo que permite a los nuevos procesadores optimizar el rendimiento.

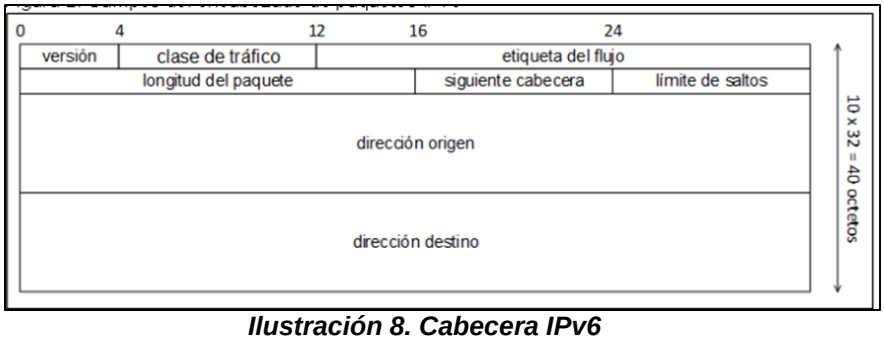


Ilustración 8. Cabecera IPv6

Tomado de http://www.ipv6go.net/cabecera_ipv6.php

Los primeros 40 bytes (320 bits) son la cabecera del paquete y contiene los siguientes campos:

Offset del octeto		0								1								2								3							
	Bit offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Versión				Clase de tráfico								Etiqueta de flujo																			
4	32	Longitud del campo de datos																Cabecera siguiente								Límite de saltos							
8	64	Dirección de origen																															
C	96																																
10	128																																
14	160																																
18	192	Dirección de destino																															
1C	224																																
20	256																																
24	288																																

Ilustración 9. Cabecera IPv6

Tomado de https://es.wikipedia.org/wiki/IPv6

- Direcciones de origen (128 bits)
- Direcciones de destino (128 bits)
- Versión del protocolo IP (4 bits)
- Clase de tráfico (8 bits, Prioridad del Paquete)
- Etiqueta de flujo (20 bits, manejo de la Calidad de Servicio)
- Longitud del campo de datos (16 bits)
- Cabecera siguiente (8 bits)
- Límite de saltos (8 bits, Tiempo de Vida).

Hay dos versiones de IPv6 levemente diferentes. La ahora obsoleta versión inicial, descrita en el RFC 1883, difiere de la actual versión propuesta de estándar, descrita en el RFC 2460, en dos campos: hay 4 bits que han sido reasignados desde "etiqueta de flujo" (flow label) a "clase de tráfico" (traffic class). El resto de las diferencias son menores.

En IPv6 la fragmentación se realiza solamente en el nodo origen del paquete, al contrario que en IPv4 en donde los routers pueden fragmentar un paquete. En

IPv6, las opciones también desaparecen de la cabecera estándar y son especificadas por el campo "Cabecera Siguiente" (Next Header), similar en funcionalidad en IPv4 al campo Protocolo.

Un ejemplo: en IPv4 uno añadiría la opción "ruta fijada desde origen" (Strict Source and Record Routing) a la cabecera IPv4 si quiere forzar una cierta ruta para el paquete, pero en IPv6 uno modificaría el campo "Cabecera Siguiente" indicando que viene una cabecera de encaminamiento. La cabecera de encaminamiento podrá entonces especificar la información adicional de encaminamiento para el paquete, e indicar que, por ejemplo, la cabecera TCP será la siguiente.

Este procedimiento es análogo al de AH y ESP en IPsec para IPv4 (que aplica a IPv6 de igual modo, por supuesto). que tener en cuenta que los campos van alineados a 64bits lo que permite a los nuevos procesadores optimizar el rendimiento.

PROTOCOLO ICMP V6.

El protocolo ICMP v6 es utilizado por los nodos IPv6 con el fin de informar sobre los errores encontrados durante el procesamiento de los paquetes y para realizar otras funciones relativas a la capa de internet como son los diagnósticos (“ping”).

Los mensajes ICMPv6 se dividen en dos tipos:

- Mensajes de error: se identifican con un 0 en su campo “Tipo de mensaje” y sus valores van desde 0 a 127.
- Mensajes informativos: sus valores están entre 128 y 255. “Mediante ICMPv6, los hosts y los enrutadores que se comunican mediante IPv6 pueden informar sobre los errores que se presentan y enviar mensajes de eco simples.

Formato de los Paquetes:

Los paquetes ICMPv6 tienen el formato Tipo, Código y Checksum.

Los 8 bits del campo Tipo indican el tipo de mensaje. Si el bit de mayor peso tiene el valor 0 (valores entre 0 y 127) entonces es un mensaje de error, por el contrario, si el bit de mayor peso es 1 (valores entre 128 y 255) entonces es un mensaje informativo.

Los 8 bits del campo Código dependen del tipo de mensaje, y son usados para crear un nivel adicional de clasificación de mensajes, de tal forma que los mensajes informativos en función del campo Código se pueden subdividir en varios tipos.

El campo Checksum es usado para detectar errores en los mensajes ICMP y en algunos de los mensajes IPv6.

DUAL STACK.

Hace referencia a la capacidad que tiene un dispositivo que hace parte de una infraestructura tecnológica de comunicaciones, de establecer el protocolo TCP/IP en protocolo IP en versión 4 y 6.

Es el método propuesto originalmente para tener una transición suave hacia IPv6. En este caso se necesita contar con suficiente cantidad de direcciones IPv4 para poder desplegar las dos versiones del protocolo en simultáneo en toda la red.

De esta forma, cuando se establece una conexión hacia un destino sólo IPv4, se utilizará la conectividad IPv4 y si es hacia una dirección IPv6, se utilizará la red IPv6. En caso que el destino tenga ambos protocolos, normalmente se preferirá intentar conectar primero por IPv6 y en segunda instancia por IPv4 (si bien esto se ha ido modificando para solucionar problemas de timeouts, ver “happy eyeballs”).

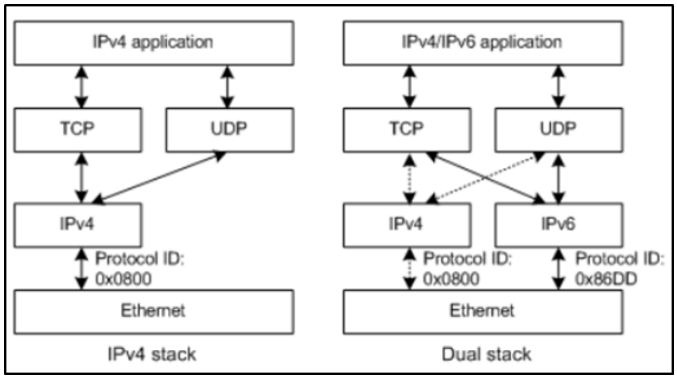
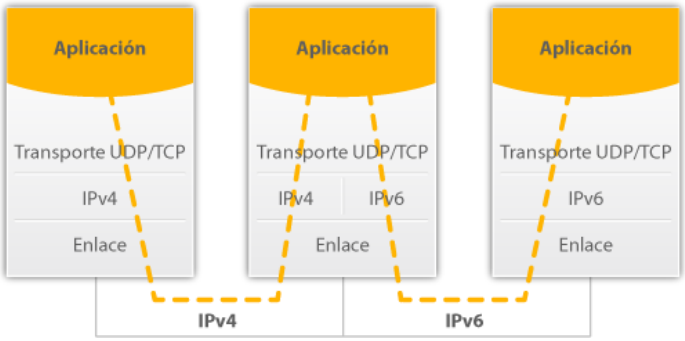


Ilustración 10. Dual Stack

Tomado de https://www.lacnic.net/3091/1/lacnic/dual-stack-o-pila-doble



Tomado de https://www.lacnic.net/3091/1/lacnic/dual-stack-o-pila-doble

TCP/IP

El modelo TCP/IP es una descripción de protocolos de red creado por Vinton Cerf y Robert E. Kahn, en la década de 1970. Fue implantado en la red ARPANET, la primera red de área amplia (WAN), desarrollada por encargo de DARPA, una agencia del Departamento de Defensa de los Estados Unidos, y predecesora de Internet; por esta razón, a veces también se le llama modelo DoD o modelo DARPA.

El modelo TCP/IP es usado para comunicaciones en redes y, como todo protocolo, describe un conjunto de guías generales de operación para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.

El modelo TCP/IP y los protocolos relacionados son mantenidos por la Internet Engineering Task Force.

Para conseguir un intercambio fiable de datos entre dos equipos, se deben llevar a cabo muchos procedimientos separados. El resultado es que el software de comunicaciones es complejo. Con un modelo en capas o niveles resulta más sencillo agrupar funciones relacionadas e implementar el software modular de comunicaciones.

Las capas están jerarquizadas. Cada capa se construye sobre su predecesora. El número de capas y, en cada una de ellas, sus servicios y funciones son variables con cada tipo de red. Sin embargo, en cualquier red, la misión de cada capa es proveer servicios a las capas superiores haciéndoles transparentes el modo en que

esos servicios se llevan a cabo. De esta manera, cada capa debe ocuparse exclusivamente de su nivel inmediatamente inferior, a quien solicita servicios, y del nivel inmediatamente superior, a quien devuelve resultados. Referencia a la capacidad que tiene un dispositivo que hace parte de una infraestructura tecnológica de comunicaciones, de establecer el protocolo TCP/IP en protocolo IP en versión 4 y 6.

Capas según el modelo OSI		Capas según el modelo DoD	
7	Aplicación *Application*	4	Aplicación *Process*
6	Presentación *Presentation*		
5	sesión *Session*		
4	Transporte *Transport*	3	Transporte *Host-to-Host*
3	Red *Network*	2	Internet *Network*
2	Enlace de datos *Data Link*	1	Acceso al medio *Media*
1	Física *Physical*		

Ilustración 11. Relación TCP/IP con el modelo OSI

Tomado de https://es.wikipedia.org/wiki/Modelo_TCP/IP

DNS.

El sistema de nombres de dominio (Domain Name System o DNS, por sus siglas en inglés) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombres de dominio asignados a cada uno de los participantes. Su función más importante es "traducir" nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres

de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

En IPv4 la asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Por ejemplo, si la dirección IP del sitio Google es 216.58.210.163, la mayoría de la gente llega a este equipo especificando www.google.com y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable.

La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre del sitio web. Incluso, en el caso de que una página web utilice una red de distribución de contenidos (Content Delivery Network o CDN, por sus siglas en inglés) por medio del DNS el usuario recibirá la dirección IP del servidor más cercano según su localización geográfica (cada CDN a su vez tiene sus propios servidores DNS).

Los componentes del protocolo DNS son: Para la operación práctica del sistema DNS se utilizan tres componentes principales:

- Los Clientes fase 1: Un programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS (Por ejemplo: ¿Qué dirección IP corresponde a nombre dominio?)
- Los Servidores DNS: Que contestan las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada.
- Las Zonas de autoridad: Es una parte del espacio de nombre de dominios sobre la que es responsable un servidor DNS, que puede tener autoridad sobre varias zonas. (Por ejemplo: subdominio.Wikipedia.ORG, subdominio.COM, etc.)

Tipos de registros DNS: Los tipos de registros más utilizados son:

- A = Dirección (address). Este registro se usa para traducir nombres de servidores de alojamiento a direcciones IPv4.
- AAAA = Dirección (address). Este registro se usa en IPv6 para traducir nombres de hosts a direcciones IPv6.
- CNAME = Nombre canónico (canonical Name). Se usa para crear nombres de servidores de alojamiento adicionales, o alias, para los servidores de alojamiento de un dominio. Es usado cuando se están corriendo múltiples servicios (como FTP y servidor web) en un servidor con una sola dirección IP. Cada servicio tiene su propia entrada de DNS (como ftp.ejemplo.com. y www.ejemplo.com.). Esto también es usado

cuando corres múltiples servidores HTTP, con diferentes nombres, sobre el mismo host. Se escribe primero el alias y luego el nombre real.

- NS = Servidor de nombres (Name Server). Define la asociación que existe entre un nombre de dominio y los servidores de nombres que almacenan la información de dicho dominio. Cada dominio se puede asociar a una cantidad cualquiera de servidores de nombres.
- MX = Intercambio de correo (Mail Exchange). Asocia un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio. Tiene un balanceo de carga y prioridad para el uso de uno o más servicios de correo.
- PTR = Indicador (Pointer). También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo IPs en nombres de dominio. Se usa en el archivo de configuración de la zona DNS inversa.
- SOA = Autoridad de la zona (Start of Authority). Proporciona información sobre el servidor DNS primario de la zona.
- SRV = Service record (SRV record).
- ANY = Toda la información de todos los tipos que exista. (No es un tipo de registro, sino un tipo de consulta)

DIRECCIÓN IPV4.

Una dirección IP es una dirección empleada para identificar a un dispositivo en una red IP. La dirección se compone de 32 bits binarios, que pueden dividirse en una porción correspondiente a la red y otra correspondiente al host, con la ayuda de una máscara de subred. Los 32 bits binarios se dividen en 4 octetos (1 octeto = 8 bits). Cada octeto se convierte a decimal y se separa con un punto.

Por esta razón, se dice que una dirección IP se expresa en formato decimal con puntos (por ejemplo, 172.16.81.100). El valor de cada octeto en decimal va desde 0 hasta 255, o desde 00000000 hasta 11111111en binario.

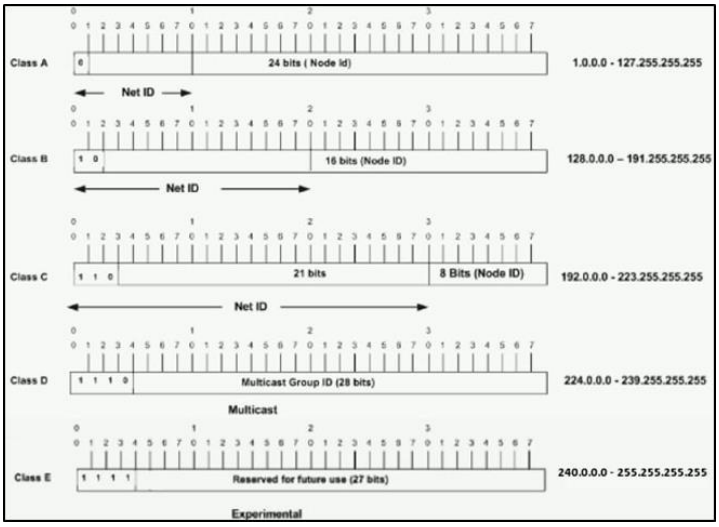


Ilustración 12. Formato IPv4

Tomado de https://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocol-rip/13788-3.html

DIRECCIÓN IPV6.

IPv6 es la nueva versión del Protocolo Internet (IP) en el cual se sustenta la navegación en la web. Las especificaciones técnicas básicas de IPv6 se desarrollaron en la década de los 90s en el IETF (Internet Engineering Task Force). Hoy el protocolo sigue añadiendo nuevas funcionalidades y se le considera un protocolo lo suficientemente maduro para soportar la operación de Internet en substitución de IPv4.

La principal motivación para el diseño y despliegue de IPv6 fue la expansión del espacio de direcciones disponible en Internet. De esta forma se permite que se conecten billones de nuevos dispositivos (tabletas, teléfonos móviles, y televisiones inteligentes entre otros), nuevos usuarios y tecnologías “siempre-conectadas” (xDSL, cable, Ethernet en el hogar, Fibra en el hogar, redes inalámbricas, etc.).

IPv6 representa quizás el cambio más importante en la historia del Internet ya que es necesario para que la red de redes pueda seguir desarrollándose de una forma segura y estable.

Tipo de dirección	Prefijo de formato en binario	Prefijo de formato en hexadecimal	Dirección
Reservada	0000 0000	00	::/8
Reservada para asignación NSAP	0000 001	02 ó 03	0200::/7
Unidifusión globales agregables	001	2ó3	2000::/3
Unidifusión locales exclusivas	1111 1101	FD	FD00::/8
Unidifusión locales del enlace	1111 1110 10	FE8 hasta FEB	FE80::/10
Unidifusión locales del sitio (obsoleta)	1111 1110 11	FEC hasta FEF	FEC0::/10
Multidifusión	1111 1111	FF	FF00::/8

Ilustración 13. Formatos IPv6

Tomado de https://sites.google.com/site/redeslocalesyglobales/6-arquitecturas-de-redes/6-arquitectura-tcp-ip/7-nivel-de-red/8-direccionamiento-ipv6/2-direccionamiento-ipv6/formato-de-direcciones-ipv

ARQUITECTURA TOPOLOGÍAS DE REDE PROYECTO

1. Arquitectura de dos niveles (2 Tier):

Esta arquitectura de dos niveles o capas, también llamado de núcleo colapsado, donde el Core y el Distribution están combinadas en una única capa

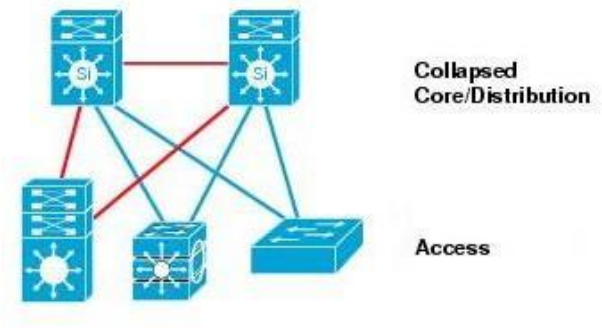


Ilustración 14. Arquitectura de dos niveles

Tomado de https://eclassvirtual.com/arquitectura-de-topologias-de-redes-ccna-200-301/

2. Arquitectura de tres niveles (3 Tier)

Esta arquitectura está compuesta por tres niveles o capas, como se muestra en la siguiente figura:

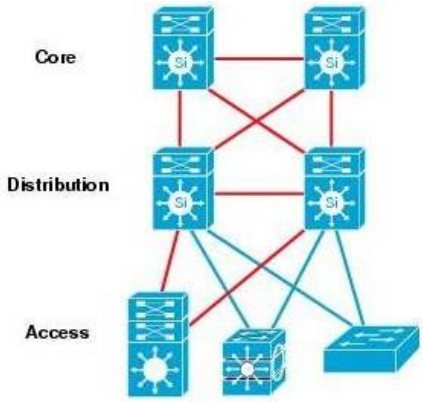


Ilustración 15. Arquitectura de tres niveles

Tomado de Cisco CCNA

En la capa de Acceso es donde los hosts se conectan a la red, como PC, impresoras, cámaras etc. Esta capa de acceso proporciona una separación entre la infraestructura de la red y los dispositivos informáticos que usan la infraestructura de la red. Existe un límite de confianza de seguridad, calidad de servicio y política.

La capa de distribución actúa como un servicio y un límite de control entre la capa de Acceso y la capa de Core, ésta capa sirve para:

- Punto de agregación para todos los conmutadores de acceso
- Proporciona servicios de conectividad y políticas para los flujos de tráfico dentro del bloque de distribución de acceso
- Proporcionar el punto de demarcación de agregación, control de políticas y aislamiento entre el bloque de construcción de distribución del campus y el resto de la red
- La capa de Core es la más simple, pero a la vez la más críticas, entre sus características tenemos:
- Proporciona un conjunto muy limitado de servicios y está diseñado para estar altamente disponible y operar en un modo siempre encendido
- Proporcionar el nivel adecuado de redundancia para permitir una recuperación casi inmediata del flujo de datos en caso de que se produzca un fallo en algún componente

El Core de la red no debe implementar ningún servicio de políticas complejas, ni debe tener conexiones de usuario/servidor conectadas directamente. Dentro de esta arquitectura está la Arquitectura Spine-Leaf

La arquitectura Spine-Leaf (espina-hoja), está pensada para centros de datos debido a su escalabilidad, fiabilidad y un mejor rendimiento, como se muestra en la siguiente figura:

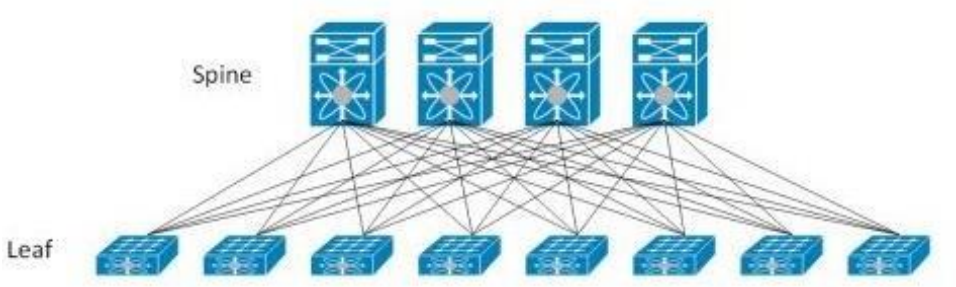


Ilustración 16. Arquitectura Spine-Leaf

Tomado de Cisco CCNA

- La capa superior tiene switches Spine y la capa de abajo tiene switch Leaf
- Los switches Spine son switches de interconexión y los switches Leaf son como los switch de acceso
- Con la configuración Spine-Leaf, todos los dispositivos tienen la misma cantidad de segmentos y contienen una latencia constante y predecible para la información que viaja.
- La capa Leaf consta de switches de acceso que se conectan a dispositivos como servidores, firewalls, balanceadores de carga y enrutadores de borde
- La capa Spine (formada por switches que realizan enrutamiento) es la columna vertebral de la red, donde cada switch Leaf está interconectado con todos y cada uno de los switch Spine.
- En este modelo, sólo hay dos niveles (tiers) de swicthes entre los servidores y core network
- El diseño de leaf-spine tiene la ventaja de colocar cada leaf switch a poca distancia de otro. No hay necesidad de crecer hacia arriba o hacia abajo el «árbol» de diseño. Se mejora la latencia y se minimizan los cuellos de botella.
- Con Spine- Leaf, la red utiliza enrutamiento de capa 3. Todas las rutas se configuran en un estado activo mediante el uso de rutas múltiples de igual costo (ECMP). Esto permite que todas las conexiones se utilicen al mismo tiempo mientras se mantiene estable y evita loops dentro de la red

- La eliminación del protocolo Spanning Tree (STP) ha llevado a una mejora drástica de la estabilidad de la red
- Las redes Spine- Leaf ofrecen muchos beneficios únicos sobre el modelo tradicional de 3 niveles

BGP.

En telecomunicaciones, el protocolo de puerta de enlace de frontera o BGP (del inglés Border Gateway Protocol) es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por ejemplo, los proveedores de servicio registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

Entre los sistemas autónomos de los ISP se intercambian sus tablas de rutas a través del protocolo BGP. Este intercambio de información de encaminamiento se hace entre los routers externos de cada sistema autónomo, los cuales deben ser compatibles con BGP. Se trata del protocolo más utilizado para redes con intención de configurar un protocolo de puerta de enlace exterior (Exterior Gateway Protocol).

La forma de configurar y delimitar la información que contiene e intercambia el protocolo BGP es creando lo que se conoce como sistema autónomo o AS. Cada uno tendrá conexiones o sesiones internas (iBGP), así como sesiones externas (eBGP). es la nueva versión del Internet Protocol (IP) en el cual se sustenta la operación de Internet.

Las características y Atributos de BGP son:

ORIGIN, AS-PATH, NEXT-HOP, MULTI-EXIT-DISCRIMINATOR (MED), LOCAL-PREF, ATOMIC AGGREGATE, COMMUNITY,

Ilustración 17. Enrutamiento BGP con ASN

Tomado de Cisco CCNP

MULTIHOMING EN IPV6.

En este enfoque, la red se conecta a múltiples proveedores y se le asignan múltiples rangos de direcciones, uno para cada proveedor, sucediendo lo mismo para cada proveedor.

Es un procedimiento más barato que multihoming clásico y puede ser utilizado sin cooperación de los proveedores (por ejemplo, en una red doméstica) pero requiere tecnología adicional para realizar el encaminamiento.

Para el tráfico entrante, los anfitriones deben estar asociados con múltiples registros DNS A o AAAA para que sean accesibles a través de todos los proveedores.

Para el tráfico saliente, se debe usar una técnica de enrutamiento específico para enrutar paquetes a través del proveedor correcto y mientras tanto, los hosts deben implementar políticas razonables de selección de direcciones de origen.

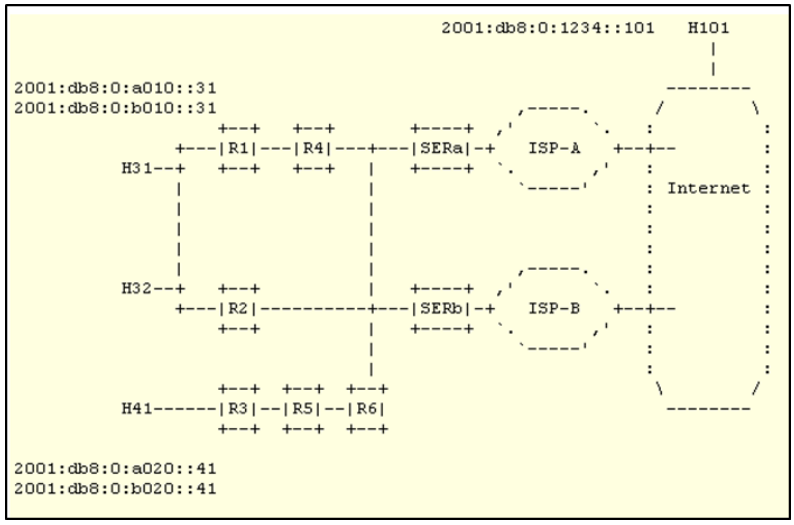


Ilustración 18. Topología Multihoming,

Tomado de https://tools.ietf.org/id/draft-ietf-rtgwg-enterprise-pa-multihoming-12.html

CAPÍTULO 3: METODOLOGÍA DEL PROYECTO

Metodológicamente hablando, este proyecto tiene un diseño de investigación no experimental aplicado, con enfoque mixto, debido a que se identifica y se mide el rendimiento de una Red Corporativa existente en la Corporación Autónoma Regional de Cundinamarca CAR, con relación a la necesidad de adoptar el protocolo IPv6, buscando el fortalecimiento de la infraestructura, como la identificación del agotamiento de direcciones IPv4 públicas, así como la necesidad de garantizar el cumplimiento de la Resolución 2710 de 2017 del MinTIC.

En la investigación no experimental, se observan fenómenos, para luego analizarlos, no se manipulan deliberadamente las variables, como señala Fred Kerlinger (1979, p. 116). "La investigación no experimental o EXPOST-FACTO es cualquier investigación en la que resulta imposible manipular variables o asignar aleatoriamente a los sujetos o a las condiciones".

De hecho, no hay condiciones o estímulos a los cuales se expongan los sujetos del estudio. Los sujetos son observados en su ambiente natural, en su realidad.

En el enfoque mixto se recolecta, analiza y vincula datos de carácter cuantitativo y cualitativo, en una misma investigación para dar respuesta a un problema, permitiendo obtener información que facilita la triangulación para lograr comprensión e interpretación. Hernández Sampieri, Fernández-Collado & Baptista Lucio (2006), señalan que el enfoque mixto va más allá de la simple recolección de datos de diferentes modos sobre el mismo fenómeno, ya que implica desde el planteamiento del problema, mezclar la lógica inductiva y la deductiva, por lo que un estudio mixto debe serlo en el planteamiento del problema, la recolección y análisis de los datos, y en el reporte del estudio.

Las fases metodológicas para el desarrollado de la siguiente propuesta están basadas en los dos escenarios y topologías descritas, teniendo en cuenta aspectos técnicos, operativos, administrativos, optimización de recursos y sobre todo la implementación de mejores prácticas.

FASES DEL PROYECTO.

Fase 0 – Diagnóstico Previo.

Esta fase comprende la recopilación de información dada por los administradores de red de la CAR Cundinamarca, en los cuales enmarca las fallas generales que han sido reportadas en el servicio de comunicaciones LAN sujetos a inconvenientes físicos y lógicos en la actual arquitectura de máscara de red 21. Así mismo, lentitud en la trasmisión de datos.

Esta información se encuentra alojada en la base de datos de la aplicación de la mesa de servicio y en conversaciones a través de correos electrónicos entre los administradores y empresas prestadoras de servicios, motivo por el cual estas evidencias no hacen parte del presente proyecto sujeto a las políticas de seguridad de la información de la corporación.

Fase 1 – Levantamiento de información y planificación.

En la fase inicial de este proyecto se realizará el levantamiento de información de activos tecnológicos, asociados a la infraestructura de telecomunicaciones de la Red Corporativa de la Corporación.

En este levantamiento de información se identificarán las características técnicas enfocadas al soporte de implementación o configuración del protocolo IP en versiones 4 y 6. En dicho informe se identificará la arquitectura actual, como los equipos que asumen el Core de la Red Corporativa para realizar la restructuración topológica de la Red Corporativa, para la ejecución de la segmentación de la red y así mismo, la posterior implementación del DUAL STACK en toda la infraestructura de la Car Cundinamarca.

Adicional se entrega el cronograma detallado de la implementación del protocolo IPv6.

Fase 2 – Diseño de la topología la red modelo TCP/IP

Con el conocimiento adquirido respecto a los componentes tecnológicos de la red de telecomunicaciones de la CAR Cundinamarca, se procede a realizar el despliegue de todo el diseño topológico del proyecto, con todos los componentes

de diseño a nivel lógico y físico, con los documentos de direccionamiento de alto nivel, topología de red, ambiente de pruebas del protocolo IPv6, documento de trámite ante LACNIC de aprobación de asignación del prefijo IPv6 y plan de transición del protocolo IPv4 e IPv6.

Se presentará en el protocolo IPv6 si el acceso de los usuarios corresponde a DHCPv6 en diseño Statefull o Stateless.

Fase 3 – Implementación del diseño planteado

En la fase 3, posterior a la aprobación de la CAR Cundinamarca, del diseño y documentación presentada se procederá a intervenir de manera controlada (controles de cambios firmados), toda la red de telecomunicaciones de la Red Corporativa.

Fase 4 – Pruebas y afinamiento de la solución

Para la fase final del proyecto, se realizará todo lo concerniente a pruebas de funcionalidad de las comunicaciones y aplicaciones de la entidad. En la ejecución de pruebas y monitoreo, se documentará los cambios realizados, si se presentan, en errores o fallas encontradas respecto a la implementación de la restructuración tecnológica de la CAR Cundinamarca.

Se realiza una Check List digital, el cual sea desarrollado por el área TI de la entidad en el cual se identifique si la restructuración e implementación del protocolo IPv6 cumplió con las expectativas, así como haya mejorado el desempeño de la red de telecomunicaciones internas y externas de la entidad.

Por último, se realizará los entregables de documentación de la ejecución del proyecto con manuales, pruebas de servicios, inventarios, planes de direccionamiento y gráficos de las topologías de red.

Resumen

Tabla 1. Resumen Alcance del Proyecto

Fase	Entregable
1	1. Levantamiento de información de la red de la Corporación, resumen.
	1. Plan de diagnóstico que debe contener los siguientes componentes: • Inventario de TI (Hardware y software) de cada Entidad diagnosticada. • Informe de cumplimiento de IPv6 por cada elemento de hardware y software (Red de comunicaciones, sistemas de almacenamiento, sistemas de cómputo, aplicativos, bases de datos, sistemas de seguridad, entre otros) • Informe con el plan de direccionamiento en IPv6
	2. Cronograma de ejecución del proyecto
	3. Informe del plan de proyecto.
2	1. Resumen de diseño topológico
	2. Direccionamiento de alto nivel en redes IPv4 e IPv6
	3. Presentación de plan de ambiente de pruebas.
	4. Documento de Plan de transición.
	5. Documento de justificación adquisición direccionamiento IPv6 ante LACNIC
3	1. Entrega documentos de control de cambios de la implementación del protocolo
	2. Ejecución de la implementación del rediseño de la red corporativa como implementación del protocolo IPv6
	3. Plan detallado de la implementación.
4	1. Ejecución de pruebas de funcionalidad de la Red Corporativa
	2. Acompañamiento de las pruebas de los servicios.
	3. Informe de ajustes de configuraciones
	4. Informe consolidado del proyecto
	5. Cierre del proyecto

CAPÍTULO 4: CRONOGRAMA DE ACTIVIDADES

Para el desarrollo de este proyecto se ha generado un cronograma basado en la ideología de no parar o provocar grandes interrupciones de las actividades de la compañía. Para ello se adjunta la siguiente tabla donde resume las grandes labores y posteriormente se darán detalles de cada una.

Tabla 2. Cronograma general del proyecto por fases.

ACTIVIDAD	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6
Levantamiento de información y creación de plan de trabajo Fase 1						
Diseño de la Topología Fase 2						
Implementación del Diseño Fase 3						
Pruebas y afinamiento de la solución Fase 4						

DETALLE LABORES

Para un detalle de las actividades de restructuración de la red Corporativa de la CAR Cundinamarca, así como posterior implementación del protocolo IPv6 y todo el plan de transición se han estimado la cantidad de días en la siguiente tabla

Tabla 3. Cronograma detalles labores Car Cundinamarca

Nombre de tarea	Duración	Comienzo	Fin
Restructuración y segmentación red ipv4 e implementación IPv6 CAR	180 días	Mes 1	Mes 2
Fase 1- Levantamiento de información y planificación.	60 días	Mes 1	Mes 2
Elaborar y validar el inventario de activos de información de servicios tecnológicos de la Corporación	30 días	Mes 1	Mes 2
Revisar compatibilidad y soporte en IPV6 de los activos de información de IPv6	5 días	Mes 2	
Revisar los equipos de computación y de comunicaciones y validar si soportan IPv6	5 días	Mes 2	

(IPv6-ready o IPv6-web), cuales requieren actualizarse y cuáles no se pueden soportar IPv6.		
Revisar compatibilidad y soporte en IPV6 de los activos de información de IPv6	2 días	Mes 2
Entrega informe de plan de proyecto	2 día	Mes 2
Entrega del inventario de activos.	5 días	Mes 2
Solicitud del segmento de direcciones IPv6 ante LACNIC	5 días	Mes 2
Fase 2- Diseño de la topología de red modelo TCP/IP.	30 días	Mes 3
Elaborar la propuesta de diseño topológico de arquitectura de comunicaciones de la CAR Cundinamarca	25 días	Mes 3
Presentar propuesta de direccionamiento de alto nivel de redes en IPv4 como IPv6 con su segmentación por VLAN.	10 días	Mes 3
Presentar ambientes de pruebas de migración de la red	3 días	Mes 4
Ejecutar pruebas de ambientes de pruebas.	8 días	Mes 4
Entrega de direccionamiento de IPV6 a la CAR, aprobado por LACNIC	1 días	Mes 4
Entrega informe de plan de proyecto, con el diseño técnico de conexión a los usuarios finales.	2 día	Mes 4
Fase 3- Implementación del diseño planteado	30 días	Mes 5
Entrega documentos de control de cambios de la implementación del protocolo	2 días	Mes 5
Implementar la segmentación de redes en VLANs IPv4	3 días	Mes 5
Realizar pruebas de comunicaciones en IPv4	1 día	Mes 5
Habilitar el direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo con el plan de diagnóstico	3 días	Mes 5
Ejecutar la configuración de las pruebas piloto de IPv6, con base en la realización de pruebas en los segmentos de red y VLANs	5 días	Mes 5
Validar la funcionalidad en IPv6 de los siguientes servicios y aplicaciones de la Corporación sobre IPv6	1 día	Mes 5
Informe de la implementación del protocolo de IPv6	5 días	Mes 5

Fase 4- Pruebas y afinamiento de la Solución	30 días	Mes 6
Realizar pruebas de comunicaciones internas en protocolo IPv4 e IPv6	5 días	Mes 6
Realizar las pruebas de funcionalidad del nuevo protocolo frente a las políticas de seguridad perimetral, de servidores de cómputo, servidores de comunicaciones y equipos de comunicaciones y presentar el Informe de las pruebas realizadas	5 días	Mes 6
Informe de ajustes de configuraciones	6 días	Mes 6
Informe consolidado del proyecto	20 días	Mes 6
Cierre del proyecto	1 día	Mes 6

CAPÍTULO 5: RECURSOS NECESARIOS

Habiendo hecho el levantamiento de la información de los activos podemos garantizar que no es requerido la adquisición de nuevos dispositivos.

El resumen de los elementos requeridos se detallan a continuación:

Tabla 4. Presupuesto General.

RECURSO	DESCRIPCIÓN	PRESUPUESTO
Equipo Humano	Dos (2) Ingenieros de Telecomunicaciones, mano de obra	$67.500.000 millones de pesos colombianos por prestación de servicios
Equipos y Software	Adquisición prefija /48 y ASN ante LACNIC.https://www.lacnic.net/solicitar-ip Portátiles de alta gama	El valor del prefijo /48 y ASN: $3.500 dólares por un año.
Viajes y Salidas de Campo	No aplica	$ 0
Materiales y suministros	La implementación sólo requiere de configuraciones y diseños de redes, no comprende consumibles ni elementos de instalación física. La CAR Cundinamarca deberá prestar los servicios de soporte con fabricantes de la infraestructura de redes, seguridad informática y servidores. Los costos de servicios especializados de soporte y acompañamiento serán independientes al presupuesto del actual proyecto.	$ 0
Bibliografía	Ninguna	$ 0
TOTAL, EL PROYECTO CONSTA DE REALIZAR LA TRANSICIÓN Y DIMENSIONAMIENTO, NO LA ADQUISICION DE LA INFRAESTRUCTURA, DE SER REQUERIDA.		

CAPÍTULO 6: DESARROLLO PROYECTO

FASE 1 – LEVANTAMIENTO DE INFORMACIÓN Y PLANIFICACIÓN.

Dentro de esta primera fase se han definido dos procesos paralelos. El primero refiere al levantamiento de inventario de los equipos tecnológicos de la CAR y el segundo a la identificación de la topología de red.

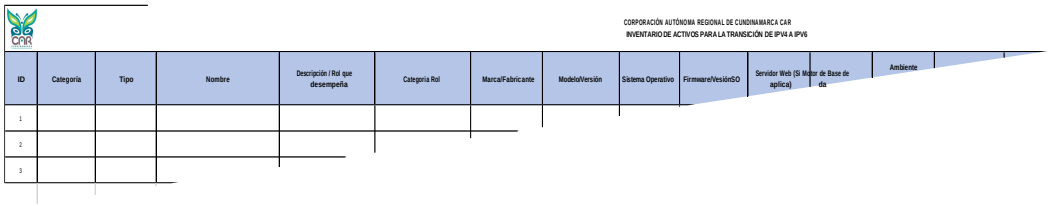
En este proceso de levantamiento de inventario de activos se ha diseñado un archivo el cual nos permita cruzar la data de acuerdo con las necesidades que se vayan presentando, así como al tiempo se pueda identificar los equipos que permiten la implementación del protocolo IPv6.

En la primera hoja se contemplan los siguientes campos y respectivamente se detalla qué valor será alojado y su explicación siendo:

- ID: Refiere a la secuencia de la cantidad de dispositivos
- Categoría: Tipo de dispositivo. Permite seleccionar:
    - Almacenamiento
    - Equipo telefónico
    - Equipos de apoyo:
        - Cámaras de red
        - UPS
    - Equipos de red
        - Access Point
        - Router
        - Switch
    - Equipos de seguridad
        - Firewall
        - WAF Web Application Firewall
        - Analizador de tráfico
    - Servidores
        - Físico
        - Virtual
- Tipo: Pertenece a la subcategoría del campo categoría
- Nombre: Asignación de una descripción que lo identifique en la red
- Descripción / Rol que desempeña: Es una etiqueta que resume su ubicación o función que desempeña
- Categoría/ Rol: Subcategoría del campo Tipo

- Marca Fabricante: Identificación del Proveedor
- Modelo Versión: Descripción o nombre exacto dado por el fabricante
- Sistema Operativo: Fabricante del Software
- Firmware /Versión SO: Identificación de la versión del Sistema Operativo instalado
- Servidor Web (Si aplica)
- Motor de Base de datos (Si aplica)
- Ambiente: Estado de operatividad del dispositivo
    - Producción
    - Pruebas
    - Desarrollo
- Ubicación: Lugar donde reposa el activo
- Dirección IP: Identificación lógica dentro de la topología
- Proveedor: Identificador del Prestador de servicio
- Observaciones: Palabras claves
- Criticidad: Clasificación de importancia del activo de 1 a 5
- Compatible IPv6: Previa validación DataSheet del fabricante
- IPv6 Ready:
    - Si: Dispositivo ya migrado
    - No: Dispositivo sin migrar

Tabla 5. Formato inventario activos CAR



CORPORACIÓN AUTÓNOMA REGIONAL DE CUNDINAMARCA CAR
INVENTARIO DE ACTIVOS PARA LA TRANSICIÓN DE IPV4 A IPV6

ID	Categoria	Tipo	Nombre	Descripción / Rol que desempeña	Categoria Rol	Marca/Fabricante	Modelo/Versión	Sistema Operativo	Firmware/VesiónSO	Servidor Web (Si aplica)	Motor de Base de da	Ambiente
1												
2												
3												

-
-

Otra de las tablas manejadas, será la validación de las referencias, artículos o datasheet de cada sistema Operativo que maneja el dispositivo dadas por el fabricante para su respectivo análisis de los procesos a seguir en caso de requerir compatibilidad o actualización para la migración.

Tabla 6. Documentación Inventario

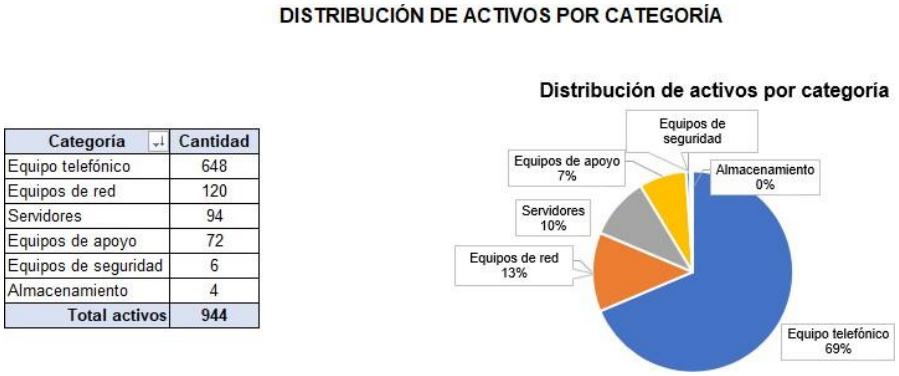
CORPORACIÓN AUTÓNOMA REGIONAL DE CUNDINAMARCA CAR INVENTARIO DE SISTEMAS OPERATIVOS				
ID	Sistema Operativo	Descripción	Compatible IPv6	Referencias

Dado que en el proceso de migración a IPv6, de los dispositivos y servidores, se tendría que actualizar los sistemas operativos, firmware y/o parches de seguridad, se hace necesario la creación de una matriz de riesgo, con tipificación de criticidad según su rol dentro la Red Corporativa de la CAR Cundinamarca, por ello, se indican los ítems mínimos a tener en cuenta dentro de esta matriz de riesgo:

- Identificación del riesgo
- Valoración del riesgo inicial
- Controles existentes
- Valoración del riesgo inherente
- Acciones
- Responsables

Después de haber llenado las respectivas tablas y haber cruzado mediante tablas dinámicas se han generado unas gráficas arrojando los siguientes resultados:

Categorización de activos, por servicios prestados en la Red Corporativa:



Categoría	Cantidad
Equipo telefónico	648
Equipos de red	120
Servidores	94
Equipos de apoyo	72
Equipos de seguridad	6
Almacenamiento	4
Total activos	**944**

Ilustración 19. Distribución de Activos por Categoría

Fuente: Autores

DISTRIBUCIÓN DE ACTIVOS POR TIPO

Tipo de activo	Cantidad
Teléfonos IP	648
Servidor Virtual	64
Access Point	56
Switch	43
Televisor	40
Servidor Físico	30
Cámaras de video	27
Router	21
Firewall	6
UPS	5
SAN	3
Nube	1
Total activos	**944**

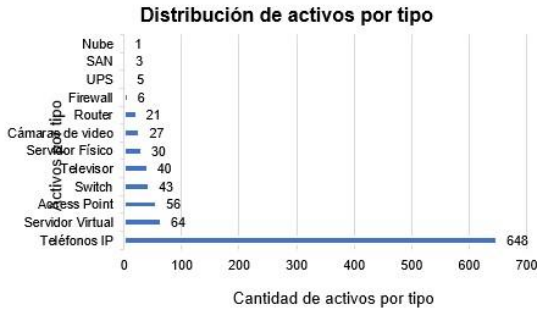


Ilustración 20. Distribución de Activos por Tipo

Fuente: Autores

Resultado de calificación por criticidad de los equipos a intervenir, sujeto a rol dentro de la Red Corporativa:

DISTRIBUCIÓN DE ACTIVOS SEGÚN NIVEL DE CRITICIDAD

Nivel de criticidad del activo	Cantidad
2	689
5	104
3	80
4	58
1	13
Total activos	**944**

Ilustración 21. Distribución de Activos por criticidad

Fuente: Autores

Adicional a la creación de un formato de levantamiento del inventario de activos físicos, se ha creado el de inventario lógico manejado en los dispositivos por categoría, en este formato será almacenada la data de las VLAN y las IPs manejadas por cada uno.

Tabla 7. Formato Inventario Lógico

	CORPORACIÓN AUTÓNOMA REGIONAL DE CUNDINAMARCA CAR INVENTARIO DE VLAN'S				
ID	**VLAN ID**	**Nombre**	**Descripción**	**ID de dispositivo de red**	**Prefijo de red**

A la par de ir llenando el formato de inventario lógico se fue construyendo la topología. Se ha identificado que la red es tipo plana y que la sede Central de la CAR posee una máscara de red 20 (255.255.240.0), lo que indica que podría permitir la conexión de 4096 dispositivos, como adicional se identifica que la red MPLS de sus sedes regionales llega directamente al Switch Core de capa dos de la entidad lo cual trae inconvenientes de saturación de broadcast fuera de ausencia de seguridad.

Para temas de facilidad de comprensión, se ha hecho el diagrama actual de conexión y sobre éste luego se harán cambios requeridos.

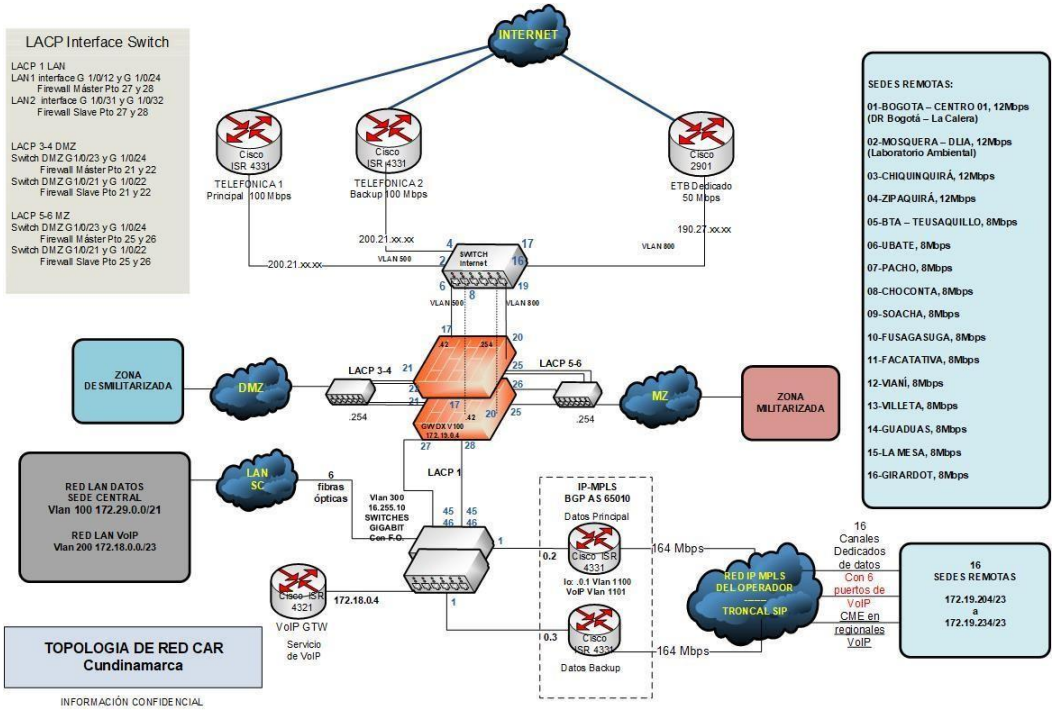


Ilustración 22. Topología Red sin intervenir CAR Cundinamarca

Fuente: Autores

Ahora se adjunta las IPs de Identificación del Core de la red, equipos que asumirán el tráfico pesado de la Red y que tanto en IPv4 como en IPv6 serán el Gateway y router de comunicación a los siguientes saltos:

Tabla 8. Red CORE CAR Cundinamarca

		CORPORACIÓN AUTÓNOMA REGIONAL DE CUNDINAMARCA CAR INVENTARIO DE EQUIPOS MENCIONADOS DENTRO DE LA TOPOLOGÍA. RED CORE	
ID	**Elemento**	**Dirección IPv4**	**VLAN**
1	Switch de Core	172.29.20.1	299
2	Firewall	172.29.20.2	
3	Firewall		
4	Router ETB	190.27.xx. xx/ 29 190.26.xx.xx /29 190.26.xx.xx/29	ETB/ Público
5	CME	172.16.255.17	Telefónica IP
6	Switch de SAN 1	172.23.80.18	6
7	Switch de SAN 2	172.23.80.19	6
8	Router Telefónica Movistar. Principal y respaldo.	200.21.xx.xx/27	Movistar/ Público

Tabla 9. Redes Sedes Regionales MPLS

SEDE REGIONAL	RED	BROADCAST	MASCARA DE RED
Dirección regional sabana occidente	172.19.104.0	172.19.105.255	255.255.254.0
Dirección regional Sumapaz	172.19.106.0	172.19.107.255	255.255.254.0
Dirección regional alto magdalena	172.19.108.0	172.19.109.255	255.255.254.0
Dirección regional Rionegro	172.19.110.0	172.19.111.255	255.255.254.0
Dirección regional Ubaté	172.19.112.0	172.19.113.255	255.255.254.0

Dirección regional Gualivá	172.19.114.0	172.19.115.255	255.255.254.0
Dirección regional sabana centro	172.19.116.0	172.19.117.255	255.255.254.0
Fiab - Teusaquillo	172.19.118.0	172.19.119.255	255.255.254.0
Dirección regional Tequendama	172.19.120.0	172.19.121.255	255.255.254.0
Dirección regional magdalena centro	172.19.122.0	172.19.123.255	255.255.254.0
Dirección regional Soacha	172.19.124.0	172.19.125.255	255.255.254.0
Dirección regional bajo magdalena	172.19.126.0	172.19.127.255	255.255.254.0
Dirección regional almeidas y municipio Guatavita	172.19.128.0	172.19.129.255	255.255.254.0
Dirección regional Chiquinquirá	172.19.130.0	172.19.131.255	255.255.254.0
Dirección regional Bogotá - la calera centro 1	172.19.132.0	172.19.133.255	255.255.254.0
Laboratorio ambiental	172.19.134.0	172.19.135.255	255.255.254.0
CAV Flora	172.19.136.0	172.19.137.255	255.255.254.0

En documentación del inventario, se pudo identificar que la Corporación cuenta con un Firewall Fortinet 1200 D, que es Gateway de enrutamiento de la red plana el cual está configurado con una dirección IP 172.19.0.1/20.

Es de aclarar que la red MPLS de las sedes regionales de la Corporación, también se encuentran llegando al mismo Gateway del Firewall de la LAN de la sede central, lo que indica que el dominio de broadcast y colisiones de la Red se presenta al unir la red LAN tan grande de la sede central, junto con todo el tráfico de red proveniente de la red MPLS.

La Corporación cuenta con un Switch Alcatel Lucent 6900, que está trabajando en modo capa 2, solo permite la conexión de los centros de cableado por fibra óptica, sin ningún tipo de segmentación, todos los hosts sin importar su ubicación ven el mismo Gateway o puerta de enlace en el Firewall.

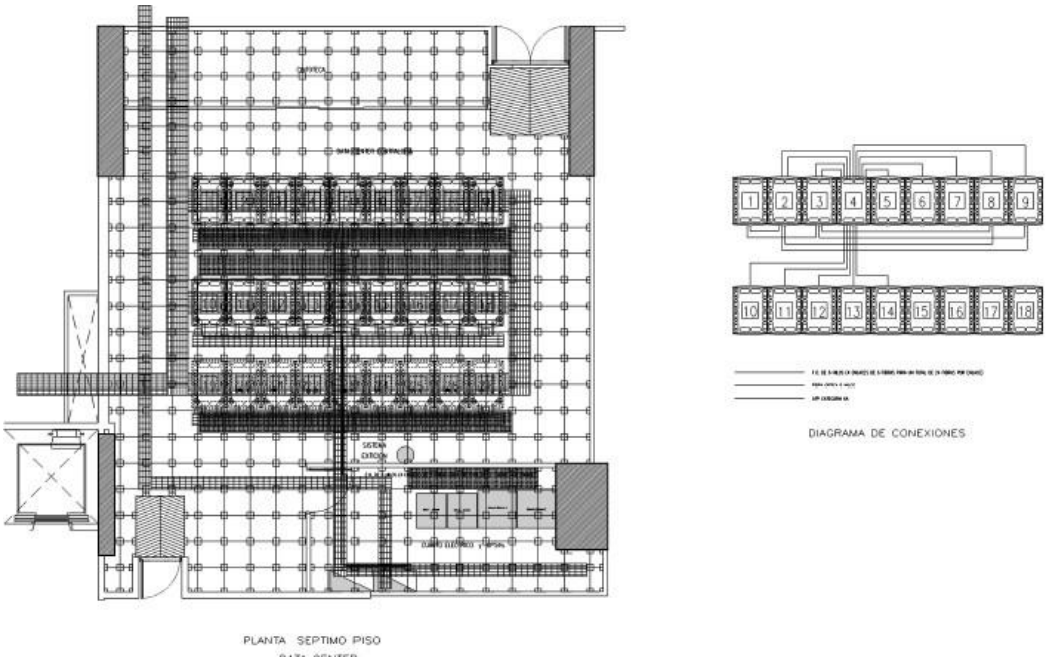
El Firewall aparte de cumplir su función de seguridad perimetral en capa 4, cumple la función de enrutamiento de un Switch de Core de capa3. Indicamos que a nivel de seguridad el Firewall perimetral a nivel de seguridad en una sola zona, interfaz LAN, filtra todo el tráfico de la Red LAN de sede central como redes LAN de la red MPLS, lo cual ocasiona que, si hay tráfico entre la Red LAN y la LAN de una

de las sedes de la MPLS, el tráfico no tendrá ningún tipo de filtrado de seguridad informática.

A nivel general se podría decir que la infraestructura física y las instalaciones tecnológicas manejadas por la CAR soportan la intervención y ejecución de actividades de restructuración a nivel lógica de la Red Corporativa y de telecomunicaciones.

Prueba de ello se adjuntará cada parte física requerida para la implementación, comenzando con un mapa eléctrico de la respectiva distribución por circuito
:

Ilustración 23. Plano Eléctrico



Fuente: CAR

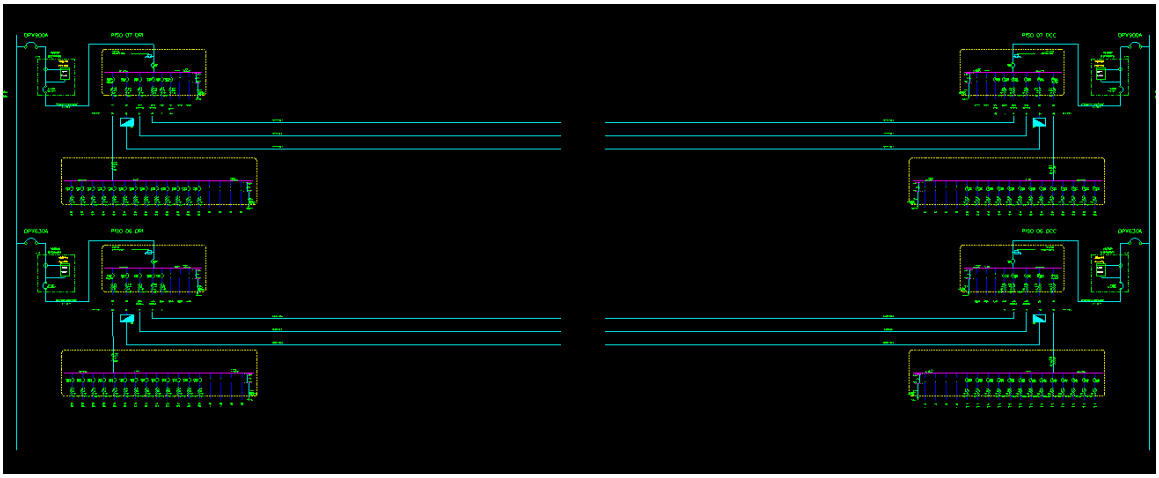


Ilustración 24. Unifilar Blindo barras y UPS

Fuente: CAR

Así mismo en las siguientes dos ilustraciones se presenta el registro fotográfico de los equipos que asumen el rol de Core de la Red Corporativa interno y externo:

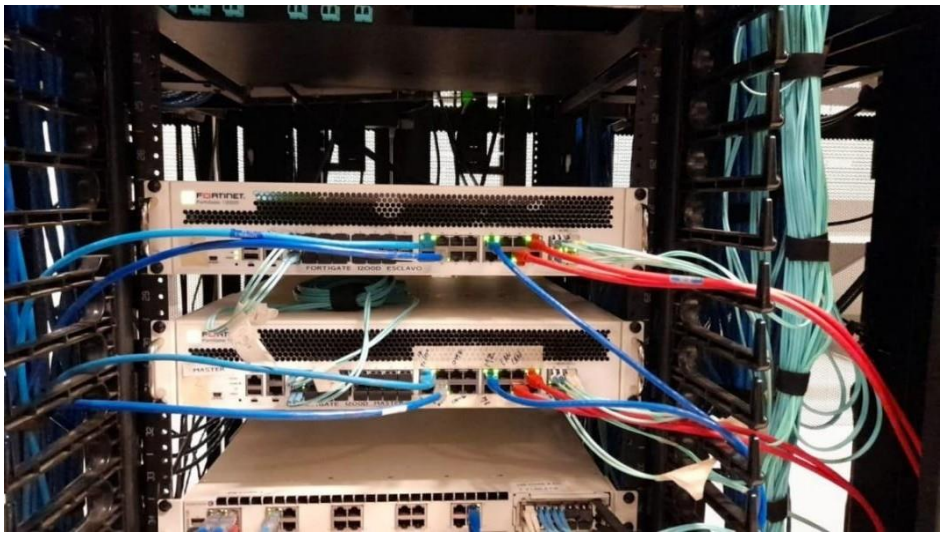


Ilustración 25. Firewall Core FortiGate1200D

Fuente: Autores

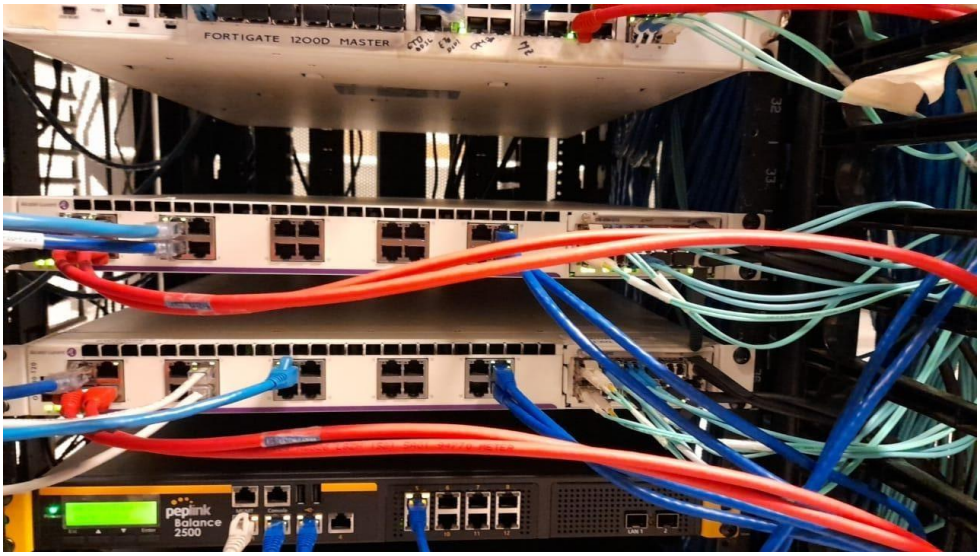


Ilustración 26. Switch Core Alcatel Lucent 6900

Fuente: Autores

Como es recomendado, se maneja elementos de seguridad ante eventos de incendio, siendo el extintor.

Ilustración 27. Extinción Agente Limpio

Fuente: Autores

Adicional, para mitigar el tema de calor se posee el aire a precisión, éste está configurado a 40 toneladas permitiendo que se mantenga una temperatura a un maximo de $20^{o}C$. El aire viaja por las tuberias que estan debajo del piso falso.

Ilustración 28. Aire a precisión

Fuente: Autores

En la siguiente imagen se deja ver de manera central la distribución de cada gabinete rack donde están almacenados la mayoría de los dispositivos de red y servidores.

Ilustración 29. Data center

Fuente: Autores

Respecto a la parte energética, se presenta el registro fotográfico del sistema eléctrico del Datacenter. Su ubicación es en otro cuarto y alejada de los equipos de

cómputo. Se maneja dos tableros y 2 UPS para soportar la carga demandante de los servidores y demás equipos de comunicación.

Ilustración 30. UPS y Tableros eléctricos

Fuente: Autores

Sobre el tema del cableado vertical, se hace uso de cable UTP categoría 6A y fibra multimodo OM3.

Ilustración 31. Centros de cableado

Fuente: Autores

Resumen técnico de la infraestructura:

Se confirma que la infraestructura existente cumple la normatividad indicada a continuación:

- EIA/TIA 942: Proporciona los requisitos y las pautas para el diseño y las consideraciones de instalación de un centro de datos o de una sala de servidores.
- ANSI/TIA/EIA-568-B.1-2, Commercial Building Telecommunications Cabling Standard.
- ANSI/TIA/EIA-568-B.3, Optical Fiber Cabling Components Standard
- ANSI/TIA-569-B, Commercial Building Standard for Telecommunications Pathways and Spaces.
- National Electrical Code (NEC) (NFPA 70 -75), IEEE42.
- ANSI/TIA/EIA-606-A, Administration Standard for Commercial Telecommunications Infrastructure.

Por todo lo anterior se resume que la red de telecomunicaciones cuenta con malla de alta frecuencia en piso, Malla de Faraday en muros y techo. Escalerilla porta cable en piso independiente para red eléctrica regulada, Escalerilla porta cable independiente por encima de los Racks para cableados de comunicaciones, Sistema eléctrico regulado redundante, PDM´s o PDU (Módulos de Distribución de Potencia), UPS´s (Unidades de Potencia On Line doble conversión), TVSS´s (Supresores de Transientes de Voltaje), SPAT (Sistema de Puesta a Tierra) Aislado y de continuidad, Tomas eléctricas de Seguridad para cada Rack. Cableado UTP Cat 6a, Canales de Fibra óptica (10 Gbps), Patch Panel Cat 6a, Switches, Sistema de distribución garantizando los radios de curvatura adecuados, Patch cords certificados de marca Panduit.

El aire a precisión de los centros de cableado cumple las siguientes características, Temperatura entre 20-23 ºC +/-1°C, Rate de Calor Sensible 0.90 - 0.99, Control de Humedad Relativa 45 –50% +/-3%, Trabajo Continuo 24 horas al día, 365 días al año.

Como dato relevante, se indica la capa 3 y puerta de enlace de las comunicaciones LAN serán manejadas en la sede central de la Corporación por el Switch de Core Alcatel Lucent 6900 hacia los hosts (Usuario final). Para los enlaces WAN de telecomunicaciones, la comunicación tanto en IPv4 como IPv6 será maneja por el Firewall Perimetral de la entidad Fortinet 1200 D.

Para las sedes regionales los Routers cisco de serie 2900 suministrados por el operador de servicio Telefónica Movistar, quienes manejan las capas 3 se mantendrán tanto en IPv4 como en IPv6.

Para dar una conocimiento más técnico y preciso de las características de cada uno de los elementos principales de la red, se relacionan los links del DataSheet:

- https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_1200D.pdf
- https://www.al-enterprise.com/-/media/assets/internet/documents/omniswitch-6900-stackable-lan-switches-datasheet-es.pdf
- https://www.cisco.com/c/dam/global/es_mx/assets/docs/pdf/2900_data_sheet_c78_553896.pdf

FASE 2 – DISEÑO DE LA TOPOLOGÍA RED MODELO TCP/IP.

Resumen Del Diseño Topológico

De acuerdo con las condiciones actuales de la infraestructura tecnológica de la Corporación Autónoma Regional de Cundinamarca y acorde con los lineamientos definidos por el Ministerio de Tecnologías la Información y las Comunicaciones, el mecanismo de transición recomendado es “Doble Pila (Dual Stack)”, dado que éste provee las opciones para la coexistencia entre el protocolo IPv4 y protocolo IPv6, permitiendo la desactivación progresiva del protocolo IPv4.

Se procederá a indicar la restructuración lógica y física a realizar, dando inicio con la segmentación de la red IPv4 de la sede central de la CAR por ubicaciones geográficas de cada centro de cableado, en razón a que la CAR, en su sede central tiene 6 centros de cableado.

En cada uno de estos centros no es requerido tantos puntos de red ya que la necesidad máxima es de 260 puntos y por ello se plantea tener una máscara de red /23 la cual nos brinda una capacidad de 512 usuarios.

A continuación, se indica el direccionamiento asignado por centro cableado, como la creación de 3 redes WiFi, identificado por su ID de VLAN:

Tabla 10. Direccionamiento IPv4 Sede Central

SEDE CENTRAL RED CAR CUNDINAMARCA	Bogotá	Impresoras 108	172.29.0.0	255.255.255.128
	Bogotá	Financiera 109	172.29.0.128	255.255.255.192
	Bogotá	Seguridad 110	172.29.6.0	255.255.255.224
	Bogotá	WIFI-FUNCION 402	172.29.16.0	255.255.252.0
	Bogotá	WIFI-INVITADOS 410	172.29.36.0	255.255.254.0
	Bogotá	RED PESCAR PISO 6° 111	172.29.34.0	255.255.254.0
	Bogotá	CORE-FW 299	172.29.20.0	255.255.255.252
	Bogotá	SWMGMT 300	172.29.20.64	255.255.255.192
	Bogotá	APMGMT 301	172.29.20.128	255.255.255.128
	Bogotá	CC1 102	172.29.22.0	255.255.254.0
	Bogotá	CC2 103	172.29.24.0	255.255.254.0
	Bogotá	CC3 104	172.29.26.0	255.255.254.0
	Bogotá	CC4 105	172.29.28.0	255.255.254.0
	Bogotá	CC5 106	172.29.30.0	255.255.254.0
	Bogotá	CC6 107	172.29.32.0	255.255.254.0
	Bogotá	VLAN 502 MZ	172.29.200.0	255.255.255.0
	Bogotá	VLAN 501 DMZ	192.168.2.0	255.255.255.0
	Bogotá	VLAN 299 FW CORE	172.29.20.0	255.255.255.252

El Gateway de la red LAN de la sede central, será asumido por el Switch de Core Alcatel Lucent 6900. En este equipo se crearán todas las subinterfaces de red con el respectivo de ID de VLAN, de modo que el trabajo de enrutamiento es asumido por el equipo de capa 3.

Entre el Switch de Core y el Firewall se creará una red de capa 3 con mascará 30, de modo que todo el tráfico de capa 3 será entregado por el Switch al Firewall, y en viceversa el Firewall devolverá todo el tráfico simétrico al Switch para así conocer las IPv4 de cada host dentro de la red LAN. La VLAN 299 será la que trabaje con interfaces de capa 3 para el enrutamiento de este tráfico.

La asignación del direccionamiento IPv4 de los usuarios estará sujeto a la implementación de servidores DHCP, en el cual el servidor será ubicado en la zona de servidores MZ, por lo tanto, se deberá implementar en la Interfaz LAN del Firewall el servicio de RELAY IP HELPER en IPv4.

A nivel del Firewall perimetral, se procederá a crear políticas por subredes definidas en la tabla anterior. A nivel de UTM, se crearán políticas que permitan aplicar filtrados WEB, perfiles IPS, según el administrador de seguridad del Firewall y el administrador del servidor de dominio consideren dar permisos de accesos a las redes internas y externas.

A nivel de la Red MPLS, se realizará la separación de la integración de esta red de datos a la sede central, creando en una Interfaz del Firewall una zona denominada como MPLS. A dicha Red, se asignará una VLAN 500 cuya red 192.168.40.0/29 se verá dentro del router de MPLS con el Firewall de la sede central de la CAR Cundinamarca.

A nivel del Firewall perimetral se replicarán los mismos perfiles de navegación creados para las subredes de la sede central.

Posterior a confirmar estabilidad de la segmentación de red en IPv4 de la sede central, se procederá a implementar el protocolo IPv6.

Para la implementación del protocolo IPv6, se asignará el mismo número de subredes sujetos al mismo ID de VLAN ya creadas y configuradas, con direccionamiento segmentado del prefijo IPv6 asignado por LACNIC a la Corporación:

Partimos del prefijo oficial asignado:
2801:001D:0800::/48
Estos primeros 48 bits son inmodificables para la red de la Corporación.
Comenzamos a trabajar con los bits 49 y siguientes hacia la derecha.
Tenemos requerimiento MACRO de tres superedes, por lo tanto aproximamos 2^n y obtenemos 2^2 = 4 superedes:

Bit	49	50	51	52	Hexadecimal	USO
	0	0	0	0	0	Servidores (DMZ & MZ)
	0	1	0	0	4	LAN Sede Central
	1	0	0	0	8	LAN Sedes Remotas (MPLS)
	1	1	0	0	C	Reservada (uso futuro)

Ilustración 32 Segmentación del prefijo General

Fuente: Autores

El direccionamiento de cada subred IPv6 se especifica en la siguiente tabla

Tabla 11. Direccionamiento IPv6 Sede Central LAN

49	50	51	52	53	54	55	56	Hexadecimal	USO	Dirección IPv6 completa a asignar
0	1	0	0	0	0	0	0	40	Impresoras	2801:001D:0800:4000::/64
0	1	0	0	0	1	0	0	44	Financiera	2801:001D:0800:4400::/64
0	1	0	0	0	1	1	0	46	PTP FW Y Switch CORE VLAN 299	2801:001D:0800:4600::/64
0	1	0	0	1	0	0	0	48	MGMT Switch VLAN 300	2801:001D:0800:4800::/64
0	1	0	0	1	0	1	0	4A	MGMT Access Point VLAN 301	2801:001D:0800:4A00::/64
0	1	0	0	1	1	0	0	4C	Piso 4 Centro	2801:001D:0800:4C00::/64
0	1	0	0	1	1	0	1	4D	Piso 4 Oeste	2801:001D:0800:4D00::/64
0	1	0	0	1	1	1	0	4E	Piso 4 Este	2801:001D:0800:4E00::/64
0	1	0	1	0	0	0	0	50	WLAN Funcionarios	2801:001D:0800:5000::/64
0	1	0	1	0	1	0	0	54	WLAN Visitantes	2801:001D:0800:5400::/64
0	1	0	1	1	1	0	0	5C	Piso 5 Centro	2801:001D:0800:5C00::/64
0	1	0	1	1	1	0	1	5D	Piso 5 Oeste	2801:001D:0800:5D00::/64
0	1	0	1	1	1	1	0	5E	Piso 5 Este	2801:001D:0800:5E00::/64
0	1	1	0	1	1	0	0	6C	Piso 6 Centro	2801:001D:0800:6C00::/64
0	1	1	0	1	1	0	1	6D	Piso 6 Oeste	2801:001D:0800:6D00::/64
0	1	1	0	1	1	1	0	6E	Piso 6 Este	2801:001D:0800:6E00::/64
0	1	1	1	0	1	1	1	77	Aplicativo empresa vigilancia	2801:001D:0800:7700::/64
0	1	1	1	1	1	0	0	7C	Piso 7 Centro	2801:001D:0800:7C00::/64
0	1	1	1	1	1	0	1	7D	Piso 7 Oeste	2801:001D:0800:7D00::/64
0	1	1	1	1	1	1	0	7E	Piso 7 Este	2801:001D:0800:7E00::/64

Así mismo por motivos de seguridad y diferente locación, se asigna una segmentación IPv6 diferente para los servidores y sedes regionales las cuales se plasman en las siguientes dos tablas.

Tabla 12. Direccionamiento IPv6 Sede central Servidores

49	50	51	52	53	54	55	56	Hexadecima	USO	Dirección IPv6 completa a asignar
0	0	0	0	0	0	0	0	00	Servidores DMZ	2801:001D:0800:0000::/64
0	0	0	1	0	0	0	0	10	Servidores MZ	2801:001D:0800:1000::/64

Tabla 13. Direccionamiento IPv6 Sedes Regionales

49	50	51	52	53	54	55	56	Hexadecimal	USO	Dirección IPv6 completa a asignar
1	0	0	0	0	0	0	0	80	Bogotá – La Calera	2801:001D:0800:8000::/64
1	0	0	0	0	0	0	1	81	Bogotá – Teusaquillo	2801:001D:0800:8100::/64
1	0	0	0	0	0	1	0	82	Bogotá – PTAR Salitre	2801:001D:0800:8200::/64
1	0	0	0	0	0	1	1	83	Bogotá – Reserva1	2801:001D:0800:8300::/64
1	0	0	0	0	1	0	0	84	Bogotá – Reserva2	2801:001D:0800:8400::/64
1	0	0	0	0	1	0	1	85	Bogotá – Reserva3	2801:001D:0800:8500::/64
1	0	0	0	0	1	1	0	86	Chiquinquirá	2801:001D:0800:8600::/64
1	0	0	0	0	1	1	1	87	Chocontá	2801:001D:0800:8700::/64
1	0	0	0	1	0	0	0	88	Facatativá	2801:001D:0800:8800::/64
1	0	0	0	1	0	0	1	89	Fusagasugá	2801:001D:0800:8900::/64
1	0	0	0	1	0	1	0	8A	Girardot	2801:001D:0800:8A00::/64
1	0	0	0	1	0	1	1	8B	Guaduas	2801:001D:0800:8B00::/64

1	0	0	0	1	1	0	0	8C	La Mesa	2801:001D:0800:8C00::/64
1	0	0	0	1	1	0	1	8D	Mosquera – LAN	2801:001D:0800:8D00::/64
1	0	0	0	1	1	1	0	8E	Mosquera – Servidores	2801:001D:0800:8E00::/64
1	0	0	0	1	1	1	1	8F	Mosquera - LAB WAN FW A Router	2801:001D:0800:8F00::/64
1	0	0	1	0	0	0	0	90	Pacho	2801:001D:0800:9000::/64
1	0	0	1	0	0	0	1	91	Rio Bogotá - Uni Sabana	2801:001D:0800:9100::/64
1	0	0	1	0	0	1	0	92	Rio Bogotá - Red Norte	2801:001D:0800:9200::/64
1	0	0	1	0	0	1	1	93	Rio Bogotá - Arrecife	2801:001D:0800:9300::/64
1	0	0	1	0	1	0	0	94	Rio Bogotá - Zona Franca	2801:001D:0800:9400::/64
1	0	0	1	0	1	0	1	95	Rio Bogotá - Red Sur	2801:001D:0800:9500::/64
1	0	0	1	0	1	1	0	96	Soacha	2801:001D:0800:9600::/64
1	0	0	1	0	1	1	1	97	Ubaté	2801:001D:0800:9700::/64
1	0	0	1	1	0	0	0	98	Vianí	2801:001D:0800:9800::/64
1	0	0	1	1	0	0	1	99	Villeta	2801:001D:0800:9900::/64
1	0	0	1	1	0	1	0	9A	Zipaquirá	2801:001D:0800:9A00::/64
1	0	0	1	1	0	1	1	9B	Reserva Sede Remota 01	2801:001D:0800:9B00::/64
1	0	0	1	1	1	0	0	9C	Reserva Sede Remota 02	2801:001D:0800:9C00::/64
1	0	0	1	1	1	0	1	9D	Reserva Sede Remota 03	2801:001D:0800:9D00::/64
1	0	0	1	1	1	1	0	9E	Reserva Sede Remota 04	2801:001D:0800:9E00::/64

Se resalta que, para una mejor administración centralizada o remota, los dispositivos que presten algún servicio, por ejemplo, las impresoras o servidores, les será configurado el direccionamiento estático, tanto en IPv4 como IPv6.

Los Host de usuarios deberán recibir la dirección IPv6 por servidor DHCPv6, siendo necesario habilitar en la interfaz de LAN del Firewall el servicio activo de DHCPv6 RELAY homologo al IP HELPER de IPv4.

La CAR cuenta con dos proveedores de Internet, por lo tanto, se debe tener en cuenta que la publicación del prefijo IPv6 junto al ASN de la Corporación, deberá ser implementado en topología WAN de Multihoming en IPv6, sujeto al uso de atributos de BGP que garanticen que por los canales de Telefónica Movistar como ETB se establezca la salida a Internet y que los saltos de retorno de las solicitudes a Internet garanticen la estabilidad de la comunicación, siendo un tráfico asimétrico.

A continuación, se presenta el diseño topológico propuesto para la segmentación de la red en el protocolo IPv4, así como la transición y adopción del protocolo IPv6 en la Red Corporativa de la entidad:

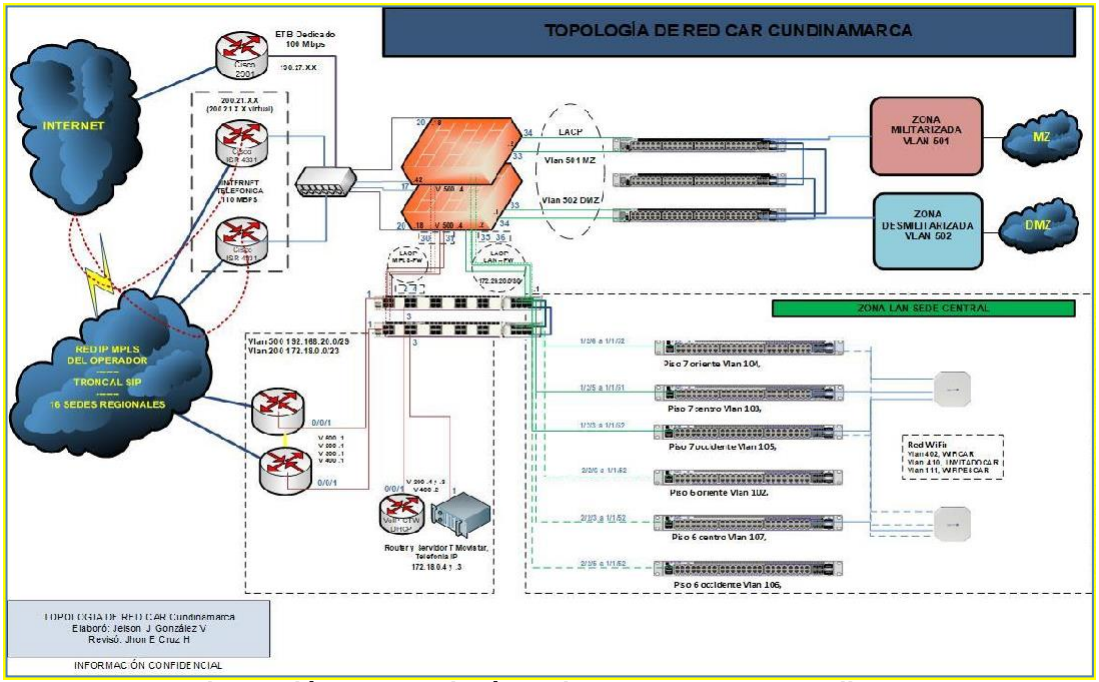


Ilustración 33. Topología Red Propuesta CAR Cundinamarca

Fuente: Autores

Creación Ambiente de Pruebas Implementación Protocolo IPv6

A continuación, se presenta el diseño de la zona controlada de pruebas para la transición de IPv4 a IPv6, se realizó un laboratorio virtual mediante el Software VMware, donde se implementó una solución de un servidor que emula la infraestructura y red actual de la CAR de sus servicios de DNS (Sistema de nombres de dominio) DHCP (Protocolo de configuración dinámica de host).

Así mismo se implementa en un Switch físico de capa 3 una VLAN 601 con direccionamiento en IPv6, en el cual se conecta un equipo de cómputo físico para recibir una dirección dinámicamente por DHCPv6 del servidor.

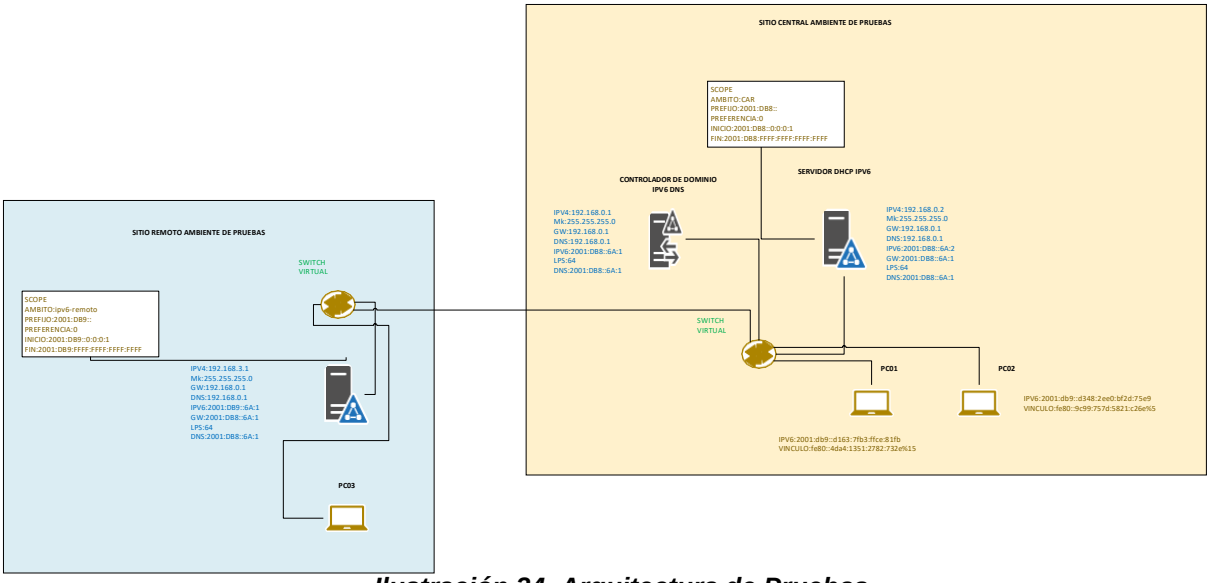


Ilustración 34. Arquitectura de Pruebas

Fuente: Autores

Para este ambiente de pruebas, se subdividió el direccionamiento como si se estuviera trabajando desde la sede principal o desde cualquier otra parte. En las siguientes dos tablas se detalla las IPs usadas y los sistemas operativos montados.

Tabla 14. Emulación Direccionamiento Servidores Prueba Sede central Bogotá

ROL	RAM	O.S	IPV4	IPV6
DC	4 GB	W 2012 R2	192.168.0.1	2001:DB8::6A:1
DHCP	4 GB	W 2012 R2	192.168.0.2	2001:DB8::6A:2
PC01	2 GB	W 10 PRO	N/A	2001:db9::d163:7fb3:ffce:81fb
PC02	2 GB	W 10 PRO	N/A	2001:db9::d348:2ee0:bf2d:75e9

Emula cualquier punto a comunicarse:

Tabla 15. Emulación Direccionamiento Pruebas

ROL	RAM	O.S	IPV4	IPV6
DC y DHCP	4 GB	W 2012 R2	192.168.3.1	2001:DB9::6A:1
PC01	2 GB	W 10 PRO	N/A	2001:db9::7514:5eb6:600:b3d

A continuación, se presenta las configuraciones que se aplicaron para el desarrollo del laboratorio de pruebas para los servicios de DNS, DHCP y la asignación dinámica del direccionamiento a una estación de trabajo.

Comenzamos con la configuración de una dirección IPv6 estática equipo cliente:

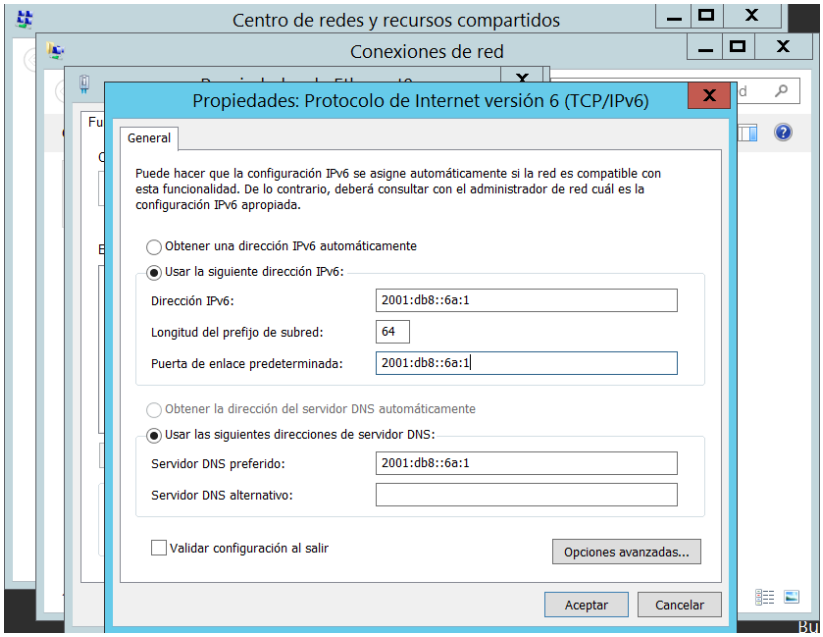


Ilustración 35.Parámetros de Red estación de trabajo

Fuente: Autores

Seguimos con la evidencia de la Configuración de zona inversa del servidor DNS de pruebas:

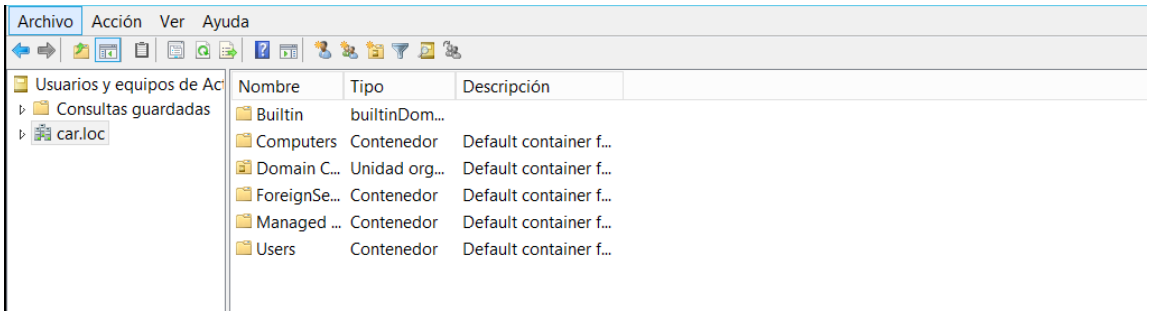


Ilustración 36. Implementación de zona inversa DNS

Fuente: Autores

Y finalizamos con la evidencia de la creación y configuración del servicio ámbito o SCOPE, DHCPv6 de pruebas, con el objeto de confirmar la viabilidad del servidor DHCPv6 en modo STATEFUL, con la asignación dinámica de información de dirección IP y DNS de resolución de nombres:

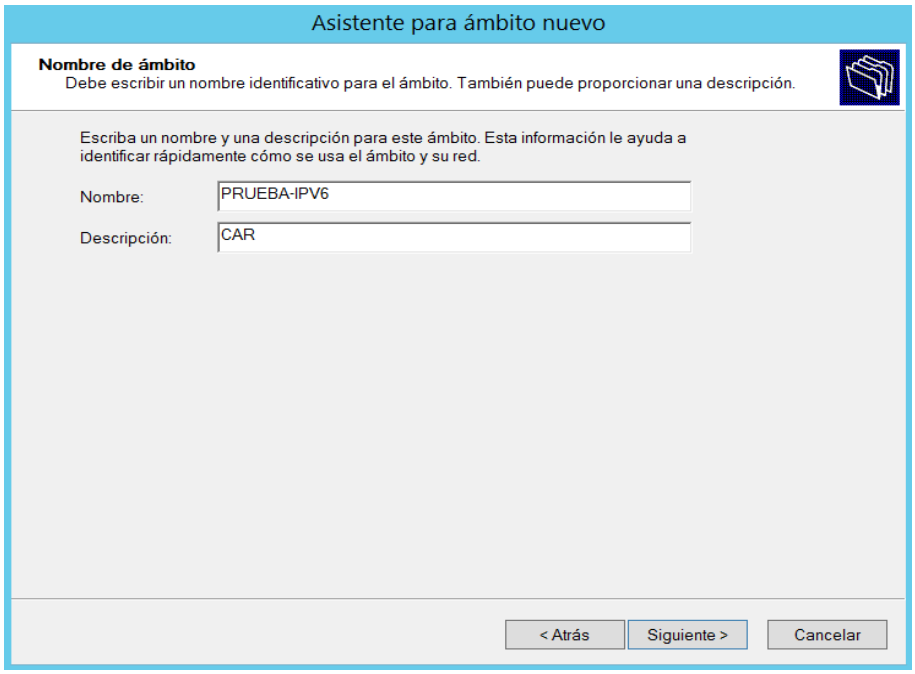


Ilustración 37. Configuración de servicio de DHCPv6

Fuente: Autores

Posterior a la creación y configuración de los servidos DNS y DHCP en el ambiente de pruebas, se verifica la correcta resolución por nombre en el servidor de pruebas:

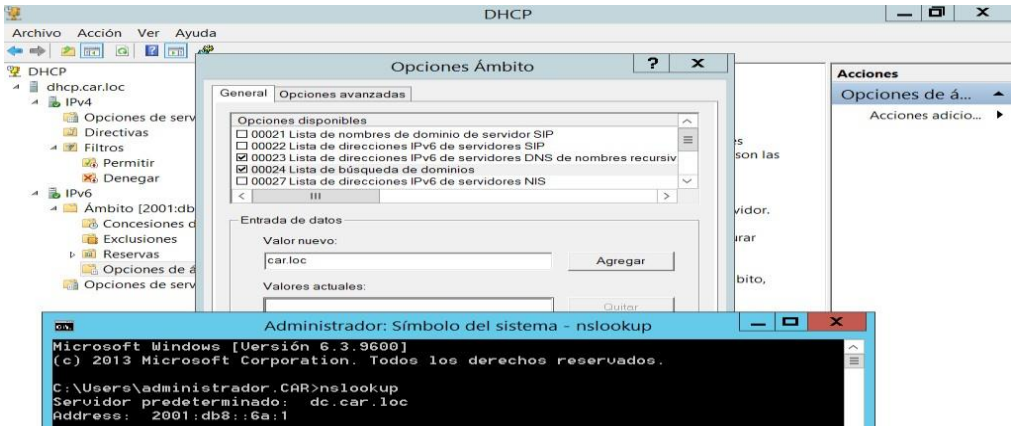


Ilustración 38. Se verificar la Resolución DNS servidor de pruebas

Fuente: Autores

Al verificar el estado UP de los servicios del Servidor de pruebas, ahora toca crear una VLAN de pruebas (Vlan 601) que comunicará la capa de red y capa de acceso en el Switch. Para este proceso se deben igresar los siguientes comandos:

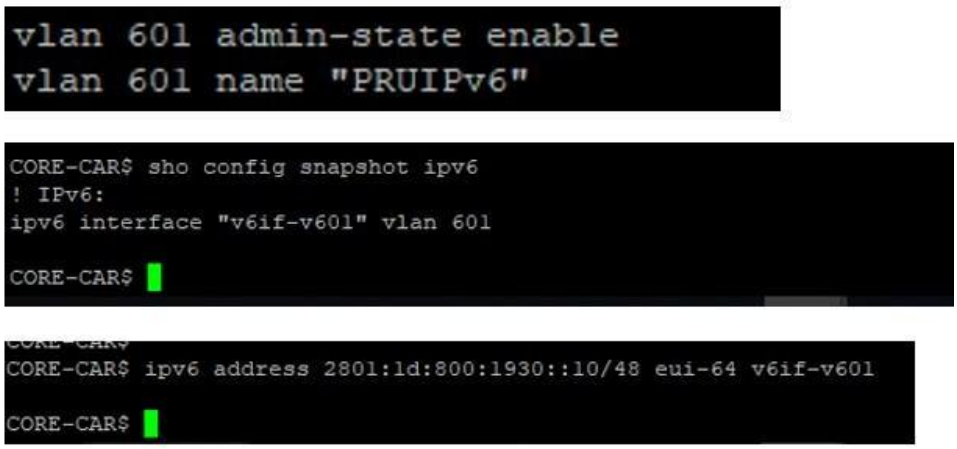


Ilustración 39. Creación de VLAN de pruebas "VLAN 601

Fuente: Autores

Una vez habilitada la comunicación de red entre el Servidor de Pruebas y la terminal de cliente, las siguientes 2 imágens mostrarían que se ha brindado un direccionamiento por parte del servidor el cual ha tomado la PC

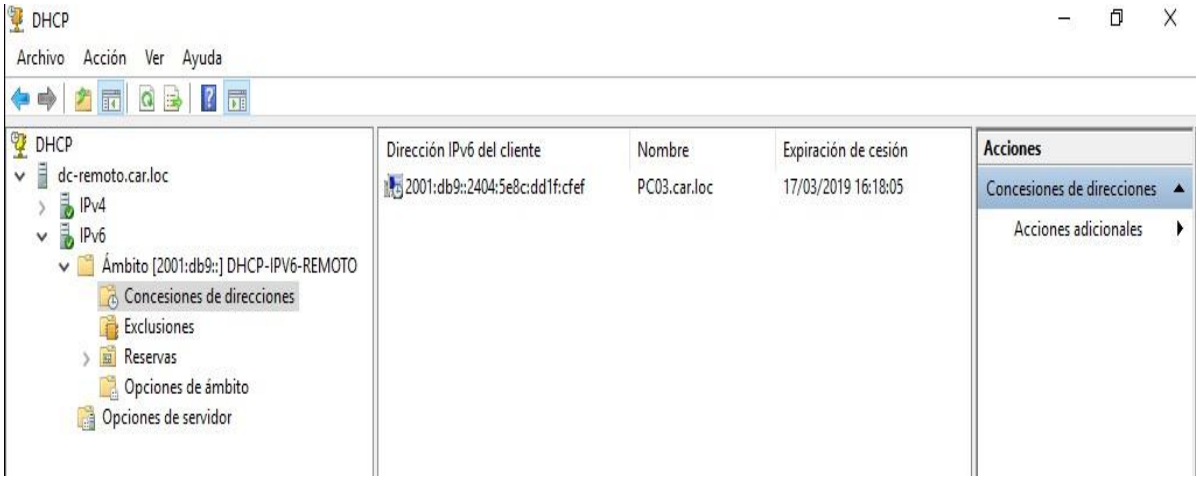


Ilustración 40. Servidor Leases DHCPv6

Fuente: Autores

```
Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . : CAR.LOC
   Descripción . . . . . . . . . . . . . . . : Intel(R) Ethernet Connection I217-LM
   Dirección física. . . . . . . . . . . . . : 54-EE-75-19-94-FA
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Dirección IPv6 . . . . . . . . . . . : 2801:1d:800:1930:5ba:dee:fe22:a665(Preferido)
   Concesión obtenida. . . . . . . . . . . . : viernes, 12 de abril de 2019 3:19:48 p. m.
   La concesión expira . . . . . . . . . . . : miércoles, 24 de abril de 2019 3:19:48 p. m.
   Vínculo: dirección IPv6 local. . . : fe80::9942:a9b:e89a:9d0%21(Preferido)
   Puerta de enlace predeterminada . . . . . : fe80::2efa:a2ff:feaa:4355%21
   IAID DHCPv6 . . . . . . . . . . . . . . . : 257224309
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-24-23-08-94-54-EE-75-19-94-FA
   Servidores DNS. . . . . . . . . . . . . . : 2801:1d:800:1930::10
   NetBIOS sobre TCP/IP. . . . . . . . . . . : deshabilitado
   Lista de búsqueda de sufijos DNS específicos de conexión:
                                       CAR.LOC
```

Ilustración 41. Toma de direccionamiento de prueba

Fuente: Autores

Ya que la PC de pruebas posee direccionamiento de la CAR, lo podemos ingresar al dominidio de red, y aún así demostrar que hay conectividad con todos los demas dispositivos:

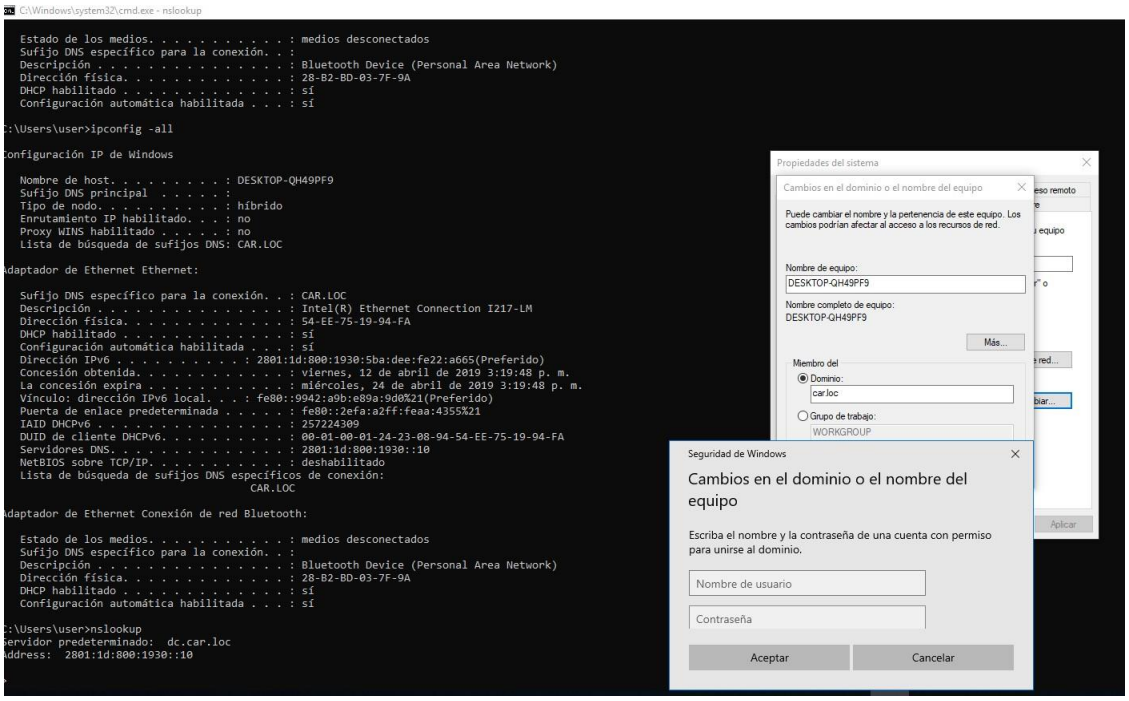


Ilustración 42. Servidor DNS y controlador de Dominio 100% funcional

Fuente: Autores

Otra manera de probar el funcionamiento de comunicación TCP/IP, es mediante la captura de tráfico hechas al servicio DHCPv6 con banderas, éstas capturas fueron realizadas mediante la ayuda del software Wireshark:

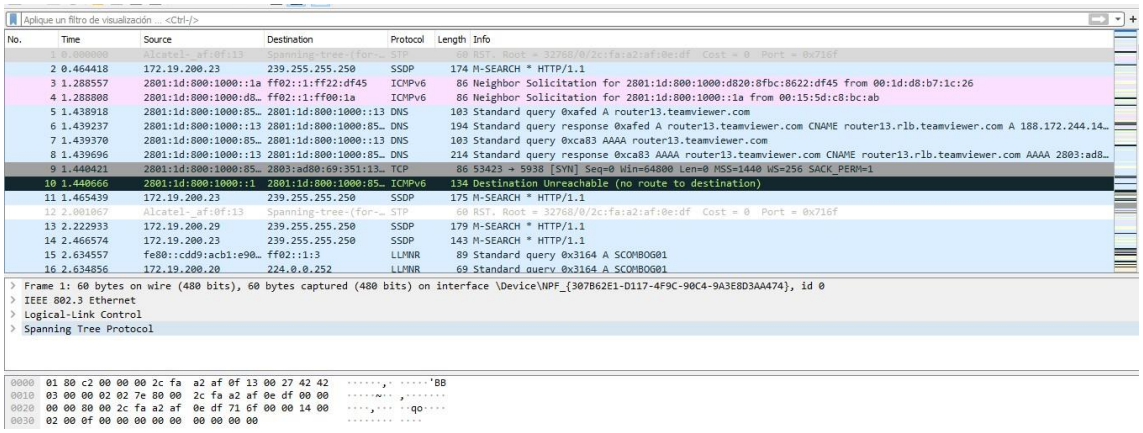


Ilustración 43. Captura tráfico desde el sniffer

Fuente: Autores

FASE 3 – IMPLEMENTACIÓN DEL DISEÑO PLANTEADO.

Una vez presentada la topología de red y los resultados exitosos en el ambiente de pruebas, se procede a ejecutar la implementación.

Dentro del cronograma se habían definido todas las labores a realizar. A nivel técnico la primera actividad es la segmentación de la capa de red en el protocolo IPv4. En este instante se procederá a la configuración de las subredes virtuales (VLAN) asignadas por cada centro de cableado, redes de servidores, e interfaces de capa 3 existentes como la VLAN 299 entre el Firewall y el Switch de la Red LAN de la sede central y La VLAN 500 entre el Firewall y el router central de la Red MPLS de todas las sedes regionales.

La Intervención del Core de toda la Red, el Firewall FortiGate 1200D, se sujeta a la configuración necesaria de interfaces o zonas de Firewall, con sus respectivas políticas de enrutamiento, enrutamiento estático y posterior implementación de políticas de permisos de comunicación entre zonas del Firewall, por políticas de permisos de todos los servicios, como políticas definidas por servicios específicos que garanticen la comunicación segura en toda la Red Corporativa de la CAR Cundinamarca.

El Firewall FortiGate 1200D asume todo el eje central de las comunicaciones internas y externas, y en el actual diseño manejará solo enrutamiento estático tanto para las redes locales red LAN sede central respecto a la comunicación desde LAN a servidores y viceversa, como la comunicación desde LAN a la zona de Internet y viceversa, y la comunicación de la zona LAN hacia las sedes regionales en la Red MPLS.

A continuación, se presenta la separación de las interfaces a nivel del Firewall FortiGate 1200D:

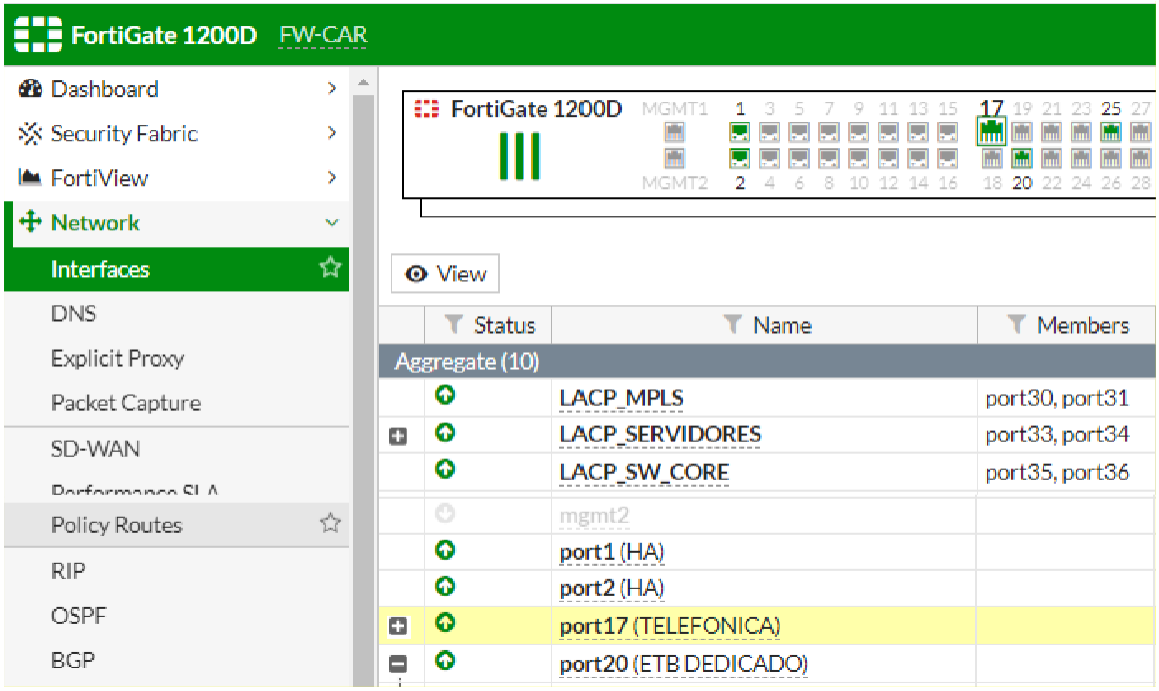


Ilustración 44. Segmentación interfaces FW

Fuente: Autores

Posterior a la intervención en el Firewall, se sigue con la creación de las subinterfaces lógicas de la red LAN de la sede central dentro del Switch Core, cada una de estas representa la segmentación de la Red en IPv4:

```
ip interface "core-fw" addr
ip interface "mgmt" address
ip interface "CC1" address
ip interface "CC2" address
ip interface "CC3" address
ip interface "CC4" address
ip interface "CC5" address
ip interface "CC6" address
ip interface "VISITANTES" a
ip interface "FUNCIONARIOS"
ip interface "IMPRESORAS" a
ip interface "Financiera" a
ip interface "apmgmt" addre
ip interface "backbone" ifi
ip interface "ESeguridad" a
ip interface "WiFiPESCAR" a
```

Ilustración 45. Creación subinterfaces para IPv4

Fuente: Autores

Finalizadas las configuraciones de capa de red, se ejecutan pruebas de conectividad:

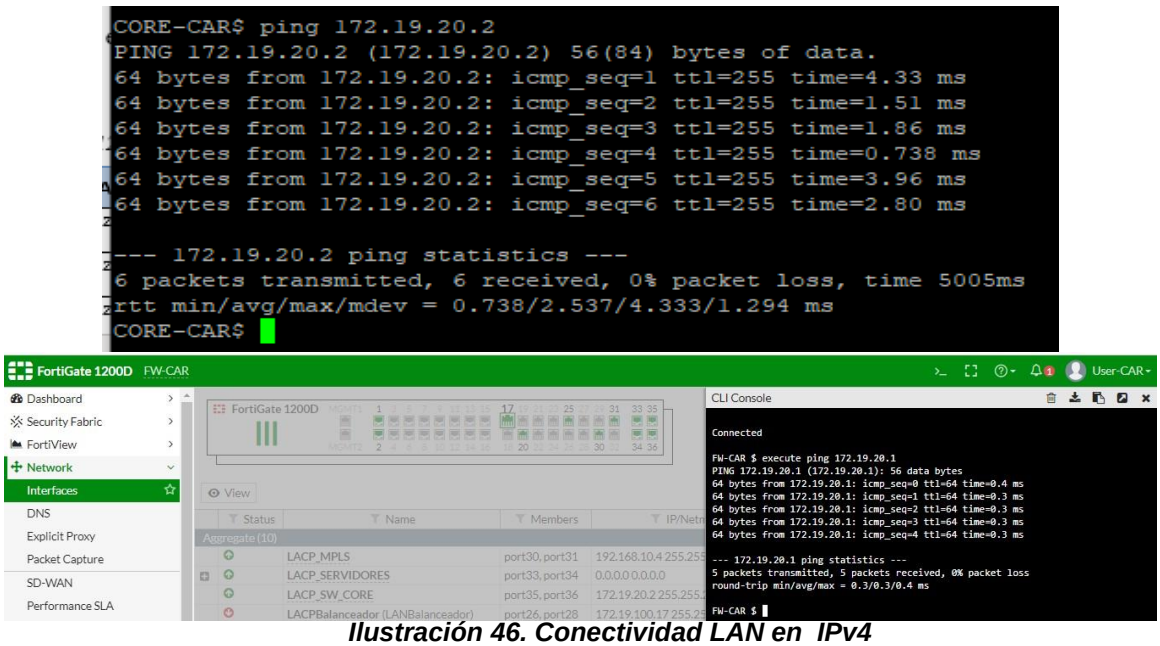


Ilustración 46. Conectividad LAN en IPv4

Fuente: Autores

Al confirmar que la comunicación de los servicios presenta estabilidad, y que la segmentación de la capa de red en IPv4, con las subredes virtuales, no presenta inconvenientes, se procede a ejecutar la transición y adopción del protocolo IPv6, con el objetivo de alcanzar una red Dual Stack, conforme a los requerimientos impartidos por el MinTIC a las entidades públicas.

Seguidamente se presenta un resumen de la implementación de protocolo IPv6 en el Firewall Core, intervención que obedece a la primera fase de intervención de la plataforma tecnológica. Se aclara que en este caso sólo se habilita el protocolo IPv6 y éste se configura sobre las interfaces existentes, ya que la implementación del protocolo se diseña de manera nativa y en convivencia con el protocolo IPv4 a través de Dual Stack.

El diseño aprobado en la fase II del proyecto no contempla ni túneles, ni otros medios de transición, debido que la plataforma tecnológica de la CAR Cundinamarca permite acoger el protocolo IPv6 con todas sus funcionalidades.

Las labores detalladas son:

Tabla 16. Configuraciones en Firewall Fortinet FortiGate 1200D

NO.	DESCRIPCIÓN DE LA ACTIVIDAD	OBSERVACIÓN
1	Habilitación de función Dual Stack en el Firewall - 1200D Sede Central.	Configuración realizada sin novedad.
2	Configuración de las interfaces en IPv6 Firewall Fortigate - 1200D Sede Central.	Configuración realizada sin novedad.
3	Configuración de política IPv6 para permitir el tráfico de la LAN hacia MZ(Servidores) en los puertos y servicios indicados anteriormente para la comunicación hacia el Active Directory.	Configuración realizada sin novedad. Nota: La política queda abierta a nivel de direcciones IPv6 origen y destino. Una vez listos los objetos se crearán políticas más específicas a nivel de direccionamiento.
4	Configuración de política IPv6 con todo libre para la comunicación entre la super red LAN Sede Central con la subred MZ.	Configuración realizada sin novedad.
5	Configuración de rutas estáticas IPv6 para alcanzar las subredes de la superred LAN de Sede Central. Se crearon 32 rutas estáticas.	Configuración realizada sin novedad.
6	Configuración en el Firewall de objetos de red IPv6. Se crearon 372 objetos de red.	Configuración realizada sin novedad.
7	Configuración en el Firewall de políticas en IPv6, este se configuro con un script de 8000 lineas. Se crearon 1526 Políticas de Firewall IPv6.	Configuración realizada sin novedad.

La intervención de capa de Core o núcleo de la Red Corporativa de la CAR Cundinamarca, se realiza debido la funcionalidad de IPv6 no se encuentra activa de fábrica, dicha funcionalidad se debe activar en el Dashboard en la pestaña System >> Feature Visibility:

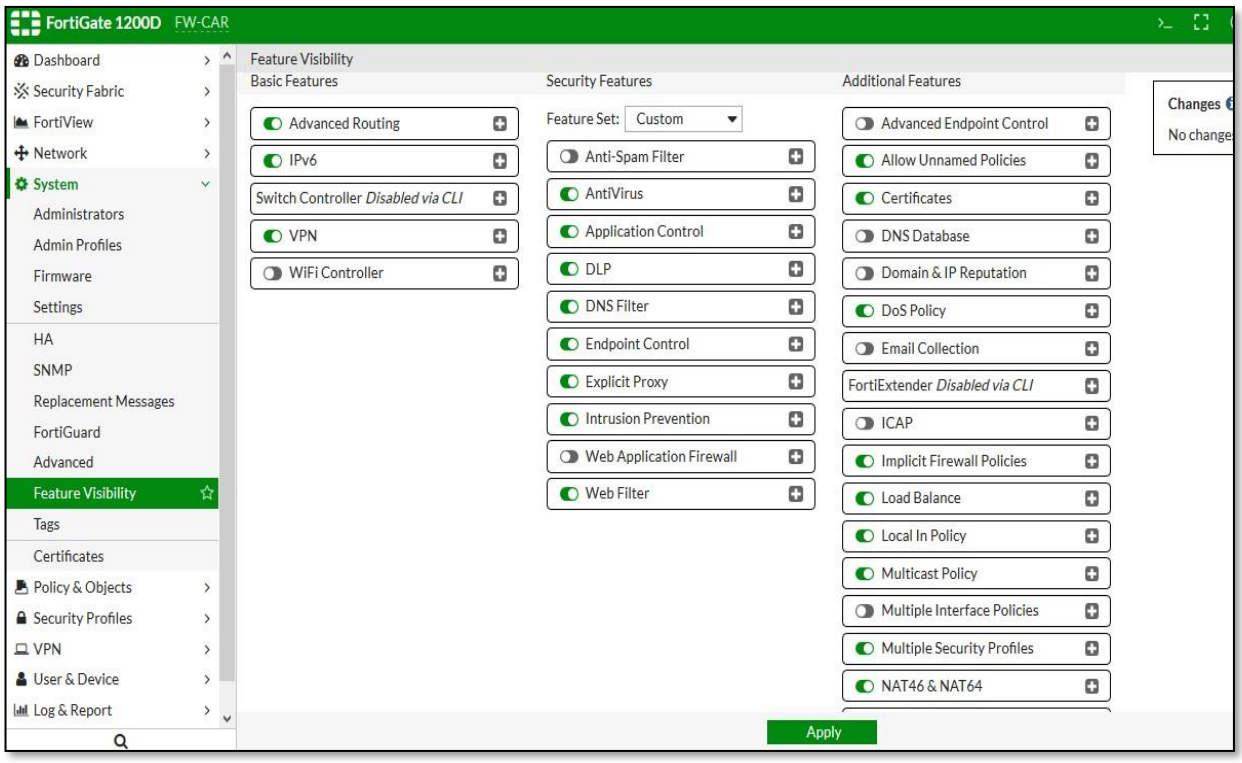


Ilustración 47. Habilitación de Dual Stack en Firewall 1200D

Fuente: Autores

Posterior a la habilitación del protocolo IPv6, se configura el direccionamoento IPv6 asignado a cada Inteface, teniendo la premisa que las interfaces físicas como virtuales se mantienen, y solo se asigna la dirección IPv6 lógica:

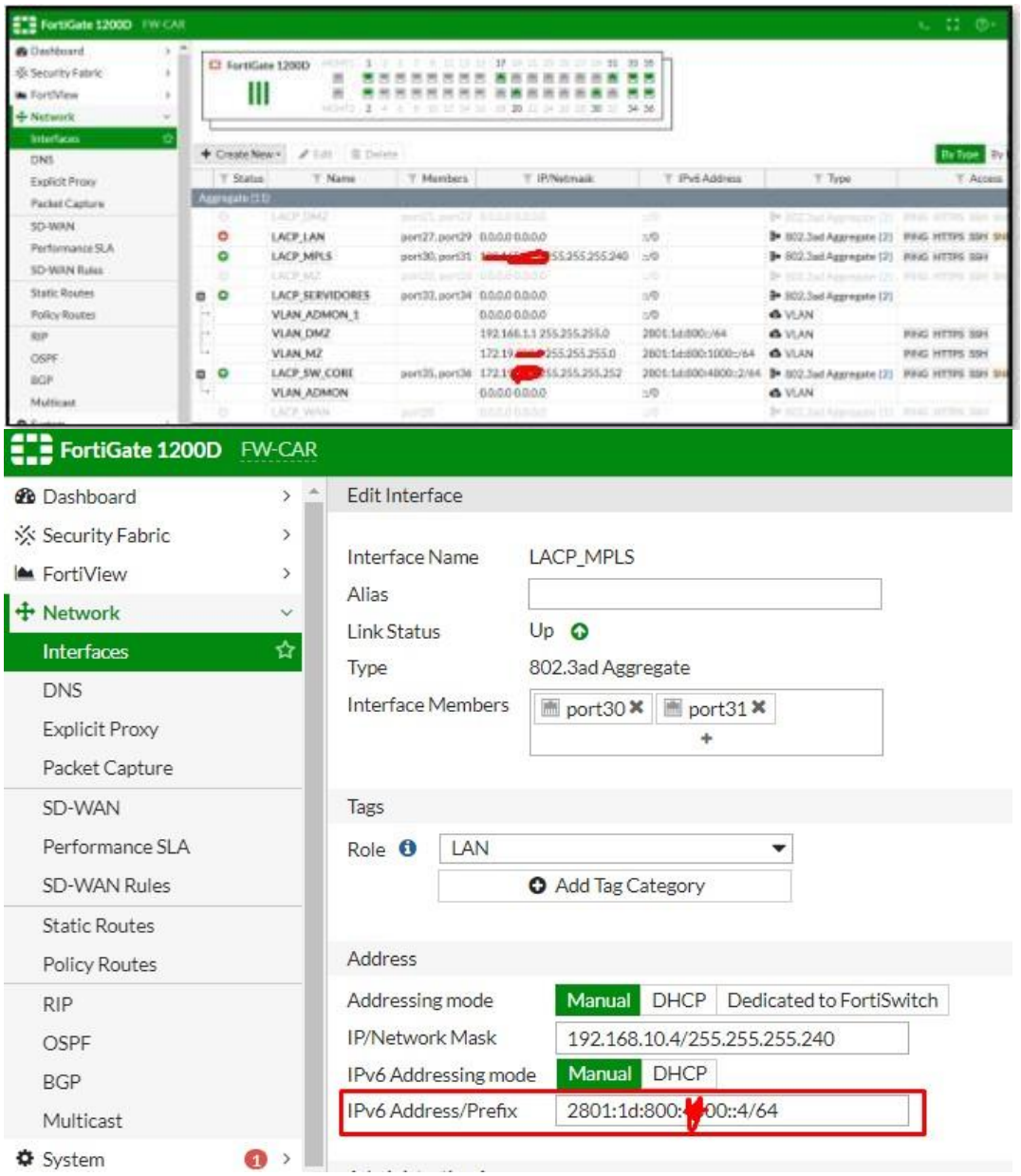


Ilustración 48. Configuración de Interfaces

Fuente: Autores

Posterior a la configuración de las interfaces, se activa las politicas de comunicaciones de servicios por zonas, igual como se encuentran en el protocolo IPv4:

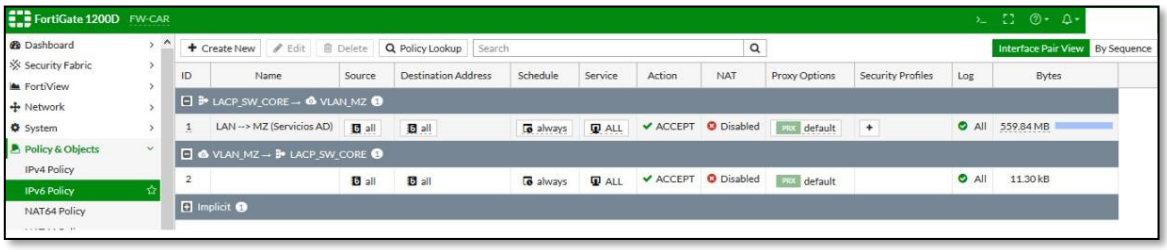


Ilustración 49. Configuración de políticas

Fuente: Autores

Así mismo la comunicación y enrutamiento del protocolo IPv6, se mantiene igual como se maneja en el protocolo IPv4:

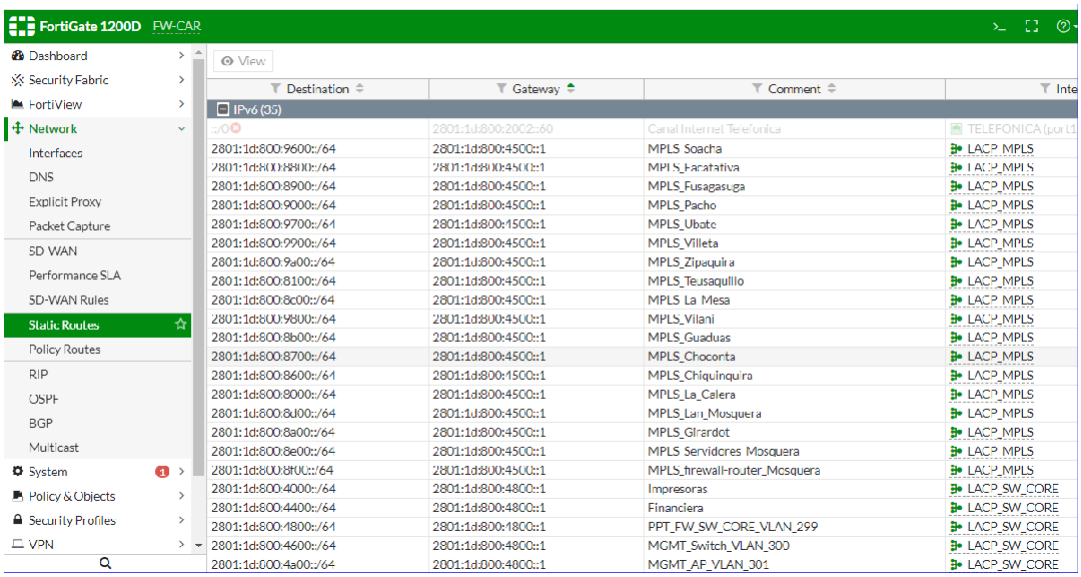


Ilustración 50. Creación Enrutamiento IPv6

Fuente: Autores

El anterior direccionamiento IPv6 a pesar de pertenecer al grupo de direccionamiento global de IPv6, que es alcanzable desde la Red pública (Internet), el Firewall a nivel de políticas de seguridad limita las conexiones entrantes y la comunicación es permitida solo a la necesidad especifica de cada subred interna.

Seguidamente al tener listo el Core de la Red Corporativa en Dual Stack, en la sede central de la CAR Cundinamarca se interviene el Switch Core de la LAN, siendo el dispositivo Alcatel Lucent 6900.

Se detalla en la tabla las labores hechas:

Tabla 17 Configuraciones Alcatel Lucent 6900

NO.	DESCRIPCIÓN DE LA ACTIVIDAD	OBSERVACIÓN
1	Configuración de Dual Stack, conexión punto a punto Firewall y Switch Core: VLAN299	Configuración realizada sin novedad.
2	Configuración de ruta estática por default, entre la conexión del Firewall y el Switch Core.	Configuración realizada sin novedad.
3	Configuración de SLAAC para las redes de centros de cableado, para las VLANs 102 y 107.	Configuración realizada sin novedad.
4	Configuración de subinterfaces de las VLANs 108,109 y 110 (impresoras, financiera y contrato de seguridad).	Configuración realizada sin novedad.
5	Configuración de las interfaces de red WiFi, VLANS 402 y 410 (funcionarios e invitados).	Configuración realizada sin novedad.
6	Configuración y encendido de banderas (Managed y Other) para la implementación de las VLANs de usuario con el servicio de DHCPv6.	Configuración realizada sin novedad.
7	Configuración de DHCP Relay.	Configuración realizada sin novedad.
8	Configuración de la VLAN 300 (Administración de los Switch) con el enrutamiento respectivo.	Configuración realizada sin novedad.

Se presenta la habilitación de las interfaces router de cada subred LAN:

Ilustración 51. Comunicación contra el Firewall

Fuente: Autores

```
CORE-CAR$ sho config snapshot ipv
! IPv6:
ipv6 interface "CC1-6" vlan 102
ipv6 address 2801:1d:800:6d00::/64 eui-64 "CC1-6"
ipv6 interface "CC2-6" vlan 103
ipv6 address 2801:1d:800:6c00::/64 eui-64 "CC2-6"
ipv6 interface "CC3-6" vlan 104
ipv6 address 2801:1d:800:6e00::/64 eui-64 "CC3-6"
ipv6 interface "CC4-6" vlan 105
ipv6 address 2801:1d:800:7d00::/64 eui-64 "CC4-6"
ipv6 interface "CC5-6" vlan 106
ipv6 address 2801:1d:800:7c00::/64 eui-64 "CC5-6"
ipv6 interface "CC6-6" vlan 107
ipv6 address 2801:1d:800:7e00::/64 eui-64 "CC6-6"
```

Ilustración 52. Configuración SLAAC redes de centros de cableado, para las VLAN 102-107

Fuente: Autores

Sujeto a que el diseño propuesto corresponde a la una conexión de los usuarios finales por asignación de direccionamiento IPv6 dinámicamente, se configura el servicio de DHCPv6 Relay, servicio apuntado al servidor de DHCP y DNS de la CAR Cundinamarca.

La información de configuración de las banderas M y O de las interfaces router en el Switch de acceso de la capa 3 de la LAN, corresponde a información privada de la implementación, banderas (flags), que son las que garantizan la asignación dinámica de la toda la información que necesita el host o terminal final para el acceso a la red:

```
CORE-CAR$
CORE-CAR$ sho config snapshot all | grep dhcp
dhcp-server enable
ipv6 dhcp relay admin-state enable
ipv6 dhcp relay "CC1-6" destination
ipv6 dhcp relay "CC1-6" admin-state
ipv6 dhcp relay "CC2-6" destination
ipv6 dhcp relay "CC2-6" admin-state
ipv6 dhcp relay "CC3-6" destination
ipv6 dhcp relay "CC3-6" admin-state
ipv6 dhcp relay "CC4-6" destination
ipv6 dhcp relay "CC4-6" admin-state
ipv6 dhcp relay "CC5-6" destination
ipv6 dhcp relay "CC5-6" admin-state
ipv6 dhcp relay "CC6-6" destination
ipv6 dhcp relay "CC6-6" admin-state enable
ipv6 dhcp relay "WiFiPESCAR" destination
ipv6 dhcp relay "WiFiPESCAR" admin-state
ipv6 dhcp relay "WIFI-FUNCION-6" destinat
ipv6 dhcp relay "WIFI-FUNCION-6" admin-st
ipv6 dhcp relay "WIFI-INVIT-6" destinatio
ipv6 dhcp relay "WIFI-INVIT-6" admin-state enable
CORE-CAR$
```

Ilustración 53. Configuración de DHCP Relay

Fuente: Autores

En la imagen anterior se oculta el objeto del servidor DHCPv6 de la CAR Cundinamarca por seguridad de la información.

Posterior a la implementación de las subredes se activa en la Red LAN Interna, enrutamiento por default, sujeto a que el Switch de Core solo entrega todo el tráfico al Firewall quien, al ser el Core la Red Corporativa, define el camino por el cual enviar el tráfico de red:

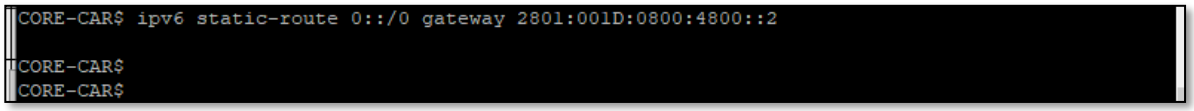


Ilustración 54. Configuración de ruta estática entre la conexión del Firewall y el Switch Core

Fuente: Autores

Cuando se ha desplegado el protocolo IPv6 en la capa 2 y capa 3 del modelo de Red global TCP/IP, se intervienen los servicios de Red. Es la tercera capa para intervenir, en este lugar de implementación encontramos los controladores de dominio.

A continuación, presentamos el resumen de actividades a realizar:

Tabla 18. Configuraciones en los controladores de domino

NO.	DESCRIPCIÓN DE LA ACTIVIDAD	OBSERVACIÓN
1	Configuración de zonas inversas en el DNS principal.	Configuración realizada sin novedad.
2	Eliminacion de GPO que deshabilitaba el uso del protocolo IPv6 a nivel interno.	Configuración realizada sin novedad.
3	Configuración del direccionamiento IPv6 correspondiente a la zona inversa de cada VLAN de la LAN Sede Central y MPLS.	Configuración realizada sin novedad.
4	Configuración de roles en el DHCP principal.	Configuración realizada sin novedad.
5	Configuración de scope en el DHCP	Configuración realizada sin novedad.
6	Configuracion de IPv6 en el clúster SHYPBOG12, SHYPBOG13	Configuración realizada sin novedad.

Tras haber ejecutado las labores, adjuntamos los resultados de configuración, siendo primero el servicio DNS de la zona autoritiva en el protocolo IPv6

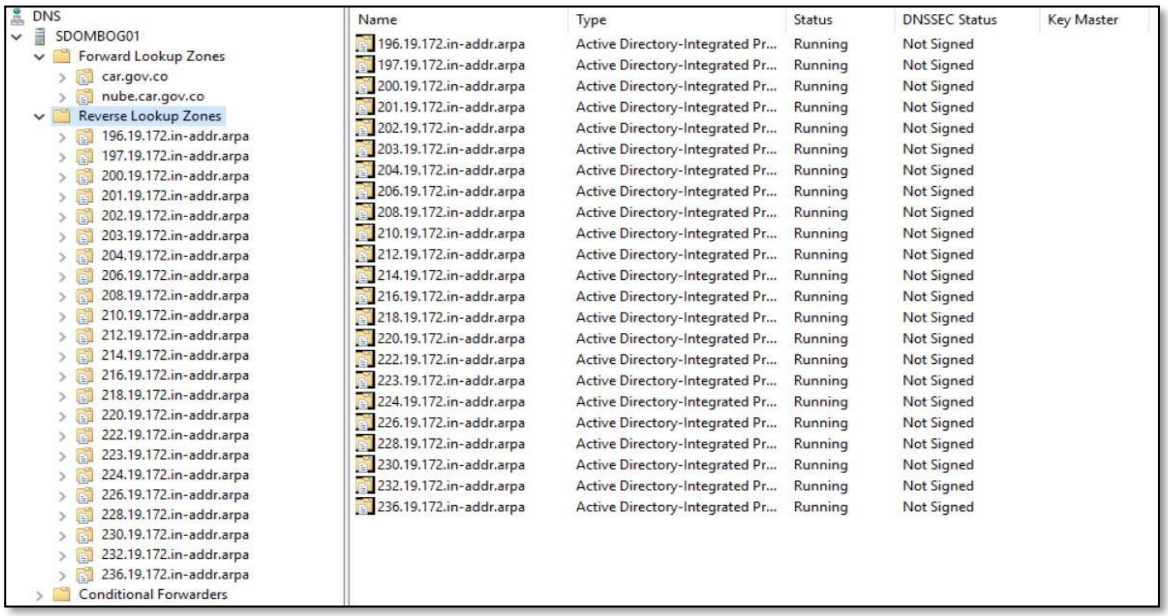


Ilustración 55. Configuración Servidor DNS

Fuente: Autores

Ahora el de las zonas inversas

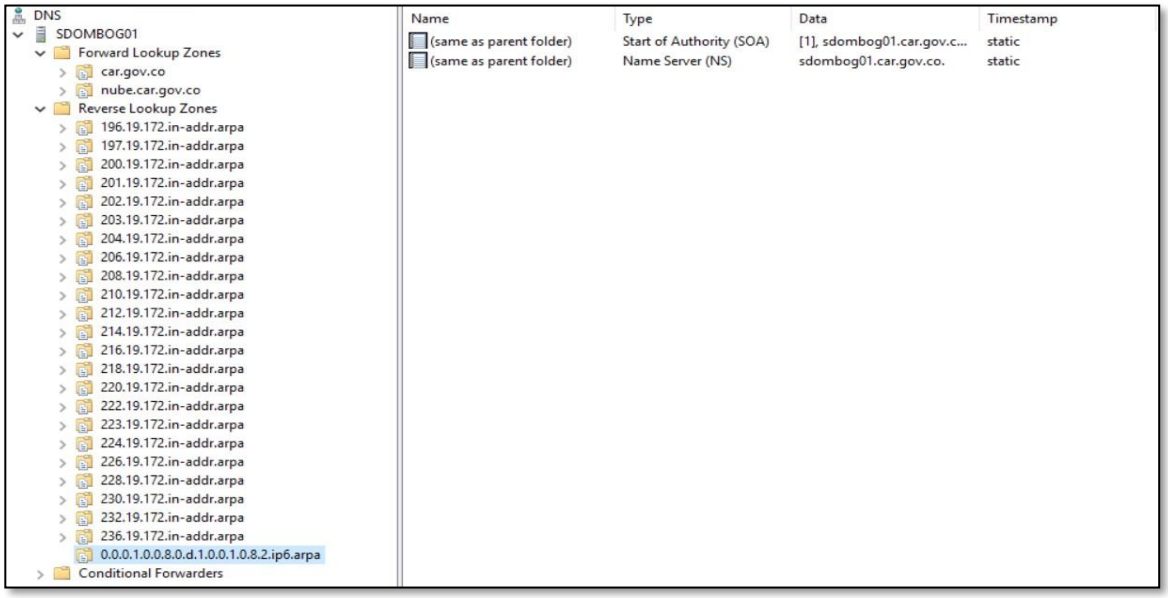


Ilustración 56. Configuración de zonas inversas

Fuente: Autores

Y por último la implementación del servicio de DHCPv6, para la conexión Stateful de los usuarios finales

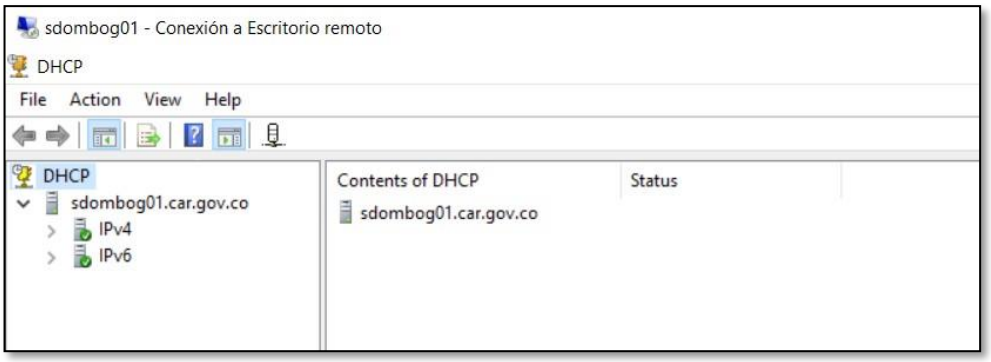


Ilustración 57. Configuración de servidor DHCPv6

Fuente: Autores

Posterior al despliegue de los Scope se verifica el leases en el servidor, donde confirmamos que el servidor asigna y administra la asignacion dinamica de la conexión de los usuarios finales:

Ilustración 58. Leases Scope Servidores DHCPv6

Fuente: Autores

FASE 4 – PRUEBAS Y AFINAMIENTO DE LA SOLUCIÓN

Esta fase resume y corrobora todas las labores previas realizadas ya que marca la finalización de la implementación del protocolo IPv6, por eso se procede a realizar una serie de pruebas de comunicación en el protocolo TCP/IP y posterior verificación de los servicios:

Conectividad y Sniffer Firewall Core FortiGate 1200D

- **Prueba y monitoreo No. 1:**

A través de un ping IPv6, probaremos la comunicación del enrutamiento desde el Firewall FG-1200D hacia la dirección IPv6 2801:1d:800:4800::1 hacia el siguiente salto del Switch Core Alcatel, que acoge la Red LAN de la sede central.

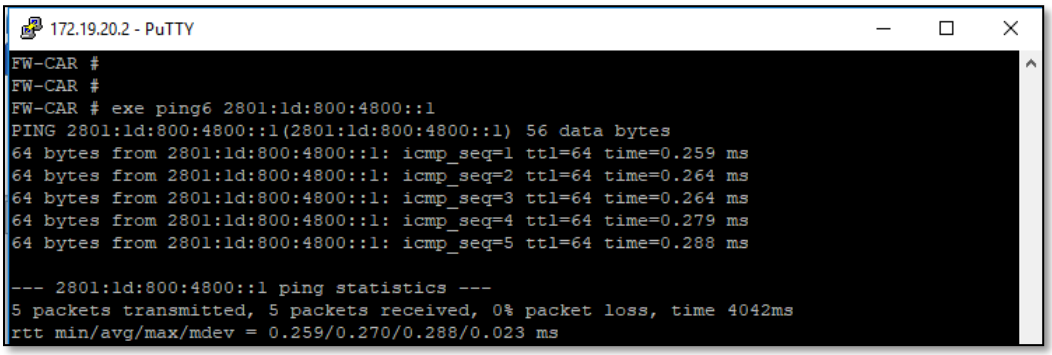


Ilustración 59. Ping IPv6 desde el firewall FG-1200D hacia la Lan del Swit-Core Alcatel

Fuente: Autores

Así mimo, desde el Firewall FortiGate 1200D se ejecuta un sniffer, con el fin de confirmar las respuestas del ping gracias al protocolo ICMP (Internet Control Message Protocol), en cada una de estas respuestas no se observa mensajes de error:

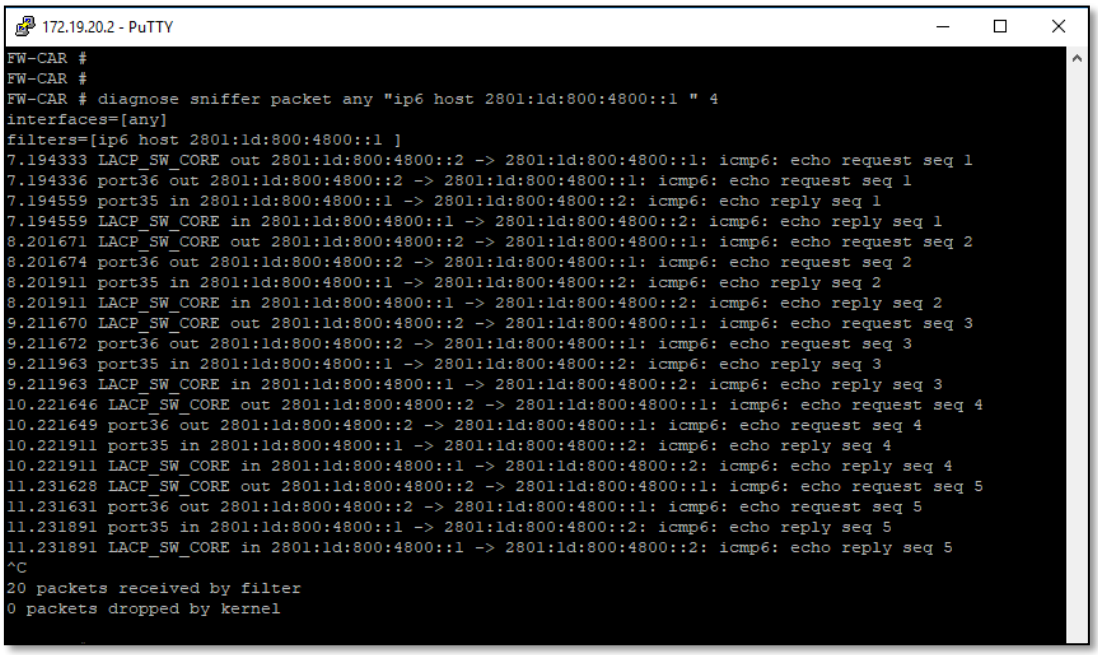


Ilustración 60. Monitoreo con Sniffer desde el firewall FG-1200D

Fuente: Autores

- **Prueba y monitoreo No. 2:**

Posterior a la verificación hecha hacia la LAN de la sede central, se ejecutan pruebas por medio de un ping IPv6 desde el firewall FG-1200D hacia la dirección IPv6 2801:1D:800:4500::1 del Router, por donde el Firewall alcanza todas las redes IPv6 de las sedes remotas de la CAR, red MPLS:

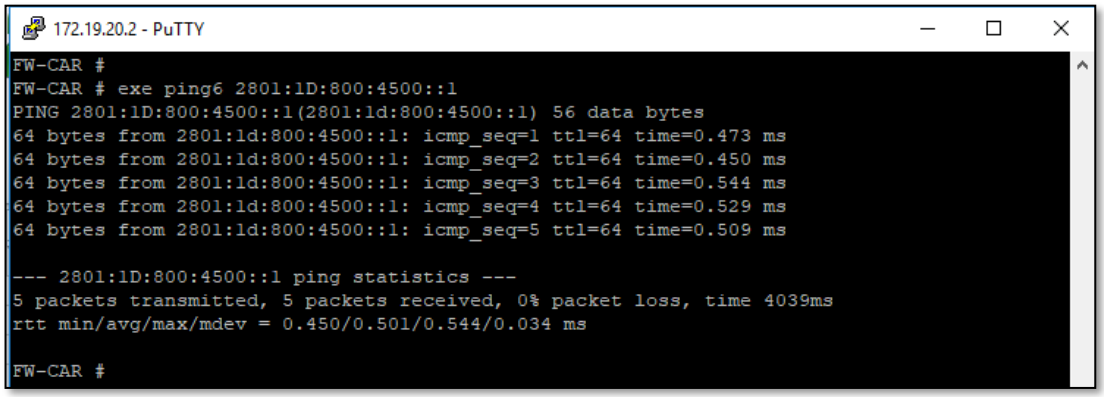


Ilustración 61. Ping IPv6 desde el Firewall FG-1200D hacia el Router de la MPLS

Fuente: Autores

Así mismo, desde el Firewall FortiGate 1200D se ejecuta un sniffer, con el fin de confirmar las respuestas del ping gracias al protocolo ICMP (Internet Control Message Protocol), en cada una de estas respuestas no se observa mensajes de error:

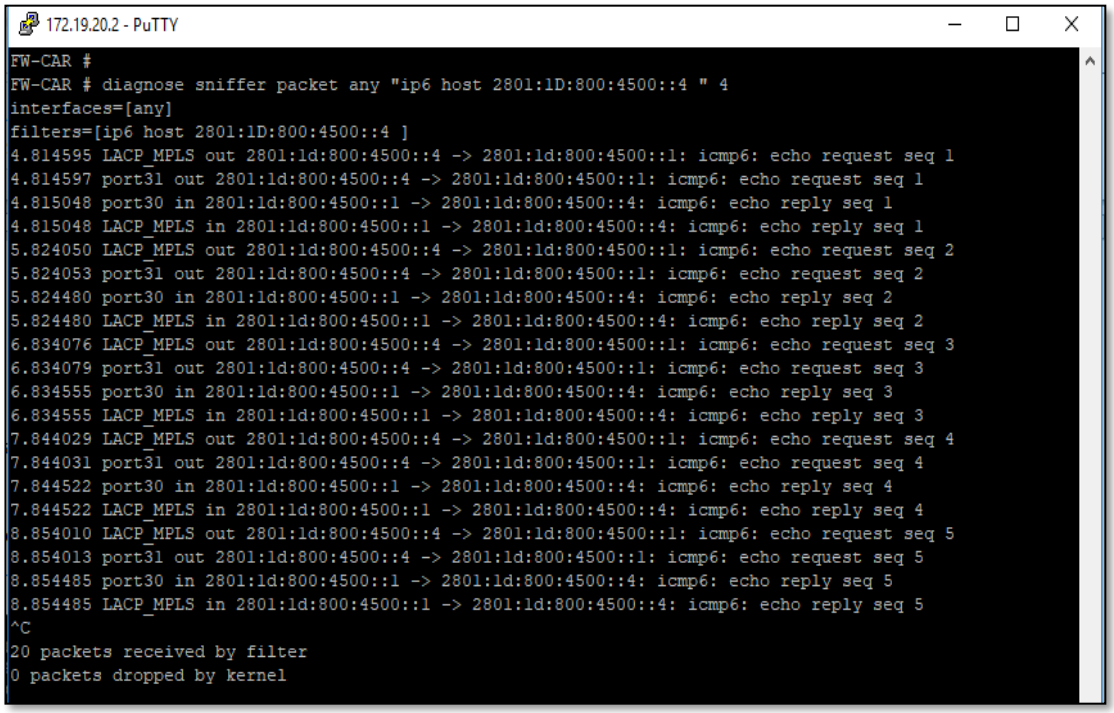
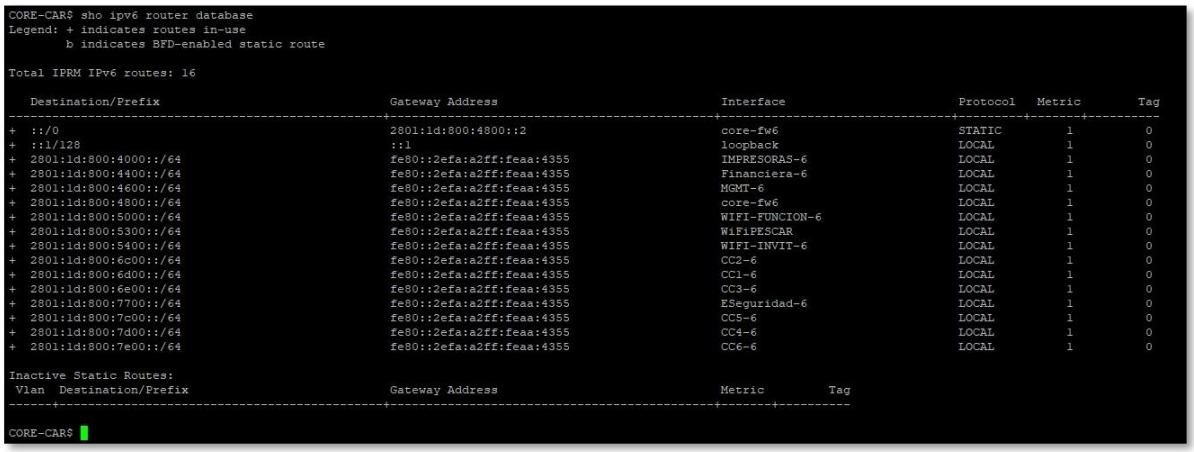


Ilustración 62. Monitoreo con Sniffer desde el firewall FG-1200D

Fuente: Autores

Conectividad LAN Sede Central

A nivel de la capa de red de acceso en capa 3 del Switch Core Alcatel Lucent 6900, se verifica la conexión de cada subred LAN:

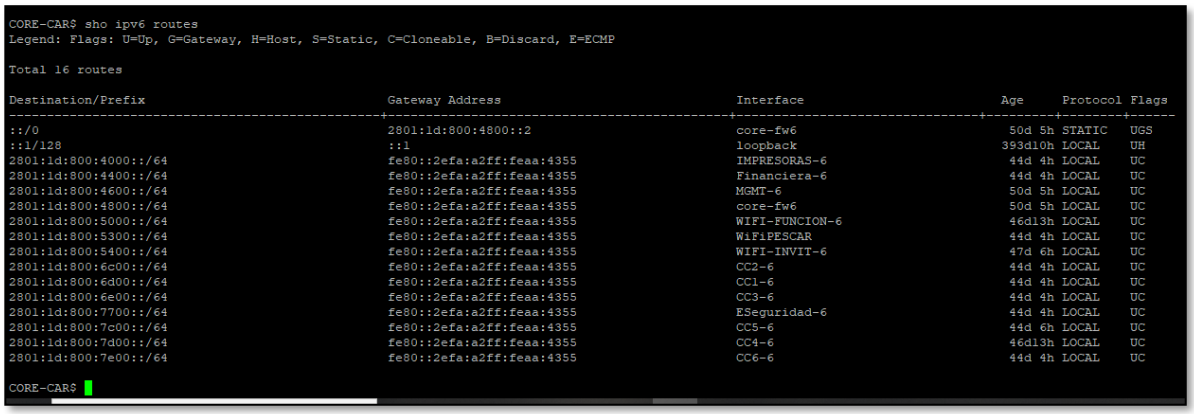


```
CORE-CAR$ sho ipv6 router database
Legend: + indicates routes in-use
        b indicates BFD-enabled static route

Total IPRM IPv6 routes: 16

   Destination/Prefix                          Gateway Address                          Interface                        Protocol   Metric        Tag
-----------------------------------------------+----------------------------------------+--------------------------------+----------+-------+----------
+  ::/0                                        2801:1d:800:4800::2                      core-fw6                         STATIC         1          0
+  ::1/128                                     ::1                                      loopback                         LOCAL          1          0
+  2801:1d:800:4000::/64                       fe80::2efa:a2ff:feaa:4355                IMPRESORAS-6                     LOCAL          1          0
+  2801:1d:800:4400::/64                       fe80::2efa:a2ff:feaa:4355                Financiera-6                     LOCAL          1          0
+  2801:1d:800:4600::/64                       fe80::2efa:a2ff:feaa:4355                MGMT-6                           LOCAL          1          0
+  2801:1d:800:4800::/64                       fe80::2efa:a2ff:feaa:4355                core-fw6                         LOCAL          1          0
+  2801:1d:800:5000::/64                       fe80::2efa:a2ff:feaa:4355                WIFI-FUNCION-6                   LOCAL          1          0
+  2801:1d:800:5300::/64                       fe80::2efa:a2ff:feaa:4355                WiFiPESCAR                       LOCAL          1          0
+  2801:1d:800:5400::/64                       fe80::2efa:a2ff:feaa:4355                WIFI-INVIT-6                     LOCAL          1          0
+  2801:1d:800:6c00::/64                       fe80::2efa:a2ff:feaa:4355                CC2-6                            LOCAL          1          0
+  2801:1d:800:6d00::/64                       fe80::2efa:a2ff:feaa:4355                CC1-6                            LOCAL          1          0
+  2801:1d:800:6e00::/64                       fe80::2efa:a2ff:feaa:4355                CC3-6                            LOCAL          1          0
+  2801:1d:800:7700::/64                       fe80::2efa:a2ff:feaa:4355                ESeguridad-6                     LOCAL          1          0
+  2801:1d:800:7c00::/64                       fe80::2efa:a2ff:feaa:4355                CC5-6                            LOCAL          1          0
+  2801:1d:800:7d00::/64                       fe80::2efa:a2ff:feaa:4355                CC4-6                            LOCAL          1          0
+  2801:1d:800:7e00::/64                       fe80::2efa:a2ff:feaa:4355                CC6-6                            LOCAL          1          0

Inactive Static Routes:
 Vlan  Destination/Prefix                     Gateway Address                          Metric        Tag
------+----------------------------------------+----------------------------------------+-------+----------

CORE-CAR$
```

Ilustración 63. LAN, Centros de cableado y Firewall con enrutamiento estático IPv6

Fuente: Autores

Seguidamente, se verifica el tiempo en que las sesiones IPv6 a nivel de subredes y enrutamiento en la LAN llevan establecidas. El tiempo que se observa es de varios días, esto nos señala que la implementación hecha presenta estabilidad:



```
CORE-CAR$ sho ipv6 routes
Legend: Flags: U=Up, G=Gateway, H=Host, S=Static, C=Cloneable, B=Discard, E=ECMP

Total 16 routes

Destination/Prefix                          Gateway Address                          Interface                        Age     Protocol Flags
-----------------------------------------------+----------------------------------------+--------------------------------+--------+--------+------
::/0                                        2801:1d:800:4800::2                      core-fw6                          50d 5h STATIC   UGS
::1/128                                     ::1                                      loopback                        393d10h LOCAL    UH
2801:1d:800:4000::/64                       fe80::2efa:a2ff:feaa:4355                IMPRESORAS-6                      44d 4h LOCAL    UC
2801:1d:800:4400::/64                       fe80::2efa:a2ff:feaa:4355                Financiera-6                      44d 4h LOCAL    UC
2801:1d:800:4600::/64                       fe80::2efa:a2ff:feaa:4355                MGMT-6                            50d 5h LOCAL    UC
2801:1d:800:4800::/64                       fe80::2efa:a2ff:feaa:4355                core-fw6                          50d 5h LOCAL    UC
2801:1d:800:5000::/64                       fe80::2efa:a2ff:feaa:4355                WIFI-FUNCION-6                   46d13h LOCAL    UC
2801:1d:800:5300::/64                       fe80::2efa:a2ff:feaa:4355                WiFiPESCAR                        44d 4h LOCAL    UC
2801:1d:800:5400::/64                       fe80::2efa:a2ff:feaa:4355                WIFI-INVIT-6                      47d 6h LOCAL    UC
2801:1d:800:6c00::/64                       fe80::2efa:a2ff:feaa:4355                CC2-6                             44d 4h LOCAL    UC
2801:1d:800:6d00::/64                       fe80::2efa:a2ff:feaa:4355                CC1-6                             44d 4h LOCAL    UC
2801:1d:800:6e00::/64                       fe80::2efa:a2ff:feaa:4355                CC3-6                             44d 4h LOCAL    UC
2801:1d:800:7700::/64                       fe80::2efa:a2ff:feaa:4355                ESeguridad-6                      44d 4h LOCAL    UC
2801:1d:800:7c00::/64                       fe80::2efa:a2ff:feaa:4355                CC5-6                             44d 6h LOCAL    UC
2801:1d:800:7d00::/64                       fe80::2efa:a2ff:feaa:4355                CC4-6                            46d13h LOCAL    UC
2801:1d:800:7e00::/64                       fe80::2efa:a2ff:feaa:4355                CC6-6                             44d 4h LOCAL    UC

CORE-CAR$
```

Ilustración 64. Tiempo establecimiento sesiones IPv6 a nivel de subredes y enrutamiento en la LAN

Fuente: Autores

Al finalizar la verificación de comunicaciones entre saltos de la red en capa de red, se verifica a nivel de capa 2 la conexión de usuarios bajo el protocolo IPv6:

```
CORE-CAR$ sho ipv6 neighbors
Total 797 neighbors

IPv6 Address                            Hardware Address  Reachability Lifetime    Port               Interface
----------------------------------------+-----------------+------------+----------+------------------+---------------------
2801:1d:800:6d00:af:b1b1:97e2:3fe       fc:4d:d4:3e:e5:dc Confirmed         7m 1s 2/2/3              CC1-6
2801:1d:800:6d00:49d:fcd0:46eb:64bc     6c:0b:84:0c:ab:64 Confirmed           39s 2/2/3              CC1-6
2801:1d:800:6d00:140f:4ba3:f9dc:96d4    00:25:ab:ac:66:36 Confirmed         1m 58s 2/2/3             CC1-6
2801:1d:800:6d00:20cd:d504:ac15:10c7    ec:a8:6b:2a:d8:8d Confirmed         1m 44s 2/2/3             CC1-6
2801:1d:800:6d00:2176:e32d:441d:cd0     f4:39:09:4a:bd:30 Confirmed         2m 10s 2/2/3             CC1-6
2801:1d:800:6d00:2513:eef7:a115:97c4    00:23:24:72:fc:ee Confirmed         2m 16s 2/2/3             CC1-6
2801:1d:800:6d00:2723:e538:b159:db44    ec:a8:6b:2a:d9:14 Confirmed         1m 53s 2/2/3             CC1-6
2801:1d:800:6d00:307b:a884:f463:5554    00:25:ab:ac:66:36 Confirmed          2m 6s 2/2/3             CC1-6
2801:1d:800:6d00:31d0:6208:c272:4dcd    10:e7:c6:4b:e6:f1 Confirmed         2m 24s 2/2/3             CC1-6
2801:1d:800:6d00:3c36:f09a:54e1:a7e     f8:b1:56:d3:ba:67 Unconfirmed       9m 22s 2/2/3             CC1-6
2801:1d:800:6d00:3cc1:e25d:e3e4:21a6    00:23:24:72:fd:d2 Confirmed         1m 54s 2/2/3             CC1-6
2801:1d:800:6d00:3d54:80f8:4671:4048    c8:d9:d2:08:42:bf Confirmed         1m 59s 2/2/3             CC1-6
2801:1d:800:6d00:4156:a429:68e3:7bed    10:e7:c6:4b:e7:06 Confirmed         7m 25s 2/2/3             CC1-6
2801:1d:800:6d00:4906:3ed6:1f72:b893    ec:a8:6b:2a:d9:14 Confirmed         1m 44s 2/2/3             CC1-6
2801:1d:800:6d00:4dd7:336a:flff:affa    6c:0b:84:0c:ba:23 Unconfirmed       7m 30s 2/2/3             CC1-6
2801:1d:800:6d00:50a0:ff42:91c9:7aef    c8:d9:d2:08:42:20 Confirmed           26s 2/2/3              CC1-6
2801:1d:800:6d00:5152:7556:4e90:b600    3c:97:0e:dd:6b:6f Confirmed         6m 47s 2/2/3             CC1-6
2801:1d:800:6d00:515f:7b3d:971e:4c7e    f8:b1:56:d1:32:29 Confirmed           10s 2/2/3              CC1-6
2801:1d:800:6d00:5180:4cf9:4dab:fce6    4c:cc:6a:19:5b:a5 Confirmed           56s 2/2/3              CC1-6
2801:1d:800:6d00:5187:e97f:eefc:155a    00:23:24:80:22:b1 Confirmed          2m 1s 2/2/3             CC1-6
2801:1d:800:6d00:5557:1b2d:b301:eb2     00:25:ab:ac:f6:24 Confirmed           54s 2/2/3              CC1-6
2801:1d:800:6d00:61f5:3f17:8e52:2a21    10:e7:c6:4b:e7:32 Confirmed         2m 17s 2/2/3             CC1-6
2801:1d:800:6d00:6944:96bb:eb5:55ee     00:23:24:72:fc:fb Confirmed           21s 2/2/3              CC1-6
```

Ilustración 65. Saltos en capa 2

Fuente: Autores

Hasta este lugar la implementación presenta estabilidad, los usuarios reciben direcciones IPv6 bajo el envío de mensajes propios del protocolo IPv6 como los RA (Router Advertisement) y RS (Router Solicitation), autoconfiguración por protocolo SLAAC acogidos en el protocolo ICMP en IPv6 del Neighbor Discovery, el cual es el homologo al ARP de IPv4.

Conectividad LAN a zona de servidores

A través de un ping veremos las respuestas exitosas a las peticiones hechas a los servidores que están alojados en la zona Militarizada:

```
ping6 2801:001D:0800:1000::13(2801:1d:800:1000::13) from 2801:1d:800:4800::1: 8 data bytes
16 bytes from 2801:1d:800:1000::13: icmp_seq=1 ttl=128 time=2.29 ms


16 bytes from 2801:1d:800:1000::13: icmp_seq=2 ttl=128 time=2.80 ms
16 bytes from 2801:1d:800:1000::13: icmp_seq=3 ttl=128 time=2.35 ms
16 bytes from 2801:1d:800:1000::13: icmp_seq=4 ttl=128 time=1.52 ms
16 bytes from 2801:1d:800:1000::13: icmp_seq=5 ttl=128 time=2.40 ms
16 bytes from 2801:1d:800:1000::13: icmp_seq=6 ttl=128 time=4.41 ms

--- 2801:001D:0800:1000::13 ping6 statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
round-trip min/avg/max = 1.528/2.634/4.413 ms
CORE-CAR$
CORE-CAR$
CORE-CAR$ ping6 2801:001D:0800:1000::1
ping6 2801:001D:0800:1000::1(2801:1d:800:1000::1) from 2801:1d:800:4800::1: 8 data bytes
16 bytes from 2801:1d:800:1000::1: icmp_seq=1 ttl=64 time=1.27 ms
16 bytes from 2801:1d:800:1000::1: icmp_seq=2 ttl=64 time=3.57 ms
16 bytes from 2801:1d:800:1000::1: icmp_seq=3 ttl=64 time=1.32 ms
16 bytes from 2801:1d:800:1000::1: icmp_seq=4 ttl=64 time=3.33 ms
16 bytes from 2801:1d:800:1000::1: icmp_seq=5 ttl=64 time=1.47 ms
16 bytes from 2801:1d:800:1000::1: icmp_seq=6 ttl=64 time=1.10 ms

--- 2801:001D:0800:1000::1 ping6 statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
round-trip min/avg/max = 1.101/2.013/3.574 ms
```

Ilustración 66. LAN a MZ

Fuente: Autores

Desde una terminal, existente dentro de la Red LAN, se acceda por medio de dirección IPv6 al servicio de RDP (escritorio remoto):

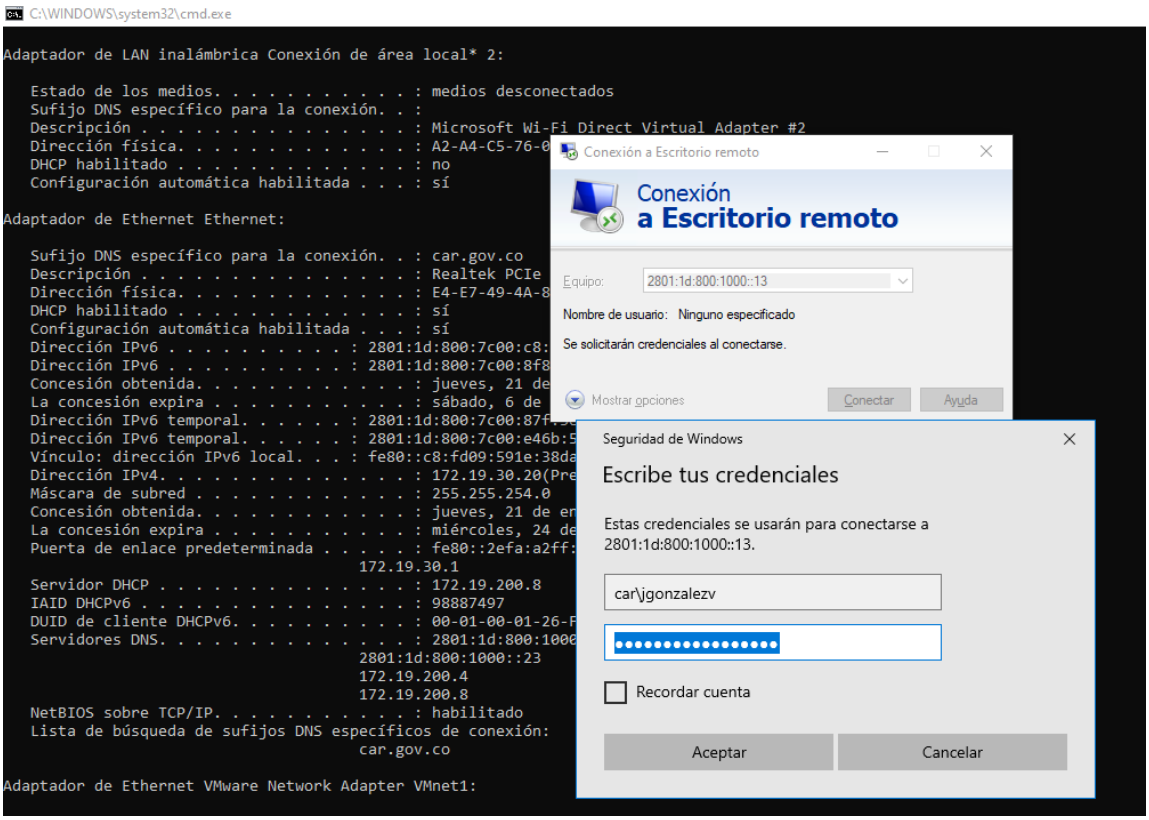
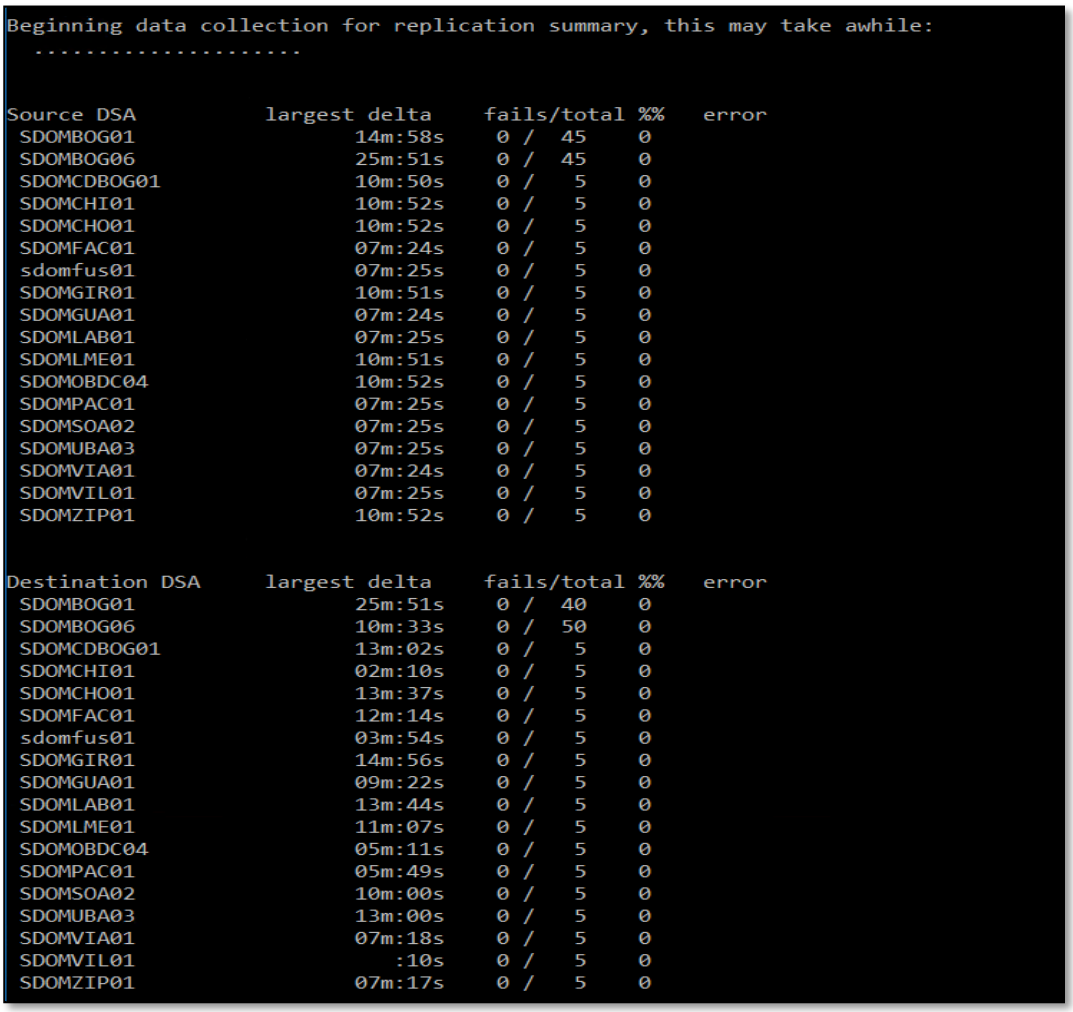


Ilustración 67. Conexión a través RDP

Fuente: Autores

Verificación de los servicios de Dominio, Servidores, DHCP, DNS

Se ejecuta el comando repadmin /replsummary, en el cual nos permite verificar todas las instancias de replicación del dominio de la CAR.



```
Beginning data collection for replication summary, this may take awhile:
  ......................


Source DSA          largest delta    fails/total %%   error
 SDOMBOG01                  14m:58s    0 /  45    0
 SDOMBOG06                  25m:51s    0 /  45    0
 SDOMCDBOG01                10m:50s    0 /   5    0
 SDOMCHI01                  10m:52s    0 /   5    0
 SDOMCHO01                  10m:52s    0 /   5    0
 SDOMFAC01                  07m:24s    0 /   5    0
 sdomfus01                  07m:25s    0 /   5    0
 SDOMGIR01                  10m:51s    0 /   5    0
 SDOMGUA01                  07m:24s    0 /   5    0
 SDOMLAB01                  07m:25s    0 /   5    0
 SDOMLME01                  10m:51s    0 /   5    0
 SDOMOBDC04                 10m:52s    0 /   5    0
 SDOMPAC01                  07m:25s    0 /   5    0
 SDOMSOA02                  07m:25s    0 /   5    0
 SDOMUBA03                  07m:25s    0 /   5    0
 SDOMVIA01                  07m:24s    0 /   5    0
 SDOMVIL01                  07m:25s    0 /   5    0
 SDOMZIP01                  10m:52s    0 /   5    0


Destination DSA     largest delta    fails/total %%   error
 SDOMBOG01                  25m:51s    0 /  40    0
 SDOMBOG06                  10m:33s    0 /  50    0
 SDOMCDBOG01                13m:02s    0 /   5    0
 SDOMCHI01                  02m:10s    0 /   5    0
 SDOMCHO01                  13m:37s    0 /   5    0
 SDOMFAC01                  12m:14s    0 /   5    0
 sdomfus01                  03m:54s    0 /   5    0
 SDOMGIR01                  14m:56s    0 /   5    0
 SDOMGUA01                  09m:22s    0 /   5    0
 SDOMLAB01                  13m:44s    0 /   5    0
 SDOMLME01                  11m:07s    0 /   5    0
 SDOMOBDC04                 05m:11s    0 /   5    0
 SDOMPAC01                  05m:49s    0 /   5    0
 SDOMSOA02                  10m:00s    0 /   5    0
 SDOMUBA03                  13m:00s    0 /   5    0
 SDOMVIA01                  07m:18s    0 /   5    0
 SDOMVIL01                     :10s    0 /   5    0
 SDOMZIP01                  07m:17s    0 /   5    0
```

Ilustración 68. Réplicas de servidores estables y funcionales en IPv6

Fuente: Autores

Se verifica la replicación del domino CAR.GOV.CO, en IPv6 puro, con el fin de validar que los directorios activos mantengan la estabilidad y comunicación para el usuario final, esto debido que la Red Corporativa de la CAR Cundinamarca brinda la opción de conexión de los usuarios finales por medio de perfiles creados en el directorio y replicados por el protocolo LDAP (Protocolo ligero de acceso a directorios) al Firewall Core, el cual despliega un portal cautivo de acceso:

Ilustración 69. Portal cautivo CAR

Fuente: Autores

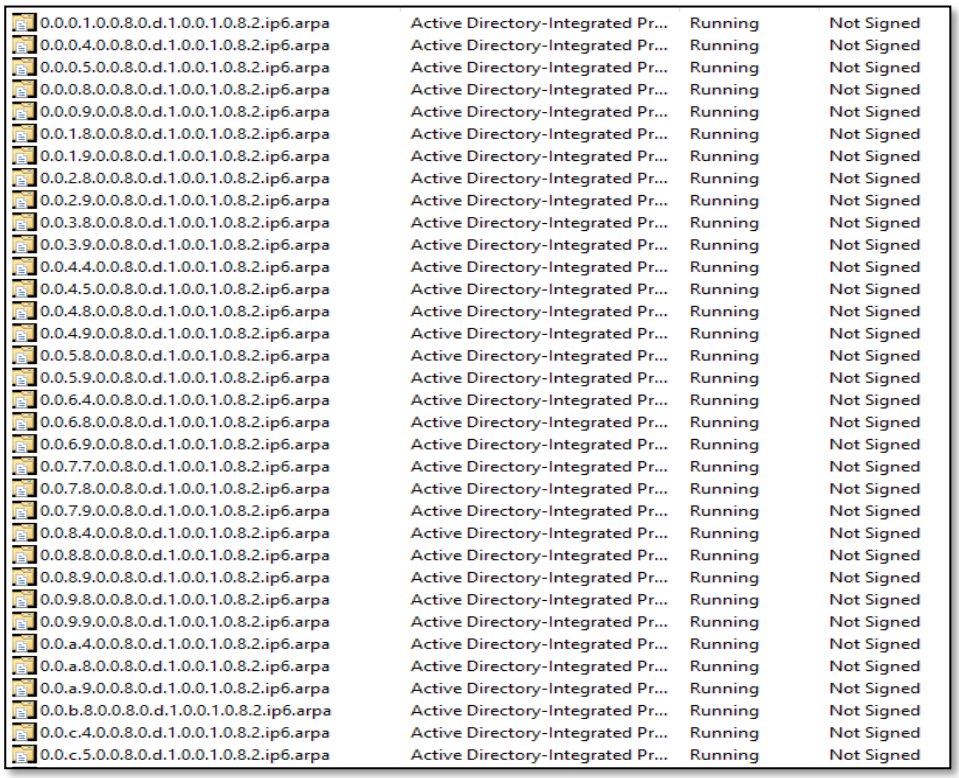
Se verifica la comunicación de las bases de datos del domino CAR.GOV.CO, en IPv6 puro, con el fin de validar el correcto estado de los servicios:

```
PS C:\Users\password> dcdiag

Directory Server Diagnosis

Performing initial setup:
   Trying to find home server...
   Home Server = SDOMBOG06
   * Identified AD Forest.
   Done gathering initial info.

Doing initial required tests

   Testing server: SITIO-BOGOTA\SDOMBOG06
      Starting test: Connectivity
         ......................... SDOMBOG06 passed test Connectivity

Doing primary tests

   Testing server: SITIO-BOGOTA\SDOMBOG06
      Starting test: Advertising
         ......................... SDOMBOG06 passed test Advertising
      Starting test: FrsEvent
         ......................... SDOMBOG06 passed test FrsEvent
      Starting test: DFSREvent
         There are warning or error events within the last 24 hours after the SYSVOL has been shared.  Failing SYSVOL
         replication problems may cause Group Policy problems.
         ......................... SDOMBOG06 failed test DFSREvent
      Starting test: SysVolCheck
         ......................... SDOMBOG06 passed test SysVolCheck
      Starting test: KccEvent
         ......................... SDOMBOG06 passed test KccEvent
      Starting test: KnowsOfRoleHolders
         ......................... SDOMBOG06 passed test KnowsOfRoleHolders
      Starting test: MachineAccount
         ......................... SDOMBOG06 passed test MachineAccount
      Starting test: NCSecDesc
         ......................... SDOMBOG06 passed test NCSecDesc
      Starting test: NetLogons
         [SDOMBOG06] User credentials does not have permission to perform this operation.
         The account used for this test must have network logon privileges
         for this machine's domain.
         ......................... SDOMBOG06 failed test NetLogons
      Starting test: ObjectsReplicated
         ......................... SDOMBOG06 passed test ObjectsReplicated
      Starting test: Replications
         [Replications Check,SDOMBOG06] DsReplicaGetInfo(PENDING_OPS, NULL) failed, error 0x2105
         "Replication access was denied."
         ......................... SDOMBOG06 failed test Replications
      Starting test: RidManager
         ......................... SDOMBOG06 passed test RidManager
      Starting test: Services
         ......................... SDOMBOG06 passed test Services
      Starting test: SystemLog
```

Ilustración 70. Test de prueba para validar el estado de las bases de datos, comando DCDIAG

Fuente: Autores

Se genera un test de las zonas inversas de los DNS de la organización en donde se observa que todas las zonas IPv6 se ejecutan y funcionan a nivel global del dominio.



0.0.0.1.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.0.4.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.0.5.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.0.8.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.0.9.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.1.8.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.1.9.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.2.8.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.2.9.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.3.8.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.3.9.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.4.4.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.4.5.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.4.8.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.4.9.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.5.8.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.5.9.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.6.4.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.6.8.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.6.9.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.7.7.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.7.8.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.7.9.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.8.4.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.8.8.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.8.9.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.9.8.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.9.9.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.a.4.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.a.8.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.a.9.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.b.8.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.c.4.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed
0.0.c.5.0.0.8.0.d.1.0.0.1.0.8.2.ip6.arpa	Active Directory-Integrated Pr...	Running	Not Signed

Ilustración 71. Test de las zonas inversas de los DNS

Fuente: Autores

Conexión por servicios de RDP (terminal services), por IPv6 las cuales fueron efectivas a nivel del protocolo implementado.

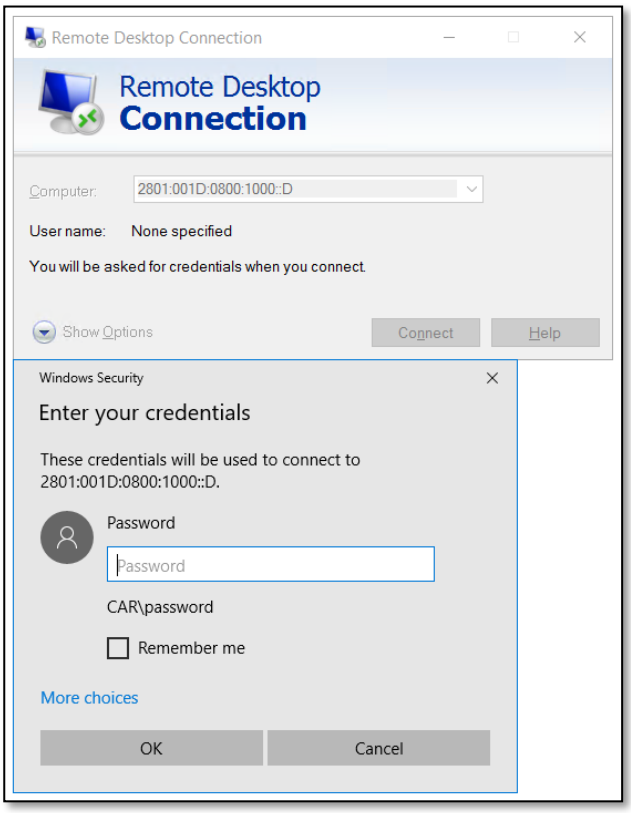
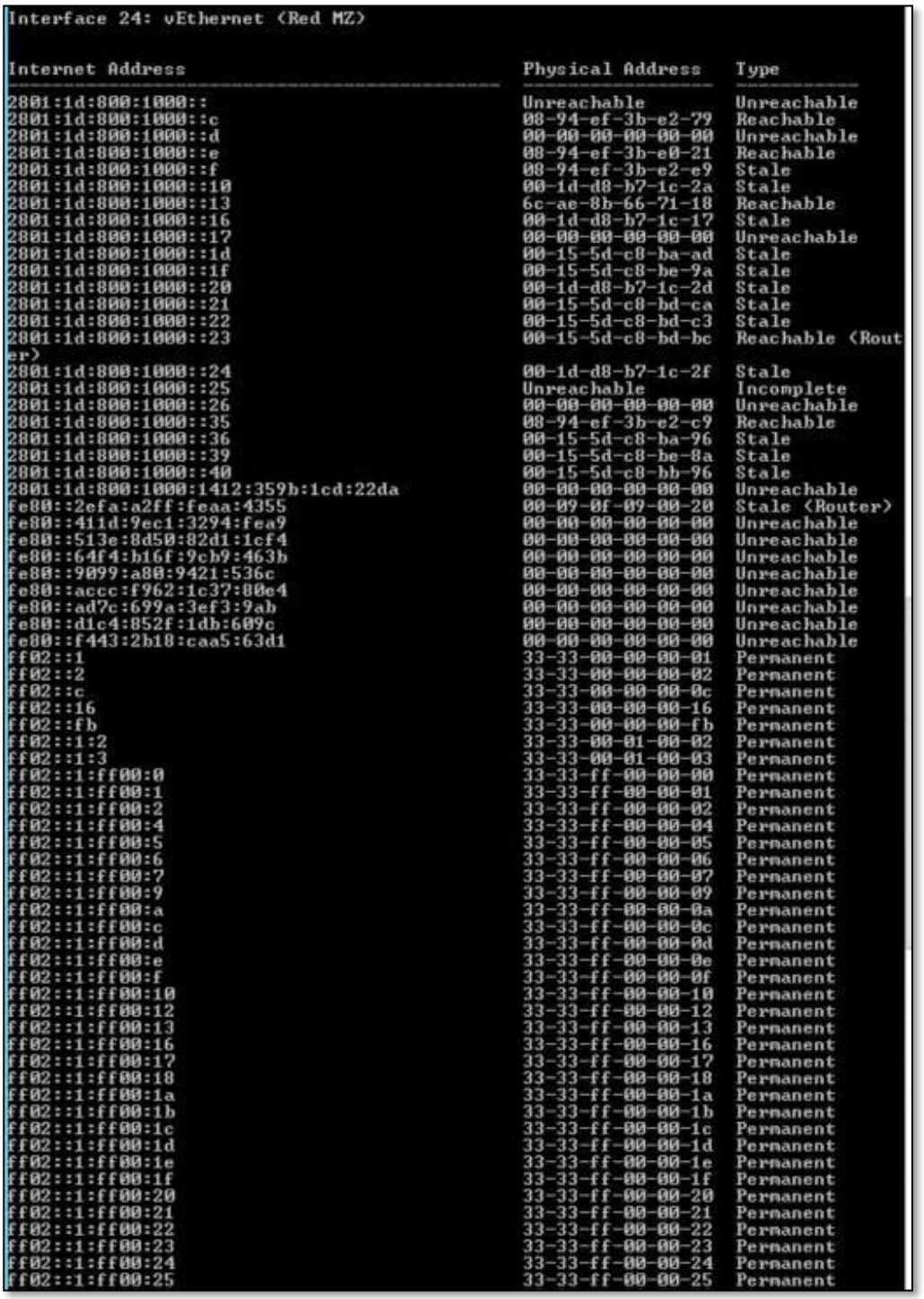


Ilustración 72. Conexión a Terminal Services por IPv6

Fuente: Autores

Dentro de la zona de servidores se ejecuta el comando **netsh interface ipv6 show neighbor** para realizar la comprobación de las conexiones por IPv6 de esos servidores:



```
Interface 24: vEthernet (Red MZ)

Internet Address                              Physical Address   Type
--------------------------------------------  -----------------  -----------
2801:1d:800:1000::                            Unreachable        Unreachable
2801:1d:800:1000::c                           08-94-ef-3b-e2-79  Reachable
2801:1d:800:1000::d                           00-00-00-00-00-00  Unreachable
2801:1d:800:1000::e                           08-94-ef-3b-e0-21  Reachable
2801:1d:800:1000::f                           08-94-ef-3b-e2-e9  Stale
2801:1d:800:1000::10                          00-1d-d8-b7-1c-2a  Stale
2801:1d:800:1000::13                          6c-ae-8b-66-71-18  Reachable
2801:1d:800:1000::16                          00-1d-d8-b7-1c-17  Stale
2801:1d:800:1000::17                          00-00-00-00-00-00  Unreachable
2801:1d:800:1000::1d                          00-15-5d-c8-ba-ad  Stale
2801:1d:800:1000::1f                          00-15-5d-c8-be-9a  Stale
2801:1d:800:1000::20                          00-1d-d8-b7-1c-2d  Stale
2801:1d:800:1000::21                          00-15-5d-c8-bd-ca  Stale
2801:1d:800:1000::22                          00-15-5d-c8-bd-c3  Stale
2801:1d:800:1000::23                          00-15-5d-c8-bd-bc  Reachable (Rout
er)
2801:1d:800:1000::24                          00-1d-d8-b7-1c-2f  Stale
2801:1d:800:1000::25                          Unreachable        Incomplete
2801:1d:800:1000::26                          00-00-00-00-00-00  Unreachable
2801:1d:800:1000::35                          08-94-ef-3b-e2-c9  Reachable
2801:1d:800:1000::36                          00-15-5d-c8-ba-96  Stale
2801:1d:800:1000::39                          00-15-5d-c8-be-8a  Stale
2801:1d:800:1000::40                          00-15-5d-c8-bb-96  Stale
2801:1d:800:1000:1412:359b:1cd:22da           00-00-00-00-00-00  Unreachable
fe80::2efa:a2ff:feaa:4355                     00-09-0f-09-00-20  Stale (Router)
fe80::411d:9ec1:3294:fea9                     00-00-00-00-00-00  Unreachable
fe80::513e:8d50:82d1:1cf4                     00-00-00-00-00-00  Unreachable
fe80::64f4:b16f:9cb9:463b                     00-00-00-00-00-00  Unreachable
fe80::9099:a80:9421:536c                      00-00-00-00-00-00  Unreachable
fe80::accc:f962:1c37:80e4                     00-00-00-00-00-00  Unreachable
fe80::ad7c:699a:3ef3:9ab                      00-00-00-00-00-00  Unreachable
fe80::d1c4:852f:1db:609c                      00-00-00-00-00-00  Unreachable
fe80::f443:2b18:caa5:63d1                     00-00-00-00-00-00  Unreachable
ff02::1                                       33-33-00-00-00-01  Permanent
ff02::2                                       33-33-00-00-00-02  Permanent
ff02::c                                       33-33-00-00-00-0c  Permanent
ff02::16                                      33-33-00-00-00-16  Permanent
ff02::fb                                      33-33-00-00-00-fb  Permanent
ff02::1:2                                     33-33-00-01-00-02  Permanent
ff02::1:3                                     33-33-00-01-00-03  Permanent
ff02::1:ff00:0                                33-33-ff-00-00-00  Permanent
ff02::1:ff00:1                                33-33-ff-00-00-01  Permanent
ff02::1:ff00:2                                33-33-ff-00-00-02  Permanent
ff02::1:ff00:4                                33-33-ff-00-00-04  Permanent
ff02::1:ff00:5                                33-33-ff-00-00-05  Permanent
ff02::1:ff00:6                                33-33-ff-00-00-06  Permanent
ff02::1:ff00:7                                33-33-ff-00-00-07  Permanent
ff02::1:ff00:9                                33-33-ff-00-00-09  Permanent
ff02::1:ff00:a                                33-33-ff-00-00-0a  Permanent
ff02::1:ff00:c                                33-33-ff-00-00-0c  Permanent
ff02::1:ff00:d                                33-33-ff-00-00-0d  Permanent
ff02::1:ff00:e                                33-33-ff-00-00-0e  Permanent
ff02::1:ff00:f                                33-33-ff-00-00-0f  Permanent
ff02::1:ff00:10                               33-33-ff-00-00-10  Permanent
ff02::1:ff00:12                               33-33-ff-00-00-12  Permanent
ff02::1:ff00:13                               33-33-ff-00-00-13  Permanent
ff02::1:ff00:16                               33-33-ff-00-00-16  Permanent
ff02::1:ff00:17                               33-33-ff-00-00-17  Permanent
ff02::1:ff00:18                               33-33-ff-00-00-18  Permanent
ff02::1:ff00:1a                               33-33-ff-00-00-1a  Permanent
ff02::1:ff00:1b                               33-33-ff-00-00-1b  Permanent
ff02::1:ff00:1c                               33-33-ff-00-00-1c  Permanent
ff02::1:ff00:1d                               33-33-ff-00-00-1d  Permanent
ff02::1:ff00:1e                               33-33-ff-00-00-1e  Permanent
ff02::1:ff00:1f                               33-33-ff-00-00-1f  Permanent
ff02::1:ff00:20                               33-33-ff-00-00-20  Permanent
ff02::1:ff00:21                               33-33-ff-00-00-21  Permanent
ff02::1:ff00:22                               33-33-ff-00-00-22  Permanent
ff02::1:ff00:23                               33-33-ff-00-00-23  Permanent
ff02::1:ff00:24                               33-33-ff-00-00-24  Permanent
ff02::1:ff00:25                               33-33-ff-00-00-25  Permanent
```

Ilustración 73. Comprobación de las conexiones por IPv6

Fuente: Autores

Se realiza la comprobación del DHCP principal SDOMBOG01, para monitorear que ya los equipos tengan asignación IPv6 dinámica:

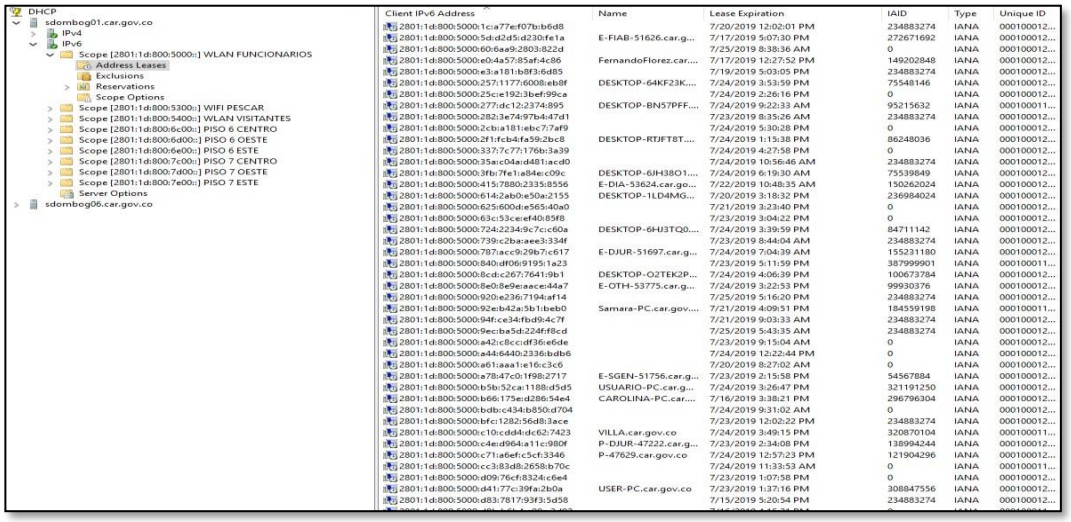


Ilustración 74. Monitoreo a DHCP principal SDOMBOG01

Fuente: Autores

Por último, se verifica que los servicios WEB se encuentren resolviendo en los protocolos IPv4 e IPv6 creados en los registros DNS de la Corporación.

Se crea el registro DNS en IPv6:

Ilustración 75. Registro DNS IPv6

Fuente: Autores

A nivel de herramientas de verificación de servicios en Internet, y redes locales, se valida con el complemento IPvFoo en el navegar WEB Google Chrome:

Ilustración 76. Servicios publicados en internet

Fuente: Autores

El Addon anterior, intercambia el valor numérico que se muestra de acuerdo a la versión del Protocolo IP con que está publicado, siendo 4 cuando resuelve a una dirección en IPv4 o 6 cuando lo hace en IPv6.

Así mismo, se confirma en la capa de red la resolución del nombre correctamente, con pruebas de ping para resolver por nombre:

Ilustración 77. Resolución de nombres

Fuente: Autores

Conectividad WAN, MPLS e Internet

La verificación WAN se inicia con la verificación de conectividad desde la Red LAN sede central a la Red MPLS:

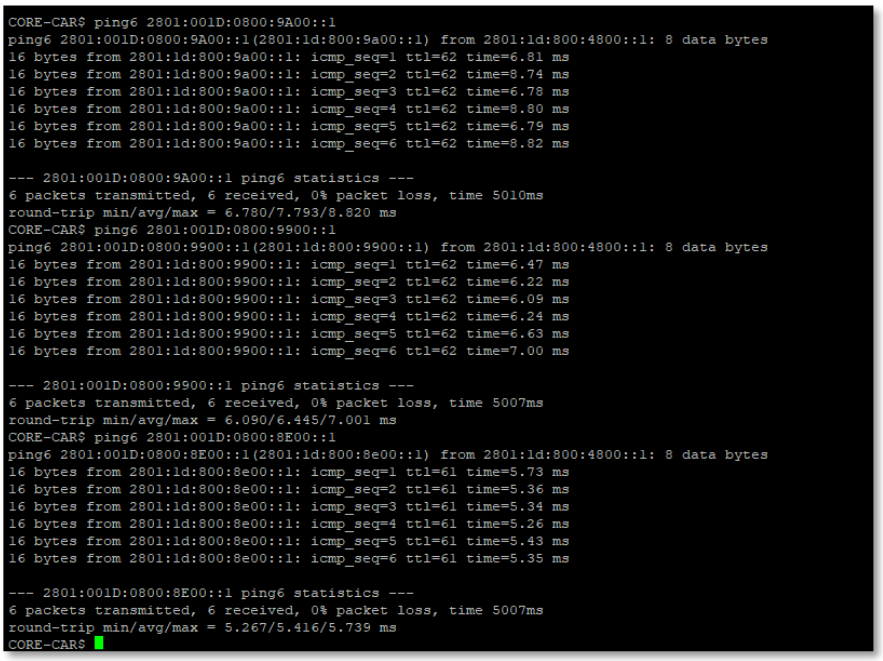


Ilustración 78. LAN a MPLS

Fuente: Autores

Siguiendo con las pruebas WAN, se verifica la correcta publicación del protocolo IPv6 en modelo Multihoming, sujeto a los dos operadores de servicio de Internet Movistar y ETB, la siguiente imagen presenta la comunicación prepend del protocolo BGP en el operador internacional Telia, operador para la ETB:

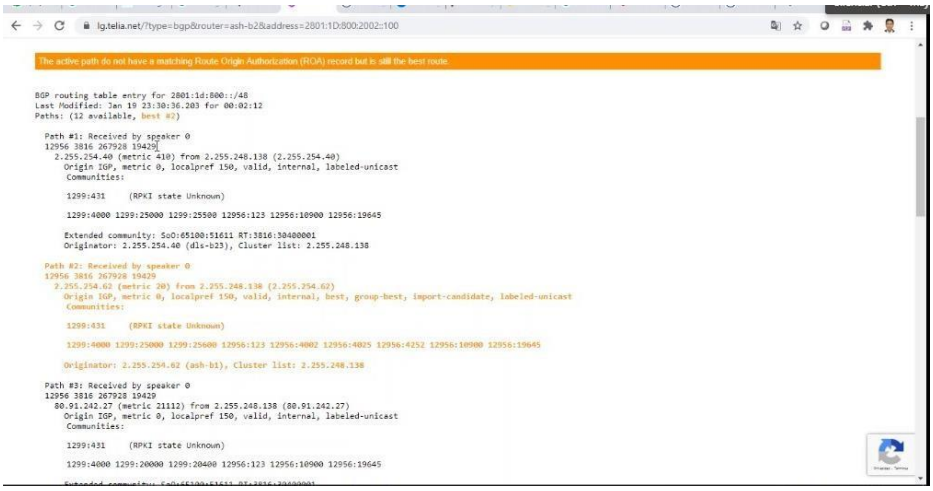


Ilustración 79. Prueba Sistema Autónomo

Fuente: Autores

Con ayuda de la plataforma Hurricane Electric, operador de servicios de Internet, se valida los saltos del ASN (Sistema Autónomo):

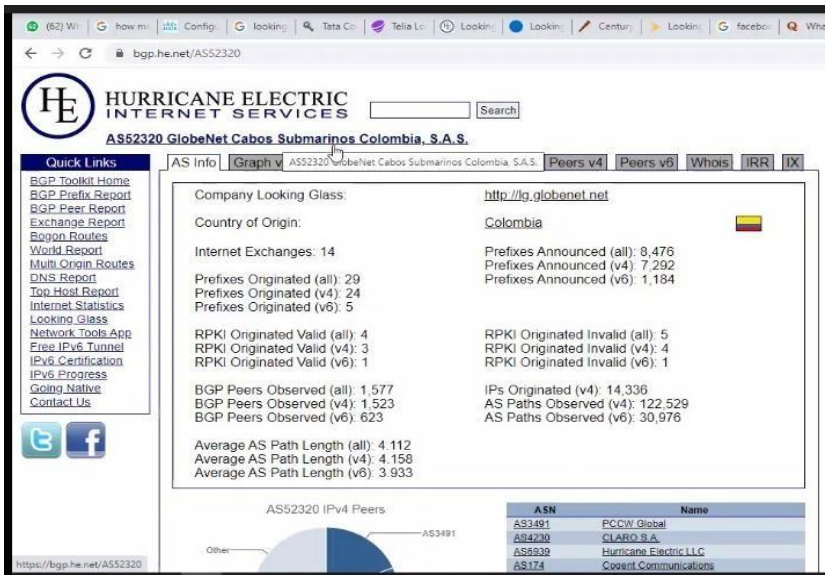


Ilustración 80. Verificación BGP Internet Hurricane

Fuente: Autores

Se verifica el prefijo IPv6 y ASN de la Corporación por medio del operador Internal para Movistar, TATA Communications, en el cual se valida la correcta publicación:

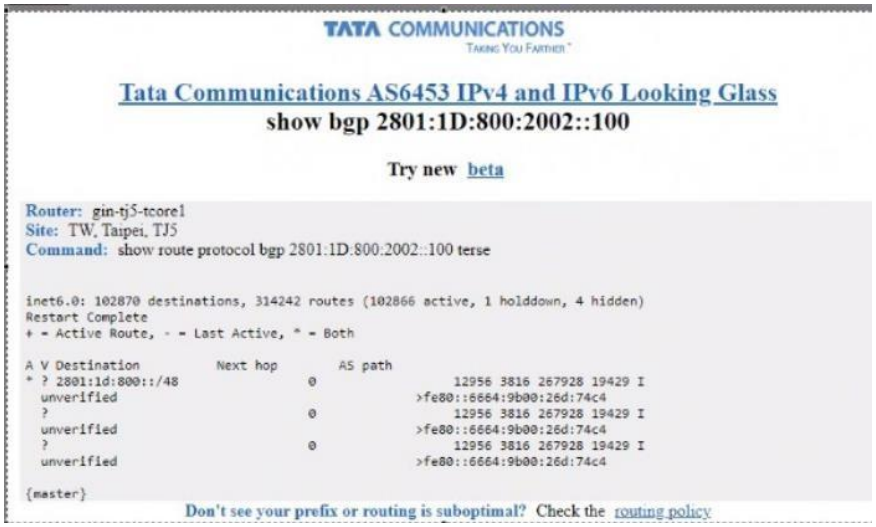


Ilustración 81. Verificación prefijo IPv6 CAR Cundinamarca Operador Internacional TATA Communication

Fuente: Autores

Se verifica el prefijo IPv6 y ASN de la Corporación por medio de la herramienta Looking Glass, herramienta que ratifica la comunicación WAN y saltos para llegar al dominio de Google.com en IPv6:

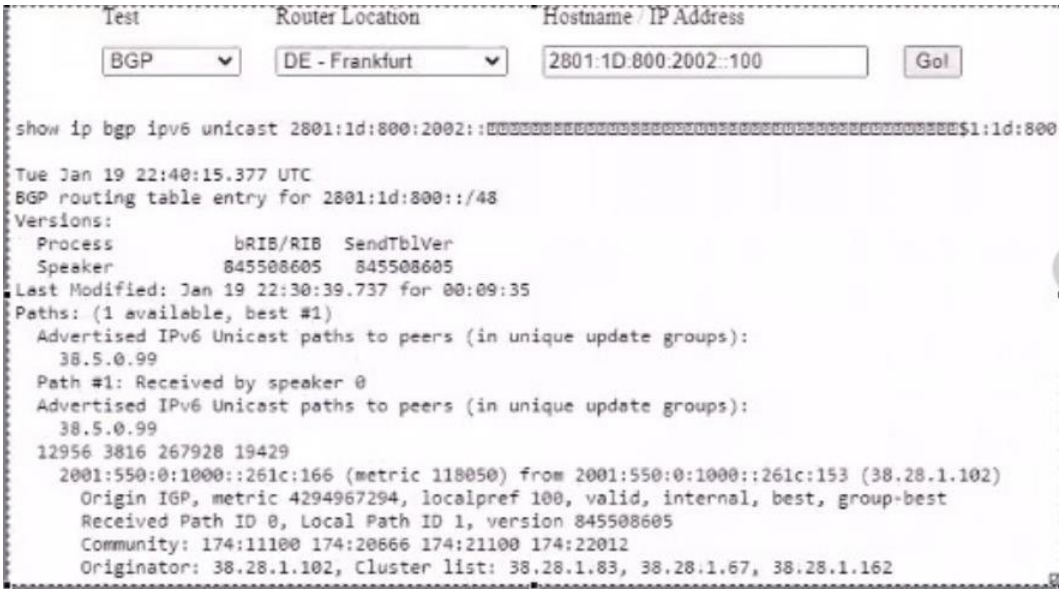


Ilustración 82. BGP Looking Glass prefijo IPv6 CAR

Fuente: Autores

Pruebas de Usuario

Se inicia con la verificación de la configuración de la tarjeta de red de la estación de trabajo del usuario:

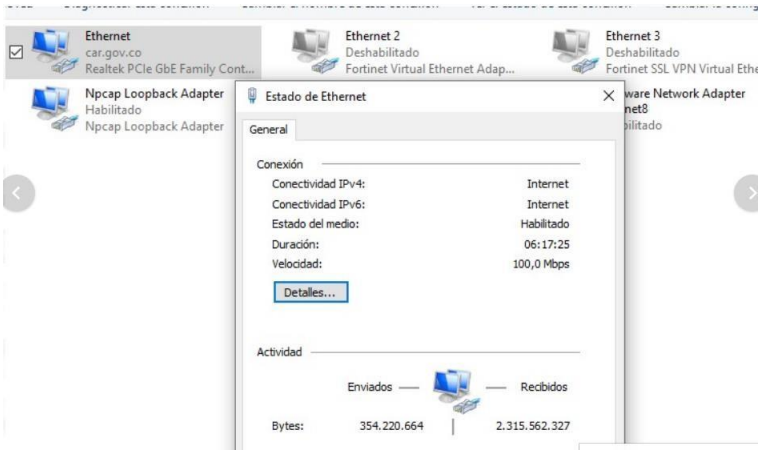


Ilustración 83. Estado adaptador ethernet terminal de usuario

Fuente: Autores

Prueba de conectividad a Internet de la PC previa mediante el uso del comando ping y tracert, con el complemento -6, el cual nos garantiza la conectividad mediante IPv6

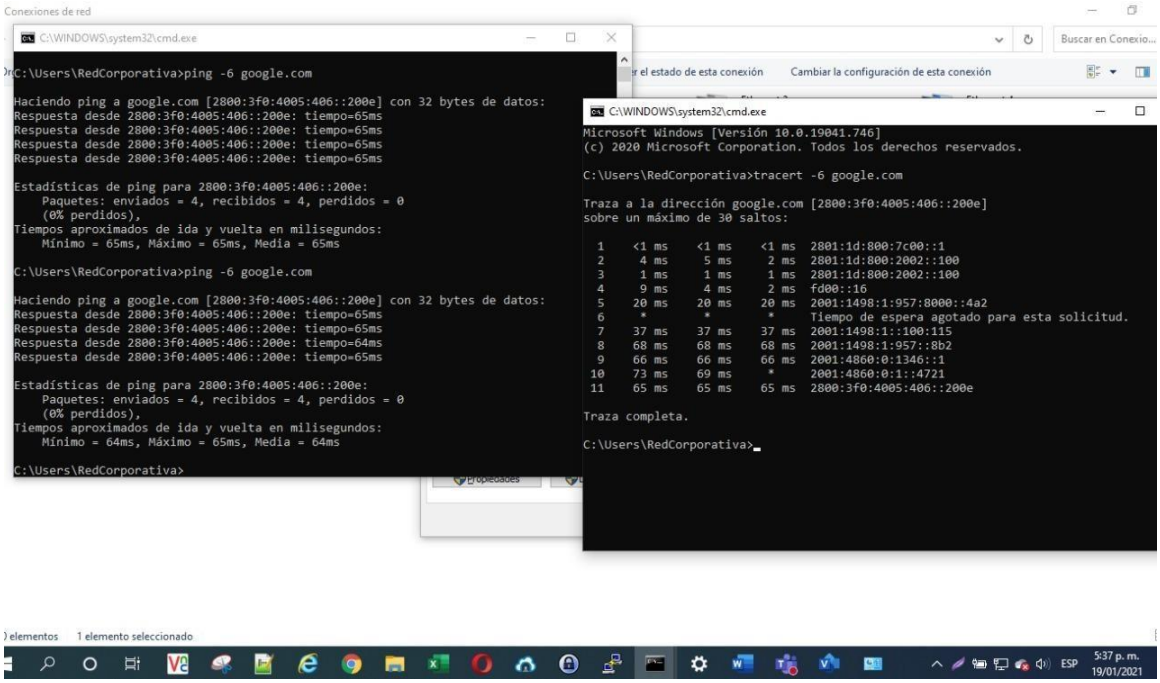


Ilustración 84. Comando ping-6

Fuente: Autores

En el ambiente tecnológico para usuario final, existen numerosas herramientas que le ayudan a gestionar o validar información desde los navegadores web, es por ello, que hemos recurrido al complemento IPvFoo el cual está instalado en la máquina del usuario en el navegador Chrome, desde este complemento vemos que se está navegando a través desde a un direccionamiento IPv6 y que así mismo acceder a los servicios WEB bajo este protocolo:

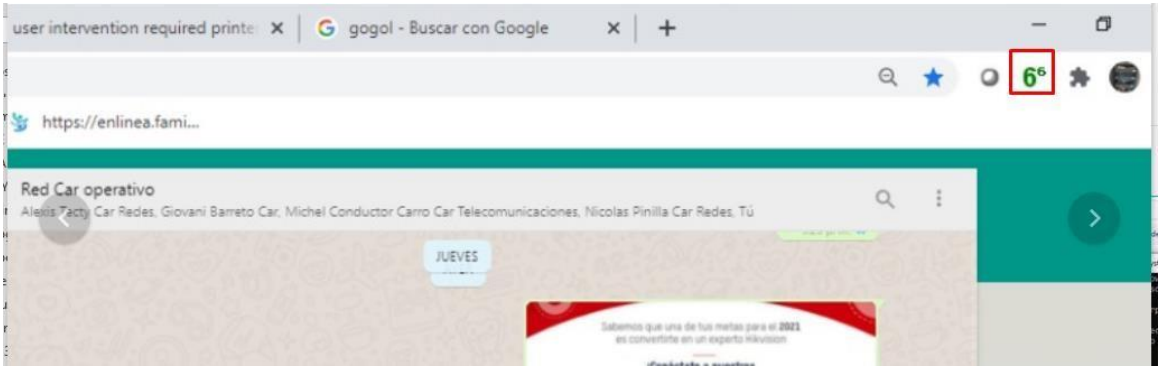


Ilustración 85. Confirmación navegación IPv6 Puro

Fuente: Autores

A modo de confirmación de satisfacción de la implementación realizada se procederá a generar encuestas (check list) de satisfacción, en dos modalidades. Dichas encuestas serán digitales mediante la herramienta de Google Forms.

Una de las encuestas será dirigida al grupo de oficina de sistemas de la Corporación, en la cual se auditará el desempeño en la plataforma tecnológica, comunicaciones internas y externas, acceso administrativo en los servidores y servicios, estabilidad en la comunicación de bases de datos con los aplicativos y así como de mayor relevancia la estabilidad de la replicación del dominio desde sitio central hacia los subsitios.

Esta encuesta de funcionamiento será diligenciada por los ingenieros a través del siguiente link https://forms.gle/rcTy2WMYBbaJ4vBP7

Ilustración 86. Formulario encuesta Interna funcionamiento de los servicios

Fuente: Autores

La segunda encuesta será dirigida al usuario final. En dicha encuesta se validaría el servicio percibido por el usuario final.

Dicha encuesta a nivel de usuario final debería tener un valor de aceptación del 70%, sujeto a que el desconocimiento tecnológico del usuario final no es garante a confirmar la fiabilidad de la implementación, sujeto a que, para un usuario sin conocimiento de tecnológico, una falla en un libro de Excel puede ser aludido a una falla de comunicaciones.

Los funcionarios podrán acceder a través del link que se podrá hacer llegar a través de un correo interno, éste hipervínculo sería https://forms.gle/qPNvV9m1ATLXCC9N8

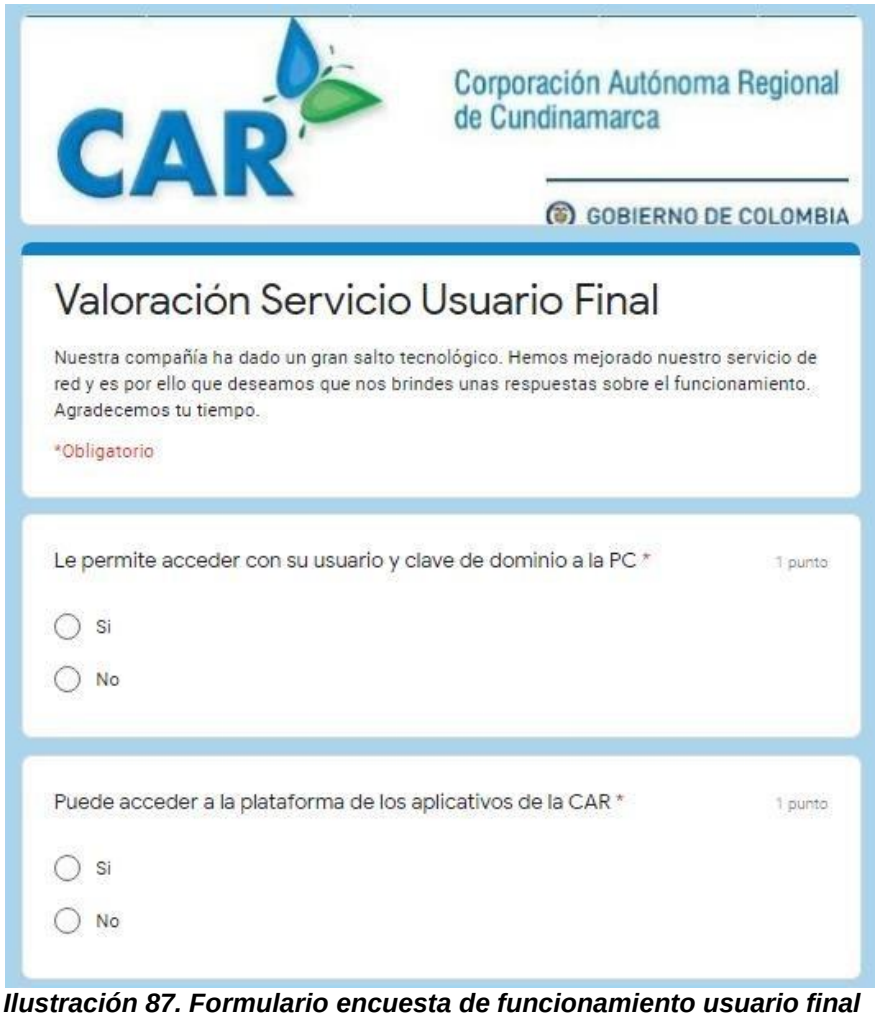


Ilustración 87. Formulario encuesta de funcionamiento usuario final

Fuente: Autores

CAPÍTULO 7: RECOMENDACIONES GENERALES

- Capacitar a todo el personal implicado en la gestión y manejo del protocolo IPv6.
- Todos los procesos de adquisición tecnológica futuro deben exigir la compatibilidad con IPv6.
- Para las aplicaciones comerciales que haya adquirido la entidad, solicitar al proveedor certificación de compatibilidad de que las aplicaciones pueden ser accedidas por IPv6. De ser posible, de una vez asignar una dirección IPv6 fija del ámbito de IPv6 a estos servidores con el fin de poder realizar el acceso tanto por IPv4 como por IPv6.

CAPÍTULO 8: TERMINACIÓN Y CONCLUSIONES DEL PROYECTO

Las actividades presentadas corresponden al desarrollo técnico de la solución dimensionada a la necesidad surgida y presentada para la CAR Cundinamarca, respecto al desempeño de su Red Corporativa.

Tras el levantamiento de la información y posterior análisis de esa data con las bases de información de los fabricantes se logró encontrar que la entidad contaba con todos los elementos requeridos para poder iniciar el plan de trabajo el cual incluyó una restructuración lógica permitiendo dar una mayor robustez en el manejo de privacidad y seguridad a la par de ir configurando el nuevo estándar de red IPv6.

Al momento de la implementación, desde la etapa de pruebas, se evidencia la operatividad de los servicios tecnológicos y acceso a la información, trayendo el menor impacto negativo. Todo eso fue logrado debido a la planeación y manejo central de cada proceso y por eso se puede decir que el presente proyecto para la entidad demuestra el acatamiento de la Resolución 2710 del 2017 del MinTIC pero que, sobre todo, debido a la naturaleza de la razón social y propósito de la entidad, ahora podrá implementar más proyectos donde involucren dispositivos IoT que requieran un direccionamiento único.

A nivel educativo, adquirimos un amplio conocimiento en la arquitectura de redes, así como afianzamos el conocimiento requerido para la puesta en marcha de la adopción del protocolo IPv6 en Dual Stack para una Red Corporativa.

REFERENCIAS BIBLIOGRÁFICAS

AL-IMAM, W. H. Un banco de pruebas IPv6 para soporte de movilidad en redes inalámbricas de próxima generación. . {En línea} 2011. Disponible en https://link.springer.com/chapter/10.1007/978-3-642-22027-2_2

BARBARA, Fred Baker. Core Protocols in the Internet Protocol Suite. {Enlínea} 2017 {Consultado en 2019}. Disponible en tools.ietf.org (en inglés).

IPv6go.Cuál es mi IPv6? {En línea} 2012. Disponible en http://www.ipv6go.net/cabecera_ipv6.php

IANA.IPv6 Addresses for the Root Servers. {En línea} 2008. {Enero 29 de 2008}. Disponible en https://www.iana.org/reports/2008/root-aaaa-announcement.html

LI, Q., JINMEI, T., & Shima, K. - DNS for IPv6. In Q. Li, T. Jinmei & K. Shima (Eds.), IPv6 advanced protocols implementation (pp. 207-288). Burlington: Morgan Kaufmann. {En línea} 2007 {Octubre de 2020} Disponible en doi:https://doi-org.bibliotecavirtual.unad.edu.co/10.1016/B978-012370479-5/50004-5

LUTZ, F. H., Bilbao, J. I., Paravan, C. A., Saade, S. D., Ostengo, A. A., & Ruiz, A. P. IPv6 firewall design. Paper presented at the 2018 IEEE Biennial Congress of Argentina, ARGENCON. {En línea} 2019 Disponible en doi:10.1109/ARGENCON.2018.8646207

MinTIC. ¿Qué es IPv6? IPv6 en Colombia. {En línea} 2019. Disponible en: https://www.min ic.gov.co/portal/inicio/Micrositios/IPV6/IPv6-Colombia/5892

Ministerio de industria, tecnología y turismo de España. Transición a IPv6. Protocolo de Internet versión 6. {En línea} 2016. {Consultado en 2019}. Disponible en https://www.mincotur.gob.es/

OBS Bussines School. Proyecto: Definición de objetivos y criterios. {En línea} 2018 (Octubre 16 de 2018) Disponible en https://www.obsbusiness.school/blog/proyecto-definicion-de-objetivos-y-criterios-para-su-seleccion

DE LA HOZ NATERA, Henry Alberto. Diseño y desarrollo de la fase de planeación del proyecto de adopción de ipv6 en la infraestructura tecnológica y de comunicaciones de una entidad adscrita al ministerio de Agricultura. {En línea} 2016 Disponible en http://polux.unipiloto.edu.co:8080/00003432.pdf

Sinnap. .Alcance de proyectos {En línea} 2019 Disponible en https://www.sinnaps.com/blog-gestion-proyectos/alcance-de-un-proyecto

SANDOVAL, R. Consideraciones del IPv6 Forum Council Colombia al Proyecto de Resolución “por la cual se formulan las políticas de adopción del protocolo ipv6. {En línea} 2017 Disponible en https://academiaipv6.org/2017/05/consideraciones-del-ipv6/

STRICKX, Tom. How Verizon and a BGP Optimizer Knocked Large Parts of the Internet Offline Today. {En línea} 2017 {Consultado en 2019}. Disponible en Cloudflare (en inglés).

Universidad Internacional de Valencia. Redes de datos. {En línea} 2019. Disponible en https://www.universidadviu.com/redes-de-datos-todo-lo-que-hay-que-saber-sobre-ellas/

VITA

Jhon Edizon Cruz Hernández, Futuro Ingeniero de Telecomunicaciones nacido en la ciudad de Bogotá en el año de 1987 rodeado de amor y apoyo brindado por su familia, pero sobre todo por dos mujeres, su madre y su tía, mujeres valientes, trabajadoras y de gran corazón que, aunque no contaban sino con educación básica, supieron brindarle los mejores principios de la vida.

En su etapa de educación primaria descubrió su propósito de vida profesional a través de la curiosidad del manejo de un regulador de voltaje que permitía operar su primer computador y que a partir de allí se adentró en la internet a través de las descargas de música, pero fue sólo hasta después de cursar dos veces la carrera de sistemas pudo entender que las telecomunicaciones harían parte de su vida no solo personal sino profesional y que por ello poco a poco, se fue instruyendo y compartiendo con personas fundamentales que lo guiarían en ese camino profesional productivo.

Jeison Jair González Vargas, nacido en el municipio de Buenavista Boyacá el año 1990, integrante de una familia de 4 miembros, papá, mamá y hermana.

Futuro ingeniero en telecomunicaciones, tecnólogo en gestión de redes de datos, conocimientos en administración de redes de datos, seguridad perimetral e implementaciones en arquitecturas de redes y telecomunicaciones en los protocolos IPv4 e IPv6.