Transición de una red IPv4 a IPv6 manteniendo la coexistencia de los protocolos

Jeisson David Novoa Socha

Universidad Nacional Abierta y a Distancia –UNAD

CEAD José Acevedo y Gómez

Especialización Redes de Nueva Generación

2022

Resumen

Es de tener en cuenta que, el protocolo de direccionamiento para la interconexión de redes global, en donde sus objetivos de función son diversos gracias a los diferentes avances en las comunicaciones y al crecimiento notorio de internet, ha llegado a su agotamiento, así que la versión en uso, IPv4; ha consumido cerca de la totalidad de sus direcciones IP, por lo tanto, fue necesario la implementación de un protocolo nuevo a nivel global, capaz de suplir y mejorar las necesidades entregadas por su antecesor, así que, se generó IPv6. Y aunque su aprovisionamiento no ha sido instantáneo se tiene previsto que la mayoría de las compañías hagan este durante los próximos años, lo que es un avance a las redes NGN de suma importancia ya que gracias a este se permitirá la convergencia de aplicaciones y servicios en producción y análisis, como por ejemplo la tecnología 5G o IOT (internet de las cosas). De tal manera que, el presente trabajo tiene como finalidad presentar una guía informativa que conceda los datos y de la manera como se podría ejecutar la transición y aprovisionamiento del protocolo IPv6 dentro de las compañías, en especial, las empresas pequeñas; se entregaran algunos apuntes de varios de los métodos de transición IPv4-IPv6 que se ejecutan en la actualidad, direccionamiento y forma de asignación de direcciones, además protocolos de encaminamiento y otros puntos importantes que tienen como diferenciador de IPv6 con IPv4.

Palabras Clave: IPv6, IPv4, Transición, Enrutamiento, Redes NGN

Abstract

It must be taken into account that the addressing protocol for the interconnection of global networks, where its function objectives are diverse thanks to the different advances in communications and the notorious growth of the Internet, has reached its exhaustion, so the version in use, IPv4 ; has consumed almost all of its IP addresses, so it was necessary to implement a new protocol at a global level, capable of supplying and improving the needs delivered by its predecessor, for which IPv6 will be followed up. And although its provisioning has not been instantaneous, it is expected that most companies will do so in the coming years, which represents an advance to NGN networks of great importance and thanks to the fact that it will allow the convergence of applications and services in production. . and analytics, such as 5G or IOT (internet of things) technology. In such a way that the purpose of this work is to present an informative guide that provides the data and the way in which the transition and provisioning of the IPv6 protocol could be executed within companies, especially small companies; Some notes will be given on the various IPv4-IPv6 transition methods currently in use, addressing and how to propose addresses, as well as routing protocols and other important points that differentiate between IPv6 and IPv4.

Keywords: IPv4, IPv6, Transition, IPv6 Routing, NGN Networks.

Tabla de Contenidos

Lista de tablas

Introducción

En el área del networking actual, es esencial tener en cuenta que, el protocolo de direccionamiento para la interconexión de redes global (IPv4), donde sus funcionalidades son diversas gracias a los diferentes avances en las telecomunicaciones y al crecimiento notorio del Internet, ha alcanzado su máxima capacidad de direcciones asignables, es decir, se encuentra en su fase final, la de agotamiento, donde la IANA (Internet Assigned Numbers Authority) confirma que se ha consumido cerca de la totalidad de las direcciones IPv4, por ende, hace algunos años se iniciaron investigaciones y se emplearon varias estrategias llegando a la conclusión de la implementación de un nuevo protocolo que pueda cumplir las mismas funcionalidades que IPv4 y además de mejorar las falencias que se identificaron del protocolo ya mencionado, de este modo se generó IPv6. No obstante, cabe recalcar que su aprovisionamiento no se ha efectuado de forma instantánea, donde se tiene previsto que la mayoría de las compañías ejecuten esto en los próximos años, sumándole un nuevo y valioso avance a las redes ngn, ya que con este nuevo protocolo se permitiría la convergencia de nuevas aplicaciones y servicios en producción y análisis, como por ejemplo la tecnología 5G o IOT (Internet de las cosas – Internet of things). De este modo, el presente trabajo tiene como finalidad brindar información relevante que conceda datos y colabore a desarrollar tácticas para la transición y aprovisionamiento de este en las diferentes redes, especialmente en Colombia teniendo en cuenta que debe coexistir con el protocolo actual. Se entregarán diferentes puntos de vista de los variantes métodos de transición, además de protocolos de enrutamiento y como sus nuevas versiones se adaptan a IPv6, así como servicios que deben reformarse para que puedan funcionar tanto en IPv4 como en IPv6

Metodología

Para ejecutar el presente documento, el cual tiene como principal meta desarrollar un marco de referencia con información relevante sobre la transición de IPv4 a IPv6 en una empresa, conociendo y entendiendo todos los parámetros teóricos y prácticos, se ha diseñado la siguiente metodología en la cual se abarcarán todos los puntos clave desplegados en varias fasesy actividades para dar cumplimiento a los objetivos planteados.

Tabla 1. Metodología del proyecto

Metodología												
ACTIVIDAD PRINCIPAL	**ACTIVIDAD COMPLEMENTARIA**	**MES 1**	**MES 2**	**MES 3**	**MES 4**	**MES 5**	**MES 6**	**MES 7**	**MES 8**	**MES 9**	**MES 10**	**MES 11**
Adquisición de información	Investigación sobre historia y actualidad del protocolo IPV6	X										
	Estudio acerca de protocolos, mecanismos y servicios que soporta y utiliza IPV6	X										
	identificación de ventajas y desventajas del		X									

	protocolo en mención				
	Análisis de los servicios y aplicaciones que se pueden utilizar con IPV6	X			
	Verificación de los equipos que soportan dicha tecnología.		X		
Obtención de los estándares Técnicos para la implementación de IPV6	Mención de toda la normativa sobre IPV6, además de los estándares establecidos para el protocolo que permitan la adecuada ejecución del mismo en Colombia.		X	X	
Revisión de la documentación sobre entidades en	Validación de diferentes proyectos que hagan uso de la transición de IPV4 a IPV6, esto para			X	X

Colombia con implementación IPV6.	partir de una base y tener una guía al momento del diseño y la ejecución del ejemplo práctico.					
Ejecución de ejemplo de transición de una red IPV4 a IPV6	Fase de investigación de los elementos que se utilizan para la transición.	X	X			
	Planeación y estrategia para la ejecución del proyecto con fines de una transición adecuada basándose en las reglas del MINTIC		X			
	Implementación de acuerdo a lo diseñado en la fase de Planeación			X	X	
	Periodo de pruebas de funcionamiento y detección de errores					X

Análisis y compilación de la información	Ejecución de las conclusiones y análisis de las mismas con el fin de argumentar los procedimientos ejecutados para la transición de IPV4 a IPV6	X

Planteamiento del problema

Las redes modernas con el pasar del tiempo, van incrementando la velocidad con la que evolucionan su tecnología y sus funcionalidades, generando efectos notorios dentro de la vida cotidiana, no obstante, tal desarrollo tecnológico genera diferentes obstáculos que los ingenieros y especialistas enfocados en sus áreas deben abarcar con varias estrategias con el fin de seguir dando pasos agigantados. Este es el caso de los protocolos de direccionamiento, en donde desde hace varios años se ha venido implementando el nuevo protocolo IPv6, resaltando que no se ha apagado la red en IPv4 así que deben mantener su coexistencia (al menos por unos cuantos años), no obstante y a pesar de la evolución continua y rápida de la tecnología, IPv6 está presentando un despliegue bastante lento, especialmente en Latinoamérica donde se puede encontrar que el mayor país de adaptación de este protocolo es Brasil con un 35.43% (ni siquiera se ha llegado a la mitad de adaptación de su infraestructura) donde Colombia lamentablemente tiene una adaptación del 8.73% para este 2020 según información de la LACNIC (Registro de Direcciones de Internet de América Latina y Caribe), esto se debe a diferentes motivos, donde algunos de estos pueden ser la escasez de recursos o la falta de conocimiento y habilidades sobre IPv6 en el País, para esto último debe tenerse en cuenta que son muy pocos los lugares donde se enseña adecuadamente el funcionamiento de este, además de que tampoco resulta tan fácil emplear una transición pronta sin tener los dos puntos mencionados anteriormente (recursos – conocimiento técnico), y esto se puede apreciar identificando cuáles son las compañías que tienen IPV6 en este momento, donde destaca que la mayoría son entidades gubernamentales o entidades públicas, es decir que en este orden de ideas las empresas privadas y más aún las

empresas medianas y pequeñas que hacen uso de las redes, ven lejos la posibilidad de apropiarse de esta nueva tecnología.

Por otro lado, y no menos importante cabe destacar que con la demora por los diferentes motivos existentes para la implementación apropiada de IPv6, se está tardando la ejecución masiva de algunos servicios que se han diseñado con anterioridad, pero que solo es posible ejecutarse por medio de este protocolo, y aunque en algunos países o en algunos puntos se implementen, aun se tiene mucho camino que recorrer para llegar a donde se quiere. Estos servicios son IOT y 5G. ¿Pero, por qué no implementarse con IPv4 mientras se despliega completamente IPv6?, la respuesta es sencilla, aunque su solución compleja, dado que este tipo de servicios necesitarían de una alta capacidad de direcciones públicas para poder por ejemplo hacer uso de los distintos dispositivos como lavadoras, estufas, carros, etc., desde lugares remotos. Y con IPv4 es imposible efectuar esto dado al agotamiento que se presenta. Igual pasa con la tecnología 5G que también debe hacer uso de un alto tamaño de direcciones que envíen el tráfico de los dispositivos a internet.

Aun se tienen varias complicaciones al momento de usar este tipo de direccionamiento, sin embargo, en el presente trabajo se darán algunos conceptos y pautas que puedan contribuir a una elaboración o diseño apropiado y rápido de una red con IPv6.

Justificación

Con la monografía a realizar se pretende brindar información detallada acerca de los diferentes aspectos y parámetros que se manejan dentro de IPV6, no solo a nivel técnico sino también pautas y recomendaciones que se pueden diseñar para un correcto funcionamiento de este tipo de red, logrando que el material sirva de forma educativa para los ingenieros y técnicos que futuramente emplearan estrategias y despliegues de IPV6 en las diferentes empresas y zonas, teniendo como punto fuerte que no solo se hará explicación teórica sino también practica con algunos equipos que se usan en la vida cotidiana del networking, como pueden ser dispositivos Cisco o Juniper.

Cabe recalcar que el propósito de la monografía es poder aumentar la celeridad del despliegue de IPv6 especialmente en Colombia donde su adaptación aún es muy baja, por ende, también se harán referencias de costos de equipos y costos de implementación a la hora de aprovisionar una red nueva o si se desea intentar hacer uso con la infraestructura actual.

Por otro lado, y no menos importante, se tratarán los estándares de las comunicaciones para IPv6, cuales entidades lo rigen y cuáles son los que se tienen pactados para el despliegue de esta nueva tecnología.

Por último, es necesario tener en cuenta que la migración puede ejecutarse de dos formas, temporal o permanente, en la temporal se tendrá coexistencia de IPv4 e IPv6. Mientras que en el aprovisionamiento permanente IPv6 será el predominante, esto es mencionado ya que se indicaran equipos y protocolos que puedan soportar ambos (IPv4 e IPv6) y cuales solo manejan un solo tipo de pila (Protocolo).

Objetivos

Objetivo general

Presentar un documento detallado de los diferentes puntos técnicos, normativos y estratégicos para la implementación y despliegue del protocolo IPv6, donde se trabaje tanto el ámbito teórico como el práctico y así lograr un mayor beneficio y apropiación de esta tecnología, con el fin de colaborar en el área e incentivar y promover el aprovisionamiento de este protocolo especialmente en Colombia.

Objetivos específicos

1. Desarrollar un marco teórico que abarque de manera clara toda la información correspondiente a la infraestructura de IPv6: protocolos de enrutamiento que se pueden usar con este protocolo, métodos de transición, tipos de direcciones IPv6, cambios de estructura en servicios como dns o dhcp, funcionamiento de Mpls/VPN sobre IPv6, seguridad y otros aspectos a tener en cuenta para un adecuado despliegue.
2. Mencionar los estándares y entidades que mantienen la reglamentación de IPv6.
3. Destacar los servicios nuevos que se podrían ejecutar y poner en producción con esta tecnología.
4. Llevar los puntos teóricos a metodologías practicas por medio de emuladores como GNS3 con el fin de adquirir mayores habilidades en la implementación de IPv6.
5. Destacar las ventajas y desventajas del protocolo, y cuáles son sus diferencias con IPv4.

Marco Teórico

Historia y estadísticas

IPv6 surge como necesidad y respuesta al agotamiento de las direcciones IPv4 que desdeinicios de los años 2000 se empezaron a ver muy notorias, por lo tanto, luego de varios estudiosy planeaciones se presentó IPv6 como medida de mitigación del agotamiento de dichas IP's, la cual se adapta a la infraestructura actual y al plan de crecimiento escalable continuo que están teniendo las redes de comunicaciones.

Sin embargo, nos podemos remontar a 1990 cuando se hicieron los primeros estudios sobre agotamiento IP, no obstante, solo se hablaron de posibles soluciones sin determinar una especifica que pudiese combatir con esto, pero se debe tener en cuenta que el internet se explota comercialmente a mediados de 1993 donde se intensifican las discusiones sobre si las direcciones en IPV4 rendirían viendo el mal uso que se estaba haciendo de estas, además del incremento de las tablas de ruteo. Por otro lado, la IEFT un año atrás (1992) creo el grupo ROAD (routing and addressing) especializado y enfocado en todo lo relacionado con una posible escasez de direcciones IP, cabe resaltar que inicialmente las distribuciones para dichas direcciones se establecieron por clases: A, B C y direcciones reservadas, donde las direcciones de clase A (tienen una mayor y amplia cantidad de IP'S) fueron asignadas a algunas empresas como IBM, HP, MIT, US ARMY, etc. Las cuales monopolizaron una gran parte de IP's, esto se menciona ya que con el grupo ROAD y con el inicio del CIDR (RFC 4632) se adoptaron nuevas estrategias con el uso de las redes, allí se apreciaron los siguientes detalles:

1. Fin del uso de clase en las direcciones
2. Uso de prefijos/longitudes para complementar el fin de las clases.

3. Agregación de rutas
4. Dhcp para poder mantener la red con mayor control de manera automática
5. Creación del NAT (address allocation for private internets) para hacer usos de pocas IP's públicas, lo cual permite hacer conectar redes con una sola IP

Este último presenta varias ventajas como:

1. Reducción de la necesidad de una gran cantidad de direcciones públicas.
2. Facilita la numeración interna de las redes proporcionando un mayor control de la infraestructura.
3. Oculta la topología de las redes.
4. Este solo permite la entrada de paquetes, produciendo una respuesta a un pedido de la red.

De igual manera esta posee algunas desventajas:

1. Quiebra el modelo ya conocido, el de punto a punto de internet
2. Dificulta el funcionamiento de algunas aplicaciones.
3. No es escalable.
4. Aumento de procesamiento en los dispositivos que efectúan la funcionalidad de NAT
5. Complicaciones al momento de rastrear el camino del paquete.
6. Impide el uso de mecanismos de seguridad.

No obstante, ninguna de las soluciones propuestas brindaba un resultado satisfactorio, ya que todo concluía en que de igual manera en algún momento se acabarían las direcciones IP, por tal motivo, en 1992 se creó IPng (Ip next generation), una propuesta de IEFT donde se unían

varios conceptos de red anteriores, y gracias a esto y con estudios más conceptualizados y con mayor profundización, se originó la idea de IPv6 en 1998:

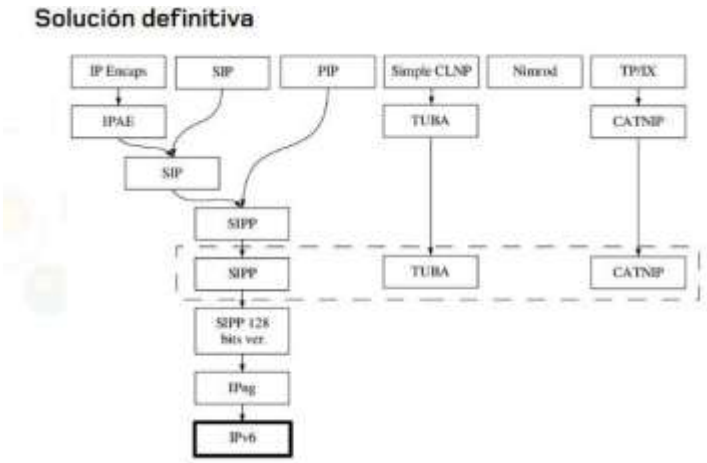


Figura 1. Estructura de grupos para la solución de agotamiento

Esta idea, se establece bajo el RFC 2460, donde a diferencia de tener 32 bits como en IPV4, tendrá 128, proporcionando una cantidad inmensa de direcciones disponibles, además de esto su cabezal se vuelve mucho más simplificado que la anterior versión, esto gracias al uso de cabezales de extensión, que son usados solo en caso de ser necesario. Por otro lado, este protocolo brinda más funcionalidades de seguridad como mecanismos IPSEC incorporados.

Este protocolo fue altamente aceptado lo cual permitió el inicio de estrategias para la implementación de esta, sin embargo, en la actualidad solo se tiene un aproximado del 32% de despliegue a nivel mundial:

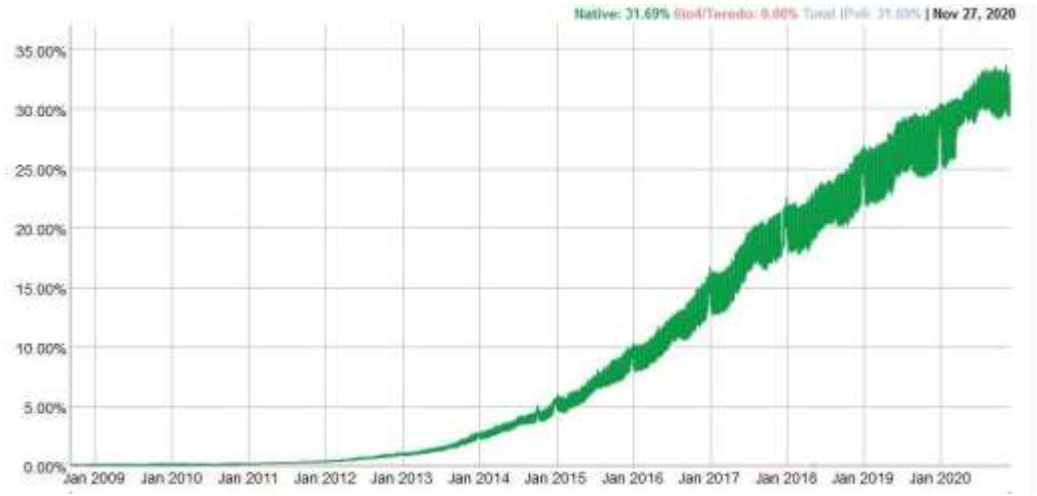


Figura 2 Grafica de crecimiento IPv6

Donde podemos identificar que Latinoamérica tiene una baja cantidad de redes en IPV6.

Figura 3 Despliegue IPv6 globalmente

Y sobre todo preocupa que, aunque el RFC de IPv6 se originó en 1998, esta grafica del 2020 muestra que Colombia solo posee un 12% aproximado de despliegue.

Figura 4 Adopción IPv6 en Colombia

Por ello, aún se encuentra en vigencia el protocolo IPv4 y aun se hacen uso de técnicas para evitar el agotamiento, como por ejemplo en el 2010 los proveedores de servicio inician la puesta en marcha del Carrier Grade NAT o mejor conocido como el NAT a gran escala donde seagrega una capa extra de NAT en la red de los ISP además de una capa adicional en la red del cliente final, no obstante, al igual que proyectos usados con anterioridad, esta posee varios problemas que impide a la red funcionar en un 100%.

Otra de las alternativas que se han optado en los últimos años, es la de re-utilizar bloques de direcciones o segmentos de red específicos, es decir, alguna empresa o entidad que deja de utilizar algún tipo de direccionamiento, retomar estas y volverlas a proporcionar. En especial con empresas como a las que se le dio grandes pools de IP’s en los comienzos del internet y que hoy en día no estaban usando estos. Pero igualmente esto no detiene el agotamiento IPv4.

En conclusión, es necesario implementar la red IPv6 haciendo visión a futuro, dado que es importante resaltar que, a pesar de los inconvenientes para el despliegue de este protocolo, al menos la mitad del contenido de internet es establecido por IPv6, donde la mayoría del tráfico se

encuentra en sitios conocidos como Google, Youtube, Netflix, Facebook. Así que, para usar las funcionalidades, aplicaciones actuales y futuras, nuevos diseños de red, servicios emergentes como 5G o IOT, es esencial poseer infraestructura en IPv6 ya sea manejando mecanismos de transición o bien sea proporcionando una solución plenamente nativa o en dual stack (ya se verá este concepto en las próximas paginas).

Cabezal IPv6

A diferencia de IPv4, este nuevo protocolo posee 40 Bytes fijos (IPv6 tiene entre 20 y 60Bytes), por lo que lo convierte en mucho más simple, además de ser más flexible esto gracias al uso de extensiones en su cabezal. También posee mucha más eficiencia, ya que reduce el procesamiento de los paquetes, y también minimiza el overhead en sus cabezales.

Para lograr lo dicho con anterioridad, se tuvo que eliminar y cambiar algunos campos que se encontraban en el protocolo IPv4, estos campos son:

1. Longitud: Fue eliminada dado que en IPv6 se tiene un tamaño fijo.
2. Fragment Offset: Ya que la fragmentación en este nuevo protocolo se maneja de manera diferente.
3. Checksum de cabecera o suma de verificación: esto se quitó porque se determinó que este tipo de validaciones se podían efectuar en capas inferiores y superiores
4. Opciones: Esto más que eliminar se puede determinar como un remplazo, dado que el nuevo campo de extensiones cumple funciones similares a la de opciones.
5. Identificación y Flags

Por otro lado 4 campos tuvieron cambio de nombre y de ubicación:

1. Tipo de servicio (TOS) – Clase de tráfico (TC)
2. Tamaño de total – Tamaño de datos
3. Protocolo – Próxima cabecera.
4. Tiempo de vida (TTL) – Limite de encaminamiento (hop limit)

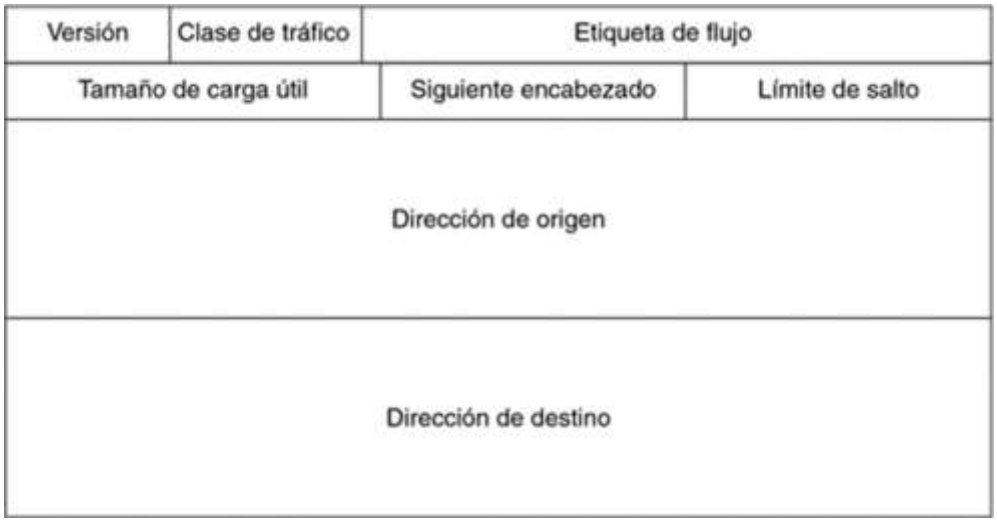


Figura 5 Cabezal IPv6

5. Versión: número de versión de 4 bits del protocolo de Internet, con este se puede identificar la versión del protocolo usado 6 o 4.
6. Clase de tráfico: Este campo posee 8 bits. En él se identifica el tipo de paquete que está siendo transmitido y recibido, se puede hacer por prioridad o por clases.
7. Etiqueta de flujo: campo de 20 bits, Este se diseñó para dar tratamiento a los diferentes flujos de datos sin necesidad de verificar las aplicaciones.
8. Tamaño de carga útil: contiene 16 bits, que indica el resto del paquete que sigue al encabezado de IPv6.
9. Próximo encabezado: Posee 8 bits, con este se determina que encabezado sigue al IPv6.

10. Límite de saltos: Con 8 bits, sirve como en TTL para determinar el salto máximo de routers que el paquete puede efectuar antes de ser descartado.
11. Dirección de origen y de destino: indica la IP que envía el paquete y a la cual va dirigida, con 128 bits cada uno de estos campos.

La cabecera de extensión se encuentra entre la capa IPv6 y la siguiente capa ya sea TCP o UDP (transporte). Por otro lado, si se requiere de varias extensiones estas se unen formando una cadena de extensiones.

Cabezales de extensión

Estas son algunos de los cabezales usados en la fracción de extensión:

1. Hop-by-Hop: Identificado por el valor 0 en el campo próxima cabecera, allí se carga información que debe ser procesada por todos los nodos a lo largo del camino que siga el paquete.
2. Routing: Identificado por el valor 43 en el campo próxima cabecera, desarrollado inicialmente para listar uno o más nodos intermedios que deben ser visitados hasta que el paquete llegue a destino.
3. Fragmentación: Identificado con el valor 44, es la información sobre los fragmentos IPV6 de los paquetes transmitidos.
4. Encapsulating Security Payload: Se identifica con el valor 52 en el campo de próximo cabezal, esta usado por IPSEC en este se garantiza la integridad y confidencialidad de los paquetes.

5. Authentication header: Identificado con el valor número 51 en el campo de próximo cabezal, se usa por IPSEC para proveer autenticación y garantía de integridad de los paquetes IPv6.

Mecanismos de transición

A pesar de que IPv6 ha sido diseñado para remplazar el protocolo IPv4, este posee un funcionamiento bastante amigable, dado que fue desarrollado para facilitar la transición y coexistencia con IPv4, debido a que los expertos esperan y proyectan que este último dure varias décadas en apagar su red. Por lo tanto, se poseen una serie amplia de opciones para poder desplegar IPv6 manteniendo la coexistencia con IPv4 o en su defecto siendo nativo:

1. Nativo: Solo manejará el protocolo IPv6, no permitirá comunicación con ninguna red o servicio en IPv4.
2. Doble pila/Dual Stack: este es el más conocido y comercial a nivel mundial. Los equipos instalados en la red a implementar poseen la capacidad de manejar ambos protocolos, lo que ayuda a tener una interconexión más amplia, y así poder acceder a servicios y aplicaciones tanto en IPv4 como IPv6.
3. Túneles: En este se encapsulan los paquetes IPv6 sobre redes IPv4 o viceversa, se encapsulan paquetes IPv4 en redes IPv6, sin embargo, este último es poco común.
4. Traducción: Permite la comunicación de dispositivos que son solo IPv4 o son solo IPv6 con la ayuda de equipos de borde, o equipos intermediarios que efectúan la traducción entre protocolos.

A continuación, se detallarán más a profundidad cada uno de los métodos mencionados con anterioridad

Dual Stack

En la actualidad la mayoría de los sistemas operativos, por no decir que todos, tiene incluidas las funcionalidades de IPv6 al igual que las de IPv4, lo que evita costes adicionales.

Por otro lado, los equipos networking, los equipos de seguridad y otros dispositivos finales, permiten establecer tanto IPv4 como IPv6, en algunos únicamente es necesario habilitar dicha funcionalidad para que se pueda usar. Se debe tener en cuenta que la preferencia actual de la red es de la siguiente manera:

1. IPv6 Nativo
2. IPv4
3. IPv6 por mecanismo de transición

Lo anterior es el orden en como los paquetes prefieren salir a la red. Gracias a esta metodología se permitirá la coexistencia indefinida entre ambos protocolos, además de la actualización gradual al IPv6, aplicación por aplicación.

En la configuración de IPv6, los nodos tienen implementada cada una de las pilas, lo que permitirá escoger el tipo de protocolo a utilizar.

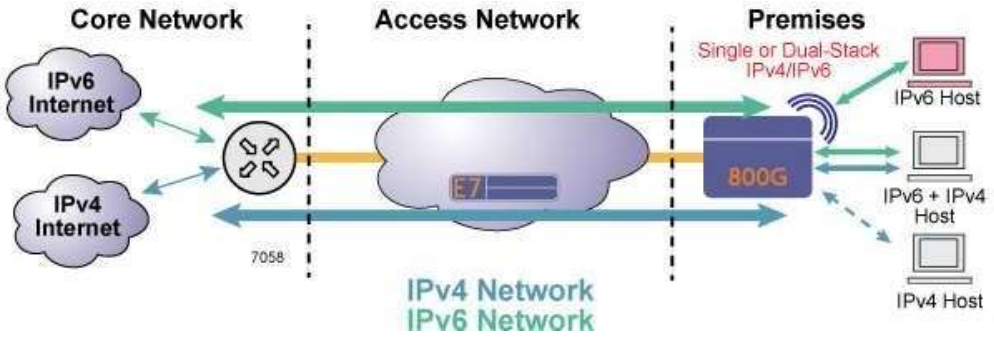


Figura 6 Comunicación Dual Stack

Es de tener en cuenta que este mecanismo presenta un inconveniente y se planteara en el siguiente ejemplo:

Se posee una red lan dual stack, donde se desea ingresar a alguna página en Internet, por tal motivo se ingresa la url donde el servidor de dominios dns resuelve y hace la traducción al direccionamiento ip, según lo mostrado anteriormente, los paquetes prefieren la red IPV6 nativo, así que se intentara resolver el dominio por IPv6, sin embargo, este dominio presenta alguna falla, así que se reenvía el paquete, pero por IPv4 y ese resuelve por este protocolo, pero esto aunque funciona ocasiona lentitudes, haciendo que la experiencia de los clientes sea mala.

Así que, para solucionar dicho inconveniente, se utiliza el mecanismo Hapy-Eyeballs, el cual ofrece a los dispositivos el servicio de doble pila para poder usar al tiempo los dns en IPv6 e IPv4, gracias a esto, las conexiones de los usuarios son mucho más rápidas; su funcionamiento consiste en enviar los paquetes de los PTR, A y AAAA (para IPv6) al mismo tiempo y así si alguno tiene inconvenientes el otro estará trabajando simultáneamente.

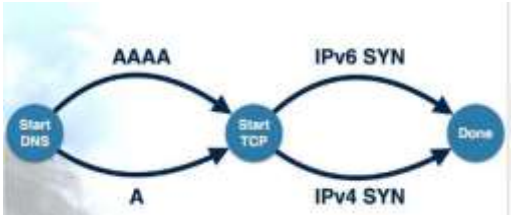


Figura 7 Happy-Eyeballs

Túneles o tunelización

Este es uno de los métodos más comunes para el uso de IPv6 e IPv4, especialmente cuando el transporte de la red es únicamente por IPv4; en este se encapsulan los paquetes IPv6sobre la red de IPv4 y así "camuflarse" sobre esta última y poder transmitir su respectiva información.

Actualmente existen varios métodos de tunelización los cuales se verán a continuación:

a. 6in4

En este método se encapsulan los paquetes IPv6 en un túnel IPV4 antes de salir a la red wan, donde desde el punto de vista IPv6 este sería un enlace punto a punto, con un salto IPv6 y varios saltos IPv4; se debe tener en cuenta que las direcciones IPv6 en ambos extremos deben pertenecer al mismo prefijo

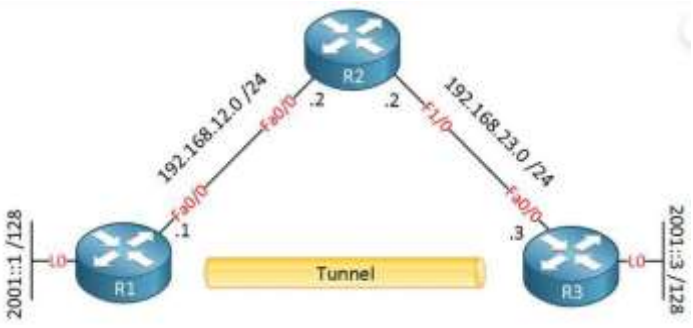


Figura 8 Comunicación por tunelización

También se puede encapsular paquetes IPv4 en redes IPv6, sin embargo, este método no se encuentra en uso actualmente.

b. Tunnel Broker

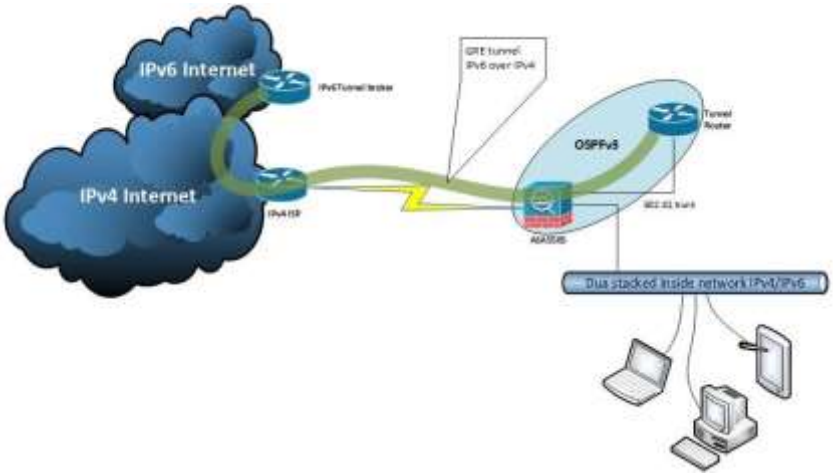


Figura 9 Tunnel bróker

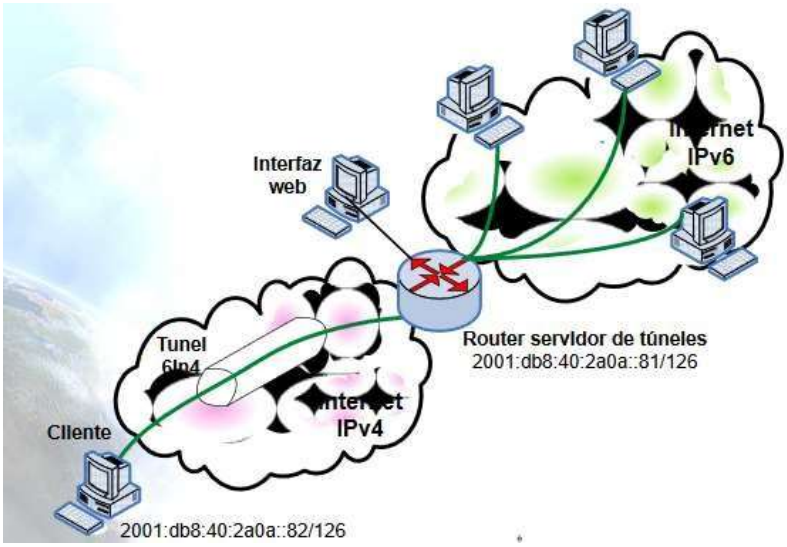


Figura 10 Comunicación por Tunnel bróker

Los tunnel Bróker son túneles que se contratan con un intermediario donde el usuario final conecta su red hacia alguno de sus servidores o router dedicado para alojar los túneles, y deallí salir a Internet, normalmente este procedimiento se efectúa por página web.

El cliente solicita al intermediario del tunnel bróker la creación de un túnel y este procede a asignarle un direccionamiento IPv6, además de esto le brinda las instrucciones correspondientes para la generación del túnel del lado del usuario y otorga la configuración del router de borde que apunta al router que aloja los túneles.

Una de las páginas para adquirir un tunnel bróker es: https://tunnelbroker.net/ [9]

c. 6to4

Este es un túnel automático multipunto que usa el prefijo reservado 2002: :/16 y necesita una IPv4 publica para la comunicación de diferentes “islas” o dominios de red aislados en IPv6 como se muestra en la siguiente imagen:

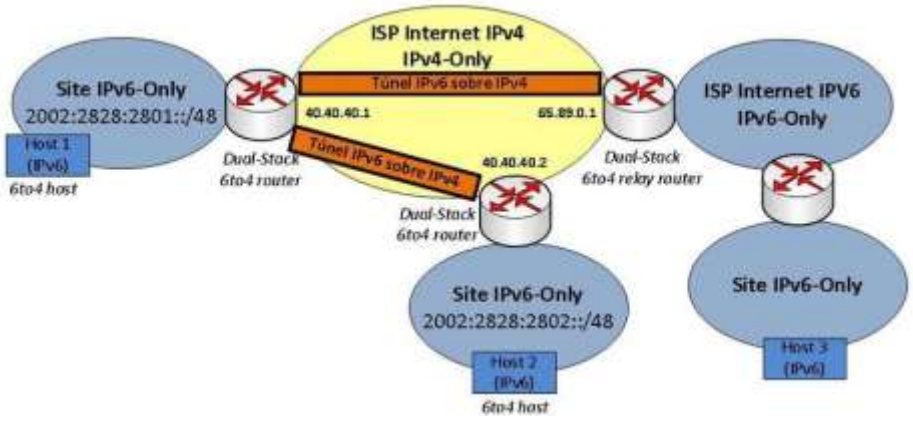


Figura 11 Comunicación por 6to4

6to4 genera un direccionamiento para cada una de las islas con el formato de la siguiente estructura:

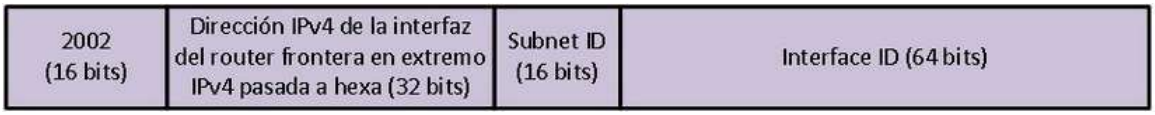


Figura 12 Estructura direccionamiento 6to4

Es decir, se posee el prefijo 2002: :/16, luego para obtener el direccionamiento lan, setomará la IPv4 configurada en la interfaz wan del router de borde y se pasará está a Hexadecimal, la IPv4 transformada se le puede llamar address_ipv4, para así obtener un direccionamiento con el siguiente formato: 2002::address_ipv4:/48

Ahora, esto funciona cuando una sede en IPv6 se quiere comunicar con otra, pero en el intermedio se encuentra la red IPv4, ahora, existe otro escenario que es cuando se desea llegar a la red de Internet IPv6 nativo, sin embargo, hay que pasar por la red IPv4, para lo anterior se usara el IPv6 router relay, es un dispositivo que se conecta en el borde de IPv4 e IPv6, es un dispositivo dual stack, donde este encapsula y desencapsula los paquetes para poder entablar dicha comunicación. Generalmente el default Gateway IPv6 del router relay debe tener un formado 2002::address_ipv4 + direccionamiento relay, address::relay teniendo el formato siguiente: 2002::address_ipv4::address_relay:/128 en donde este adicional es una dirección IPV4 unicast (usualmente 192.88.99.X), por ende, los paquetes enviados a esta dirección son tratados como si hubieran sido enviados a la dirección anycast del Router Relay.

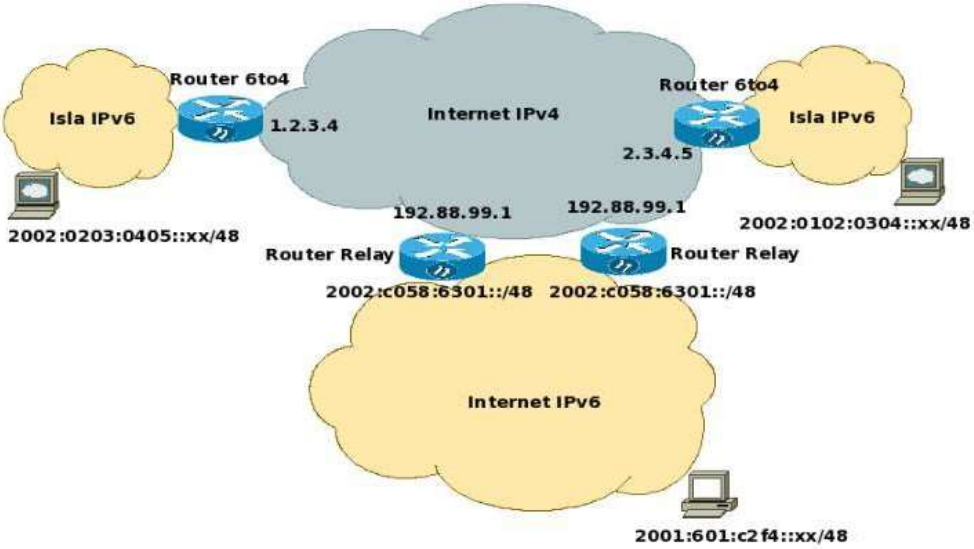


Figura 13 Interconexión por 6TO4

No obstante, hay que destacar una de las desventajas de este método, y es que al tener que reenviarse a diferentes equipos, las latencias son mayores que en otro tipo de métodos, lo que ocasiona mala percepción al usuario final.

d. 6rd

Este mecanismo de transición es la evolución del 6to4, donde al igual que este anterior se usará la red IPv4 para transportar la información IPv6 generalmente dentro de la infraestructura de algún ISP; algunos de los cambios presentados con 6rd respecto a 6to4 es la del remplazo del prefijo 2001::/16 por un prefijo destinado directamente por el ISP por parte de su respectivo RIR igualmente sucede con la dirección unicast 192.88.99.1 por otra IP elegida por el ISP contratado, también se identifican múltiples instancias anunciadas mediante una dirección unicast. Por último, un cambio que podría ser su mayor ventaja es que no es necesario hacer uso de una IP

publica únicamente, se puede usar también una ipv4 privada, lo que permite hacer un uso más eficiente del direccionamiento existente.

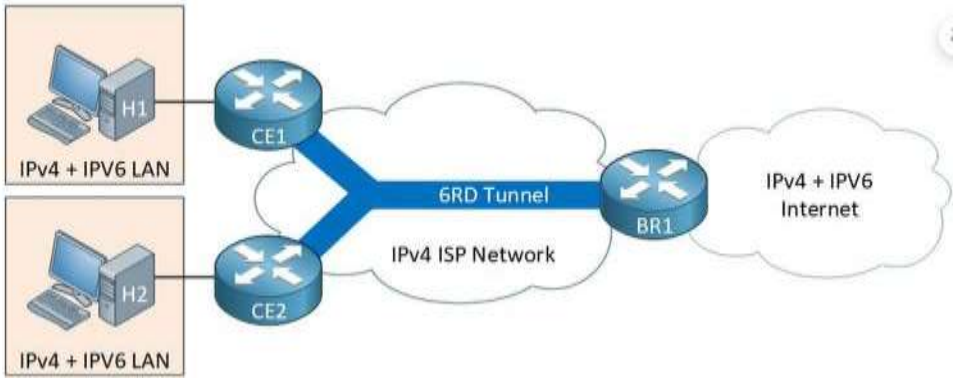


Figura 14 Comunicación por 6rd

En teoría, este método se ve como una arquitectura normal de un ISP, donde la red IPv4podría ser la MPLS de ellos, y por medio de esta y de túneles generaría la comunicación hacia las diferentes sedes IPv6 o en su defecto hacia la red IPv6 nativa.

A continuación, se apreciará la manera como 6rd determina el direccionamiento lan dependiendo de la IPv4 asignada por el ISP y el prefijo IPv6.

Se toma como ejemplo que el ISP contratado brinda un direccionamiento 2001:db8::/32 y la IPv4 del cpe será 10.0.0.0/8, se resta 32 (número de bits en ipv4) menos la máscara del cpe que es 8:

32-8=24

Seguidamente se suma este resultado con 32 (número de bits en ipv4)

24+32=56

Eso quiere decir que la máscara será /56: 2001:db8::/56

Ahora ya tenemos la máscara de subred para determinar cuántos dispositivos tendremos en nuestra red; lo siguiente será saber la IP que se tendrá asignada, como el cpe usa la red wan 10.0.0.0 donde la ip Gateway wan es la 10.0.0.2, se usan los 24 bits de menor peso, es decir: 0.0.2 y se pasan estos a Hexadecimal:

0.0.2 = 000002

Se concatena este número en la dirección IPV6:

2001:2b8:0000:0200::/56

Donde la máscara mínima a tener es 64, por lo tanto

64-56=8

El subnet ID será de 8 bits, lo que equivale a unas 256 redes posibles.

Algunas de las ventajas de este mecanismo de transición es la de poseer el control sobre todo el tráfico que circula a través de la red también disminuye el riesgo de ataques de spoofing y DoS.

Mecanismos de traducción

La traducción es una técnica de extensión de NAT que convierte las direcciones IPv6 enIPv4, igualmente se puede ejecutar en viceversa, pero esto no es algo muy común.

Por lo general un equipo intermedio modifica las direcciones y cabeceras para simular que el tráfico es IPv4 y así poder entablar el respectivo flujo de datos.

Algunos métodos de traducción son los siguientes:

a. NAT64:

Comúnmente conocido como CGN o LSN; El cual consiste en usar la misma función del nat. Las direcciones IP versión 4 son traducidas algorítmicamente desde IP versión 6 manejando el algoritmo indicado en el estándar RFC6052, además de un prefijo IPv6 el cual es designado al nat64 con estado. Por otro lado, para traducir direcciones IPv6 desde direcciones IPv4 se instalan mapeos que realizan traducción del puerto de red.

nat64 es un método útil debido a que contribuye con el agotamiento de las direcciones IPv4, ya que se usarían host IPv4 en las lan de los clientes y se traduciría a IPv6 para poder acceder a Internet, dando grandes campos de aplicabilidad como el internet de las cosas. Sin embargo, esto solo funciona como solución temporal, ya que su metodología de uso no es muy eficiente y solo sirve para prolongar artificialmente la vida de IPv4.

Hay que aclarar que este método presenta un inconveniente; como aún está en despliegue el nuevo protocolo, se tiene previsto que aun tarde varios años en que toda la red sea IP versión 6, por lo que coexistirán varias aplicaciones que solo soportan IPv4 con la nueva versión IP y este método mencionado es IPv6-only, es decir, que servicios como el de Skype no trabajarían con nat64, así que si se usan direcciones literales no funcionara este mecanismo, si se usan sockets APIs tampoco servirá este.

Por otro lado, se debe tener en cuenta, que para el acceso a páginas web o resolución de nombres en IPv6 también se debe disponer de algún mecanismo que realice esta función, es por eso que agregaron al nat un dns64, el cual se encarga de la resolución de nombres en IPv6:

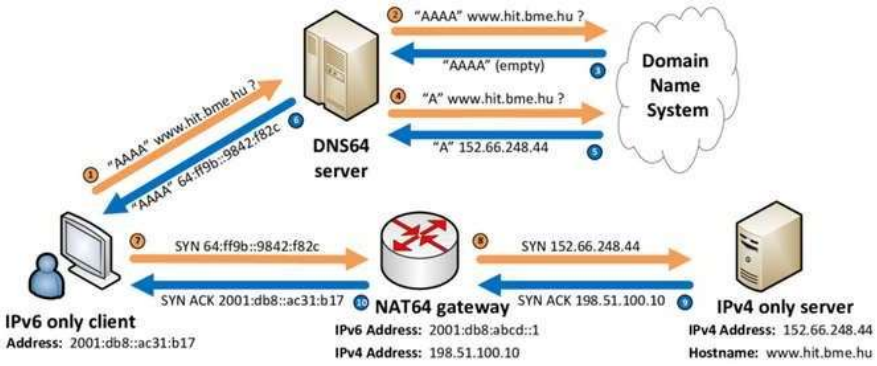


Figura 15 Comunicación por NAT64

b. 464XLAT

Como se manifestó con anterioridad, el nat64 presenta una falencia bastante notoria para usarse en la actualidad, es por eso por lo que se combinó el uso del RFC6145 y el RFC6146 con el fin de proporcionar a los clientes servicios básicos en IPv4 sobre la infraestructura de IPv6.

Para ello se harán uso de servidores los cuales traducirán el direccionamiento internamente antes de que los paquetes viajen a través de la red externa:

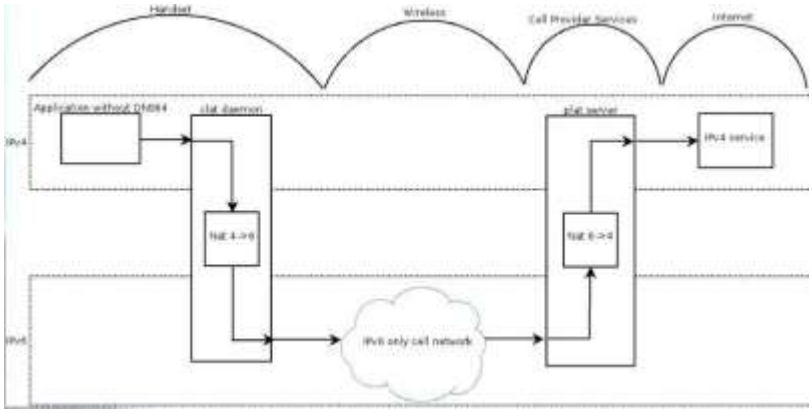


Figura 16 Flujo de tráfico de 464XLAT

Gracias la combinación indicada, podremos ver las distintas soluciones para usar en la red:

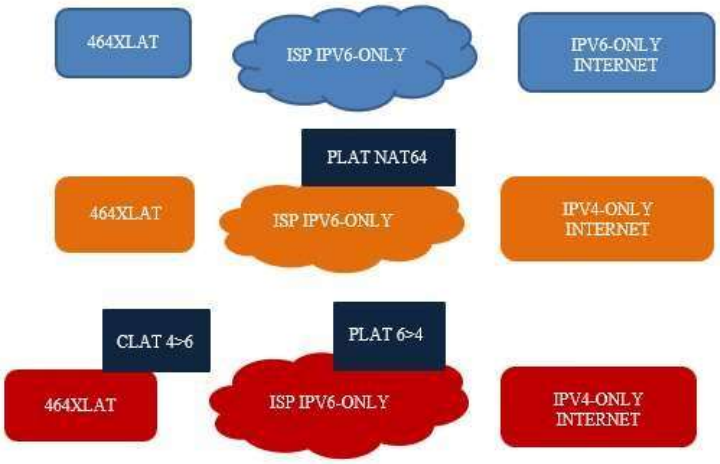


Figura 17 Soluciones de 464XLAT

Direccionamiento IPv6

Como se conoce ya, las IPv4 poseen una cantidad de 32 bits en su arquitectura a diferencia de IPv6 que está compuesta de 128 bits, lo que le proporciona una gran cantidad dedirecciones IP para su uso, en pocas palabras se puede decir que una sola red lan puede poseermás direcciones que toda la internet actual.

La estructura de este nuevo direccionamiento es de 8 grupos de números separados por dos puntos, cada uno de estos tiene 16 bits y con estos se puede representar hasta 4 números en base 16 o hexadecimal, donde de manera resumida son 8 grupos de 4 dígitos hexadecimales ej: 2001:0DB8:2345:ABCD:1234:FFFF:9876:EEEE, donde se aprecia lo expuesto con anterioridad.

También es de tener en cuenta que IPv6 maneja al igual que IPv4 máscara de subred para denotar la cantidad de Hosts y subredes que se pueden conectar o usar en la red, esta se representa con el signo / y luego el número de mascara, ejemplo: 2001:0DB8:2345:ABCD:1234:FFFF:9876:EEEE/56

Uno de los puntos a apreciar en IPv6, es que el estándar indica que los 64 bits de la izquierda son usados para el prefijo de red y los 64 bits a la derecha son el ID de la interfaz.

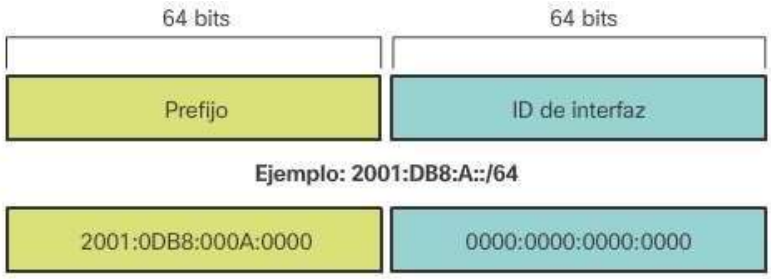


Figura 18 Estructura direccionamiento IPv6

El prefijo de red es el que ayuda a identificar las subredes que se pueden utilizar dentro del segmento de red brindado, por esto una longitud de prefijo IPv6 típica para lan y la mayoría de los demás tipos de redes es /48 o hasta /64. Lo que significa que la porción de prefijo o de red de la dirección tiene una longitud de 64 bits, lo cual deja otros 64 bits para la ID de interfaz (porción de host) de la dirección.

IPv6 ayuda a la simplificación de su protocolo con dos reglas:

1. En cada grupo de dígitos separados por los dos puntos, los 0 a la izquierda pueden ser omitidos, como se muestra en el siguiente ejemplo:

2001:0DB8:0045:000D:0000:0FFF:0000:EEEE

Aplicando la regla

2001:DB8:45: D:0:FFF:0:EEEE

2. Cuando existen varios conjuntos de 0 consecutivos, estos al igual que la regla anterior se pueden omitir y se representaría con dos puntos seguido de otros dos puntos (::), como se evidencia en el ejemplo:

2001:0000:0000:0000:0000:0000:0000:EEEE

Aplicando la regla

2001::EEEE

Sin embargo, se debe tener en cuenta que esta regla solo se puede aplicar una vez por direccionamiento, es decir:

2001:0000:0000:0000:ABCD:0000:0000:EEEE

Solo se aplica la regla o al primer conjunto de 0 o al segundo conjunto:

2001::ABCD:0000:0000:EEEE

No obstante, acá también se puede usar la primera regla:

2001::ABCD:0:0:EEEE

Ahora se comentará cuáles son los tipos de direcciones que existen dentro de la familia IPv6.

a. Unicast: Son las direcciones que poseen un identificador individual.
b. Anycast: Estas direcciones tienen una selección especifica.
c. Multicast: El identificador se efectúa en un grupo indicado.

Nota: las direcciones de broadcast no existen en IPv6

Unicast

i. Unicast Global:

Se puede decir que estas son el semejante de las IPV4 públicas, dado que son las que se enrutan en la red de INTERNET, donde son alrededor del 13% del total de las direcciones posibles, que, aunque parece poco son demasiadas direcciones.

El espacio reservado para este direccionamiento es el 2000::/3.

ii. Link Local:

Son direcciones agregadas en cada dispositivo LAN para usarse únicamente de manera local, se puede determinar como la puerta de enlace, este tipo de direccionamiento no atraviesan router y se pueden configurar manualmente o también se pueden auto configurar. El espacio reservado es la FE80::/64

El direccionamiento en ocasiones se asigna automáticamente en varios dispositivos, en especial los equipos finales, para ello se utiliza el formato EUI-64 el cual se explicará a continuación como hace la respectiva asignación:

a. Se agrega las direcciones FF-FE entre el tercer y cuarto byte de la MAC del dispositivo.
b. Se complementa con el bit elemental U/L (si es un 1 se cambia a 0 y viceversa, el séptimo bit desde la izquierda).

Ejemplo: MAC 48:2E:C9:21:85:0C

Se agrega ahora la dirección FF-FE

48:2E:C9:FF:FE:21:85:0C

El siguiente paso es tomar el primer byte y pasarlo a binario

48 – 01001000

Se aplica U/L

0100 1010 – lo que equivale al número 4 y al 10 en decimal, este último a A en hexadecimal.

Por lo tanto, quedaría de la siguiente manera la dirección IPV6 del dispositivo con la MAC mencionada:

FE80::4A1E:C9FF:FE21:850C.

iii. ULA (Unique Local)

Son usadas dentro de las comunicaciones de un enlace, donde su prefijo es globalmente único (o con alta probabilidad de ser único), se asemeja a las direcciones privadas IPV4 ya que no se encuentran enrutadas en Internet.

El espacio reservado para ULA es FC00::/7.

iv. Unicast especiales

Dentro de las direcciones UNICAST, existen algunas que fueron generadas para un propósito particular:

a. IPv6 Loopback: ::1/128

b. No especificadas: ::/128

c. IPV6 mapeada: ::FFFF:WXYZ

Unicast rangos especiales:

d. 6to4: 2002::/16

e. Documentación: 2001:db8::/32

f. Teredo: 2001:0::/32

v. Unicast obsoletas:

Dentro de la formación de IPV6 existieron varios direccionamientos utilizados con el propósito de mejorar y fortalecer el protocolo, que a día de hoy no están siendo usadas:

a. Site local: FEC0::/10

b. IPV4: ::WXYZ

c. 6BONE: 3FFE::/16

Anycast

Las direcciones Anycast están compuestas para seleccionar y establecer un identificador a un grupo de interfaces o que varias interfaces posean esta una dirección anycast, no obstante, cuando un paquete es enviado a esta la dirección ipv6 anycast, esta es entregada solo a una de las interfaces asociadas, puntualmente a la más próxima según el protocolo de ruteo, en pocas palabras el paquete se entrega a la interfaz más cercana al origen.

Es usada para:

a. Descubrir servicios
b. Balanceo de carga
c. Localizar routers que proveen acceso a una subred
d. Redes con soporte para movilidad IPv6, para localizar los agentes de origen.

Multicast

Este tipo de direcciones al igual que las Anycast, es un identificador para un conjunto de interfaces, sin embargo, se diferencia de Anycast ya que los paquetes enviados no son entregados solo a una interfaz sino a todas las que están identificadas con dicha dirección.

Todas las direcciones Multicast comienzan con FF, es decir se derivan del bloque FF::/8; A continuación se apreciaran algunos de los grupos multicast que existe:

Dirección	Descripción	Ámbitos disponibles
ff0X::1	Dirección all-nodes (todos los nodos). Identifica al grupo de todos los nodos IPv6	Disponible en el ámbito (scope) 1 (*interface-local*) y 2 (*link-local*): • ff01::1 → Todos los nodos en el interface local • ff02::1 → Todos los nodos en el enlace local
ff0X::2	Dirección all-routers (todos los routers). Identifica al grupo de todos los routers IPv6	Disponible en el ámbito (scope) 1 (*interface-local*), 2 (*link-local*) y 5 (*site-local*): • ff01::2 → Todos los routers en el interface local • ff02::2 → Todos los routers en el enlace local • ff05::2 → Todos los routers en el site-local
ff02::5	OSPFIGP	2 (enlace-local)
ff02::6	OSPFIGP Designated Routers	2 (enlace-local)
ff02::9	Routers RIP	2 (enlace-local)
ff02::a	Routers EIGRP	2 (enlace-local)
ff02::d	Todos los routers PIM	2 (enlace-local)
ff0X::fb	mDNSv6	Disponible en todos los ámbitos
ff0X::101	Todos los servidores de NTP (*Network Time Protocol*)	Disponible en todos los ámbitos
ff02::1:1	Link Name	2 (enlace-local)
ff02::1:2	All-dhcp-agents	2 (enlace-local)
ff02::1:3	Link-local Multicast Name Resolution	2 (enlace-local)
ff05::1:3	All-dhcp-servers	5 (site-local)
FF02::1:FF00:0000/104	Dirección *Solicited-Node*. Véase explicación más abajo	2 (enlace-local)
FF02:0:0:0:0:2:FF00::/104	Node Information Queries	2 (enlace-local)

Figura 19 Grupo de direcciones multicast

Algunos puntos importantes en el tema de las direcciones que se puede distinguir al hacer uso de IPv6, se pueden encontrar a continuación:

a. En IPv6 una interfaz puede poseer varias direcciones IP, no como en IPv4
b. La IANA le asigna a cada RIR un bloque /12
c. LACNIC tiene asignado el espacio 2800::/12
d. El mínimo direccionamiento que un RIR le puede dar a un ISP es de /32
e. Según las recomendaciones del RFC3177 las redes para usuarios finales deben tener una máscara /48
    a. Las redes de mascara /64 se usarán cuando hay una certeza de que solamente una subred es necesaria por ejemplo redes celulares.

f. Las redes /128 son usadas cuando se tiene certeza de solo una interfaz conectada

g. Las conexiones punto a punto son /64

NDP (Neighbor Discovery Protocolo):

Definido por el estándar RFC4861, asume las funciones de:

a. ARP

b. ICMP Router Discovery

c. ICMP Redirect

Generalmente usado para:

a. La autoconfiguración

b. Redireccionamiento de paquetes IP

c. Determinar la dirección MAC de los nodos

d. Encontrar routers vecinos

e. Determinar la accesibilidad de paquetes de router

f. Identificar direcciones IP duplicadas

g. Encontrar prefijos

Este protocolo para utilizar icmp IPv6, maneja una serie de mensajes con el fin de llevar a cabo sus funcionalidades

a. Router Solicitation (RS): Cuando se activa una interfaz de un nodo, este envía a todos los router de la red este tipo de mensaje 133.
b. Router Advertisement (RA): Cuando los nodos envían el mensaje RS y el router responde, este es el tipo de mensaje RA 134.
c. Por otro lado, los router también envían este mensaje periódicamente para informar a los nodos que aún siguen activos.
d. Neighbor Solicitation (NS): Este se usa para que los nodos conozcan las direcciones MAC de los vecinos 135
e. De igual manera se ejecuta este para identificar direcciones duplicadas.
f. Neighbor Advertisement (NA): Usa la respuesta de los NS, 136. Por otro lado, se utiliza cuando los equipos son cambiados, entonces se detecta una nueva MAC
g. Redirect: Es usado cuando un nodo le indica a un router de una mejor ruta para su destino, 137.

Entendiendo los anteriores mensajes, se puede comprender a mayor escala como es que NDP opera, donde estas funcionan se usan en combinación entre sí para que la red trabaje correctamente, el siguiente paso es apreciar cada una de las actividades en las que se encuentra relacionado NDP:

1. Funciones de ARP

Esto lo hacen los distintos equipos al descubrir direcciones por medio del enlace de datos, con esta se pretende determinar la dirección MAC buscando remplazar el arp. Su principal diferencia con IPv4 es que no utiliza las direcciones de broadcast sino hará uso de los diferentes

mensajes anteriormente mostrados, más específicamente los mensajes Neighbor Solicitation los cuales son enviados al grupo multicast Solicited Node, cuando por medio de este grupo multicast el destino es alcanzado, este equipo responde con un mensaje Neighbor Advertisement brindando la información de su dirección Mac y de su IP al grupo multicast donde se encuentra el nodo.

2. Descubrimiento de Routers y Prefijos:

Esta funcionalidad es usada para localizar routers dentro de un mismo enlace, así como también aprender prefijos y parámetros relacionados con la autoconfiguración de direcciones.

Este maneja dos tipos de mensajes: Router solicitation y Router advertisement. Estos mensajes se usan al igual que la anterior función a un grupo multicast, pero esta vez es enviado al grupo all-routers.

3. Detección de vecinos inaccesibles:

Es usado para detectar el acceso a los nodos a lo largo del camino, para esto se utiliza la comunicación host-host, host-router o router-host. Un vecino es considerado accesible cuando se ha enviado algún paquete a este vecino y se recibe confirmación de entrega. Es de tener en cuenta que este proceso se efectúa cuando se envían paquetes a una dirección unicast.

4. Almacenamiento de Tablas:

El almacenamiento de tablas mantiene la información sobre los destinos a los cuales se ha enviado tráfico, esto incluye los destinos remotos como los locales y se va actualizando por medio de los mensajes Redirect, para ello usa los siguientes cache:

a. Destination Cache: Información de destinos a los cuales se envió paquetes recientes, este se actualiza por medio de mensajes Redirect.
b. Neighbor Cache: Es similar a la tabla arp, mantiene la lista de vecinos locales con la dirección IP y la dirección MAC, además de un flag para determinar si se trata de un host o de un router.

5. NDP Redireccionamiento:

En este caso, los router envían mensajes Redirect con el fin de redireccionar un host o algún equipo de forma automática a un router más apropiado o en su defecto le informa al host que el destino está ubicado en el mismo enlace, hay que aclarar que en este escenario solamente los router harán uso de los mensajes Redirect.

6. Direcciones IP duplicadas:

Los nodos utilizan NDP con el fin de identificar si dentro de la información que ellos poseen, existen direcciones IP iguales, este proceso se debe efectuar antes de atribuir cualquier dirección unicast a alguna interfaz. Para ellos el host envía un mensaje de tipo Neighbor Solicitation con su propia dirección, ya sea configurada automáticamente o manual, este mensaje es dirigido hacia el grupo multicast Solicited-Node. Es de resaltar que este grupo multicast será escuchado por todos los nodos donde la dirección IPv6 en sus últimos 24 bits coincidan con la

dirección Solicited-Node, si luego de enviarse el anterior mensaje se tiene como respuesta un Neighbor Advertisement, esto quiere decir que dicha dirección IP ya está siendo usada por otro dispositivo.

Path Mtu Discovery

Es de recordar que MTU es la unidad máxima de transferencia en un enlace, es decir, el peso o cantidad de bytes que un canal o interfaz puede soportar en sus paquetes, no obstante, existen técnicas para que una interfaz pueda recibir o enviar paquetes con mayor peso del que se tiene configurado en la MTU, esto se le llama fragmentación.

Dado lo anterior con PMTUD se puede descubrir la unidad máxima de transferencia del camino para garantizar que los paquetes no se fragmenten más allá del origen, es decir que estos ya vayan fragmentados desde que salen de la fuente.

Se debe tener presente que en IPv4, un host envía un paquete con mayor peso que el permitido por el MTU, así que los routers intermedios se encargan de la fragmentación, algo que ya no será de esta manera ya que como se mencionó, este proceso se realiza cuando sale el paquete, en pocas palabras el Host se encargara de ejecutar esto; con este procedimiento se pretende reducir el procesamiento de cálculo de los encabezados modificados por la fragmentación en los diferentes router. Cabe resaltar que en IPv4 el tamaño mínimo del paquete es de 68 mientras que en IPv6 es de 1280.

La manera en cómo funciona Path Mtu Discovery (descrito en la RFC 8201) es la siguiente: se descubre de manera dinámica el tamaño máximo de cada uno de los enlaces por los que tiene que pasar el paquete, PMTUD supone que todo el camino tiene el mismo mtu del primer salto, así que si este paquete supera el mtu en algunos de los caminos, se envía al host un

mensaje ICMPV6 llamado Packet Too Big que junto con el mensaje también le envía la información del mtu que tiene dicho enlace, el paquete se descarta y estos datos los obtiene el host de origen donde ya sabe si debe o no fragmentar el paquete enviado.

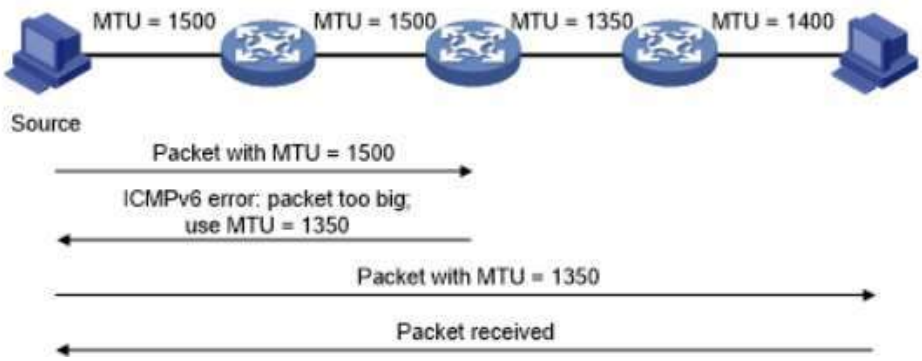


Figura 20 Path MTU Discovery

En el anterior ejemplo, se envía desde un PC de origen un paquete de 1500 bytes, no obstante, al llegar router 2 se encuentra con que el enlace del router 2 al router 3 tiene un mtu menor (1350), por lo tanto, se envía un mensaje Packet Too Big al emisor y se debe reenviar el mensaje con paquetes fragmentados cumpliendo con el mtu encontrado.

Autoconfiguración:

La autoconfiguración es el mecanismo con el que los diferentes dispositivos de la red adquieren un direccionamiento IPv6 sin necesidad de asignarlo de forma manual, esto es lo que se conoce en IPv4 como DHCP, no obstante, IPv6 posee dos mecanismos para ejecutar este procedimiento:

1. Autoconfiguracion Stateless (SLAAC)

Este mecanismo es bastante sencillo de entender, el cual permite atribuir direccionamiento IPv6 a las diferentes interfaces y equipos sin necesidad de configuraciones manuales o hacer uso de algún tipo de servidor, lo único que hay que hacer para hacer efectivo esto, es realizar una modificación mínima en los router.

Para que un dispositivo tome una IP es necesario que posea algunos datos como: La dirección mac o un valor aleatorio que la remplace, información de los prefijos de red configurados en el equipo de enrutamiento (si no existen routers, en su defecto no habrá alguna información de direcciones IP, por tal motivo se utilizara la IP Link Local el prefijo FE80::).

Los router también hacen uso de este tipo de configuración, no obstante, solo la usan para autoconfigurar su Link Local.

La autoconfiguración SLAAC utiliza dos mensajes ICMPV6: Router Solicitation y Router Advertisement. De esta manera es que el router le brinda un identificador de interfaz para establecer un direccionamiento.

Los pasos para que un host tome un direccionamiento IP por SLAAC es el siguiente (se usara como ejemplo configuraciones efectuadas con equipo router del fabricante Cisco):

a. Habilitar el router con IPV6

Para ello se utiliza el siguiente comando:

Figura 21 Comando para habilitar IPv6 Cisco

b. Se conectan los equipos y se configura IPV6 en la interfaz del router.

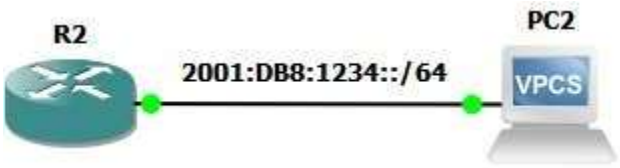


Figura 22 Conexión de ejemplo

```
R2#show running-config interface gigabitEthernet 2/0
Building configuration...

Current configuration : 115 bytes
!
interface GigabitEthernet2/0
 no ip address
 negotiation auto
 ipv6 address 2001:DB8:1234::/64
 ipv6 enable
end
```

Figura 23 Configuración ejecutada router Cisco

c. El cliente, es decir el PC2 enviara un mensaje RS al grupo multicast para informarle al router IPv6 local que necesita un RA.

d. El router Responde con el mensaje RA, donde en este va incluido el prefijo de red y la longitud de esta misma, por otro lado, este se envía a la dirección IPv6 del respectivo grupo multicast, así mismo lleva la dirección Link Local para que el PC2 la conozca

e. Ahora el PC2 tiene el prefijo de red, pero necesita un id de Interfaz para crear su propia dirección IPV6 unicast global, para obtener este id se puede efectuar de dos maneras, por medio de EUI-64 haciendo uso de su dirección mac o a través de la originario aleatoria donde el id de 64 bits puede ser un número aleatorio generado por el sistema operativo cliente. Por lo general se procede con el primer método.

f. Luego de que el PC genere una IPv6 unicast global, con ayuda del protocolo ndp se revisa las direcciones duplicadas en el enlace, si no existe una igual, el dispositivo toma este direccionamiento.

g. Se configura el PC para que obtenga la dirección IPv6 por Slaac:

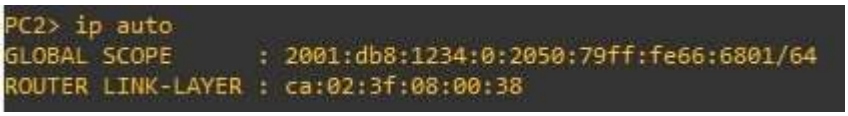


Figura 24 Verificación de direccionamiento

Consideración de la configuración de SLAAC:

Cuando el router envía un mensaje RA y este no contiene prefijo de red, el host no puede configurar automáticamente una dirección global, pero si se puede configurar por medio del default Gateway o Link Local

Los mensajes RA contienen dos mensajes FLAG para determinar su configuración, es decir tienen un flag llamado MANAGED FLAG (M) donde indica que los hosts deben usar una configuración stateful para obtener el direccionamiento IP, mientras que el flagOther ConfigFlag (O) el cual dice que los hosts usan la configuración stateful para

obtener información adicional como por ejemplo servidor dns o algunos otros parámetros.

Usualmente las direcciones IPV6 están basadas en direcciones mac, aunque en algunas ocasiones se utilizan extensiones privadas.

2. Configuración por STATEFULL

Esta es la configuración dhcp en IPv6 o dhcpv6 el cual se define en el RFC 8415, este al igual que el servicio convencional puede usarse tanto en el router como servidor, o apuntando a un servidor dhcp (dhcp relay). El dhcp escucha dos tipos de direcciones multicast, el All_dhcp_Relay_Agents_and_Servers y el grupo All_dhcp_Servers, el primer grupo se utiliza para que los clientes se comuniquen con los agentes relay y servidores ubicados en el enlace, mientras que el segundo se emplea por los agentes relay para comunicarse con el server.

Para obtener los parámetros de configuración IP, el cliente inicia la comunicación al enviar solicitudes, esto lo hace por medio de la dirección link-local que ya debe poseer el dispositivo, por otro lado, el destino de los mensajes es el grupo multicast de todos los agentes relay y servers All_dhcp_Relay_Agents_and_Servers, en donde el agent relay tendrá la función de intermediario entre el servidor y el cliente ya que se encuentra dentro del mismo enlace.

La manera de configurar este mecanismo de asignación automática es bastante similar al dhcp de ipv4, en donde se establece un pool al cual se le asigna algún segmento de red, se seleccionan los servidores dns y otros parámetros como exclusión de IP’s, algunas direcciones reservadas o tiempo de arrendamiento.

DNS:

Se debe tener en cuenta que dns opera de manera jerárquica, en donde traduce los nombres de dominio en direcciones IP y viceversa; para que este protocolo funcione adecuadamente maneja distintos elementos con diferentes roles, efectuando la traducción en base a consultas y respuestas.

Los 3 componentes importantes utilizados en los dns son:

Resolver: Es un componente ejecutado en el dispositivo que origina las peticiones dnsel cual su función es la de realizar las consultas a algún servidor dns, interpretar dichas consultas y a su vez enviarle esta información al programa solicitante de la consulta.

Servidor recursivo: Son aquellos que responden las solicitudes dns de los clientes, estos están en la capacidad de reenviar la petición a otro servidor si en su información(memoria cache) no encuentra la dirección solicitada. Se puede decir que sirven comoservidor dns o como cliente dns (Resolver).

Servidor autoritativo: Este espacio del nombre de dominio es donde los servidorestienen la autoridad sobre varias zonas, ellos reciben las solicitudes de “mejor respuesta” de los clientes dns.

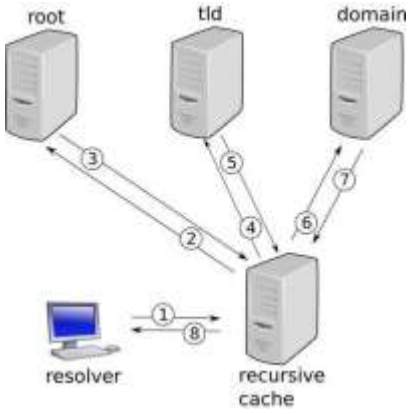


Figura 25 Estructura DNS

Como se puede apreciar en la imagen anterior, el cliente (Resolver) realiza peticiones dnsal servidor dns que tiene conformado en su configuración generalmente el de los ISP (servidor recursivo), este responderá las solicitudes si dentro de su memoria local tiene información alguna de estas, sino, hará estas mismas preguntas a los diferentes servidores autoritativos, así como esta en la imagen, donde hay 3 de estos (root, tld y domain), donde estos se van resolviendo de manera sucesiva, se debe comprender que un servidor no brinda el resultado final de la búsqueda sino que en cada una de las etapas los servidores autoritativos brindan información por las zonas que tienen configuradas.

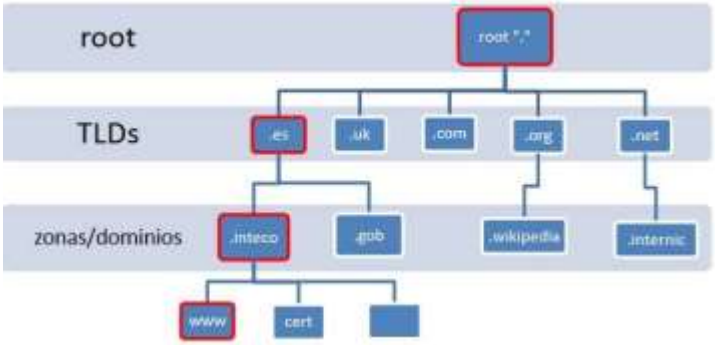


Figura 26 Servidores autoritativos

Por otro lado, dns se ha encargado de satisfacer de manera eficiente todas las consultas que se realicen, para ellos los diferentes servidores deben poseer en su almacenamiento un conjunto de registros para identificar el tipo de solicitud que se está efectuando.

Common DNS Record Types	
Record	Description
A	Address record (IPv4)
AAAA	Address record (IPv6)
CNAME	Canonical Name record
MX	Mail Exchanger record
NS	Nameserver record
PTR	Pointer record

Figura 27 Tipos de registros DNS

Estos son algunos de los registros utilizados por dns, donde A es el similar de AAAA,pero en IPv4 e IPv6 correspondientemente, CNAME, MX, NS y PTR trabajan tanto en IPv4 como en IPV6 solo cambia la metodología y algunos parámetros de funcionamiento.

A y AAAA: Estos registros son utilizados para mapear un nombre en una dirección IP, ya sea IPv4 (A) o IPv6 (AAAA); su función es asignar una cadena de nombre dehost a su dirección IP.

CNAME: También conocido como Alias, este es usado para crear un apodo o alias aalgún registro A o AAAA, por ejemplo, se le puede poner el alias google.com a la página www.google.com.

MX (mail Exchange): Es el intercambio de mensajes de correo, el cual especifica cómo debe ir encaminado un correo por internet, estos registros apuntan a los servidores donde se encuentra alojado el respectivo dominio de correo.

NS: Funciona exactamente igual en IPv6 como en IPv4, este es el encargado de indicar que servidor o servidores almacenan la información de dominio consultado.

PTR: Es la manera inversa de un registro A o AAAA, este lo que hace es mapear unadirección IP en un nombre de dominio, en IPV4 se toman los dígitos de la dirección yse escriben en su forma reversa con el sufijo in.addr.arpa; para IPv6 funciona de manera similar solo que en este ultimo la zona reversa se modifica a ip6.arpa.

Existe un aspecto importante en los servicios dns y es que el transporte de una consulta puede ser tanto en IPv6 como en IPv4, sin importar el tipo de registro o de consulta que se haga; esta característica es muy útil y se puede aprovechar con bastante eficiencia en especial en entornos dual-stack.

Otro de los puntos a tener en cuenta con dns es el Happy-Eyeballs, tema que se trató con anterioridad, el cual permite que las solicitudes dns se realicen al tiempo, es decir IPv6 e IPv4 simultáneamente, esto ayuda a mantener una buena conexión y que a su vez la percepción del usuario final sea la mejor posible ya que si no fuese así, cuando una solicitud en un sentido no funcione, esta se debe repetir causando retrasos en las consultas y así mismo en las respuestas, se debe indicar que se utilizara primero la conexión que haya respondido más rápido, no obstante, se otorga cierta ventaja a IPv6 con un alrededor de 50 Ms, esto se guardara en la memoria cache y las próximas consultas utilizaran esta, periódicamente se hará consultas para conocer si existe alguna actualización de dicho cache.

Enrutamiento IPv6:

Actualmente la mayoría de los protocolos de enrutamiento poseen versiones y derivaciones para poder hacer uso de IPv6, no obstante, se verán a continuación los más

relevantes y utilizados tanto protocolos de enrutamiento internos (OSPF, Estático e IS-IS) como externos (BGP).

Enrutamiento estático:

Este tipo de enrutamiento funciona igual tanto en IPv4 como en IPv6, se efectúa de manera manual, en ella se especifican las redes de destino, y aunque generalmente se usan las rutas dinámicas para redes grandes/medianas, este enrutamiento es utilizado confrecuencia debido a los beneficios que proporciona. En una ruta estática se debe configurar además de una IP de red de destino, la máscara de red de destino, la interfaz ola IP del siguiente salto y la distancia administrativa.

Algunas de las ventajas que posee el enrutamiento estático son:

Ya que sus rutas no son anunciadas a través de la red de forma periódica y dinámicamente, aumenta su seguridad.

Este tipo de enrutamiento consume menos procesamiento y ancho de banda que losenrutamientos dinámicos.

Sin embargo, posee varias desventajas como las siguientes:

Cuando las redes son pequeñas la configuración es sencilla de hacer, no obstante, cuando la red va a aumentando su tamaño su complejidad de configuración tambiénse incrementa.

La configuración puede ser propensa a errores humanos.

Requiere un conocimiento completo de toda la red para una correcta implementación

Ahora se verán algunos ejemplos de configuración para los diferentes fabricantes

Cisco

R# configure terminal

R (config)# ipv6 route 2001:db8:cafe::/64 2001:db8:efac::1

R (config)# ipv6 route ::/0 2001:db8:efca::1

Huawei

<R> system-view

[R] ipv6 route-static 2001:db8:cafe:: 64 2001:db8:efac::1

[R] ipv6 route-static :: 0 2001:db8:efca::1

Juniper

root@R1> edit

root@R1# set routing-options rib inet.6 static route 2001:db8:cafe::/64 next-hop 2001:db8:efac::1

OSPF:

Este es un protocolo de enrutamiento dinámico de tipo estado enlace, el cual es usado comúnmente en redes medianas y grandes, no obstante, inicialmente solo fue diseñadopara el protocolo IPV4 así que se realizó modificaciones en la versión 3 de OSPF paraque permitiera IPv6, esta versión es muy similar a la versión 2 pero al inicio solo

soportaba IPv6 y no IPv4 así que se debía correr dos procesos de OSPF a la vez lo que generaba sobreprocesamientos y mayor ancho de banda, esto cambio con el tiempo y actualmente soporta ambos protocolos, donde se diferencian usando el concepto de address family, lo anterior quiere decir que existe familia para IPv4 y una familia para IPv6, de esta manera ayuda a simplificar la operación para el administrador de redes. Sinembargo, cabe destacar que en algunos router como los de marca Cisco, el servicio de enrutamiento OSPF no se debe configurar a nivel global como se ejecutaba en la versión2, sino que esto se efectúa sobre las interfaces que se desean utilizar, es decir se deben configurar los prefijos por interfaz.

Otros puntos para tener en cuenta sobre OSPF V3 es que este protocolo utiliza grupos de direcciones multicast para funcionar donde se agrupan los distintos routers que usan el protocolo de enrutamiento, los grupos multicast implementados son FF02::5 y FF02::6. Así mismo el router-id sigue siendo una dirección IPv4 (32 bits), igualmente los área-id ylos link-id también utilizaran este formato de 32 bits. Por otro lado, las diferentes adyacencias entre los equipos se usan por medio de las direcciones IPv6 link-local de los distintos router.

A nivel de seguridad, OSPF V3 se diferencia a su anterior versión en que OSPF V2 utiliza como autenticación el texto no cifrado o autenticación MD5, mientras que OSPFV3 utiliza autenticación IPv6.

Como se mencionó con anterioridad, los demás parámetros de configuración son similares entre versiones, se debe habilitar el protocolo de enrutamiento, modificar lasinterfaces pasivas (si las posee), establecer un router-id, la implementación de la

redistribución de rutas es semejante, de igual manera la configuración del hello-interval oel dead-interval.

En conclusión, OSPF V3 es muy idéntico a OSPF V2, hay que identificar acertadamente los pequeños cambios que se hacen, pero a niveles generales sus beneficios son iguales, por lo tanto, continúa siendo un protocolo bastante potente y altamente usado en redes medianas y grandes.

IS-IS:

Este protocolo también es de estado-enlace, no obstante, intercambia información por medio de mensajes LSP los cuales se transportan a través de la capa de enlace de datos o capa 2, dentro de la información de este protocolo se mencionan extensiones con el fin deanunciar prefijos IPv6 y también IPV4 definiendo 2 TLVs (type length value) para este protocolo (IPv6), el IPV6 reachability el cual contiene información de prefijos IPV6 y el otro es el IPV6 interfaces address el cual posee el next-hop IPV6. Por otro lado, también se relacionan las address families donde incluyen a IPV6 allí se tiene en cuenta que para su implementación en dual-stack se utilizan los modos de multitopologia y de topología única.

Para el primero, el modo permite que las topologías se mantengan independientes para ambos protocolos (IPv4 e IPv6) dentro de un área, con esta manera de configuración se omine una restricción de que las interfaces donde se establece IS-IS tengan que soportar el mismo conjunto de address families y a su vez la restricción de que dentro del área implementada los dispositivos de enrutamiento tengan que igualmente soportar el mismoconjunto de address families.

Para el segundo caso de topología única, para configurar este modelo todas las interfacesdeben implementarse con el mismo conjunto de address families igualmente los enrutadores de la misma área tienen que poseer el mismo conjunto de address families entodas sus interfaces.

BGP:

Es un protocolo de ruteo externo, generalmente utilizado por los ISP en sus conexiones wan, al igual que los dos protocolos anteriores este utiliza el término de address family para distinguir entre IPv4 e IPv6 en donde aquí se define un identificador llamado AFI para detectar el protocolo y un identificador SAFI para saber si es una comunicación unicast o multicast, si el AFI tiene identificador 1 este informa que es una familia IPv4, siel AFI es 2 dice que la familia es IPv6; de igual manera para el identificador SAFI si estees 1 quiere decir que la comunicación es unicast, si el SAFI es 2 esta será multicast.

Uno de los parámetros a tener en cuenta en el BGP es el router-id, donde al igual que OSPF este maneja una dirección de 32 bits, es decir el router id posee IPv4

Otros aspectos en la configuración del BGP son la de los prefijos, ya que generalmente dentro de estos se establecen las redes que se quieren anunciar al vecino BGP, esto se efectúa de forma similar que en IPv4 donde solo se establece el Prefix-List correspondiente y allí se agregan dichos segmentos de red, varia depende del fabricantede los enrutadores, por ejemplo, en los dispositivos de marca Cisco se ejecuta de la siguiente manera:

Figura 28 Configuración prefix-list Cisco

Este es uno de muchos ejemplos de cómo se puede aprovisionar los Prefix-List para el anunciamiento de redes en IPv6.

Cabe destacar que como se mencionó, BGP es establecido generalmente en las rede wande los ISP así que ellos lo adhieren a la tecnología MPLS, por lo que se verá a continuación puntos importantes de cómo funciona IPV6 con la tecnología VPN/MPLS.Los mecanismos de transición usados para la tecnología MPLS con BGP en IPV6 son 6PE y 6VPE los cuales poseen varios beneficios como:

Costos y riesgos operativos mínimos, donde no se afectarán los servicios IPV4existentes

Se pueden utilizar enrutadores existentes o se pueden destinar alguno dedicado para el tráfico IPV6, por lo que son muy flexibles de utilizar.

Los servicios IPV6 se pueden desplegar sin alguna afectación de manera eficiente e inmediata.

Se pueden agregar nuevos routers 6PE o 6VPE sin afectar la red.

6PE: Esta es una técnica que brinda conectividad IPV6 por medio de la red IPV4 MPLS, donde se permite que la tabla de enrutamiento comparta su información de enrutamiento con los demás dispositivos. 6PE permite que los dominios IPV6 se comuniquen entre sí por medio de IPV4 sin una configuración de túnel explicita requiriendo solo una dirección IPV4 por dominio, mientras se establece 6PE los enrutadores que proporcionan soporte a 6PE son actualizados continuamente para admitir dicho protocolo mientras que el resto de la red central no se toca, esta implementación no requiere reconfiguración de los routers de core ya que el reenvió de

paquetes se basa en etiquetas (no en encabezado IP). Esto proporciona una estrategia rentable para implementar IPv6. La información de accesibilidad de IPv6 es intercambiada por enrutadores PE utilizando extensiones MPLS.

Otro punto importante de 6PE es que este se fundamenta en extensiones iBGP en la configuración de la red IPV4 en el router del PE para intercambiar información de accesibilidad IPv6 además de una etiqueta MPLS para cada prefijo de dirección IPv6 que se anunciará. De igual manera los PE deben ser dual stack y utiliza la dirección IPv6 asignada a IPv4 para el intercambio de accesibilidad de prefijo IPv6.

También es importante saber que el siguiente salto anunciado por el PE para 6PE sigue siendo la dirección IPv4 que se utiliza para las rutas VPN IPv4 L3.

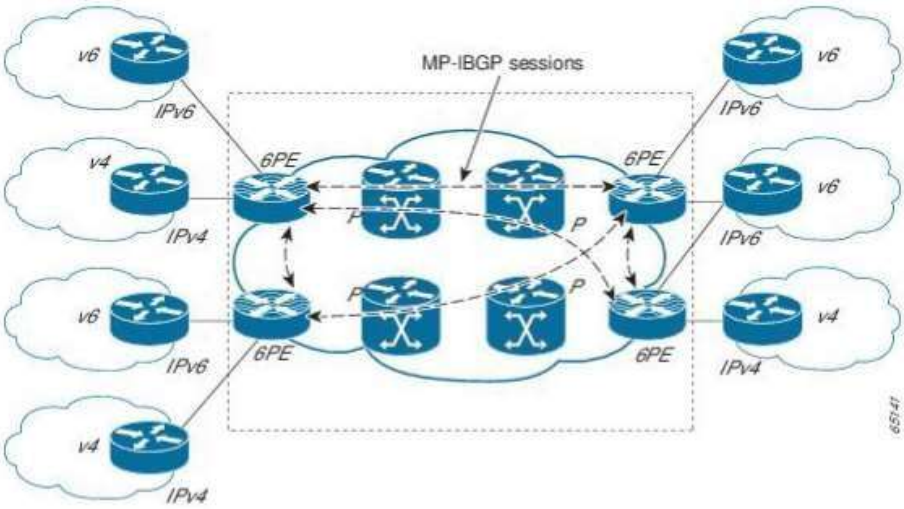


Figura 29 Rutas 6PE

6VPE: Este mecanismo usa el Backbone IPV4 para proveer los servicios de IPV6, es decir, IPV6 aprovecha las troncales IPV4 en funcionamiento para transportar el tráfico. Este funciona más como un proveedor de borde MPLS-VPN normal con una adición de soporte IPV6

dentro de las vrf, por lo que se proporcionan entradas a la tabla de enrutamiento lógicamente separadas por los equipos miembros de las vpn (instancias vrf). La diferencia entre este método y el 6PE es que este maneja las vrf.

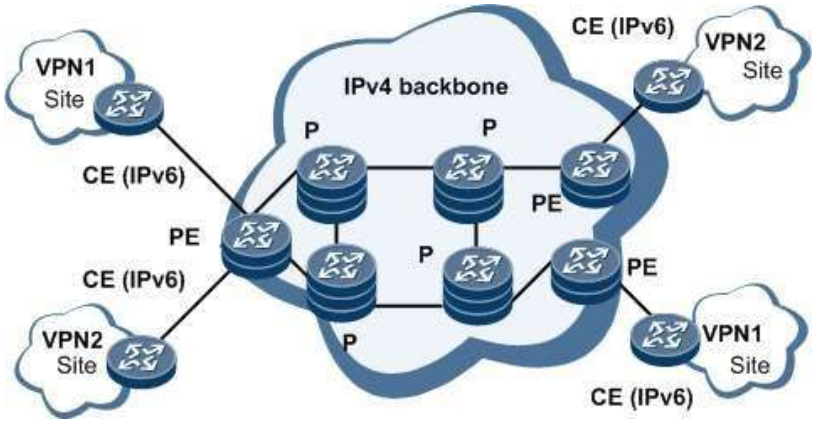


Figura 30 Rutas 6VPE

Ventajas y desventajas de IPv6

Ventajas

1. Mayor cantidad de direcciones IP disponibles y asignables.
2. Infraestructura de red más eficiente.
3. Seguridad integrada y más confiable.
4. La cabecera utilizada es simplificada en comparación a la de ipv4

   Ipv6 incluye estándar Plug and Play lo que permite facilitar a los usuarios cualquier tipo de conexión a sus redes.
5. Los mecanismos de movilidad empleados poseen mayor eficiencia que los utilizados con ipv4, lo que garantiza una mejor conectividad al cambiar de red.

Desventajas

1. Al ser un protocolo nuevo y emergente, para muchos ingenieros puede ser difícil de emplear al inicio, no obstante, esto puede ser mientras se genera la respectiva adaptación, estudio y experiencia de los diferentes cambios que se presentan con esa nueva versión.
2. Demoras actuales de implementación ya sea por medio de transición o usando la red ipv6 nativa desde un inicio, se ha observado que a pesar de que el protocolo se estandarizo hace ya varios años, aun se tiene un porcentaje muy bajo de despliegue a nivel global.

Servicios y aplicaciones

Ipv6 se originó con el fin de satisfacer las necesidades de conectividad imposibles de lograr con el protocolo Ipv4, como se mencionó anteriormente, debido a la cantidad tan baja de direcciones que hay actualmente, donde en muchas partes del mundo se han agotado, esto a pesarde los esfuerzos de varios RIR como LACNIC, que efectúan diferentes proyectos de recuperación de direcciones IP, es decir, se ejecuta un estudio de las IP's que no están siendo usadas por las diferentes compañías que inicialmente se les otorgó estas y se reutiliza, también protocolos como nat que intenta mitigar al máximo el consumo de direcciones IP, inclusive los diferentes ISP otorgan sus servicios a clientes masivos, haciendo uso de una IP o un pool de IPs publicas localizadas en algún nodo y que proveen servicios a varios clientes finales, en otras palabras, se configuran redes privadas para una cantidad X de usuarios los cuales saldrán a internet por medio del mismo segmento de red público, igualmente sucede con los servicios empresariales, donde se contrata un servicio el cual se operara centralizadamente, lo que quiere decir que todas las sedes de una corporación X enrutaran sus redes hacia un sitio principal y de allí por medio de un |canal de internet, ya sea con una IP o un segmento de red público, brindara salida a internet a toda la corporación, sin embargo, aunque estas metodologías parezcan ser ideales, tiene una serie de inconvenientes que hacen necesario el uso de IPv6:

El uso de nat aumenta retrasos en la red, ya que debe efectuar la traducción de las direcciones IP privadas a las/la IP publica, esto demora dado que el router debe procesar la información, validar si las redes se encuentran dentro de las reglas de traducción, hacer modificación de los encabezados, etc. Esto afecta servicios quedeben usarse en tiempo real como VoIP, o el streaming.

Otra falencia que tiene el protocolo nat es que el direccionamiento de extremo a extremo se pierde, lo que en ocasiones es una desventaja para ciertas aplicaciones oservicios que necesitan conocer esta información en su comunicación, igualmente elseguimiento de los paquetes que pasan por varios cambios de dirección a través de varios saltos de nat se torna complejo y en consecuencia de esto dificulta la resolución de problemas.

Cuando se hace uso de tunelización nat modifica algunos valores de los encabezadosy en ocasiones puede generar falla de comprobaciones.

Por ultimo y no menos importante es el hecho de que nat solo mitiga temporalmenteel agotamiento de direcciones IP, de tal motivo que cuando se ocupen todas las direcciones no se pueden generar redes escalables lo que afectara con el desarrollo tecnológico.

Lo anterior explica los motivos por los cuales IPv6 es importante implementarse, para aplacar los inconvenientes que se tienen en la actualidad, ya que con IPv6 todos los dispositivos usaran una IP valida en internet sin necesidad de aplicar protocolos intermediarios como nat, mejorando la funcionalidad de varios servicios y permitiendo el despliegue de otros:

Los servicios de Voz sobre IP poseen actualmente una gran ventaja sobre los servicios de voz tradicionales, ya que proporciona mayor ahorro económico, brinda movilidad y a su vez más flexibilidad, de esta manera se pueden monitorear las llamadas, también se pueden brindar más servicios y funcionalidades; no obstante, enIPv4 se presentan varios inconvenientes mencionados en páginas previas, estos son solventados con la llegada del protocolo IPv6, con este protocolo se tendrá solución a

Uno de los principales problemas que se posee la red de voz sobre IP el cual es la integridad de extremo a extremo que afecta tanto a nivel de seguridad como de señalización de VoIP, por lo tanto ya no habrían complicaciones con los firewalls o con el NAT, igualmente la seguridad de transmisión será mucho más efectiva dado que no se puede decodificar el audio porque IPV6 cifra las llamadas desde el protocolo base utilizando IPSEC, lo cual no sucede con IPV4 donde con este tambiénes posible hacerlo pero en capas superiores complicando la implementación de la redde VoIP.

Otro beneficio que se obtendrá con IPV6 es que al haber tantas direcciones disponibles es posible adicionar una IP por dispositivo móvil lo que colabora con laVoIP móvil así que no es necesario utilizar direcciones dinámicas y ya que los equipos tendrán una IP única a nivel global también eliminará los impedimentos de conectividad de extremo a extremo, generando mayor velocidad de comunicación loque influirá en llamadas mucho más fluidas y estables.

Los servicios de streaming y de IPVT igualmente se verán beneficiados ya que al utilizar dispositivos con una IP conocida en la red global no habrá tampoco problemas de conectividad de extremo a extremo, eliminando el uso de protocolos detraducción como el NAT permitiendo mejorar los tiempos de respuesta en la transmisión de paquetes, por tal motivo percepción a nivel de usuario final será mucho mejor.

Uno de los servicios que ha estado emergiendo desde hace varios años, pero por el limitante de las direcciones IP que tiene el protocolo IPV4 no se ha podido implementar como se desea, es el de IOT (internet of things) el cual pretende que

todos los objetos cotidianos o de uso corporativo posean conexión a internet parapoderlos administrar en lo posible de manera centralizada.

Con lo anterior se pueden desplegar varias e interesantes soluciones que con anterioridad solo parecían ficción, pero gracias a IOT se pueden hacer realidad, porejemplo, el uso de casas o edificios inteligentes, aplicaciones para dispositivos médicos, servicios de movilidad integrando vehículos inteligentes, servicios de administración a gran escala, aplicaciones agropecuarias, etc.,

Pero que mejoría posee IPV6 con respecto a IPV4 para el despliegue de servicios de IOT exceptuando la cantidad de direcciones IP mencionado con anterioridad. Una delas necesidades que presenta IOT es la necesidad de la autoconfiguración lo cual puede realizarse con IPV6 ya que se encuentra dentro de su diseño, usos de memoriamás eficientes esto ya que los dispositivos de IOT tienen varias restricciones de memoria lo que genera la necesidad de solo escoger un solo tipo de red (IPV6 o IPV4) no puede usarse dual stack si se quisiera; además de que IPV6 puede proporcionar mayor rendimiento al momento de su despliegue esto debido a que a futuro la red debe quedar totalmente en IPV6 así que si se deseara usar IPV4 con algunos de sus métodos de traducción sería más costoso y compleja la transición a IPV6 además de que debería pasar por dual stack lo que no se podría por las complicaciones de memoria.

Con la adopción del nuevo protocolo IPV6 este podrá ayudar al despliegue de la tecnología 5G beneficiando a la experiencia del usuario al obtener mayores tasas de transmisión, latencia y movilidad. Por otro lado, sus sistemas tendrán un mayor

desempeño, agregándole a esto servicios mejorados como la localización, seguridad, confiabilidad y transparencia en la conectividad.

IPV6 y 5G van de la mano dado que ambas significan una revolución tecnológica a las redes existentes, donde con 5G se proporcionarán anchos de banda y latencias enservicios móviles nunca vistas anteriormente además si a esto se le agrega la funcionalidad que brinda IPV6 con los servicios de extremo a extremo, las velocidades de respuesta como se mencionó inicialmente serán mucho mejor que lasque se tienen actualmente con IPV4 y con 4G. Por otro lado, La calidad de servicio (QoS) y la calidad de la experiencia (QoE) se convierten en consideraciones importantes que combinando ambas tecnologías se puede satisfacer proporcionandomejor experiencia de los usuarios.

Estándares IPV6

Tabla 2. Estándares RFC (Request For Comments) para el uso del protocolo IPV6

TIPO DE RFC	NUMERO DE RFC	NOMBRE DE RFC
Especificaciones generales	RFC2460	Especificación de IPv6
	RFC2461	Especificaciones de NDP (NEIGHBOR DISCOVERY PROTOCOL)
	RFC2462	Especificación de Autoconfiguración de Direcciones "stateless"
	RFC2463	Especificación de ICMPv6
	RFC1886	Especificación de extensión DNS
	RFC1981	Especificación de PATH MTU DISCOVERY
	RFC2147	TCP y UDP sobre IPV6
	RFC2428	Especificación de extensiones FTP para IPv6 y NAT
	RFC2474	Campo de Servicios Diferenciados y cabeceras
	RFC1909	Flow Label Field
Especificaciones de direccionamiento	RFC2373	Arquitectura de direccionamiento IPV6
	RFC1887	Especificación de arquitectura para la Asignación de Direcciones Unicast
	RFC2374	Formato de Direcciones Unicast Agregables Globales
	RFC1924	Representación Compacta de Direcciones IPv6
	RFC1881	Especificación de gestión para la asignación de Direcciones IPv6

	RFC2450	Propuesta de normas de asignación de TLA y NLA
Especificación de enrutamiento	RFC2080	Especificación de protocolo RIP
	RFC2081	Aplicabilidad de RIPng
	RFC2083	Extensiones Multiprotocolo para BGP
	RFC2545	Uso de las extensiones multiprotocolo para enrutamiento entre dominios IPV6
	RFC2546	Prácticas de Routing en 6Bone
	RFC2772	Guías de Routing en el troncal 6Bone
	RFC2740	OPSF V3
Especificaciones de seguridad	RFC2401	Especificación de arquitectura de seguridad para IPV6
	RFC2402	Especificación de la cabecera de autenticación IPV6
	RFC2406	Encripcion de datos en IP (ESP)
	RFC2408	Especificaciones ISAKMP
Grupos de direcciones	RFC2375	Asignación de direcciones multicast
	RFC2710	Descubrimiento de nodos IPV6
	RFC2776	Especificaciones MZAP
	RFC2526	Especificación de direcciones ANYCAST
Transición IPv6	RFC1933	Mecanismos de transición
	RFC2185	Parámetros de enrutamiento de la transición IPV6
	RFC2473	Especificaciones de tunelización
	RFC2529	Transmisión de IPv6 sobre Dominios IPv4
	RFC2765	Especificación para el algoritmo de Traslación Stateless IP/ICMP (SIIT)

	RFC2766	Protocolo de Traslación
	RFC2767	Dual Stack con la técnica "Bump-In-the-Stack" (BIS)
MIB	RFC2466	Especificación base de la información ICMPv6
	RFC2454	Base de Información de Gestión para IPv6: UDP
	RFC2452	Base de Información de Gestión para IPv6: TCP
Redes de transmisión	RFC2464	Especificación de transmisión sobre ethernet
	RFC2467	Especificación de transmisión sobre redes FDDI
	RFC2470	Especificación de transmisión sobre redes token rinkg
	RFC2472	Especificación para el uso de PPP
	RFC2491	IPv6 sobre redes de Acceso Múltiple Sin Broadcast
	RFC2492	Especificación para el uso de ATM

Ejemplo de transición de una red Lan de IPv4 a IPv6

A continuación, se ejecutará un ejemplo de transición de la red IPV4 a la infraestructura IPV6 de una empresa mediana, para ello se tendrán en cuenta todos los conceptos apreciados con anterioridad, donde es importante resaltar que se mantendrán ambos protocolos, es decir, será una red dual stack.

Para la realización del proyecto de ejemplo se ejecutará una metodología por fases, basándose en la guía de transición propuesta por el MINTIC para Colombia, donde ellos proponen 3 fases (planeación, implementación y pruebas), no obstante, en este ejemplo se añadirá una fase adicional, lo que permitirá dar mayor orden y por ende estructurar más eficientemente la migración, identificando los puntos críticos y no tan críticos de la transición.

Las fases que se utilizaran son las siguientes:

Fase de investigación

En esta se realizará todo el levantamiento de información sobre la topología de red, equipos finales, servidores, dispositivos networking, seguridad, servicios, y todo elemento a tener en cuenta que pueda involucrarse dentro de la transición del protocolo IP, esto será de gran utilidad para identificar que equipos soportan la versión IPV6 y cuales no, si se llegase a tener uno que no lo soporta se ejecutara en las siguientes fases el respectivo análisis y el procedimientoa realizar para remplazar estos por unos que si cumplan y satisfagan las necesidades de la solución.

Fase de Diseño o Planeación

Al ya haber observado y analizado la información disponible en la fase anterior, lo que se procederá a hacer es el desarrollo de la arquitectura de la red con el nuevo protocolo, identificando si se mantiene la topología actual, se harán cambios pequeños, o se modificara toda la estructura. De igual manera allí se debe detallar el direccionamiento IPv6 a utilizar, adquiriendo este por medio ya sea de un ISP o de la LACNIC y a su vez distribuyendo ese a través de los diferentes segmentos de red teniendo en cuenta la posible escalabilidad de la misma, es decir, manteniendo una reserva de direcciones adecuada para el futuro.

Así mismo se debe establecer el respectivo protocolo de pruebas para ejecutar al final de la implementación y que permita determinar que la transición sea satisfactoria.

Fase de implementación

En esta fase se configurará en los equipos el direccionamiento IPV6 establecido con anterioridad, ubicando las VLAN que se utilizaran las cuales también se deben detallar en la fasede planeación. Igualmente se habilitará la opción de IPV6 en los dispositivos que se identificaronpor medio del inventario que se debe realizar.

Por otro lado, se ejecutará el montaje de los diferentes servicios esenciales para el funcionamiento de la red de la empresa, teniendo en cuenta la coexistencia de ambos protocolos (IPV4 e IPV6)

Fase de pruebas de funcionalidad

Después de ejecutar las respectivas configuraciones y procesos de implementación, se harán las pruebas de funcionamiento correspondientes para determinar que el protocolo IPV6 se

encuentra operando adecuadamente y no haya generado algún conflicto sobre la red. Se probarán los servicios, se revisará la conectividad entre dispositivos, y de igual manera comunicación hacia Internert.

Fase 1: Investigación

Como se mencionó con anterioridad en esta etapa se hará la identificación de elementosque se tienen actualmente en la organización, y en especial cuales de estos soportan y no soportan el protocolo IPV6, dado lo mencionado se tiene la siguiente información recolectada:

Tabla 3. Inventario equipos finales

Inventario so equipos finales

Área	Sistema operativo	Cantidad	Soporta IPV6
Presidencia	Windows 10	3	si
Gerencia	Windows 10	3	si
Área comercial	Windows 10	48	si
	Windows 7	7	si
TI	Windows 10	3	si
Implementación	Windows 10	7	Si
Preventa	Windows 10	15	Si
	Windows 7	5	Si
Servicios	Windows 10	15	Si
Área financiera	Windows 10	4	Si

	Windows 7	2	Si
HSEQ	Windows 10	3	Si
Almacén	Windows 10	10	Si
	Windows 7	2	Si
Talento humano	Windows 7	3	Si
Área jurídica	Windows 10	3	si
Impresoras	HP MFP M428dw	2	Si

Tabla 4. Inventario servidores

Inventario servidores

Servicio	**Servidor**	**Soporta IPV6**
Directorio Activo	Windows Server 2016	SI
Solar Winds Storage server Data base server	Windows server 2019	Si
SIIGO SAP	Windows Server 2016	si

Tabla 5. Inventario cctv

CCTV

Dispositivo	Referencia	Cantidad	Soporta IPV6
Cámara IP	IPC-HFW5241E-S Dahua	40	Si
Cámara IP	IPC-HDW5241H-AS-PV - Dahua	15	Si
NVR	DHI-NVR608-32-4KS2 - Dahua	2	Si

Tabla 6. *Inventario Wireless*

Wlan

Dispositivo	Referencia	Cantidad	Soporta IPV6
Access point	AirEngine6760-X1 - Huawei	16	si
Public cloud Huawei	iMaster NCE-Campus	1	si

Tabla 7. *Inventario Networking*

Networking

Dispositivo	Referencia	Cantidad	Soporta IPV6
Switch Core	WS-C2960-24PC-L	2	Si
Switch acceso	WS-C2960-24TT-L	7	Si
Router (ISP)	Cisco c881 K9	2	Si

Tabla 8. *Inventario Seguridad*

Seguridad

Dispositivo	Referencia	Cantidad	Soporta IPV6
Firewall	fortigate 30e	1	Si

Además del inventario, se muestra también la topología de red de la organización:

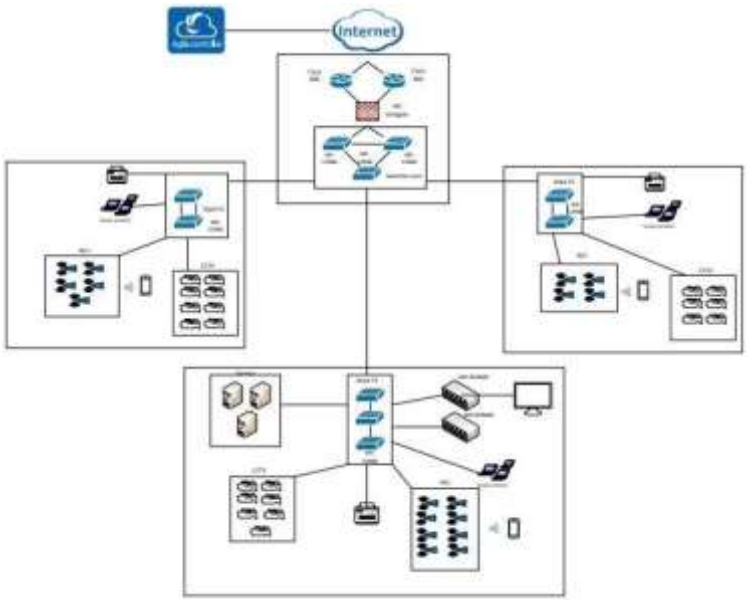


Figura 31 Topología de red ejemplo

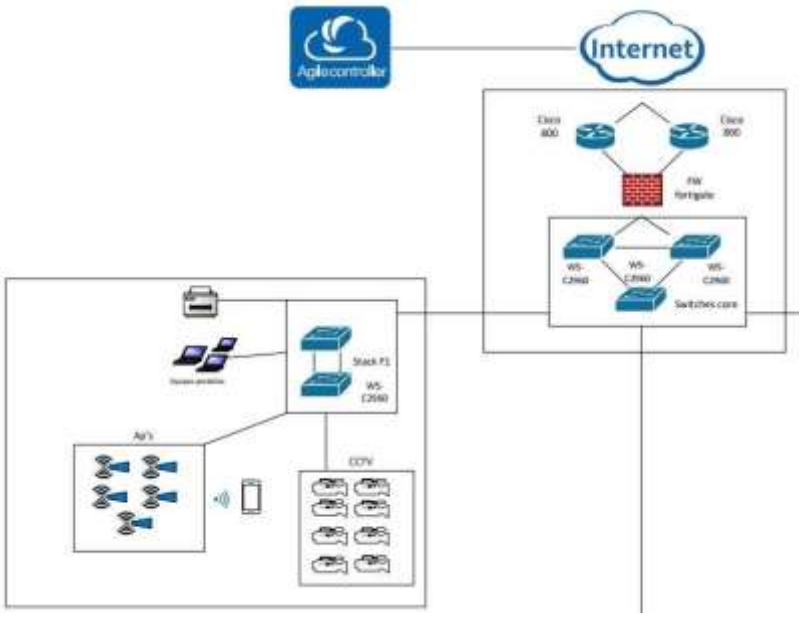


Figura 32 Topología Piso 1

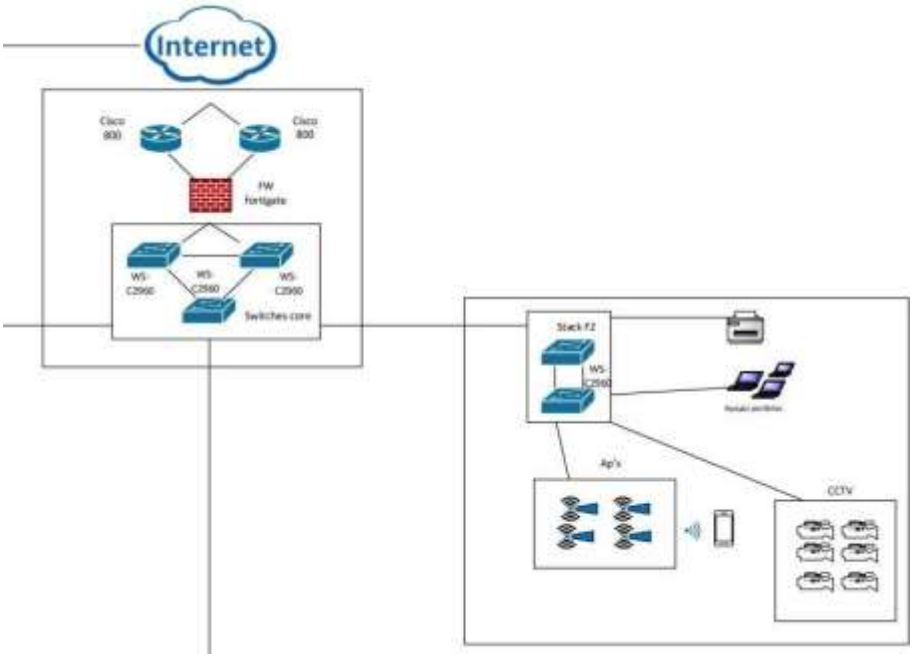


Figura 33 Topología Piso 2

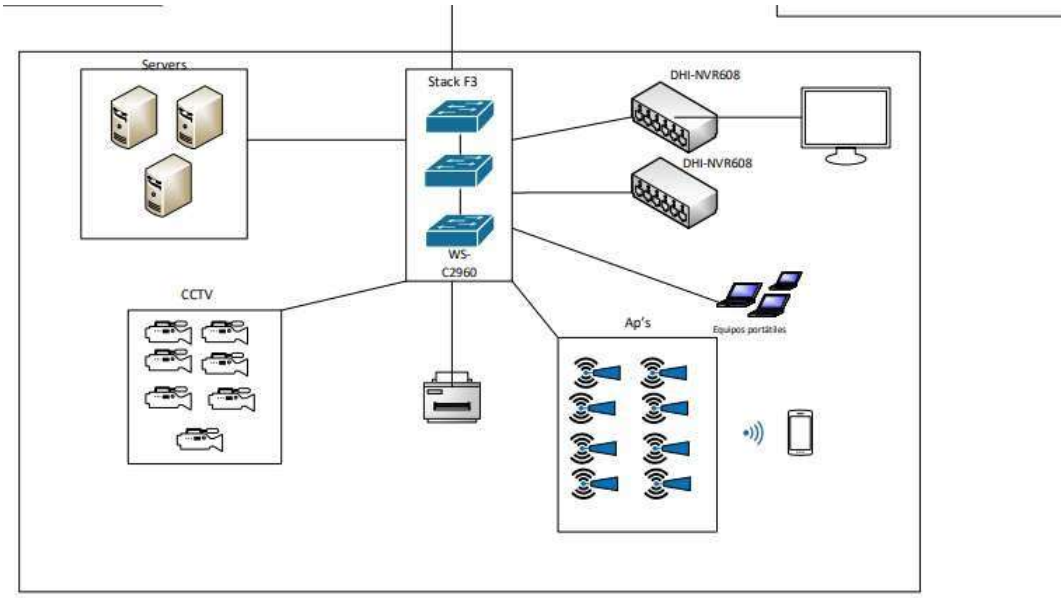


Figura 34 Topología Piso 3

Por otro lado, se determina la configuración de las VLAN actualmente implementadas:

Tabla 9. *Vlan Implementadas*

ID Vlan	Nombre Vlan
1	WAN
10	WIFI Funcionarios
20	WIFI Invitados
30	CCTV
40	VoIP
100	Servers
110	Presidencia / Gerencia
120	Área comercial / Área financiera
130	TI
140	Implementación
150	Preventa
160	Servicios
170	HSEQ
180	Almacén
190	Talento humano
200	Área jurídica

Fase 2: Planeación

Ya con la información obtenida se pueden analizar los datos, donde se consigue lo siguiente:

1. Los equipos finales utilizados en la compañía manejan un sistema operativo Windows que soporte el protocolo IPV6, por tal motivo no es necesario hacer cambios de estos
2. Los servidores también manejan sistema operativo WINDOWS, donde sus versiones son las más recientes así que también soportan el protocolo IPV6.
3. Las cámaras y NVR utilizados por la empresa tienen dentro de sus características el soporte de IPV6, se debe hacer la activación de este protocolo y asignar el direccionamiento correspondiente
4. El servicio WIRELESS no es indiferente al protocolo IPV6, esta solución dentro de su datasheet especifica que soporta esta versión, solo hay que activar la funcionalidad e igualmente adicionar el direccionamiento a los AP's
5. Los equipos networking de switching son compatibles con IPV6, se debe activar la opción
6. Los router del ISP soportan IPV6, se debe generar caso con el proveedor para la activación del protocolo y configuración de los parámetros. Esto dependiendo del pool IP que se adquiera.
7. El firewall utilizado para la seguridad de la compañía dentro de sus especificaciones indica que soporta IPV6, se debe realizar el respectivo procedimiento de activación del protocolo.
8. El protocolo de enrutamiento utilizado a nivel interno desde el FW hacia los router del ISP con una ruta por defecto.
9. El servicio de DHCP se establece desde el firewall.

El paso a seguir es la adquisición del pool IPV6, para ello se deben comprender algunos de los requisitos informados por la LACNIC:

1. Estar legalmente establecido dentro de la región y utilizar los recursos dentro del área de cobertura de LACNIC.
2. Documentar un plan detallado sobre los servicios y la conectividad en IPv6 a ofrecer a otras organizaciones.
3. Anunciar en el sistema de rutas inter-dominio de Internet el bloque asignado, con la mínima desagregación que le sea posible, en un plazo no mayor a 12 meses.
4. Realizar una descripción detallada de los planes de enrutamiento, incluyendo los protocolos a ser usados.

Si se poseen estos, se puede hacer la solicitud de un dominio IPv6, obteniendo el siguiente direccionamiento: 2001:0db8:cafe::/48.

El siguiente paso a realizar es distribuir el direccionamiento en las redes que se tienen actualmente, las cuales son 16, al desarrollar las subredes con el segmento entregado por el ISP, se consigue lo siguiente:

Tabla 10. Direccionamiento *por Vlan*

ID Vlan	Nombre Vlan	Direccionamiento
1	WAN	2001:0db8:cafe:0::/52
10	WIFI FUNCIONARIOS	2001:0db8:cafe:1000::/52

20	WIFI INVITADOS	2001:0db8:cafe:2000::/52
30	CCTV	2001:0db8:cafe:3000::/52
40	VoIP	2001:0db8:cafe:4000::/52
100	Servers/printer	2001:0db8:cafe:5000::/52
110	Presidencia / Gerencia	2001:0db8:cafe:6000::/52
120	Área comercial / Área financiera	2001:0db8:cafe:7000::/52
130	TI	2001:0db8:cafe:8000::/52
140	Implementación	2001:0db8:cafe:9000::/52
150	Preventa	2001:0db8:cafe:a000::/52
160	Servicios	2001:0db8:cafe:b000::/52
170	HSEQ	2001:0db8:cafe:c000::/52
180	Almacén	2001:0db8:cafe:d000::/52
190	Talento humano	2001:0db8:cafe:e000::/52
200	Área jurídica	2001:0db8:cafe:f000::/52

Para el enrutamiento, se hará uso del modelo actual, donde se posee una comunicación ruta estática desde el firewall, desde los CPE del ISP hacia el PE es por medio de BGP

Por otro lado, el DHCP a usar se establecerá desde el firewall como actualmente se encuentra configurado, donde este equipo funcionará como servidor y proporcionará los parámetros correspondientes, como, por ejemplo: un lease de 1 día para todas las subredes, no habrá exclusión de direccionamiento, se utilizarán los DNS IPV6 de Google:

2001:4860:4860::8888

2001:4860:4860::8844

De igual manera, se determinará el protocolo de pruebas que se manejará:

1. El primer punto a revisar será la configuración de cada uno de los dispositivos (switch, router, firewall, wlan, voip), identificar que esta sea la adecuada, para que los servicios funcionen adecuadamente tanto por IPV4 como por IPV6
2. Verificar la distribución de puertos de los swtiches en las distintas zonas de la compañía, para que la configuración llegue correctamente a los departamentos
3. Hacer pruebas de direccionamiento para cada una de las VLAN propagadas a través de la LAN, y validar que la IP que esta asignando el firewall este dentro de la respectiva segmentación para cada una de las mismas.
4. Efectuar pruebas de conectividad para observar la correcta implementación del direccionamiento IPV6 en los equipos tanto de core, como dispositivos de acceso, de servicio y finales.
5. Validar que las políticas aplicadas en el firewall no afecten el protocolo IPV6.

Fase 3: Implementación

La implementación se ejecutará de manera simulada por medio del software GNS3, allíse utilizará el diseño topológico de la estructura de red revisada en la fase de investigación, se configurarán los parámetros en capa 3, se realizará la implementación del protocolo IPV6 y se ejecutará la revisión de los diferentes parámetros.

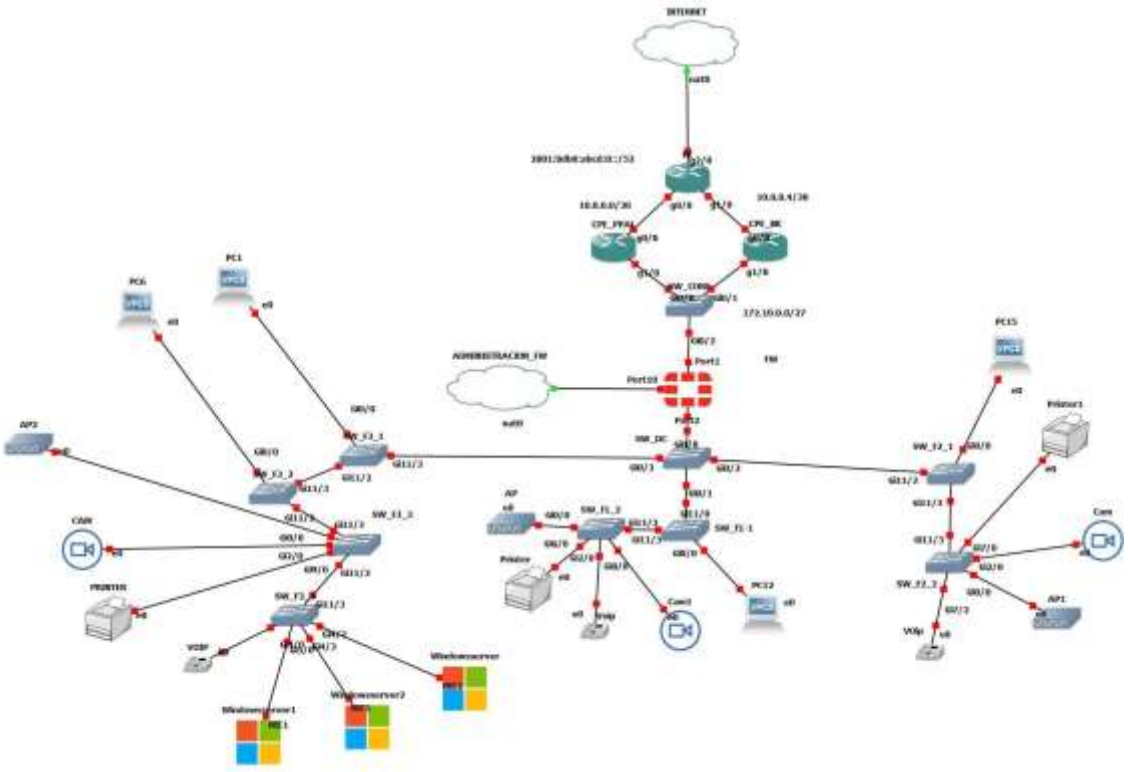


Figura 35 Topología GNS3

Lo primero será hacer la configuración de los CPE para el uso del protocolo IPV6, normalmente esto lo efectúa el ISP, pero para medio de estudio se ejecutará esta también:

A continuación, se mostrará la implementación de IPV6 para los router del ISP, tanto el PE como el CPE:

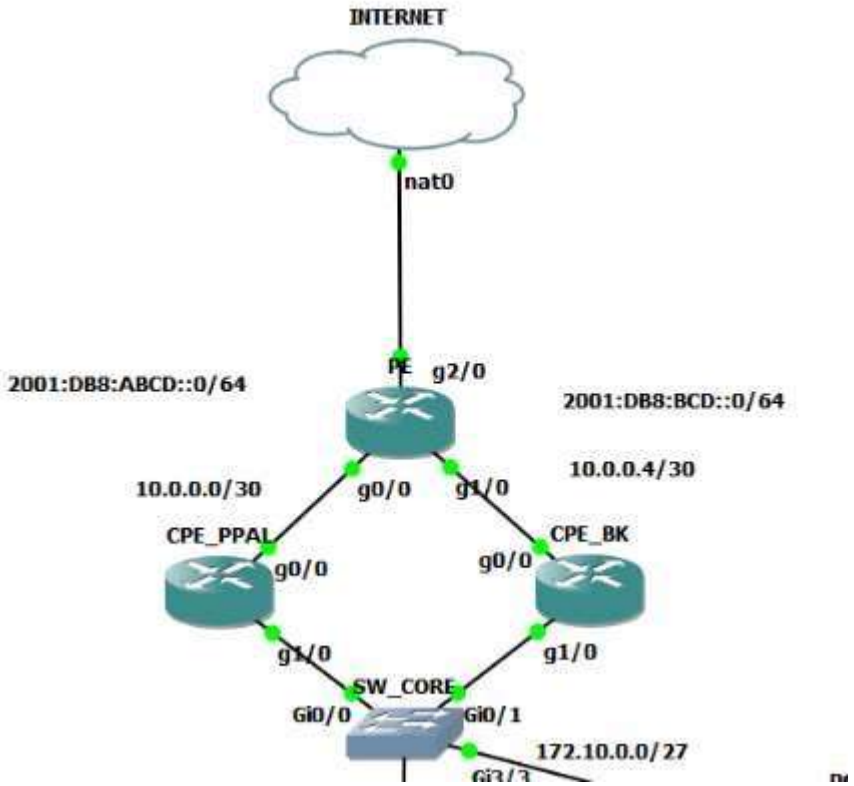


Figura 36 Equipos Core

Se resalta estos equipos ya deben tener todas las demás configuraciones para que el servicio opere en IPv4, únicamente se explicara el aprovisionamiento de IPv6 además de que al estar la compañía en funcionamiento cada cambio que se haga sobre los equipos se deberá hacer programando una ventana de mantenimiento, con las áreas correspondientes y tener a la mano los backup respectivos de los equipos a intervenir.

Se iniciará habilitando el servicio IPv6 en los router

PE:

```
PE(config)#ipv6 unicast-routing
```

CPE Ppal: `CPE_PPAL(config)#ipv6 unicast-routing`

CPE Backup: `CPE_BK(config)#ipv6 unicast-routing`

Se procede a asignar el direccionamiento WAN en cada una de sus interfaces:

Tabla 11. *Direccionamiento e Interfaces Router ISP*

	PE	CPE Ppal	CPE Bk
GIG 0/0	2001:DB8:ABCD::1/64 FE80::C803:33FF:FEF8:8	2001:DB8:ABCD::2/64 FE80::1	2001:DB8:BCD::2/64 FE80::2
GIG 1/0	2001:DB8:BCD::1/64 FE80::C803:33FF:FEF8:1C	2001:DB8:CAFE::2/52 FE80::1	2001:DB8:CAFE::3/52 FE80::2

1. PE

```
interface GigabitEthernet0/0
 ip address 10.0.0.1 255.255.255.252
 duplex full
 speed auto
 media-type gbic
 negotiation auto
 ipv6 address 2001:DB8:ABCD::1/64
 ipv6 enable
!
interface GigabitEthernet1/0
 ip address 10.0.0.5 255.255.255.252
 negotiation auto
 ipv6 address 2001:DB8:BCD::1/64
 ipv6 enable
```

Figura 37 Configuración interfaces PE

2. CPE Ppal

```
interface GigabitEthernet0/0
 ip address 10.0.0.2 255.255.255.252
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ABCD::2/64
 ipv6 enable
!
interface GigabitEthernet1/0
 ip address 172.10.0.1 255.255.255.0
 standby version 2
 standby 1 ipv6 autoconfig
 standby 1 priority 120
 standby 1 preempt delay minimum 30
 standby 1 track 1 decrement 90
 negotiation auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:CAFE::2/52
 ipv6 enable
```

Figura 38 Configuración interfaces CP Ppal

Dentro de la configuración de las interfaces se aprecian otros parámetros como el HSRP en ipv6 que más adelante se explicara.

3. CPE Bk

```
interface GigabitEthernet0/0
 no ip address
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:BCD::2/64
 ipv6 enable
!
interface GigabitEthernet1/0
 ip address 172.10.0.2 255.255.255.0
 standby version 2
 standby 1 ipv6 autoconfig
 standby 1 preempt delay minimum 30
 negotiation auto
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:CAFE::3/52
 ipv6 enable
```

Figura 39 Configuración interfaces CPE Bk

Luego de esto, se realizarán pruebas de conectividad entre los equipos CPE hacia el PE

4. CPE > PE

```
CPE_PPAL#ping 2001:DB8:ABCD::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ABCD::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms
```

Figura 40 Ping CPE Ppal> PE

5. CPE Bk > PE

```
CPE_BK#ping 2001:DB8:BCD::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:BCD::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/17/20 ms
```

Figura 41 PING CPE Bk > PE

El siguiente paso es habilitar el sw de core, para que los router se comuniquen con la red LAN de la compañía, esta configuración en ambiente real ya se encuentra establecida y no se explicara en este documento ya que solo se activaran las interfaces y se pondrán estas en modo troncal.

Luego de efectuar lo anterior se establece comunicación entre los CPE:

```
CPE_PPAL#ping 2001:DB8:CAFE::3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:CAFE::3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/23/32 ms
CPE_PPAL#
```

Figura 42 PING CPE PPAL> CPE BK

El siguiente paso es lograr establecer las reglas de enrutamiento a nivel WAN, para ello se utilizará el protocolo de enrutamiento BGP, el cual permitirá hacer uso de las familias para el anunciamiento y aprendizaje de las redes LAN, se configurará primero el PE de la siguiente manera:

```
router bgp 200
 bgp router-id 1.1.1.1
 bgp log-neighbor-changes
 neighbor 2001:DB8:BCD::2 remote-as 100
 neighbor 2001:DB8:ABCD::2 remote-as 100
 !
 address-family ipv4
  no neighbor 2001:DB8:BCD::2 activate
  no neighbor 2001:DB8:ABCD::2 activate
 exit-address-family
 !
 address-family ipv6
  neighbor 2001:DB8:BCD::2 activate
  neighbor 2001:DB8:BCD::2 soft-reconfiguration inbound
  neighbor 2001:DB8:ABCD::2 activate
  neighbor 2001:DB8:ABCD::2 soft-reconfiguration inbound
 exit-address-family
```

Figura 43 Configuración BGP PE

Como se puede apreciar, se utiliza la función address-family ipv6, no se debe confundir con la función address-family vpnv6, ya que estas se utilizan en la comunicación interna de una MPLS, pero en este caso la conectividad va desde el PE el cual es el equipo de borde de la MPLS hacia un CPE el cual se encuentra en la sede de la empresa.

El próximo paso será configurar los BGP de tanto el router principal como el router backup:

```
router bgp 100
 bgp router-id 2.2.2.2
 bgp log-neighbor-changes
 neighbor 2001:DB8:ABCD::1 remote-as 200
 !
 address-family ipv4
  no neighbor 2001:DB8:ABCD::1 activate
 exit-address-family
 !
 address-family ipv6
  network 2001:DB8:CAFE::/52
  network 2001:DB8:CAFE:1000::/52
  network 2001:DB8:CAFE:2000::/52
  network 2001:DB8:CAFE:3000::/52
  network 2001:DB8:CAFE:4000::/52
  network 2001:DB8:CAFE:5000::/52
  network 2001:DB8:CAFE:6000::/52
  network 2001:DB8:CAFE:7000::/52
  network 2001:DB8:CAFE:8000::/52
  network 2001:DB8:CAFE:9000::/52
  network 2001:DB8:CAFE:A000::/52
  network 2001:DB8:CAFE:B000::/52
  network 2001:DB8:CAFE:C000::/52
  network 2001:DB8:CAFE:D000::/52
  network 2001:DB8:CAFE:E000::/52
  network 2001:DB8:CAFE:F000::/52
  neighbor 2001:DB8:ABCD::1 activate
  neighbor 2001:DB8:ABCD::1 soft-reconfiguration inbound
 exit-address-family
```

Figura 44 Configuración BGP CPE Ppal

```
router bgp 100
 bgp router-id 3.3.3.3
 bgp log-neighbor-changes
 neighbor 2001:DB8:BCD::1 remote-as 200
 neighbor 2001:DB8:BCD::1 update-source GigabitEthernet0/0
 !
 address-family ipv4
  no neighbor 2001:DB8:BCD::1 activate
 exit-address-family
 !
 address-family ipv6
  network 2001:DB8:CAFE::/52
  network 2001:DB8:CAFE:1000::/52
  network 2001:DB8:CAFE:2000::/52
  network 2001:DB8:CAFE:3000::/52
  network 2001:DB8:CAFE:4000::/52
  network 2001:DB8:CAFE:5000::/52
  network 2001:DB8:CAFE:6000::/52
  network 2001:DB8:CAFE:7000::/52
  network 2001:DB8:CAFE:8000::/52
  network 2001:DB8:CAFE:9000::/52
  network 2001:DB8:CAFE:A000::/52
  network 2001:DB8:CAFE:B000::/52
  network 2001:DB8:CAFE:C000::/52
  neighbor 2001:DB8:BCD::1 activate
  neighbor 2001:DB8:BCD::1 soft-reconfiguration inbound
 exit-address-family
```

Figura 45 Configuración BGP CPE Bk

En esta ocasión se anuncian las redes LAN que se propagaran a través de la red para que estas sean enrutadas hacia internet además de que tenga alcanzabilidad a otras sedes de la compañía.

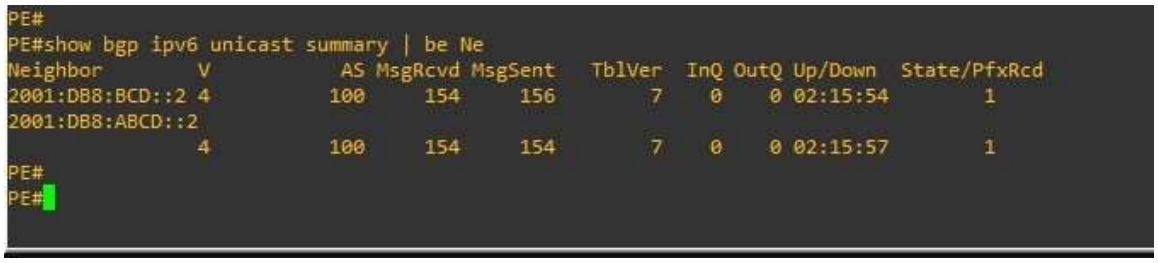


Figura 46 adyacencias BGP

Desde el PE se puede confirmar que se establecen las sesiones BGP con sus dos PEER, esto se puede identificar en la imagen anterior. Ahora se observará que el router PE este aprendiendo las redes anunciadas por los CPE:

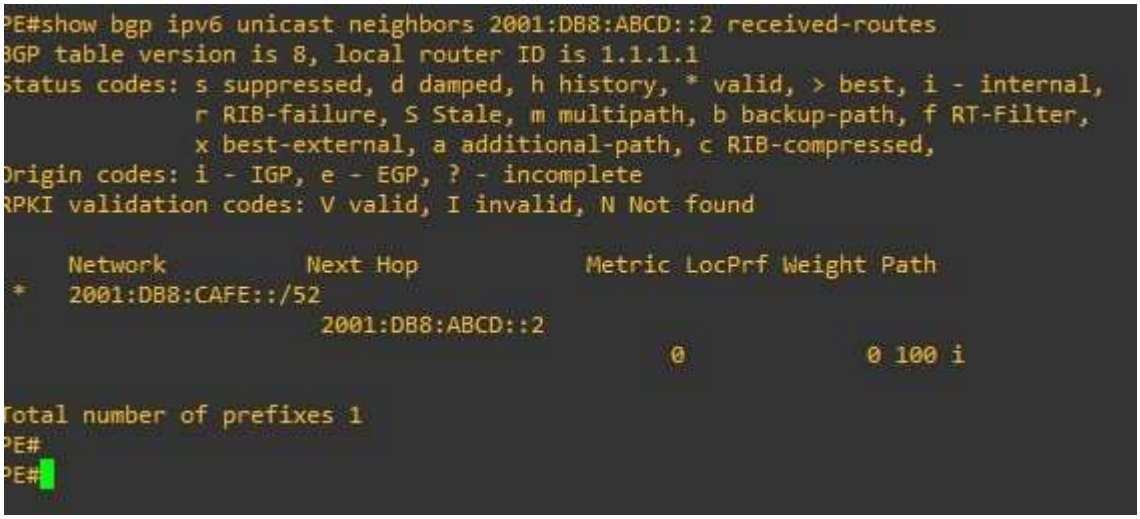


Figura 47 Rutas aprendidas por CPE Ppal

```
PE#show bgp ipv6 unicast neighbors 2001:DB8:BCD::2 received-routes
BGP table version is 8, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  2001:DB8:CAFE::/52
                      2001:DB8:BCD::2          0             0 100 i

Total number of prefixes 1
PE#
PE#
```

Figura 48 Rutas aprendidas por CPE Bk

Lo que se hará ahora, es la ejecución del HSRP para darle redundancia a los enlaces de datos, como se observó con anterioridad en la imagen de la configuración de las interfaces, esta implementación se ejecuta sobre los puertos LAN, y allí se le determina la prioridad más alta al router principal, por otro lado se coloca que la ip virtual del hsrp en ipv6 sea autoconfigurado, además de esto, se establece un track para que cada vez que se caiga la comunicación WAN el HSRP principal decremente y se active el otro canal de datos:

El track se asocia a un objeto, en este caso un IP SLA, el cual se configura inicialmente, de la siguiente manera:

```
ip sla 1
 icmp-echo 2001:DB8:ABCD::1 source-ip 2001:DB8:ABCD::2
 frequency 5
ip sla schedule 1 life forever start-time now
ip sla responder
```

Figura 49 Configuración IPSLA

Seguidamente se asocia el IP SLA al TRACK:

```
!
track 1 ip sla 1 reachability
!
```

Figura 50 Configuración TRACK 1

```
CPE_PPAL#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi1/0       1    120 P Active  local           FE80::2         FE80::5:73FF:FEA0:1
CPE_PPAL#
```

Figura 51 HSRP Ppal

A continuación, se iniciará el firewall y se configurará el parámetro del puerto WAN para que tenga comunicación con los CPE, para ello se debe habilitar la opción de IPv6 en el dispositivo:

Esto se hace en system – feature visibility – ipv6

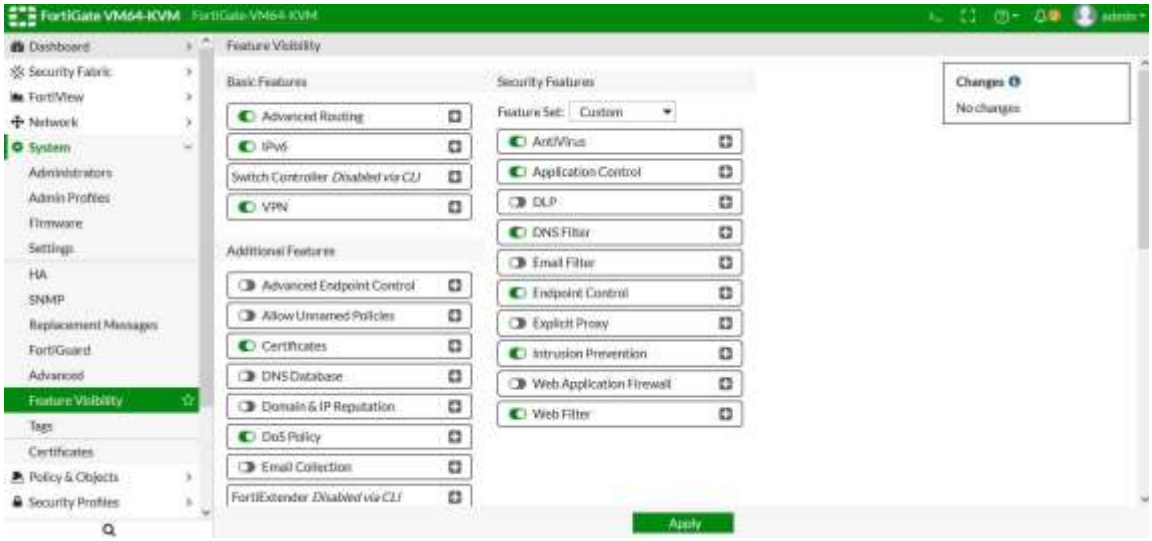


Figura 52 Habilitar IPv6 fw fortinet

Seguidamente, se configurará la interfaz del puerto 1 como WAN y se le asignara un direccionamiento IPV6 del segmento de red WAN anteriormente expuesto, así mismo se activará el puerto 10 para que a través de este se realice el management del equipo.

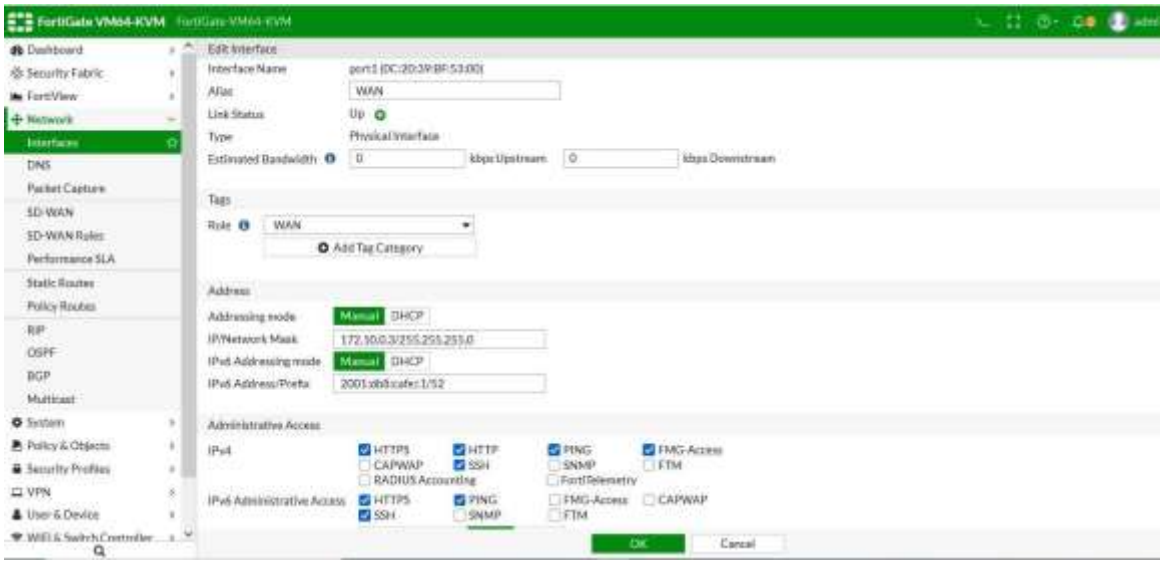


Figura 53 Configuración puerto Wan fw

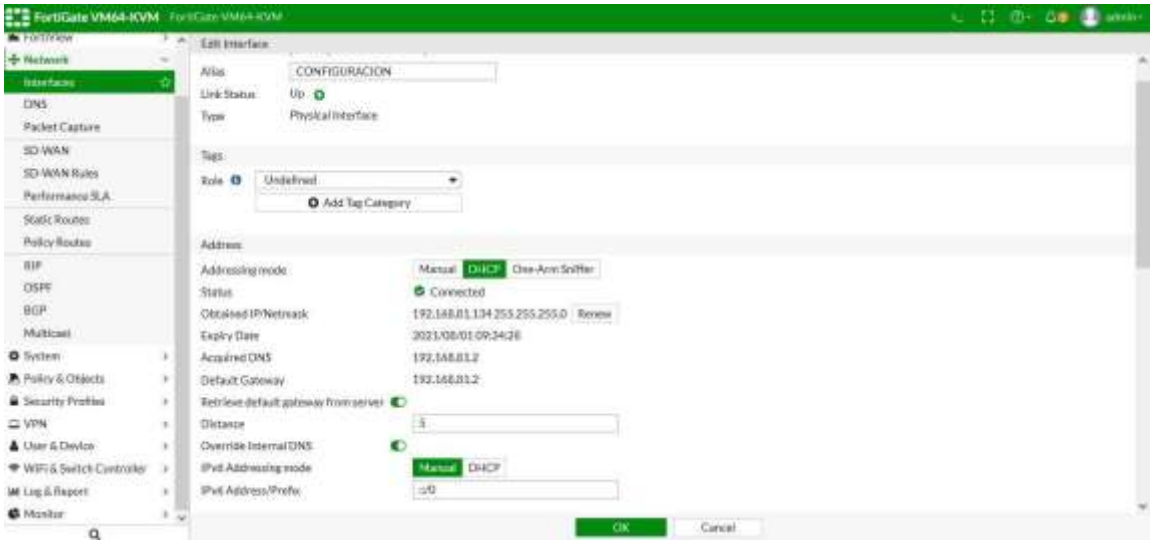


Figura 54 Configuración puerto Management fw

A continuación, se crearán las Vlan dentro del firewall y se le asignara la IP respectiva según la información de la fase anterior, además de esto se adicionarán en la sección addresses dentro del firewall, cada uno de los segmentos IPv6:

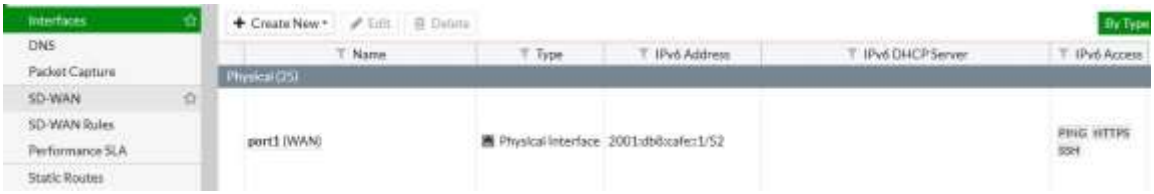


Figura 55 Interfaz Wan

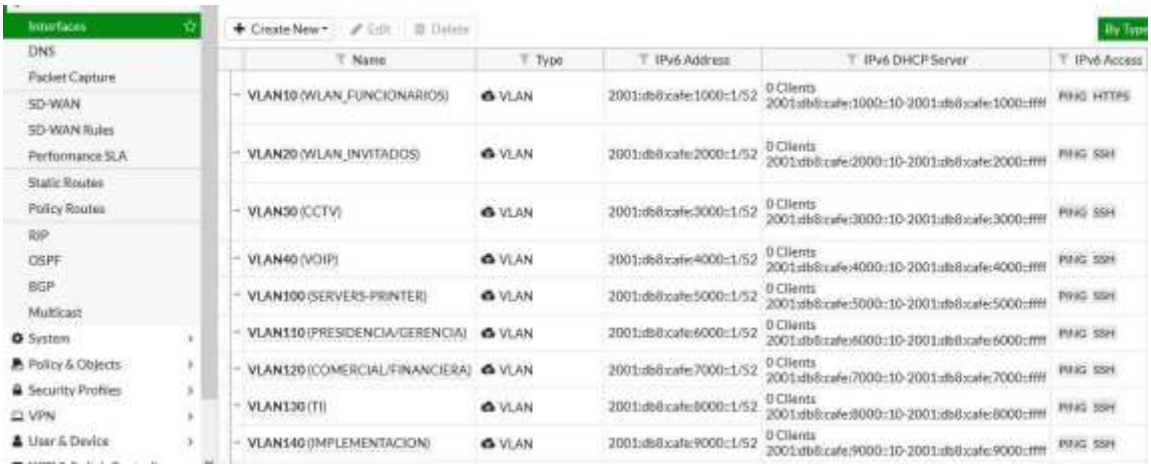


Figura 56 Interfaz Lan

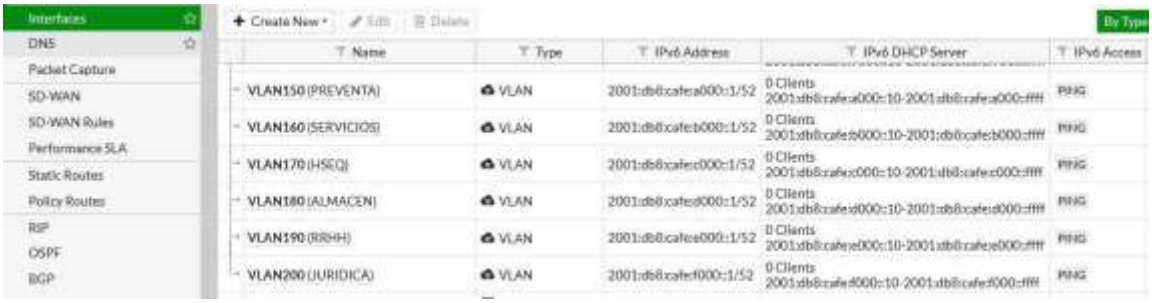


Figura 57 Interfaces Lan

Y como se mencionó, se agregan los segmentos:

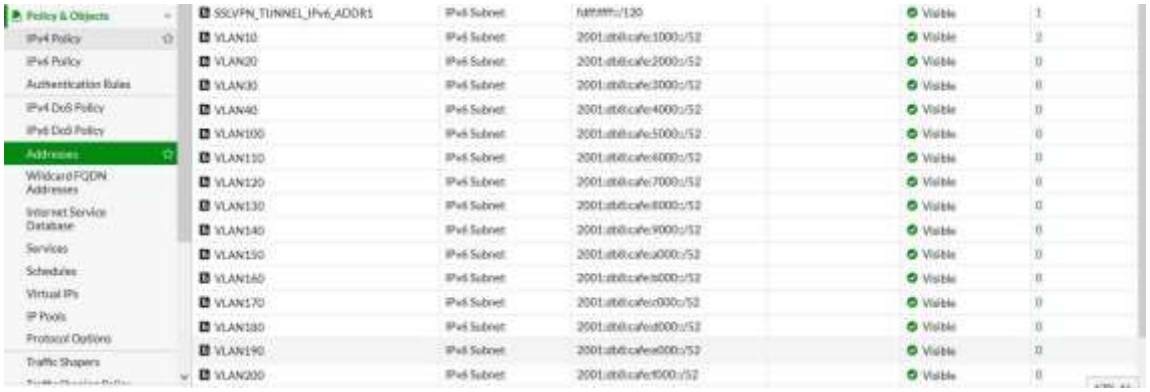


Figura 58 Segmentos ipv6

El siguiente paso es la creación de las políticas, se crearán unas políticas sencillas para las diferentes comunicaciones de las redes.

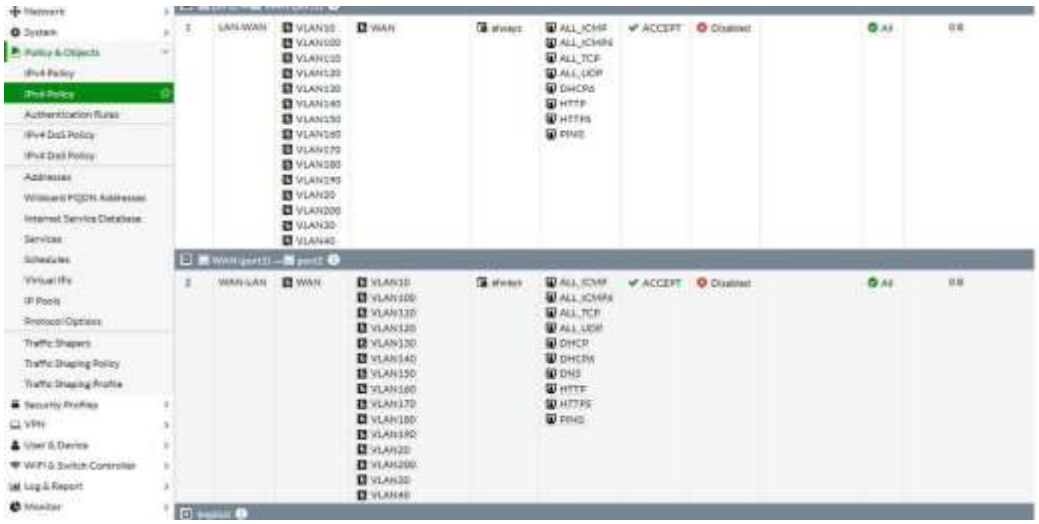


Figura 59 Politicas Lan-Wan, Wan-Lan

Con anterioridad se identificó que en la imagen de la visualización de las interfaces se posee la configuración del DHCP versión 6, no obstante, a continuación, se apreciara con más detalle la configuración de esta para cada uno de los segmentos LAN que se tienen involucrados en la topología:

Figura 60 Dhcp_1

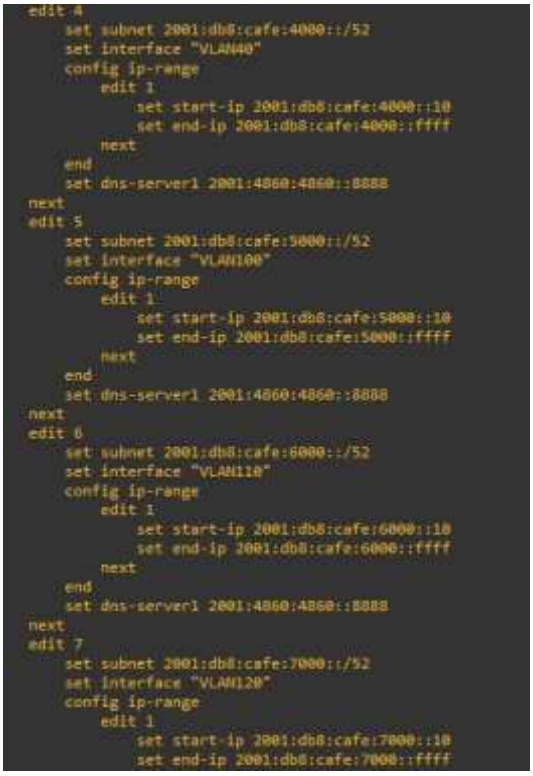


Figura 61 Dhcp_2

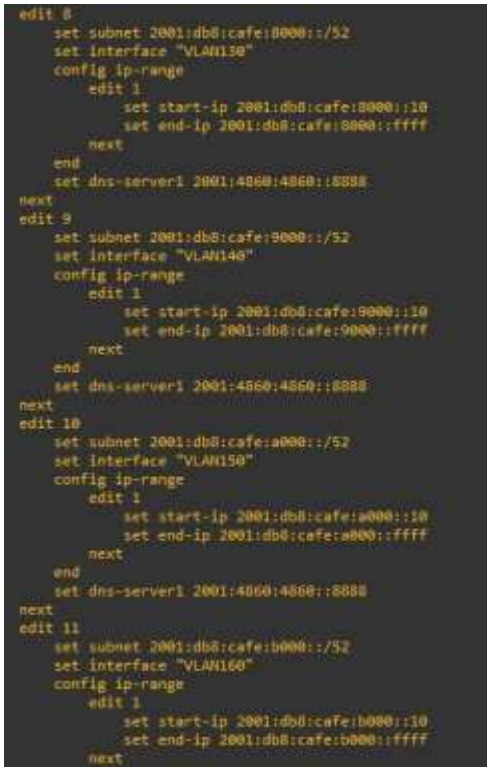


Figura 62 Dhcp_3

Figura 63 Dhcp_4

Con lo anterior, se establecen los parámetros más importantes para la transición de IPv4 a IPv6, lo siguiente en realizar es activar el protocolo en los demás servicios como VoIP, donde aquí se implementa el respectivo direccionamiento en los teléfonos IP y en la PBX. Por otro lado, para el servicio WIFI se activa el protocolo desde la controladora en la nube y se le asigna el correspondiente direccionamiento a los Access point, por temas de simulación y licenciamiento no es posible demostrar el funcionamiento de este tipo de servicios, no obstante, se resaltará a continuación donde se activa el protocolo IPV6 en la controladora de Huawei iNCE MASTER:

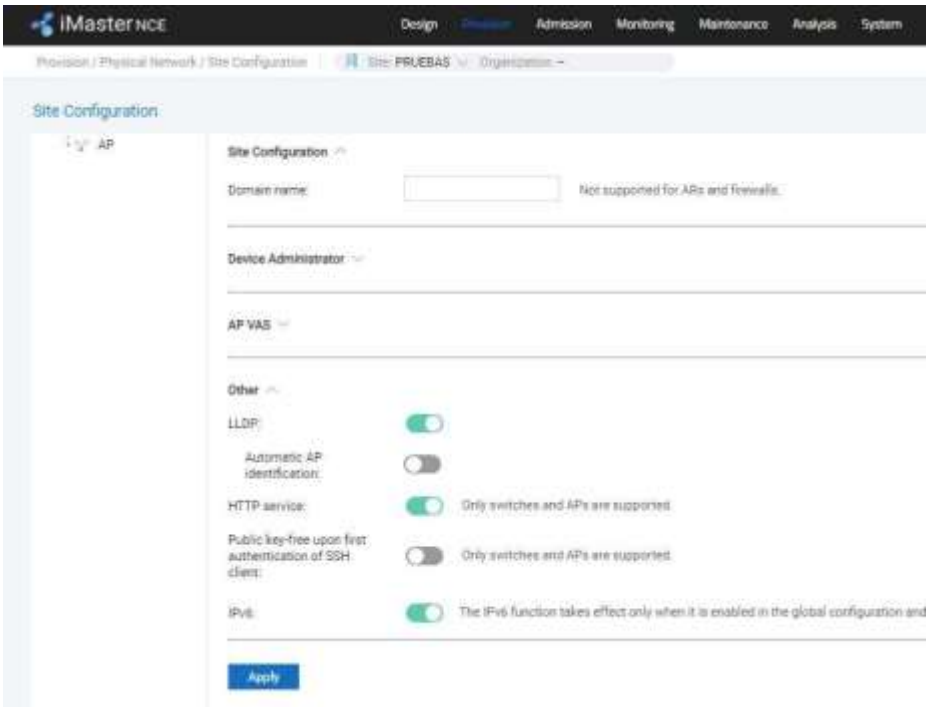


Figura 64 Activación IPv6 iNCE MASTER Huawei

Luego se adicionará el direccionamiento especifico a los diferentes AP en la red, para que estos posean la salida a internet por medio de IPv6.

Para el servicio de Impresoras, únicamente se les adiciona la IP a los dispositivos y se valida que se encuentren dentro del segmento de red IPv6 respectivo, como se evidencio con anterioridad.

Tratamiento similar hay que ejecutar para el servicio de CCTV, donde se le agregara una IP versión 6 a los NVR y consecuentemente a las diferentes cámaras instaladas.

Fase 4: Pruebas

Para la fase de pruebas se realizarán unos testing básicos para la identificación del funcionamiento del protocolo IPv6, estos se efectuarán de la siguiente manera.

1. Validación de conectividad entre los equipos de borde.

Se inicia realizando ping desde el PE a los dos CPE:

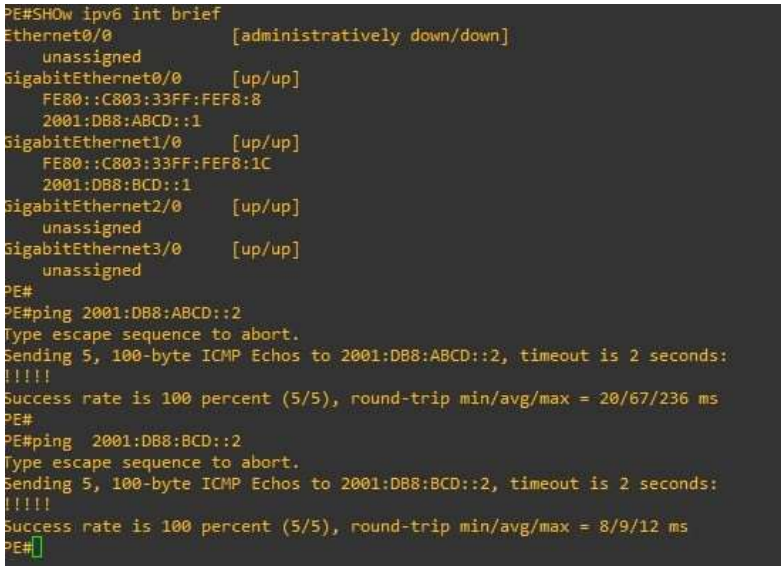


Figura 65 Ping CPE ppal y CPE bk desde PE

Seguidamente, se realiza una nueva prueba de ping, pero esta vez desde el FW a los CPE:

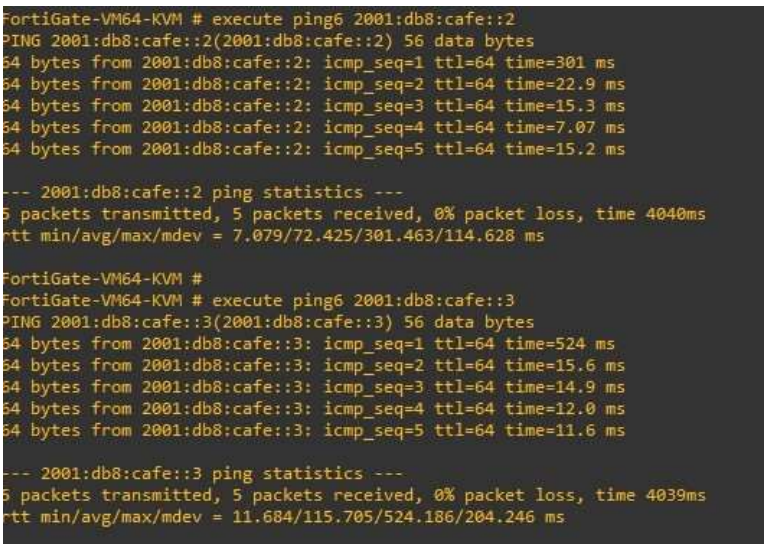


Figura 66 Ping CPE ppal y CPE bk desde FW

2. Revisión y comprobación del protocolo Dhcp.

Para este punto es de importancia resaltar que dado a que la validación se encuentra en un entorno de simulación, no es posible ejecutar stack con los switches por ende todas las interfaces que se desean validar no están disponibles, sin embargo, se probaran los diferentes servicios en cada uno de uno de los switches de los diferentes pisos de la compañía, con el fin de identificar que se propaguen las vlan a nivel lan y que además de esto se ejecuten las solicitudes DHCP adecuadamente, proporcionando el respectivo direccionamiento a las diferentes subredes.

I. Piso 3

A. Funcionarios

Primeramente, se evidencia la configuración del puerto VLAN10 del FW

```
edit "VLAN10"
    set vdom "root"
    set ip 192.168.10.1 255.255.255.0
    set allowaccess ping https ssh
    set alias "WLAN_FUNCIONARIOS"
    set device-identification enable
    set role lan
    set snmp-index 12
    config ipv6
        set ip6-address 2001:db8:cafe:1000::1/52
        set ip6-allowaccess ping https
        set ip6-send-adv enable
        set ip6-manage-flag enable
        set ip6-other-flag enable
        config ip6-prefix-list
            edit 2001:db8:cafe:1000::/52
            next
        end
    end
    set interface "port2"
    set vlanid 10
```

Figura 67 Config VLAN10 FW

A continuación, se observan en el SW de core y en el SW de acceso del piso 3 las MAC que aprende para la vlan 10

```
SW_CORE#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0c20.3963.330f    DYNAMIC     Gi0/3
  10    0c20.39af.f901    DYNAMIC     Gi0/0
  10    0c20.39ff.e200    DYNAMIC     Gi0/3
Total Mac Addresses for this criterion: 3
SW_CORE#
```

Figura 68 MAC aprendidas desde SW Core

```
SW_PISO_3#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    0c20.3906.f703    DYNAMIC     Gi3/3
  10    0c20.39af.f901    DYNAMIC     Gi3/3
  10    0c20.39ff.e200    DYNAMIC     Gi0/0
Total Mac Addresses for this criterion: 3
```

Figura 69 MAC aprendidas desde SW acceso piso 3

Como se aprecia con anterioridad, la MAC de la interfaz GIG 0/0 es la mac del pc conectado el cual deberá tomar una dirección IPV6 por medio de la vlan 10, es de recordar que el segmento de la VLAN 10 de funcionarios es: 2001:0db8:cafe:1000::/52:

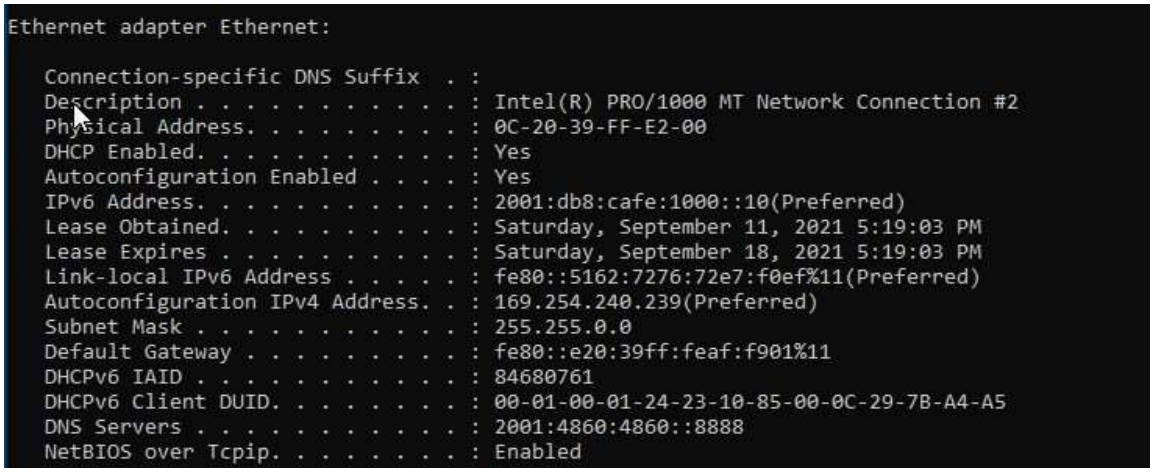


Figura 70 Direccionamiento Dhcp en PC VLAN10

Como se puede observar, toma el direccionamiento IPV6 respectivo para la VLAN 10, además de que obtiene los DNS configurados previamente. Igualmente podemos revisar por medio de NDP la comunicación entre el FW y el dispositivo:

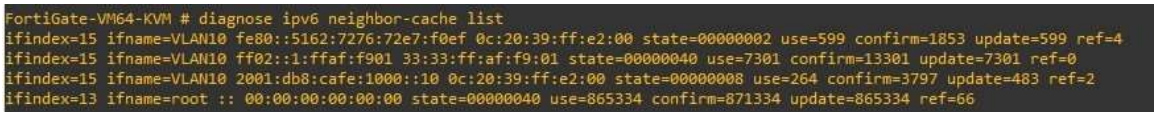


Figura 71 NDP desde FW

Con la demostración anterior, ahora se demostrará únicamente como se asigna el direccionamiento IP a los demás servicios y el NDP del FW:

B. Invitados

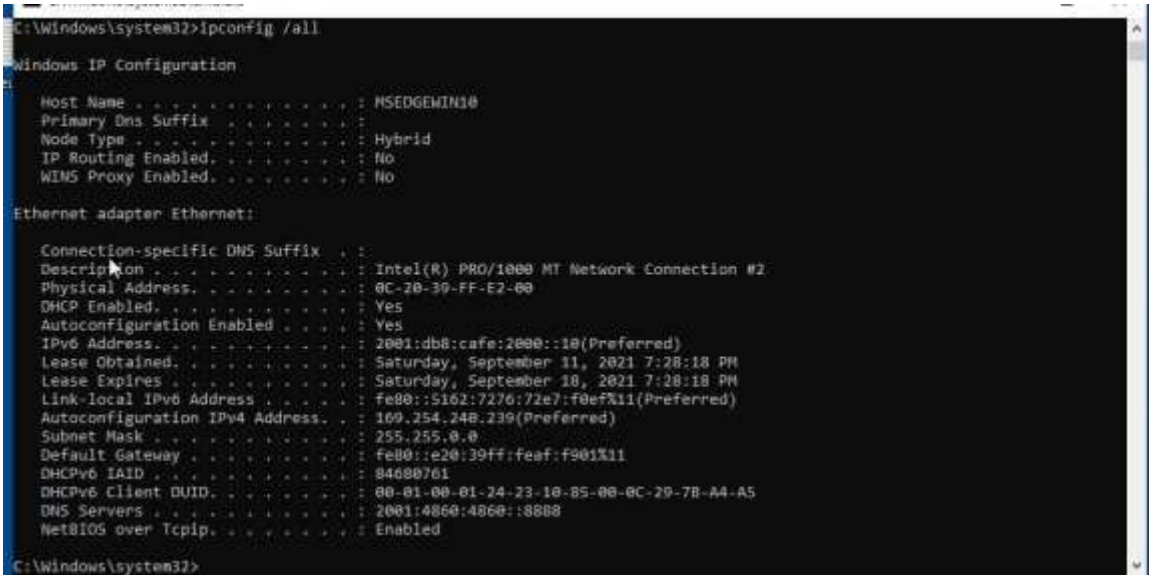


Figura 72 Direccionamiento Dhcp en PC VLAN20

```
FortiGate-VM64-KVM # diagnose ipv6 neighbor-cache list
ifindex=16 ifname=VLAN20 fe80::5162:7276:72e7:f0ef 0c:20:39:ff:e2:00 state=00000004 use=4199 confirm=4199 update=569 ref=0
ifindex=13 ifname=root :: 00:00:00:00:00:00 state=00000040 use=1116908 confirm=1122908 update=1116908 ref=66
ifindex=16 ifname=VLAN20 2001:db8:cafe:2000::10 0c:20:39:ff:e2:00 state=00000004 use=4367 confirm=5347 update=1721 ref=0
```

Figura 73 NDP desde FW

C. CCTV

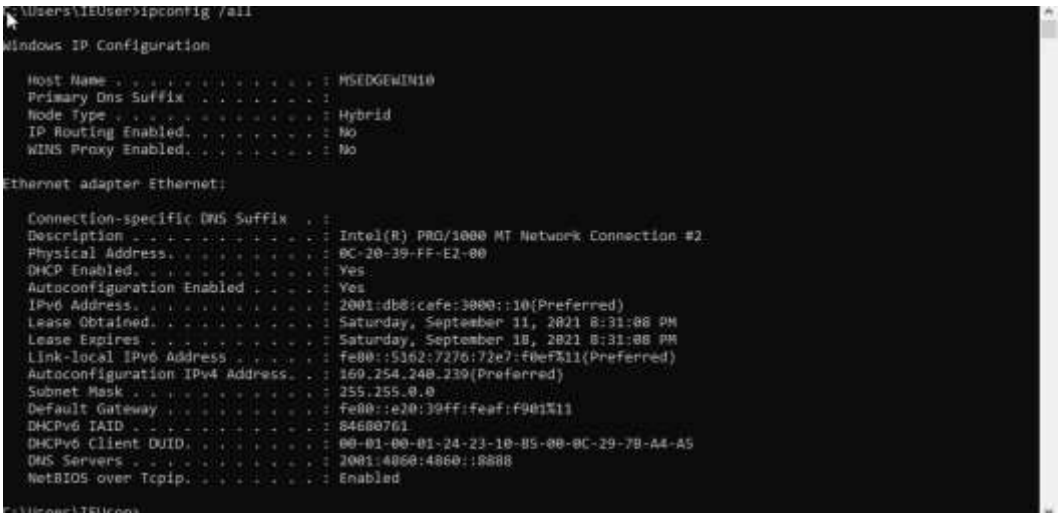


Figura 74 Direccionamiento Dhcp en PC VLAN30

```
FortiGate-VM64-KVM # diagnose ipv6 neighbor-cache list
ifindex=13 ifname=root :: 00:00:00:00:00:00 state=00000040 use=81276 confirm=87276 update=81276 ref=66
ifindex=17 ifname=VLAN30 2001:db8:cafe:3000::10 0c:20:39:ff:e2:00 state=00000002 use=541 confirm=540 update=540 ref=3
ifindex=17 ifname=VLAN30 fe80::5162:7276:72e7:f0ef 0c:20:39:ff:e2:00 state=00000002 use=2051 confirm=2048 update=2048 ref=3
ifindex=18 ifname=VLAN40 ff02::1 33:33:00:00:00:01 state=00000040 use=2629 confirm=8629 update=2629 ref=1
ifindex=18 ifname=VLAN40 fe80::e20:39ff:feaf:f901 0c:20:39:af:f9:01 state=00000004 use=2629 confirm=8629 update=2629 ref=0
```

Figura 75 NDP desde FW

D. VoIP

```
Command Prompt
C:\Users\IEUser>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : MSEDGEWIN10
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection #2
   Physical Address. . . . . . . . . : 0C-20-39-FF-E2-00
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:db8:cafe:4000::10(Preferred)
   Lease Obtained. . . . . . . . . . : Monday, September 13, 2021 1:21:46 PM
   Lease Expires . . . . . . . . . . : Monday, September 20, 2021 1:21:46 PM
   Link-local IPv6 Address . . . . . : fe80::5162:7276:72e7:f0ef%11(Preferred)
   Autoconfiguration IPv4 Address. . : 169.254.240.239(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::e20:39ff:feaf:f901%11
   DHCPv6 IAID . . . . . . . . . . . : 84680761
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-23-10-85-00-0C-29-7B-A4-A5
   DNS Servers . . . . . . . . . . . : 2001:4860:4860::8888
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\IEUser>
```

Figura 76 Direccionamiento Dhcp en PC VLAN40

```
FortiGate-VM64-KVM # diag ipv6 nei list
ifindex=13 ifname=root :: 00:00:00:00:00:00 state=00000040 use=146164 confirm=152164 update=146164 ref=66
ifindex=18 ifname=VLAN40 fe80::5162:7276:72e7:f0ef 0c:20:39:ff:e2:00 state=00000008 use=101 confirm=6382 update=101 ref=2
ifindex=18 ifname=VLAN40 2001:db8:cafe:4000::10 0c:20:39:ff:e2:00 state=00000002 use=71 confirm=70 update=70 ref=3

FortiGate-VM64-KVM #
```

Figura 77 NDP desde FW

E. Servers/Printer

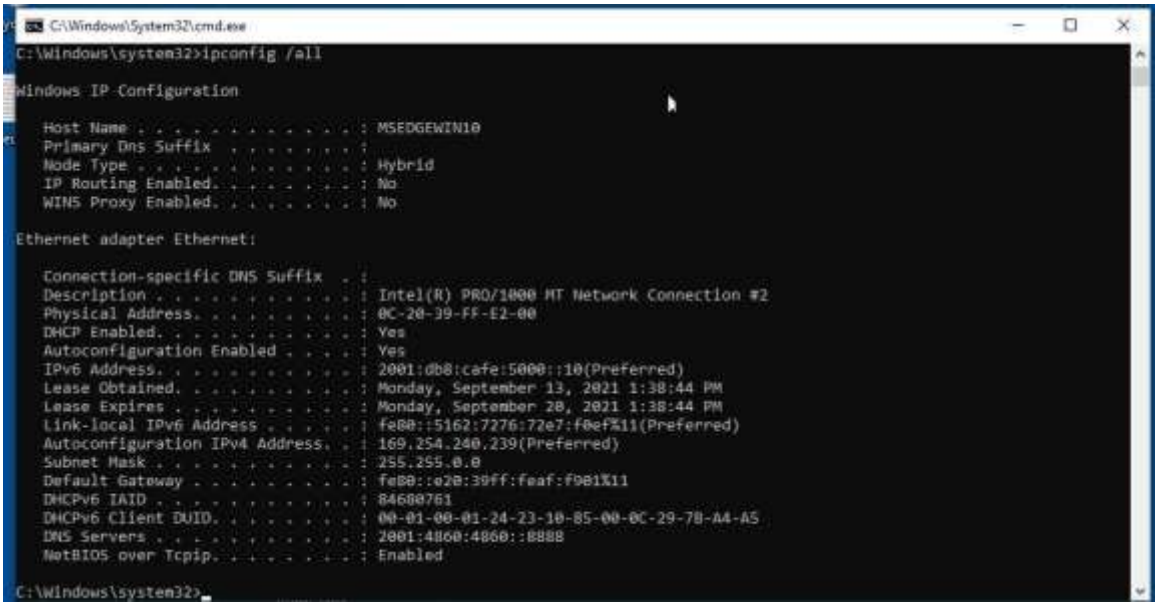


Figura 78 Direccionamiento Dhcp en PC VLAN100

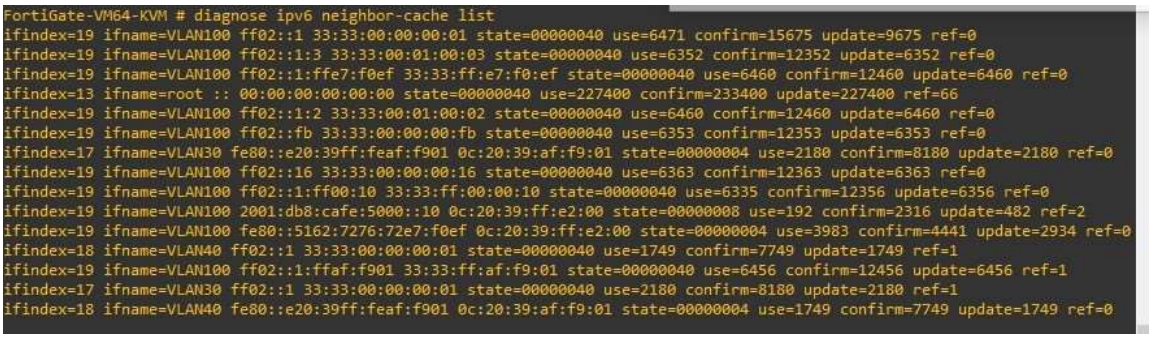


Figura 79 NDP desde FW

F. Presidencia/Gerencia

Figura 80 Direccionamiento Dhcp en PC VLAN110

```
FortiGate-VM64-KVM #
FortiGate-VM64-KVM # diagnose ipv6 neighbor-cache list
ifindex=13 ifname=root :: 00:00:00:00:00:00 state=00000040 use=261944 confirm=267944 update=261944 ref=66
ifindex=17 ifname=VLAN30 fe80::e20:39ff:feaf:f901 0c:20:39:af:f9:01 state=00000004 use=3122 confirm=9122 update=3122 ref=0
ifindex=17 ifname=VLAN30 ff02::1 33:33:00:00:00:01 state=00000040 use=3122 confirm=9122 update=3122 ref=0
```

Figura 81 NDP desde FW

G. Comercial/Financiera

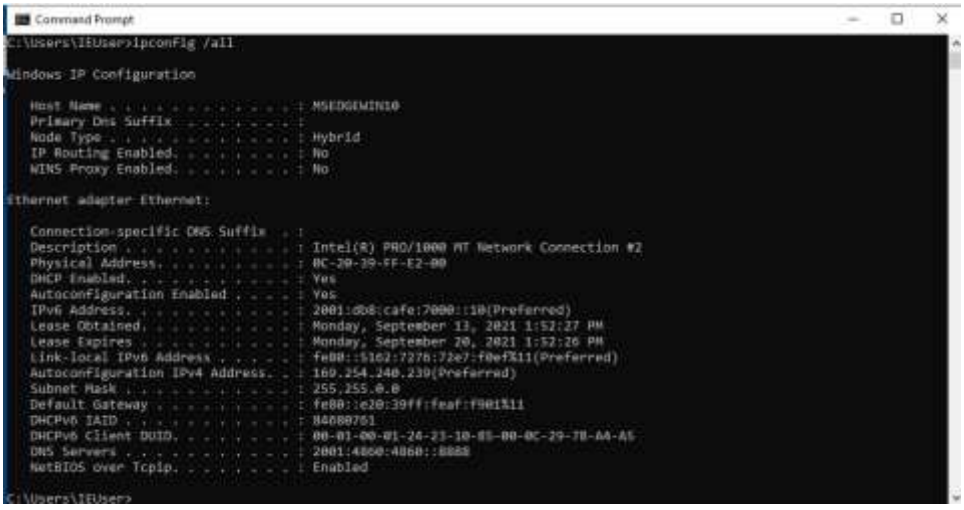


Figura 82 Direccionamiento Dhcp en PC VLAN120

```
FortiGate-VM64-KVM # diagnose ipv6 neighbor-cache list
ifindex=13 ifname=root :: 00:00:00:00:00:00 state=00000040 use=319543 confirm=325543 update=319543 ref=66
ifindex=21 ifname=VLAN120 fe80::5162:7276:72e7:f0ef 0c:20:39:ff:e2:00 state=00000008 use=271 confirm=3970 update=271 ref=2
ifindex=20 ifname=VLAN110 ff02::1 33:33:00:00:00:01 state=00000040 use=648 confirm=6648 update=648 ref=1
ifindex=21 ifname=VLAN120 2001:db8:cafe:7000::10 0c:20:39:ff:e2:00 state=00000002 use=740 confirm=1736 update=1736 ref=2
ifindex=20 ifname=VLAN110 fe80::e20:39ff:feaf:f901 0c:20:39:af:f9:01 state=00000004 use=648 confirm=6648 update=648 ref=0
```

Figura 83 NDP desde FW

H. TI

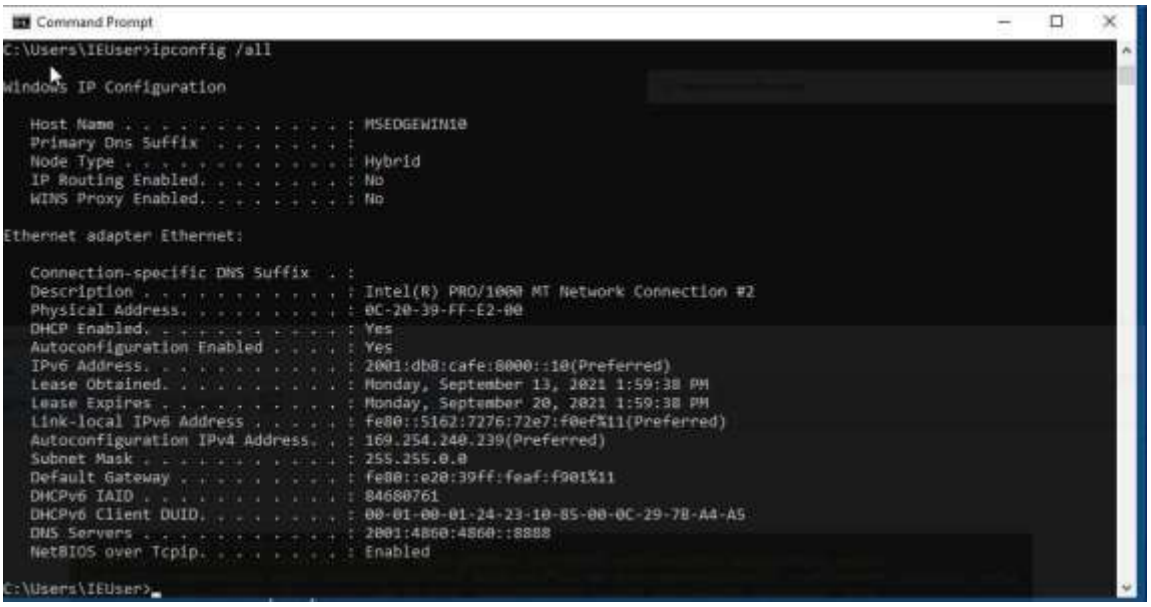


Figura 84 Direccionamiento Dhcp en PC VLAN130

```
FortiGate-VM64-KVM # diagnose ipv6 nei lis
ifindex=13 ifname=root :: 00:00:00:00:00:00 state=00000040 use=346618 confirm=352618 update=346618 ref=66
ifindex=22 ifname=VLAN130 ff02::1:ff00:10 33:33:ff:00:00:10 state=00000040 use=5027 confirm=11265 update=5265 ref=1
ifindex=22 ifname=VLAN130 ff02::1:3 33:33:00:01:00:03 state=00000040 use=5252 confirm=11252 update=5252 ref=1
ifindex=22 ifname=VLAN130 ff02::1:2 33:33:00:01:00:02 state=00000040 use=5260 confirm=11260 update=5260 ref=1
ifindex=22 ifname=VLAN130 2001:db8:cafe:8000::10 0c:20:39:ff:e2:00 state=00000002 use=697 confirm=1050 update=1050 ref=3
ifindex=22 ifname=VLAN130 ff02::fb 33:33:00:00:00:fb state=00000040 use=5253 confirm=11253 update=5253 ref=1
ifindex=22 ifname=VLAN130 ff02::16 33:33:00:00:00:16 state=00000040 use=5263 confirm=11263 update=5263 ref=1
ifindex=22 ifname=VLAN130 fe80::5162:7276:72e7:f0ef 0c:20:39:ff:e2:00 state=00000002 use=795 confirm=795 update=795 ref=4
ifindex=22 ifname=VLAN130 ff02::1:ffaf:f901 33:33:ff:af:f9:01 state=00000040 use=5268 confirm=11268 update=5268 ref=1
ifindex=22 ifname=VLAN130 ff02::1 33:33:00:00:00:01 state=00000040 use=5258 confirm=11258 update=5258 ref=1
ifindex=22 ifname=VLAN130 ff02::2 33:33:00:00:00:02 state=00000040 use=5264 confirm=11264 update=5264 ref=0
ifindex=22 ifname=VLAN130 ff02::1:ffe7:f0ef 33:33:ff:e7:f0:ef state=00000040 use=5265 confirm=11265 update=5265 ref=0
```

Figura 85 NDP desde FW

I. Implementación

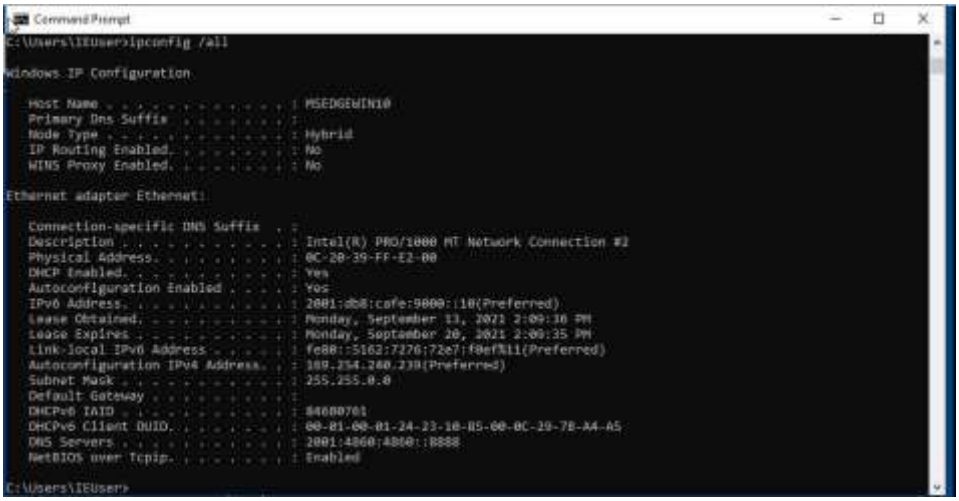


Figura 86 Direccionamiento Dhcp en PC VLAN140

```
FortiGate-VM64-KVM # diagnose ipv6 nei lis
ifindex=13 ifname=root :: 00:00:00:00:00:00 state=00000040 use=414181 confirm=420181 update=414181 ref=66
ifindex=22 ifname=VLAN130 fe80::e20:39ff:feaf:f901 0c:20:39:af:f9:01 state=00000004 use=2756 confirm=8756 update=2756 ref=0
ifindex=22 ifname=VLAN130 ff02::1 33:33:00:00:00:01 state=00000040 use=2756 confirm=8756 update=2756 ref=1

FortiGate-VM64-KVM #
```

Figura 87 NDP desde FW

J. Preventa

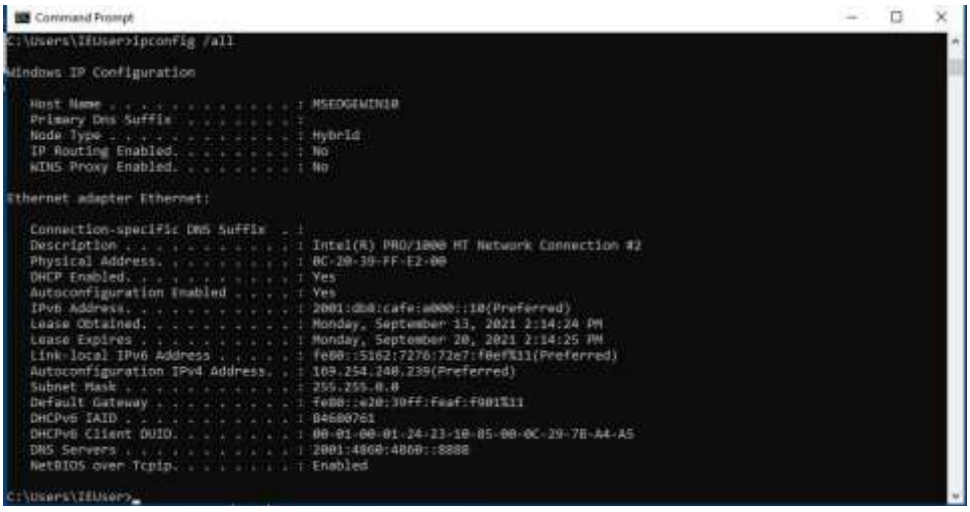


Figura 88 Direccionamiento Dhcp en PC VLAN150

```
FortiGate-VM64-KVM # diagnose ipv6 neig lis
ifindex=13 ifname=root :: 00:00:00:00:00:00 state=00000040 use=446396 confirm=452396 update=446396 ref=66
ifindex=22 ifname=VLAN130 fe80::e20:39ff:feaf:f901 0c:20:39:af:f9:01 state=00000004 use=5870 confirm=11870 update=5870 ref=0
ifindex=24 ifname=VLAN150 2001:db8:cafe:a000::10 0c:20:39:ff:e2:00 state=00000004 use=5531 confirm=7107 update=4162 ref=0
ifindex=22 ifname=VLAN130 ff02::1 33:33:00:00:00:01 state=00000040 use=5870 confirm=11870 update=5870 ref=0
ifindex=16 ifname=VLAN20 fe80::e20:39ff:feaf:f901 0c:20:39:af:f9:01 state=00000004 use=4772 confirm=10772 update=4772 ref=0
ifindex=16 ifname=VLAN20 ff02::1 33:33:00:00:00:01 state=00000040 use=4772 confirm=10772 update=4772 ref=1
```

Figura 89 NDP desde FW

K. Servicios

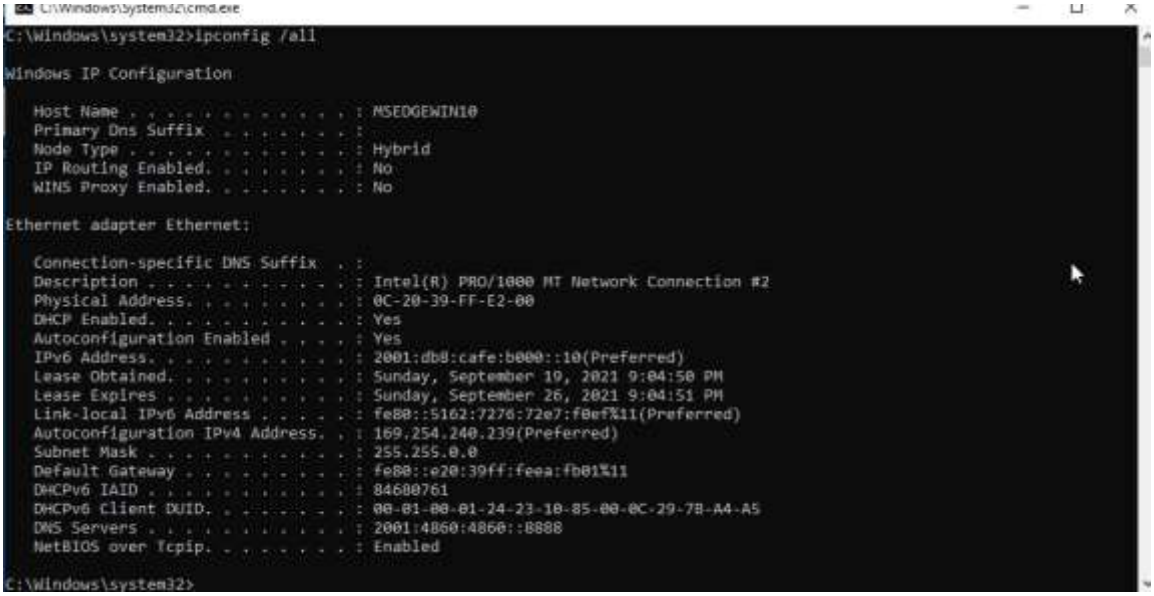


Figura 90 Direccionamiento Dhcp en PC VLAN160

```
FortiGate-VM64-KVM # diagnose ipv6 neighbor-cache list
ifindex=21 ifname=VLAN120 fe80::e20:39ff:feea:fb01 0c:20:39:ea:fb:01 state=00000004 use=4193 confirm=10193 update=4193 ref=0
ifindex=24 ifname=VLAN150 fe80::e20:39ff:feea:fb01 0c:20:39:ea:fb:01 state=00000004 use=4090 confirm=10090 update=4090 ref=0
ifindex=25 ifname=VLAN160 2001:db8:cafe:b000::10 0c:20:39:ff:e2:00 state=00000002 use=56 confirm=1637 update=1637 ref=2
ifindex=13 ifname=root :: 00:00:00:00:00:00 state=00000040 use=149569 confirm=155569 update=149569 ref=66
ifindex=25 ifname=VLAN160 fe80::5162:7276:72e7:f0ef 0c:20:39:ff:e2:00 state=00000002 use=1213 confirm=1209 update=1209 ref=2
ifindex=24 ifname=VLAN150 ff02::1 33:33:00:00:00:01 state=00000040 use=4090 confirm=10090 update=4090 ref=1
ifindex=21 ifname=VLAN120 ff02::1 33:33:00:00:00:01 state=00000040 use=4193 confirm=10193 update=4193 ref=1
```

Figura 91 NDP desde FW

L. HSEQ

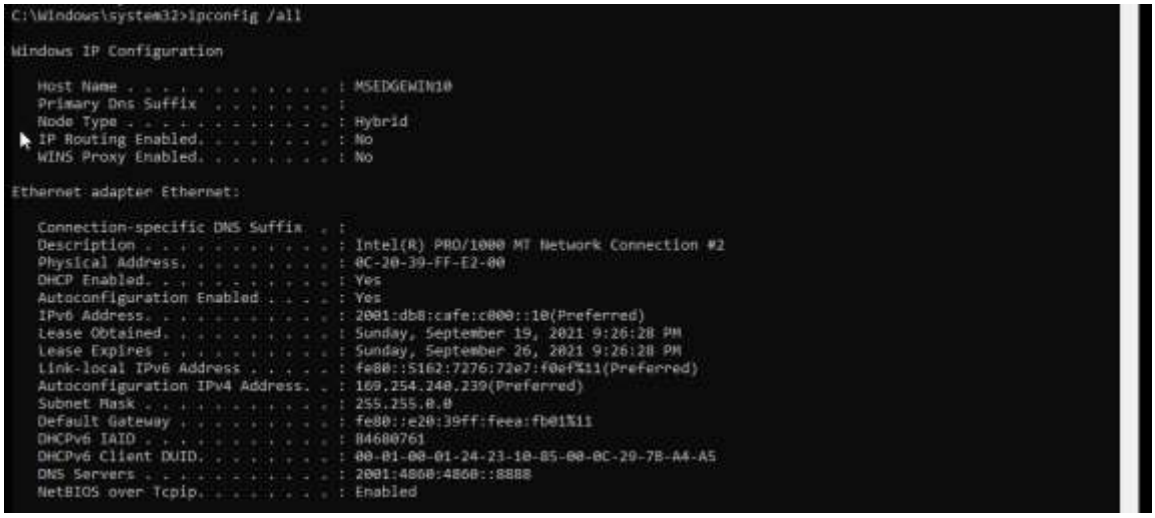


Figura 92 Direccionamiento Dhcp en PC VLAN170

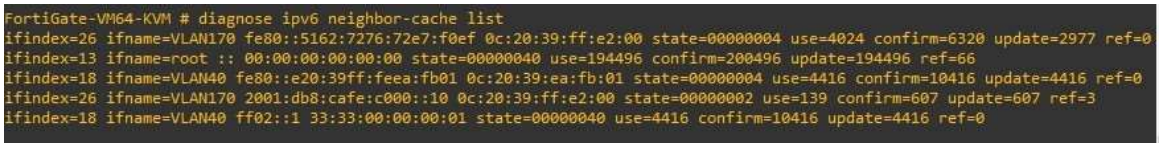


Figura 93 NDP desde FW

M. Almacén

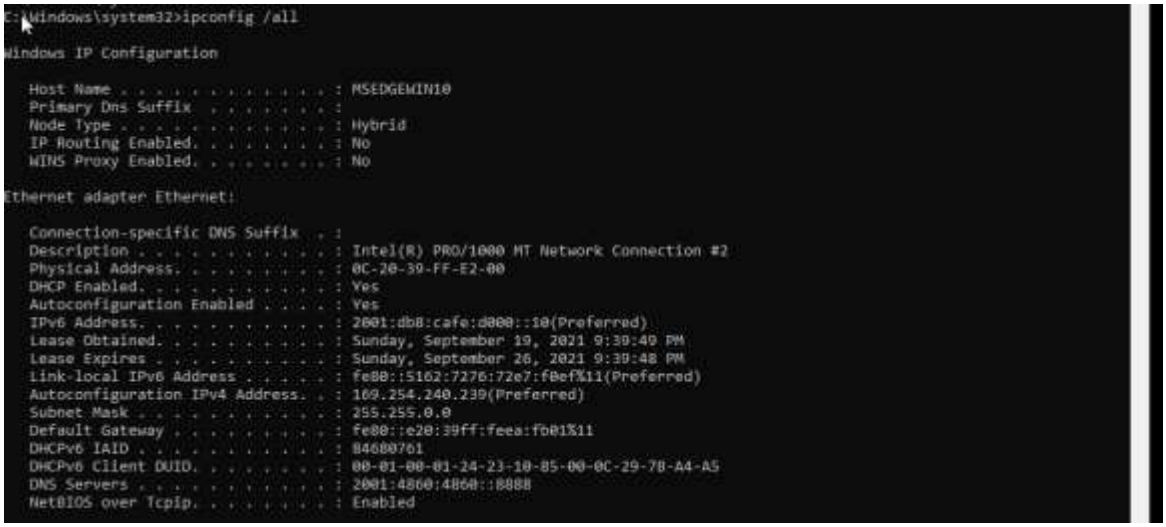


Figura 94 Direccionamiento DHCP en PC VLAN180

```
FortiGate-VM64-KVM # diag ipv6 neig list
ifindex=13 ifname=root :: 00:00:00:00:00:00 state=00000040 use=274988 confirm=280988 update=274988 ref=66
ifindex=27 ifname=VLAN180 fe80::5162:7276:72e7:f0ef 0c:20:39:ff:e2:00 state=00000004 use=5379 confirm=5379 update=2501 ref=0
ifindex=17 ifname=VLAN30 ff02::1 33:33:00:00:00:01 state=00000040 use=2408 confirm=8408 update=2408 ref=1
ifindex=17 ifname=VLAN30 fe80::e20:39ff:feea:fb01 0c:20:39:ea:fb:01 state=00000004 use=2408 confirm=8408 update=2408 ref=0
ifindex=22 ifname=VLAN130 ff02::1 33:33:00:00:00:01 state=00000040 use=3710 confirm=9710 update=3710 ref=1
ifindex=22 ifname=VLAN130 fe80::e20:39ff:feea:fb01 0c:20:39:ea:fb:01 state=00000004 use=3710 confirm=9710 update=3710 ref=0
ifindex=27 ifname=VLAN180 2001:db8:cafe:d000::10 0c:20:39:ff:e2:00 state=00000004 use=5339 confirm=5636 update=2757 ref=1
```

Figura 95 NDP desde FW

N. Talento Humano

```
C:\Windows\system32>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : MSEDGEWIN10
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection #2
   Physical Address. . . . . . . . . : 0C-20-39-FF-E2-00
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:db8:cafe:e000::10(Preferred)
   Lease Obtained. . . . . . . . . . : Sunday, September 19, 2021 9:45:31 PM
   Lease Expires . . . . . . . . . . : Sunday, September 26, 2021 9:45:31 PM
   Link-local IPv6 Address . . . . . : fe80::5162:7276:72e7:f0ef%11(Preferred)
   Autoconfiguration IPv4 Address. . : 169.254.240.239(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 84680761
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-23-10-85-00-0C-29-7B-A4-A5
   DNS Servers . . . . . . . . . . . : 2001:4860:4860::8888
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Figura 96 Direccionamiento Dhcp en PC VLAN190

```
FortiGate-VM64-KVM # diagnose ipv6 neig list
ifindex=28 ifname=VLAN190 fe80::5162:7276:72e7:f0ef 0c:20:39:ff:e2:00 state=00000004 use=4564 confirm=4564 update=2721 ref=0
ifindex=25 ifname=VLAN160 ff02::1 33:33:00:00:00:01 state=00000040 use=292 confirm=6292 update=292 ref=1
ifindex=28 ifname=VLAN190 2001:db8:cafe:e000::10 0c:20:39:ff:e2:00 state=00000004 use=4748 confirm=5331 update=3489 ref=1
ifindex=13 ifname=root :: 00:00:00:00:00:00 state=00000040 use=173217 confirm=173217 update=488576 ref=66
ifindex=16 ifname=VLAN20 ff02::1 33:33:00:00:00:01 state=00000040 use=4691 confirm=10691 update=4691 ref=1
ifindex=16 ifname=VLAN20 fe80::e20:39ff:feea:fb01 0c:20:39:ea:fb:01 state=00000004 use=4691 confirm=10691 update=4691 ref=0
ifindex=25 ifname=VLAN160 fe80::e20:39ff:feea:fb01 0c:20:39:ea:fb:01 state=00000004 use=292 confirm=6292 update=292 ref=0
```

Figura 97 NDP desde FW

O. Área Jurídica

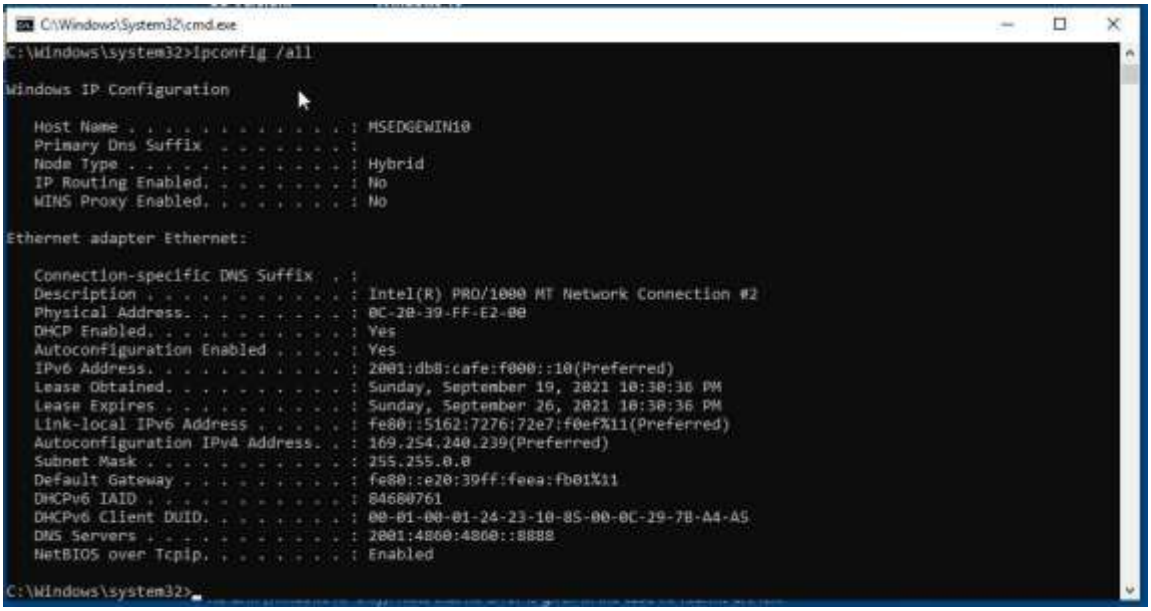


Figura 98 Direccionamiento Dhcp en PC VLAN200

Figura 99 NDP desde FW

Con la información anterior se identifica que para el piso 3, en todas las subredes IPV6 se obtiene el correcto direccionamiento en los terminales, sin embargo, en el presente trabajo no se mostrara toda la configuración para los demás pisos, ya que esta es igual que la ya mencionada, únicamente se debe hacer modificaciones de capa 2 en los equipos de acceso para propagar las Vlan correspondientes.

3. Verificación de enrutamiento, revisión de rutas anunciadas y aprendidas.

El firewall fortinate posee dos rutas estáticas apuntando a los dos CPE donde se le tiene modificada una distancia administrativa mayor a la por defecto a la ruta Backup con fines de redundancia, la cual permite que todos los segmentos de red IPV6 se anuncien a ambos CPE:

```
FortiGate-VM64-KVM # show router static6 1
 <Enter>

FortiGate-VM64-KVM # show router static6 1
config router static6
    edit 1
        set gateway 2001:db8:cafe::2
        set device "port1"
    next
end

FortiGate-VM64-KVM #
FortiGate-VM64-KVM # show router static6 2
config router static6
    edit 2
        set gateway 2001:db8:cafe::3
        set device "port1"
        set distance 30
    next
end
```

Figura 100 ruta estática FW Fortinet

Con esto, podemos revisar las redes anunciadas desde el CPE y las redes aprendidas por el PE cuando el servicio de la entidad funciona por su canal PPAL

I. Redes anunciadas CPE

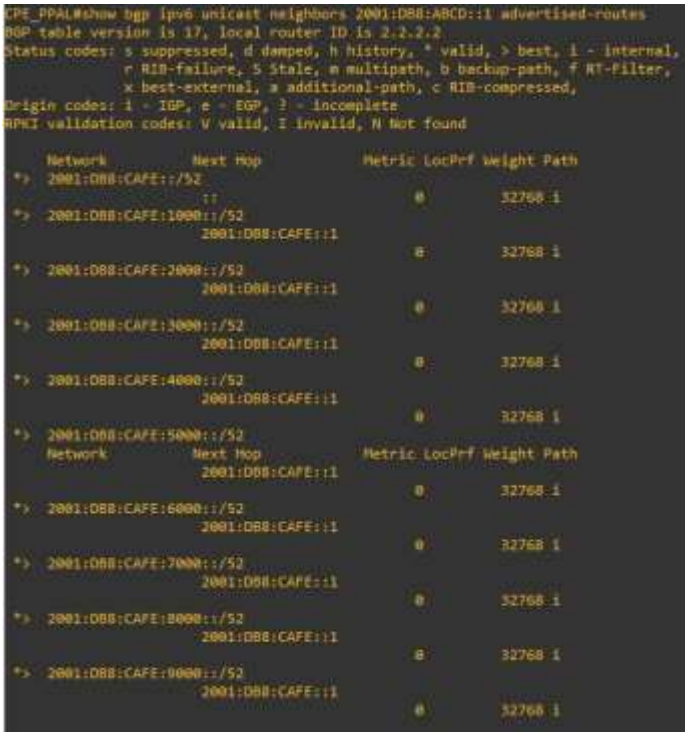


Figura 101 redes anunciadas CPE ppal

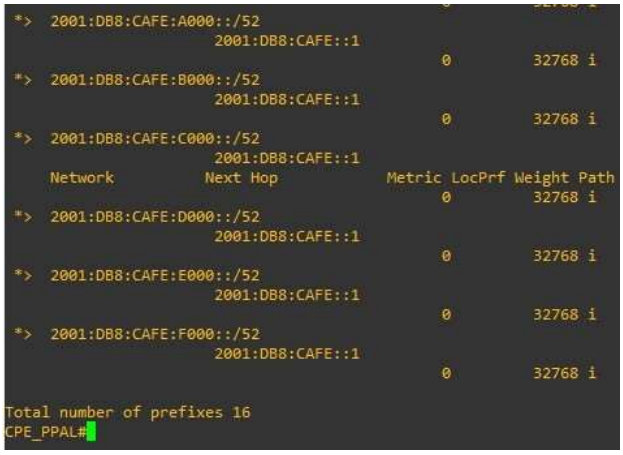


Figura 102 redes anunciadas CPE ppal

II. Redes aprendidas PE

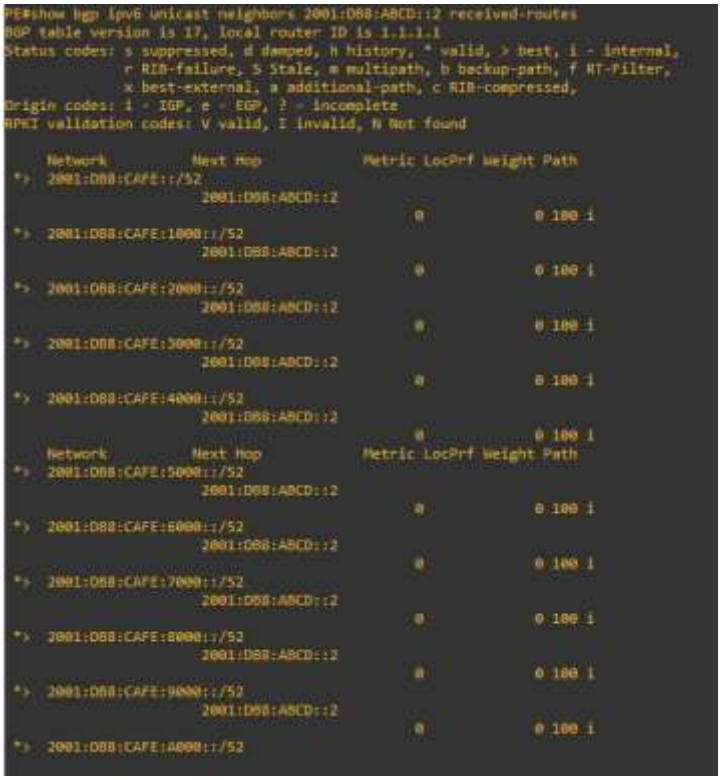


Figura 103 redes aprendidas PE desde CPE ppal

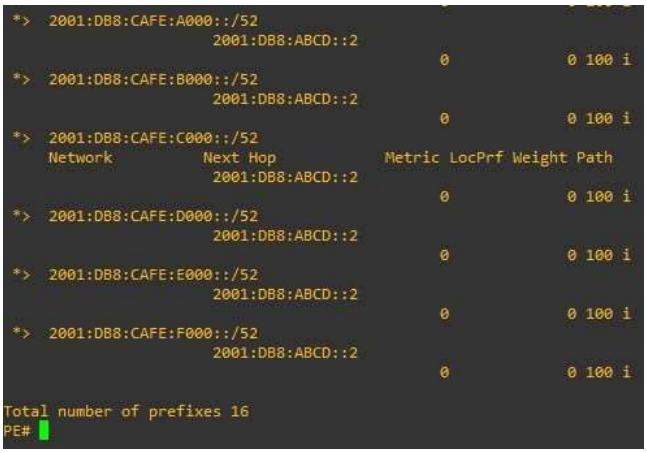


Figura 104 redes aprendidas PE desde CPE ppal

Ahora si utilizamos únicamente el enlace backup, también podremos ver las redes anunciadas y aprendidas

III. Redes anunciadas CPE bk

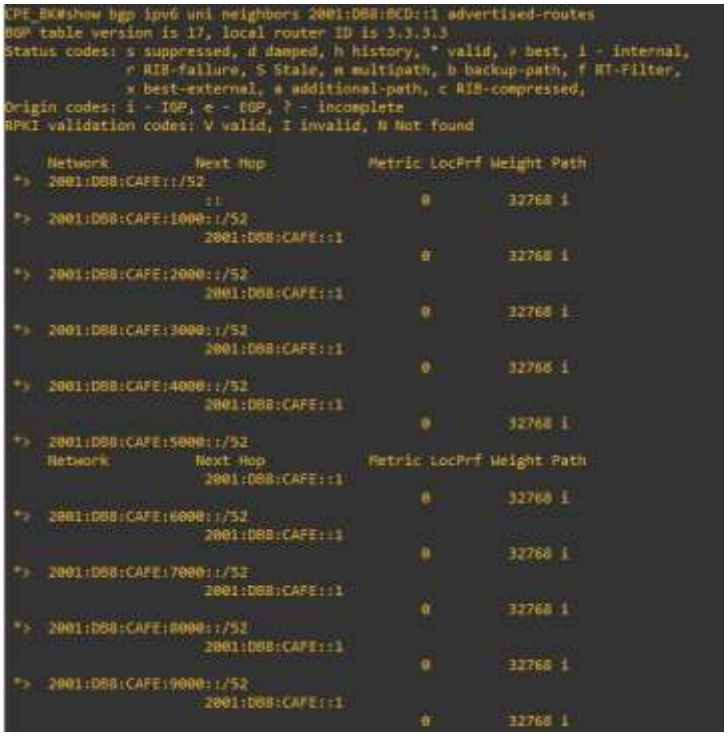


Figura 105 redes anunciadas CPE bk

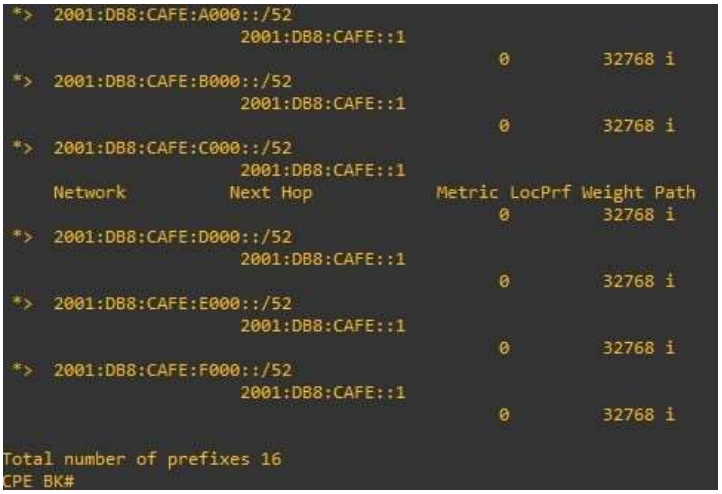
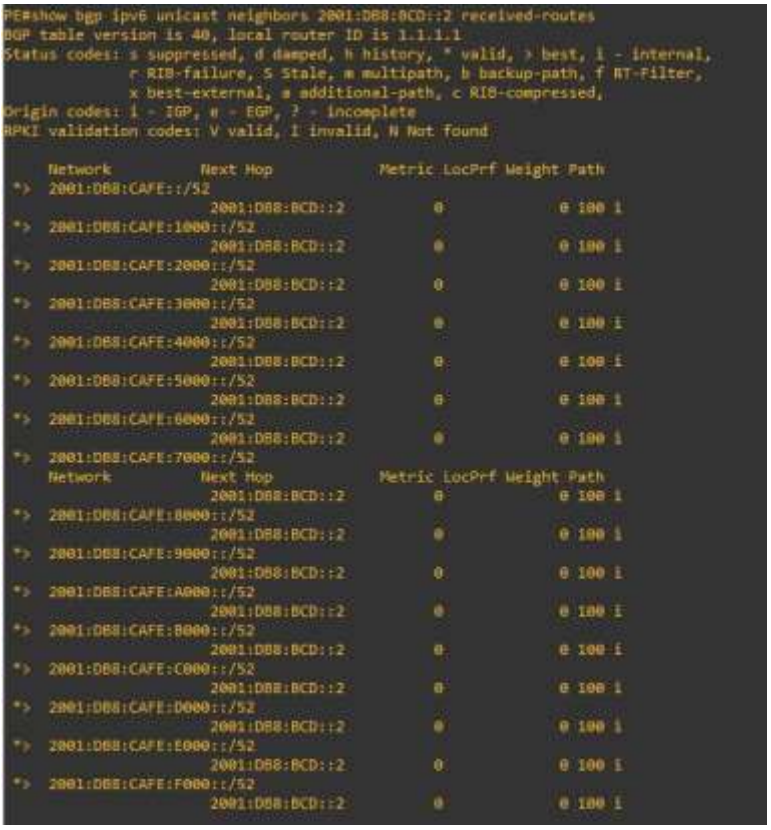


Figura 106 redes anunciadas CPE bk

IV. Redes aprendidas PE



```
PE#show bgp ipv6 unicast neighbors 2001:DB8:0CD::2 received-routes
BGP table version is 40, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  2001:DB8:CAFE::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:1000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:2000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:3000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:4000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:5000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:6000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:7000::/52
     Network          Next Hop            Metric LocPrf Weight Path
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:8000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:9000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:A000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:B000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:C000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:D000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:E000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:F000::/52
                      2001:DB8:BCD::2          0             0 100 i
```

Figura 107 redes aprendidas PE desde CPE bk

4. Prueba de conectividad entre dispositivos.

Ya que son demasiados segmentos de red distribuidos en 3 pisos, solo se efectuarán algunas pruebas al azar entre dispositivos de la misma VLAN y de diferentes VLAN, cabe resaltar que las políticas configuradas en el FW están hechas para que no haya comunicaciónentre VLANs, únicamente se podrán conectar entre ellas mismas y solamente la VLAN de servidores y printer puede recibir comunicación de todas las demás a excepción de la red de Invitados.

Con la información anterior, se procede a verificar las respectivas pruebas:

I. Red Invitados

Desde móvil en el piso 3 a móvil en el piso 1

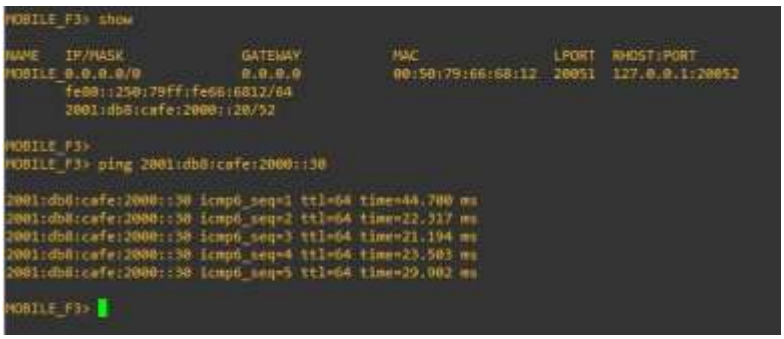


Figura 108 Ping entre equipos red INVITADOS

Figura 109 IP pc red invitados

II. CCTV

Desde cámara en 2 piso a Cámara en primer piso

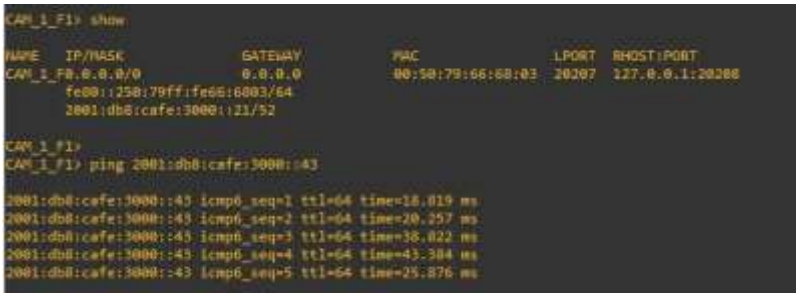


Figura 110 Ping entre equipos red CCTV

Figura 111 IP pc red CCTV

III. VoIP

Desde un teléfono en el tercer piso, a la ext de otro teléfono en el primer piso

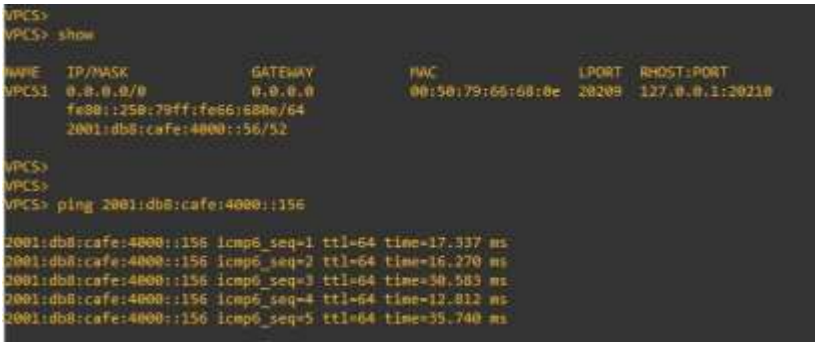


Figura 112 Ping entre equipos red VoIP

Figura 113 IP pc red VOIP

IV. Server/Printer

Como se mencionó anteriormente, todos los segmentos tienen acceso al segmento de servidores e impresoras, a excepción de la red de invitados, por ende, se hará prueba desde la Vlan de funcionarios hacia una ip del segmento Servers/Printer

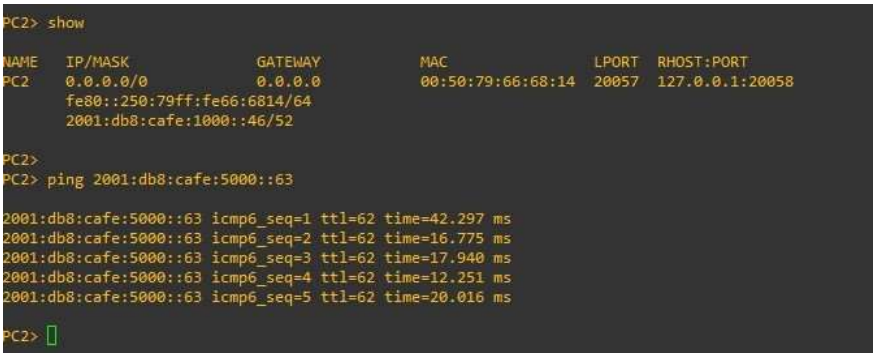


Figura 114 Ping entre equipos red Servers/Printer

Figura 115 IP pc red Servers/Printer

V. Presidencia/Gerencia

```
PC4> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC4    0.0.0.0/0            0.0.0.0           00:50:79:66:68:13  20207  127.0.0.1:20208
       fe80::250:79ff:fe66:6813/64
       2001:db8:cafe:6000::291/52

PC4> ping 2001:db8:cafe:6000::472

2001:db8:cafe:6000::472 icmp6_seq=1 ttl=64 time=78.385 ms
2001:db8:cafe:6000::472 icmp6_seq=2 ttl=64 time=17.028 ms
2001:db8:cafe:6000::472 icmp6_seq=3 ttl=64 time=24.329 ms
2001:db8:cafe:6000::472 icmp6_seq=4 ttl=64 time=12.674 ms
2001:db8:cafe:6000::472 icmp6_seq=5 ttl=64 time=19.326 ms

PC4>
```

Figura 116 Ping entre equipos red Presidencia/Gerencia

```
PC2> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC2    0.0.0.0/0            0.0.0.0           00:50:79:66:68:14  20057  127.0.0.1:20058
       fe80::250:79ff:fe66:6814/64
       2001:db8:cafe:6000::472/52
```

Figura 117 IP pc red Presidencia/Gerencia

VI. Área comercial y financiera

```
PC2> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC2    0.0.0.0/0            0.0.0.0           00:50:79:66:68:14  20057  127.0.0.1:20058
       fe80::250:79ff:fe66:6814/64
       2001:db8:cafe:7000::296/52

PC2> ping 2001:db8:cafe:7000::a579

2001:db8:cafe:7000::a579 icmp6_seq=1 ttl=64 time=76.410 ms
2001:db8:cafe:7000::a579 icmp6_seq=2 ttl=64 time=11.113 ms
2001:db8:cafe:7000::a579 icmp6_seq=3 ttl=64 time=43.093 ms
2001:db8:cafe:7000::a579 icmp6_seq=4 ttl=64 time=30.567 ms
2001:db8:cafe:7000::a579 icmp6_seq=5 ttl=64 time=41.264 ms
```

Figura 118 Ping entre equipos red Área comercial y financiera

```
PC4> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC4    0.0.0.0/0            0.0.0.0           00:50:79:66:68:13  20207  127.0.0.1:20208
       fe80::250:79ff:fe66:6813/64
       2001:db8:cafe:7000::a579/52

PC4>
```

Figura 119 IP pc red Área comercial y financiera

VII. TI

```
PC4> show

NAME   IP/MASK             GATEWAY          MAC                LPORT  RHOST:PORT
PC4    0.0.0.0/0           0.0.0.0          00:50:79:66:68:13  20207  127.0.0.1:20208
       fe80::250:79ff:fe66:6813/64
       2001:db8:cafe:8000::346f/52

PC4> ping 2001:db8:cafe:8000::23d/52

2001:db8:cafe:8000::23d icmp6_seq=1 ttl=64 time=30.668 ms
2001:db8:cafe:8000::23d icmp6_seq=2 ttl=64 time=16.514 ms
2001:db8:cafe:8000::23d icmp6_seq=3 ttl=64 time=21.864 ms
2001:db8:cafe:8000::23d icmp6_seq=4 ttl=64 time=10.404 ms
2001:db8:cafe:8000::23d icmp6_seq=5 ttl=64 time=17.954 ms

PC4>
```

Figura 120 Ping entre equipos red TI

```
PC2> show

NAME   IP/MASK             GATEWAY          MAC                LPORT  RHOST:PORT
PC2    0.0.0.0/0           0.0.0.0          00:50:79:66:68:14  20057  127.0.0.1:20058
       fe80::250:79ff:fe66:6814/64
       2001:db8:cafe:8000::23d/52

PC2>
```

Figura 121 IP pc red TI

VIII. Implementación

```
PC4> show

NAME   IP/MASK             GATEWAY          MAC                LPORT  RHOST:PORT
PC4    0.0.0.0/0           0.0.0.0          00:50:79:66:68:13  20207  127.0.0.1:20208
       fe80::250:79ff:fe66:6813/64
       2001:db8:cafe:9000::32e9/52

PC4>
PC4> ping 2001:db8:cafe:9000::974

2001:db8:cafe:9000::974 icmp6_seq=1 ttl=64 time=37.874 ms
2001:db8:cafe:9000::974 icmp6_seq=2 ttl=64 time=17.199 ms
2001:db8:cafe:9000::974 icmp6_seq=3 ttl=64 time=6.496 ms
2001:db8:cafe:9000::974 icmp6_seq=4 ttl=64 time=8.322 ms
2001:db8:cafe:9000::974 icmp6_seq=5 ttl=64 time=16.394 ms

PC4>
```

Figura 122 Ping entre equipos red Implementación

```
PC2> show

NAME   IP/MASK             GATEWAY          MAC                LPORT  RHOST:PORT
PC2    0.0.0.0/0           0.0.0.0          00:50:79:66:68:14  20057  127.0.0.1:20058
       fe80::250:79ff:fe66:6814/64
       2001:db8:cafe:9000::974/52
```

Figura 123 IP pc red Implementación

IX. Preventa

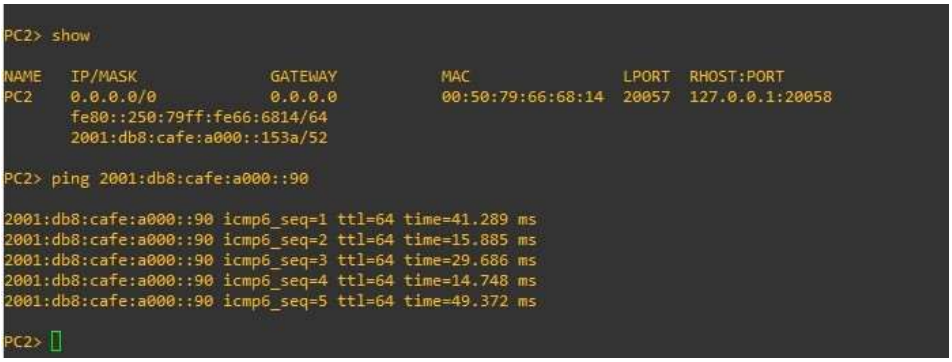


Figura 124 Ping entre equipos red Preventa

Figura 125 IP pc red Preventa

X. Servicios

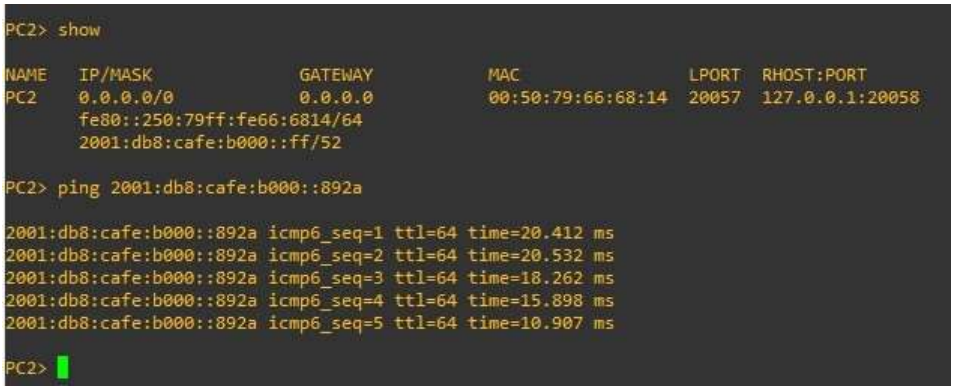


Figura 126 Ping entre equipos red Servicios

Figura 127 IP pc red Servicios

XI. HSEQ

```
PC2> show

NAME   IP/MASK             GATEWAY          MAC               LPORT  RHOST:PORT
PC2    0.0.0.0/0           0.0.0.0          00:50:79:66:68:14  20057  127.0.0.1:20058
       fe80::250:79ff:fe66:6814/64
       2001:db8:cafe:c000::c10/52

PC2> ping  2001:db8:cafe:c000::b271

2001:db8:cafe:c000::b271 icmp6_seq=1 ttl=64 time=16.351 ms
2001:db8:cafe:c000::b271 icmp6_seq=2 ttl=64 time=31.873 ms
2001:db8:cafe:c000::b271 icmp6_seq=3 ttl=64 time=62.113 ms
2001:db8:cafe:c000::b271 icmp6_seq=4 ttl=64 time=45.748 ms
2001:db8:cafe:c000::b271 icmp6_seq=5 ttl=64 time=18.078 ms

PC2>
```

Figura 128 Ping entre equipos red HSEQ

```
PC4> show

NAME   IP/MASK             GATEWAY          MAC               LPORT  RHOST:PORT
PC4    0.0.0.0/0           0.0.0.0          00:50:79:66:68:13  20207  127.0.0.1:20208
       fe80::250:79ff:fe66:6813/64
       2001:db8:cafe:c000::b271/52

PC4>
```

Figura 129 IP pc red HSEQ

XII. Almacén

```
PC2> show

NAME   IP/MASK             GATEWAY          MAC               LPORT  RHOST:PORT
PC2    0.0.0.0/0           0.0.0.0          00:50:79:66:68:14  20057  127.0.0.1:20058
       fe80::250:79ff:fe66:6814/64
       2001:db8:cafe:d000::e135/52

PC2> ping 2001:db8:cafe:d000::b9

2001:db8:cafe:d000::b9 icmp6_seq=1 ttl=64 time=25.206 ms
2001:db8:cafe:d000::b9 icmp6_seq=2 ttl=64 time=29.521 ms
2001:db8:cafe:d000::b9 icmp6_seq=3 ttl=64 time=16.608 ms
2001:db8:cafe:d000::b9 icmp6_seq=4 ttl=64 time=24.412 ms
2001:db8:cafe:d000::b9 icmp6_seq=5 ttl=64 time=19.905 ms

PC2>
```

Figura 130 Ping entre equipos red Almacén

```
PC4> show

NAME   IP/MASK             GATEWAY          MAC               LPORT  RHOST:PORT
PC4    0.0.0.0/0           0.0.0.0          00:50:79:66:68:13  20207  127.0.0.1:20208
       fe80::250:79ff:fe66:6813/64
       2001:db8:cafe:d000::b9/52

PC4>
```

Figura 131 IP pc red Almacén

XIII. Talento Humano

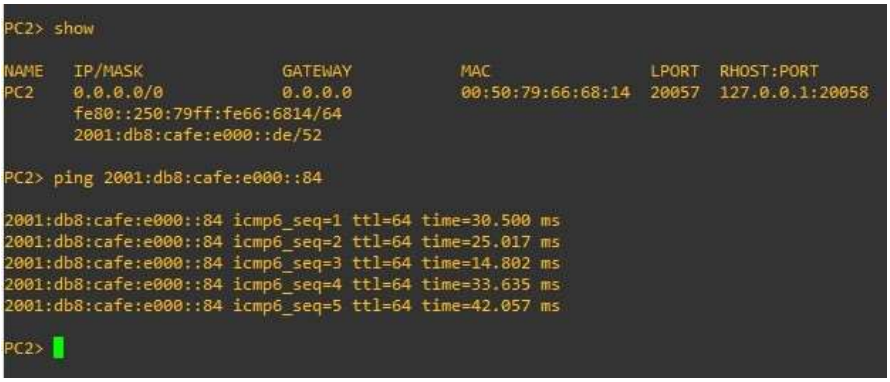


Figura 132 Ping entre equipos red Talento Humano

Figura 133 IP pc red Talento Humano

XIV. Área Jurídica

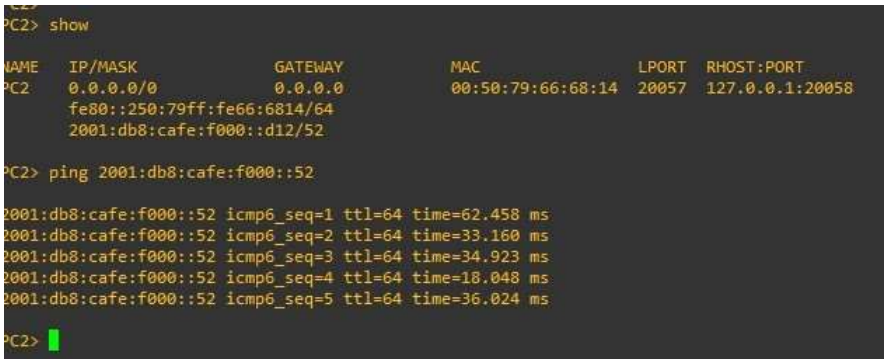


Figura 134 Ping entre equipos red Área jurídica

Figura 135 IP pc red Área Jurídica

5. Prueba de conectividad hacia la red externa

Al observar que a nivel LAN se tiene comunicación, el próximo paso es revisar que posea acceso a internet, para ello se realizara un ping a la ip versión 6 de Google:

2001:4860:4860::8888

I. Funcionarios

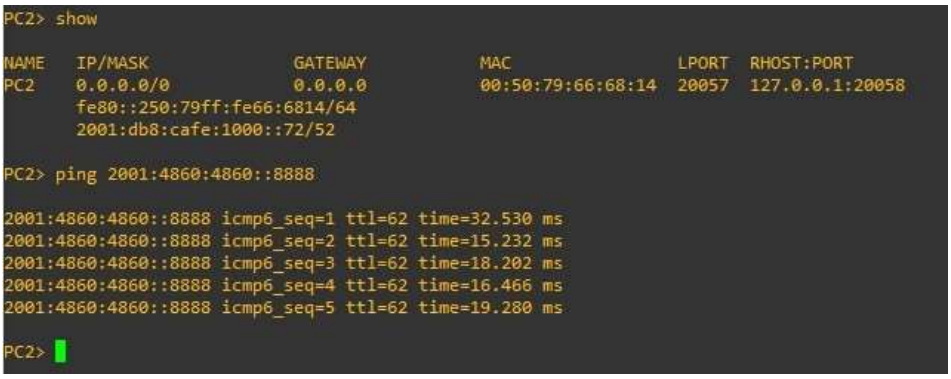


Figura 136 Ping hacia IPV6 google desde red funcionarios

II. Ivitados

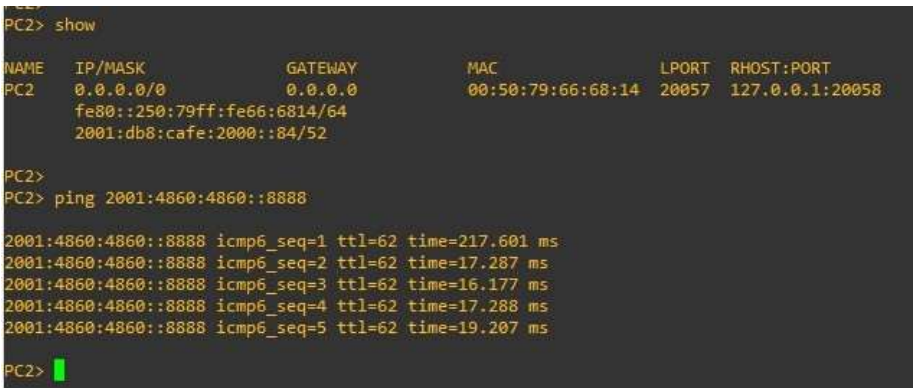


Figura 137 Ping hacia IPV6 google desde red Invitados

III. CCTV

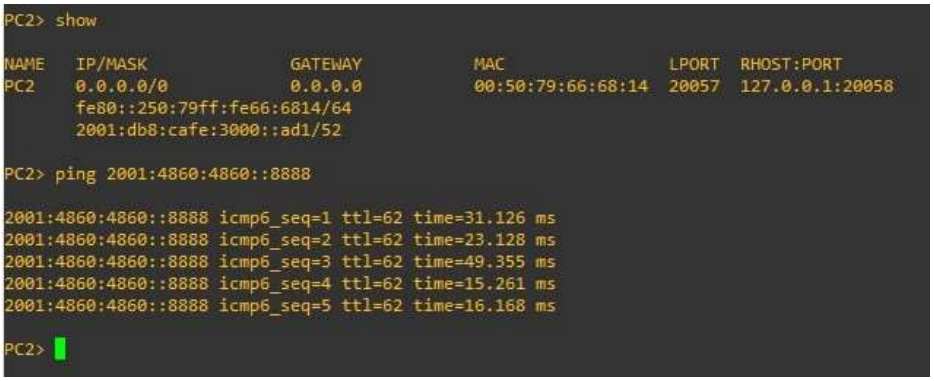


Figura 138 Ping hacia IPV6 google desde red CCTV

IV. VoIP

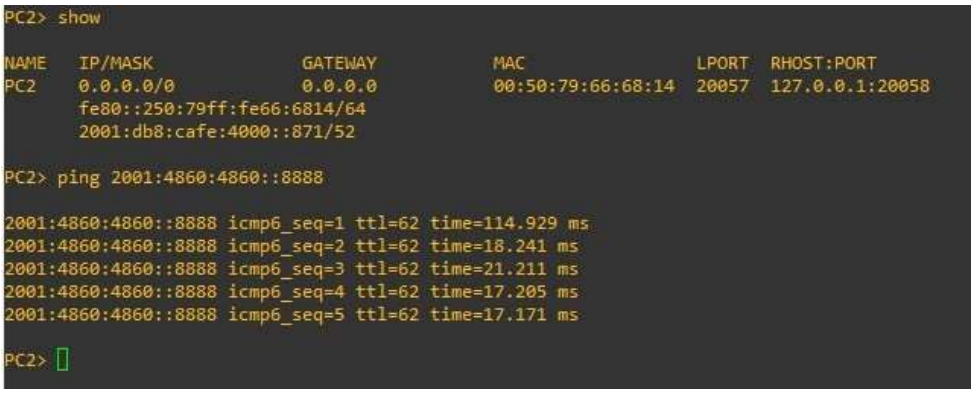


Figura 139 Ping hacia IPV6 google desde red VoIP

V. Servers/Printers

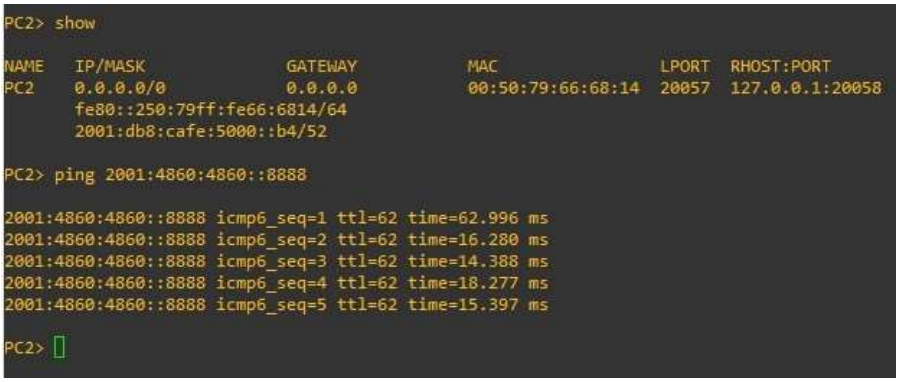


Figura 140 Ping hacia IPV6 google desde red Servers/Printers

VI. Presidencia/Gerencia

```
PC2> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC2    0.0.0.0/0            0.0.0.0           00:50:79:66:68:14  20057  127.0.0.1:20058
       fe80::250:79ff:fe66:6814/64
       2001:db8:cafe:6000::f82/52

PC2> ping 2001:4860:4860::8888

2001:4860:4860::8888 icmp6_seq=1 ttl=62 time=100.006 ms
2001:4860:4860::8888 icmp6_seq=2 ttl=62 time=19.257 ms
2001:4860:4860::8888 icmp6_seq=3 ttl=62 time=22.140 ms
2001:4860:4860::8888 icmp6_seq=4 ttl=62 time=21.166 ms
2001:4860:4860::8888 icmp6_seq=5 ttl=62 time=13.313 ms

PC2>
```

Figura 141 Ping hacia IPV6 google desde red Presidencia/Gerencia

VII. Área comercial y financiera

```
PC2> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC2    0.0.0.0/0            0.0.0.0           00:50:79:66:68:14  20057  127.0.0.1:20058
       fe80::250:79ff:fe66:6814/64
       2001:db8:cafe:7000::db1/52

PC2> ping 2001:4860:4860::8888

2001:4860:4860::8888 icmp6_seq=1 ttl=62 time=48.038 ms
2001:4860:4860::8888 icmp6_seq=2 ttl=62 time=22.225 ms
2001:4860:4860::8888 icmp6_seq=3 ttl=62 time=19.167 ms
2001:4860:4860::8888 icmp6_seq=4 ttl=62 time=19.208 ms
2001:4860:4860::8888 icmp6_seq=5 ttl=62 time=28.179 ms

PC2>
```

Figura 142 Ping hacia IPV6 google desde red Área comercial y financiera

VIII. TI

```
PC2> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC2    0.0.0.0/0            0.0.0.0           00:50:79:66:68:14  20057  127.0.0.1:20058
       fe80::250:79ff:fe66:6814/64
       2001:db8:cafe:8000::9131/52

PC2> ping 2001:4860:4860::8888

2001:4860:4860::8888 icmp6_seq=1 ttl=62 time=53.135 ms
2001:4860:4860::8888 icmp6_seq=2 ttl=62 time=20.152 ms
2001:4860:4860::8888 icmp6_seq=3 ttl=62 time=15.484 ms
2001:4860:4860::8888 icmp6_seq=4 ttl=62 time=16.258 ms
2001:4860:4860::8888 icmp6_seq=5 ttl=62 time=19.240 ms

PC2>
```

Figura 143 Ping hacia IPV6 google desde red TI

IX. Implementación

```
PC2> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC2    0.0.0.0/0            0.0.0.0           00:50:79:66:68:14  20057  127.0.0.1:20058
       fe80::250:79ff:fe66:6814/64
       2001:db8:cafe:9000::65/52

PC2> ping 2001:4860:4860::8888

2001:4860:4860::8888 icmp6_seq=1 ttl=62 time=23.039 ms
2001:4860:4860::8888 icmp6_seq=2 ttl=62 time=18.269 ms
2001:4860:4860::8888 icmp6_seq=3 ttl=62 time=16.146 ms
2001:4860:4860::8888 icmp6_seq=4 ttl=62 time=17.157 ms
2001:4860:4860::8888 icmp6_seq=5 ttl=62 time=17.172 ms

PC2>
```

Figura 144 Ping hacia IPV6 google desde red Implementación

X. Preventa

```
PC2> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC2    0.0.0.0/0            0.0.0.0           00:50:79:66:68:14  20057  127.0.0.1:20058
       fe80::250:79ff:fe66:6814/64
       2001:db8:cafe:a000::81/52

PC2> ping 2001:4860:4860::8888

2001:4860:4860::8888 icmp6_seq=1 ttl=62 time=51.073 ms
2001:4860:4860::8888 icmp6_seq=2 ttl=62 time=15.397 ms
2001:4860:4860::8888 icmp6_seq=3 ttl=62 time=17.222 ms
2001:4860:4860::8888 icmp6_seq=4 ttl=62 time=17.142 ms
2001:4860:4860::8888 icmp6_seq=5 ttl=62 time=17.420 ms

PC2>
```

Figura 145 Ping hacia IPV6 google desde red Preventa

XI. Servicios

```
PC2> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC2    0.0.0.0/0            0.0.0.0           00:50:79:66:68:14  20057  127.0.0.1:20058
       fe80::250:79ff:fe66:6814/64
       2001:db8:cafe:b000::76a/52

PC2> ping 2001:4860:4860::8888

2001:4860:4860::8888 icmp6_seq=1 ttl=62 time=42.097 ms
2001:4860:4860::8888 icmp6_seq=2 ttl=62 time=20.462 ms
2001:4860:4860::8888 icmp6_seq=3 ttl=62 time=16.245 ms
2001:4860:4860::8888 icmp6_seq=4 ttl=62 time=12.232 ms
2001:4860:4860::8888 icmp6_seq=5 ttl=62 time=17.287 ms

PC2>
```

Figura 146 Ping hacia IPV6 google desde red Servicios

XII. HSEQ

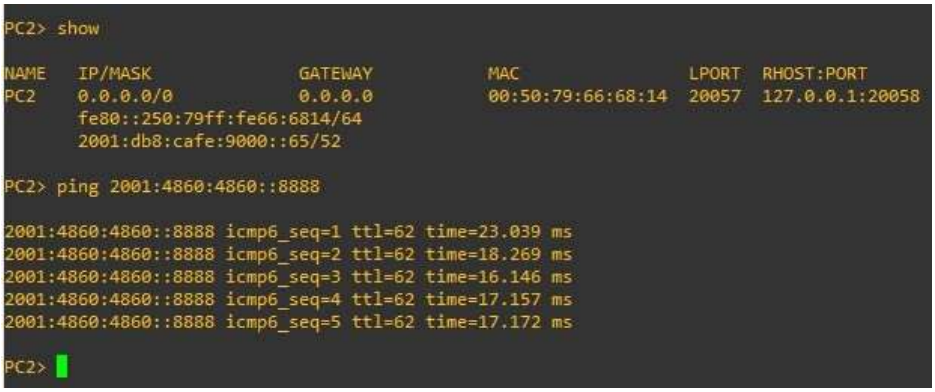


Figura 147 Ping hacia IPV6 google desde red HSEQ

XIII. Almacén

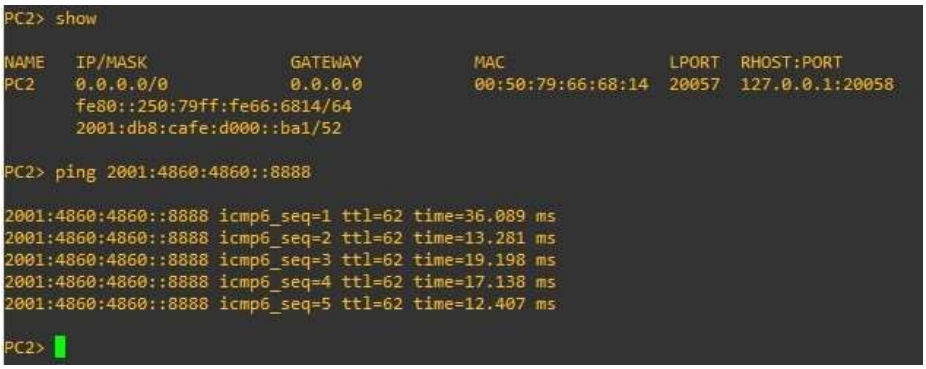


Figura 148 Ping hacia IPV6 google desde red Almacén

XIV. Talento humano

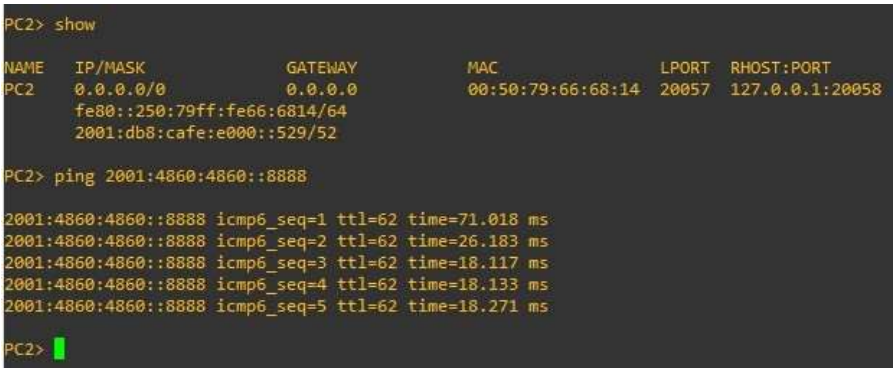


Figura 149 Ping hacia IPV6 google desde red Talento humano

XV. Área jurídica

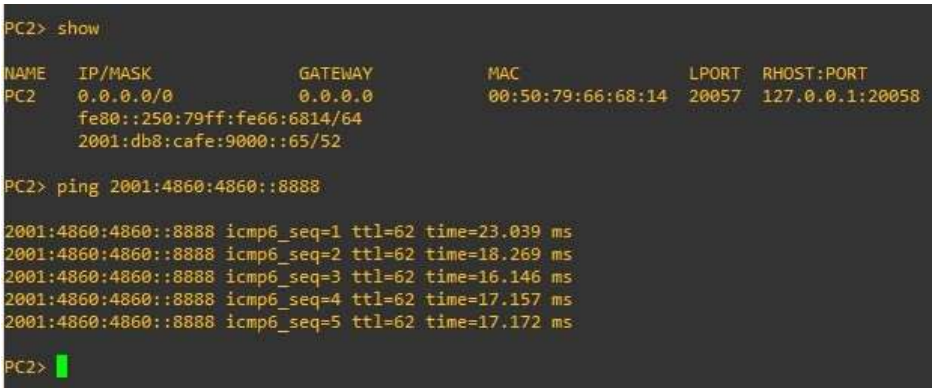


Figura 150 Ping hacia IPV6 google desde red Área jurídica

6. Verificación de los protocolos de redundancia

Para la revisión de este punto, se procederá a validar la redundancia que se tiene en los CPE por medio de su protocolo HSRP, para ello se apagara el enlace Ppal y se revisara el tráfico por medio del canal BK:

I. BGP CPE Ppal

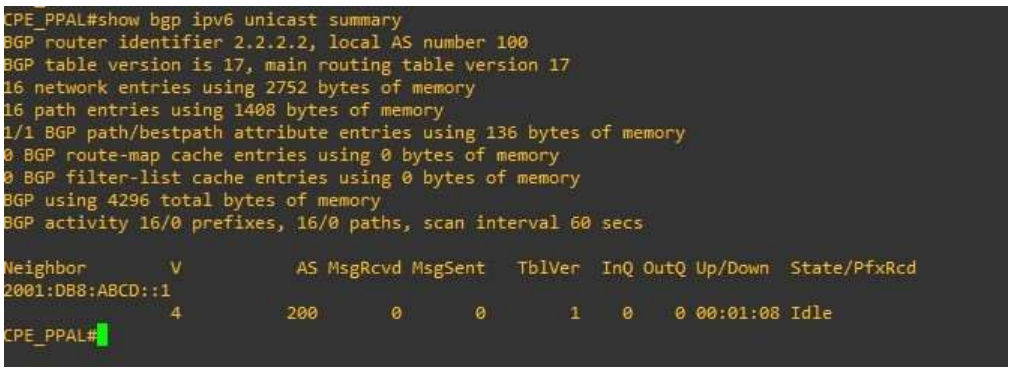


Figura 151 BGP down CPE ppal

II. BGP CPE Bk

```
CPE_BK#show bgp ipv6 unicast summary
BGP router identifier 3.3.3.3, local AS number 100
BGP table version is 17, main routing table version 17
16 network entries using 2752 bytes of memory
16 path entries using 1408 bytes of memory
1/1 BGP path/bestpath attribute entries using 136 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 4296 total bytes of memory
BGP activity 16/0 prefixes, 16/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:DB8:BCD::1 4          200      34      32       17    0    0 00:25:52        0
CPE_BK#
```

Figura 152 BGP established CPE bk

III. BGP PE

```
PE#show bgp ipv6 unicast summary
BGP router identifier 1.1.1.1, local AS number 200
BGP table version is 17, main routing table version 17
16 network entries using 2752 bytes of memory
16 path entries using 1408 bytes of memory
1/1 BGP path/bestpath attribute entries using 136 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 4320 total bytes of memory
BGP activity 16/0 prefixes, 32/16 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:DB8:BCD::2 4          100      34      36       17    0    0 00:27:39       16
2001:DB8:ABCD::2
                4          100       0       0        1    0    0 00:06:22 Idle
PE#
```

Figura 153 BGP status PE

IV. HSRP Bk

```
CPE_BK#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi1/0       1    100 P Active  local           FE80::1         FE80::5:73FF:FEA0:1
CPE_BK#
```

Figura 154 HSRP CPE bk

V. Aprendizaje IP desde PE

```
PE#show bgp ipv6 unicast neighbors 2001:DB8:BCD::2 received-routes
BGP table version is 17, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  2001:DB8:CAFE::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:1000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:2000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:3000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:4000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:5000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:6000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:7000::/52
     Network          Next Hop            Metric LocPrf Weight Path
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:8000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:9000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:A000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:B000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:C000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:D000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:E000::/52
                      2001:DB8:BCD::2          0             0 100 i
 *>  2001:DB8:CAFE:F000::/52
                      2001:DB8:BCD::2          0             0 100 i
```

Figura 155 Rutas aprendidas en PE desde CPE bk

Con estas pruebas se puede apreciar el funcionamiento del sistema de redundancia gracias al protocolo HSRP, se eliminó la comunicación del PE al CPE principal e inmediatamente se activó el canal secundario, propagando los segmentos LAN por medio de este, de esta manera se puede brindar una alta disponibilidad de servicio sin importar el protocolo IP que se implemente.

Conclusiones

El nuevo protocolo de direccionamiento IP (IPv6) brinda una gran variedad de funcionalidades que permite a las distintas compañías implementar más servicios que con el protocolo antecesor (IPv4) no se podía ejecutar, añadiendo mayor seguridad a su infraestructura,además de robustez a su diseño y software, convirtiendo estas soluciones emergentes en objetivos ambiciosos para satisfacer las necesidades de los usuarios finales. De igual manera y no menos importante se resalta el hecho de poder emplear un vasto número de direcciones IP lo que concluye en redes altamente escalables lo cual es imprescindible en las redes de telecomunicaciones modernas.

Por otro lado, es indispensable contemplar todas las variaciones y riesgos existentes en la migración de IPv4 a IPv6, esto con el fin de que esta sea satisfactoria, también es importante considerar los inconvenientes que puede traer no realizar dicho cambio, por lo que se recomienda ejecutar la transformación de las redes de IPv4 a IPv6 manteniendo la coexistencia de ambos protocolos.

Además de lo mencionado, es ideal basarse en los estándares y pautas planteadas por los diferentes entes reguladores con el objetivo de presentar un diseño optimo y eficiente al momento de efectuar algún proyecto en IPv6, esto mejorara la calidad de la solución a establecer generando mayores oportunidades de negocio y servicio.

Lista de referencias

Adrian Vernazza. “Happy Eyeballs para IPv4 e IPv6”. 2106. Available: https://blog.baehost.com/happy-eyeballs-acelera-cambio-desde-ipv4-hacia-ipv6/

AKAMAI. “Visualización de la adopción de IPv6”. 2020. Available: https://www.akamai.com/es/es/resources/our-thinking/state-of-the-internet-report/state-of-the-internet-ipv6-adoption-visualization.jsp

Cisco, "Dual Stack Network", Cisco.com, 2010. Available: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/IPV6at_a_glance_c45-625859.pdf.

CISCO, “MPLS: Layer 3 VPNs Configuration Guide, Cisco IOS Release 15M&T”, 2019, Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15- mt/mp-l3-vpns-15-mt-book/ip6-mpls-6vpn.html

D., & D. (2020, 25 agosto). IPv6 y SRv6 llevan el 5G. Comunidad Huawei Enterprise. https://forum.huawei.com/enterprise/es/ipv6-y-srv6-llevan-el-5g/thread/649203-100235

De Admin, V. T. L. E. (2017, 16 mayo). DESVENTAJAS DE LA NAT. Interpolados. https://interpolados.wordpress.com/2017/05/16/desventajas-de-la-nat/

DHCPv6 | Handbook. (s. f.). Fortinet. Recuperado 6 de octubre de 2021, de https://docs.fortinet.com/document/fortigate/6.0.0/handbook/800956/dhcpv6

ediciones-eni. “IPv6 - Principios e implementación”. Available: https://www.ediciones-eni.com/open/mediabook.aspx?idR=a5df9907f9d4f8c833b4249bff06747c

Ener.co. “Todo lo que necesitas saber sobre el IP versión 6”. 2019. Available: https://www.enter.co/cultura-digital/colombia-digital/protocolo-internet-ip-version-6/

González, C. (2018, 27 febrero). «El 5G e IPv6 serán un infierno» para los gobiernos. ADSLZone. https://www.adslzone.net/2018/02/27/ipv6-5g-seguridad/

Gr, R. (2021, 16 septiembre). Qué es CG-NAT y por qué compartes la IP pública. ADSLZone. https://www.adslzone.net/reportajes/operadores/que-es-cg-nat-operadores/

HUAWEI, "NE40E V800R010C00 Configuration Guide - VPN 0", 2018, Available: https://support.huawei.com/enterprise/en/doc/EDOC1100028543?section=j03h&topicNam e=configuring-a-basic-bgp-mpls-ipv6-vpn

IANA. "Internet Protocol Version 6 (IPv6) Parameters". 2020. Available: https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml

IBM, "Tunelización de IPv6", 2018, Available: https://www.ibm.com/support/knowledgecenter/es/ssw_aix_72/network/tcpip_ipv6_tunnel. html

IEFT. "Internet Protocol, Version 6 (IPv6) Specification". 1998. Available: https://tools.ietf.org/html/rfc2460

IEFT. "Neighbor Discovery for IP version 6 (IPv6)". 2007. Available: https://tools.ietf.org/html/rfc4861

IEFT. "Unique Local IPv6 Unicast Addresses". 2005. Available: https://tools.ietf.org/html/rfc4193

IPV6, "Transición IPv4 --> IPv6", Redesdecomputadores.umh.es, Available: http://redesdecomputadores.umh.es/ipv6/Transici%C3%B3n.html#.

Ivan Pepelnjak," NAT64 and DNS64 in 30 minutes", 2010, Available: https://www.slideshare.net/IOSHints/nat64-and-dns64-in-30-minutes

J. Martinez, "Using 464XLAT in residential networks", 2017. Available: https://ripe74.ripe.net/presentations/151-ripe-74-ipv6-464xlat-residential-v2.pdf.

Jose Luis de Abreu. “Introduccion al direccionamiento IPv6”.2014. Available: https://es.slideshare.net/zona802/introduccion-al-direccionamiento-ipv6

Kapil Digani “6rd – IPv6 gets a ride over IPv4”. Available: https://www.citrix.com/blogs/2012/03/02/6rd-%E2%80%93-ipv6-gets-a-ride-over-ipv4/

LACNIC. “Configuraciones - Bloque IPv6”. Available: https://www.lacnic.net/987/1/lacnic/centro-de-capacitaciones

Lista de hardware VoIP con soporte de IPv6. (2020, 31 octubre). Sinologic.net :: La web más leída sobre VoIP en Español. https://www.sinologic.net/2012-02/hardware-voip-con-soporte-de-ipv6.html

Matango, F., Matango, F., Matango, F., Matango, F., Matango, F., Matango, F., Matango, F., Matango, F., Matango, F., Matango, F., & Matango, F. (s. f.). IPv6 |. VoIP. Recuperado 6 de octubre de 2021, de http://www.servervoip.com/blog/tag/ipv6/

MINTIC. “Diez consejos para implementar IPv6 de forma segura”. 2019. Available: https://www.mintic.gov.co/portal/inicio/Micrositios/IPV6/5866:Diez-consejos-para-implementar-IPv6-de-forma-segura

Revista espacios, “Propuesta método de migración y coexistencia de IPV6 sobre red IP/MPLS para proveedor de servicios”. 2019. Available: https://www.google.com/search?client=firefox-b-d&q=MPLS+VPN+IPV6#

Sankaranarayanan K. “Tunnel Broker Testbed”. Available: https://www.researchgate.net/figure/Tunnel-Broker-Testbed_fig9_237620132

Sinchai Kamolphiwong. “The IPv4 connectivity establishment using DS-lite”. Available: https://www.researchgate.net/figure/The-IPv4-connectivity-establishment-using-DS-lite_fig2_269310013

TINYURI. Best Current Operational Practice for operators: IPv6 prefix assignment for end-users - persistent vs non-persistent, and what size to choose. 2017. Available: https://docs.google.com/document/d/1o58YbFx7v4_6AM_kSbPFslesPKq4mt-9ZaizIqFQEBs/edit

Tutorialspoint. “IPv6 – Enrutamiento”. 2019. Available: https://www.tutorialspoint.com/es/ipv6/ipv6_routing.htm