

**ESQUEMA DE TRANSICIÓN DEL PROCESO ESTABLECIDO PARA LA
MIGRACIÓN DEL PROTOCOLO IPV4 A IPV6 DE ACUERDO CON LOS
LINEAMIENTOS ESTABLECIDOS POR EL MINISTERIO DE TECNOLOGÍAS
DE LA INFORMACIÓN Y LAS COMUNICACIONES (MINTIC)**

HENRY FABIÁN ESPEJO GUERRERO

**UNIVERSIDAD NACIONAL ABIERTA Y/A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERA
BOGOTÁ, DC
2020**

**ESQUEMA DE TRANSICIÓN DEL PROCESO ESTABLECIDO PARA LA
MIGRACIÓN DEL PROTOCOLO IPV4 A IPV6 DE ACUERDO CON LOS
LINEAMIENTOS ESTABLECIDOS POR EL MINISTERIO DE TECNOLOGÍAS
DE LA INFORMACIÓN Y LAS COMUNICACIONES (MINTIC)**

HENRY FABIÁN ESPEJO GUERRERO

Monografía presentada como requisito parcial para optar al título de:

Especialista en seguridad Informática

Director

Ing. Joel Carroll

**UNIVERSIDAD NACIONAL ABIERTA Y/A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
BOGOTÁ, DC
2020**

Infraestructura Tecnológica Y Seguridad En Redes

UNIVERSIDAD NACIONAL ABIERTA Y/A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
BOGOTÁ, DC
2020

NOTA DE ACEPTACIÓN:

Comité de Grado en cumplimiento de los requisitos exigidos por la Universidad Abierta y a Distancia UNAD para optar al título de Especialización en Seguridad Informática

Jurado

Jurado

Dedicatoria

Esta monografía se la dedico a Dios por darme salud y sabiduría para desarrollar este trabajo, así mismo, le agradezco enormemente a mis padres ya que sin su apoyo no sería posible continuar con mis estudios y cumplir esta meta, a mi madre, una persona ejemplar, una persona noble, la cual recibí apoyo 100%, jamás me dejó desfallecer, siempre confió en mi potencial, siempre me dijo “TU PUEDES”, a mi padre, con su ejemplo como ser humano, como profesional, como papá, un guía ejemplar en este proceso, gracias infinitas por tu apoyo, eres un ser maravilloso. A mis hermanas las cuales son unas personas profesionales y saben lo que es hacer una especialización, (ya que están en las mismas) a ellas, las amo con todo mi corazón.

A mi esposa, una persona única, la cual siempre confió en mí, mi motor, mi apoyo, mi estabilidad, a ella le debo gran parte de este logro porque siempre estuvo ahí acompañándome en este proceso, a mis hijas, por ser mi motivación, por ser mi alegría, por ser mi todo, ellas fueron mi estimulación para realizar esta especialización, si Dios lo permite quiero siempre darles lo mejor. A mi abuela, una persona que siempre estuvo en las buenas y en las malas, gracias por todo tu apoyo y por último a la Familia Castellanos Pulido, Familia de mi esposa, gracias por todo su apoyo, gracias por acogerme en su núcleo familiar como uno más de ustedes, a todos, lo llevo en mi corazón y los quiero mucho.

Agradecimientos

Agradezco a la Universidad Nacional Abierta y a Distancia por todo lo enseñado en este tiempo, el cual me enseñó la responsabilidad y algo muy importante que fue el trabajo en equipo, muchas gracias por la oportunidad, gracias a todos los tutores y directores de grupo los cuales me aportaron un grano de arena para lograr el título profesional y ahora el título de especialista. A mi director de este proyecto el Ingeniero Joel Carroll, gracias por su paciencia, por sus enseñanzas, por su apoyo y por brindarme sus conocimientos. A mi tutora de este proyecto a la Ingeniera Yina Alexandra Gonzalez Sanabria, también gracias por su paciencia y sus correcciones.

Contenido

1	Introducción.....	12
2	Definición del problema.....	14
2.1	Antecedentes	14
2.2	Formulación del problema.....	14
2.3	Descripción del problema	16
3	Justificación	17
4	Objetivo General.....	18
5	Objetivos Específicos	18
6	Marco Referencial	19
6.1	Marco Conceptual y Teórico.....	19
6.2	Protocolos TCP/IP	19
6.3	Protocolo IPV4	20
6.4	Direcciones IPV4.....	21
6.5	Desventajas IPv4	22
6.6	Formato de dirección.....	22
6.7	Clases de direcciones ip.....	23
6.8	Protocolo IPv5	25
6.9	Protocolo IPv6	26
6.10	Cabecera IPv6 vs IPv4	27

6.11	Direcciones IPv6	28
6.12	Características de la IPV6	29
6.13	Para el desarrollo de esta monografía se tendrán en cuenta 3 variables planteadas en el objetivo general:	30
6.14	Diferencias	32
6.15	¿Es IPv6 más seguro que IPv4?	32
6.16	Protocolo GRE	34
6.17	Protocolo de Enrutamiento	35
6.18	Marco Histórico	38
6.19	Estado del arte	40
6.20	IPv6 posibles problemas y desafíos con la seguridad informática.....	44
7	Marco Legal	46
7.1	Resolución 2710 de 2017	46
7.2	Circular Numero 00002 de 2011 MinTIC	47
7.3	Resolución 180 de 2010 UIT	47
7.4	Ley 1341 de 2009.....	48
8	Diseño Metodológico	49
8.1	Metodología.....	49
8.2	Etapa 1 – Revisión del estado del arte	49
8.3	Etapa 2 – Simulación de la migración ipv4 – ipv6	50
8.4	Etapa 3 – Construcción de la monografía	50
9	Estructura de la Red.....	51
9.1	Pruebas migración ipv6	52
9.2	Configuración direcciones IPv6	53
9.2.1	Implementación Red IPv6	57

9.2.2	Pruebas de conexión.....	58
10	Buenas practicas.....	60
11	Resultado y Discusión	63
12	Conclusiones.....	64
13	Bibliografía.....	66
14	ANEXOS	70
14.1	Anexos 1 (Formato RAE)	70
14.2	Etapa 1 – Revisión del estado del arte.....	74
14.3	Etapa 2 – Simulación de la migración ipv4 – ipv6	74
14.4	Etapa 3 – Construcción de la monografía	74
14.5	ANEXO 2.....	77
14.5.1	Configuración topología de red	77

Lista de figuras

Figura 1. Formato de direccion IPv4	23
Figura 2. Clases Direcciones IP	24
Figura 3. Cabecera ipv6.....	27
Figura 4. Direcciones ipv6.....	29
Figura 5. Encapsulación de enrutamiento genérico GRE	35
Figura 6. Topología de la red	51
Figura 7. Interfaz.....	52
Figura 8. Configuración ipv6 en los pc.....	53
Figura 9. Interfaz Gigabit Ethernet.....	54
Figura 10. Show IPv6 interface brief	55
Figura 11. Show ip route	56

Figura 12. Implementación Red IPv6.....57

Figura 13. Ping PC1 a PC6.....58

Figura 14. Comando Tracert.....59

Lista de tablas

Tabla 1. Diferencias IPv4 IPv6.....	32
Tabla 2. Propuesta de métrica para evaluar los protocolos de enrutamientos y direccionamiento IP	40
Tabla 3. La transición del protocolo ipv4 a ipv6 en una empresa: revisión y caso.	41
Tabla 4. Transición de ipv4 a ipv6: revisión	41
Tabla 5. Metodología para hacer una transición en una red IPv4 a IPv6	42
Tabla 6. Planeación para adoptar el protocolo de internet versión 6 (IPv6) en la alcaldía de Acacías (meta).....	42

Resumen

La tecnología progresa a enormes pasos, esto hace que pongan en producción miles de aplicaciones cada día y del mismo modo, miles de dispositivos requieran acceso a estas aplicaciones, así como a la red. El internet es uno de los desarrollos de la tecnología que tiene la mayor relevancia en el servicio de la conectividad, ya que estos nuevos dispositivos solicitan una IP o identificador único, pero desafortunadamente el protocolo existente no proporciona dichas demandas de cobertura.

Es de suma importancia que todas las entidades implementen y pongan en funcionamiento el proceso de transición para la coexistencia del protocolo IPv4 – IPv6, así como la verificación del funcionamiento de estos realizando las respectivas pruebas.

La ejecución del Protocolo IPV6, otorgará una mejor comunicación en cualquier ordenador, mayor volumen de direccionamiento, seguridad, autoconfiguración, movilidad y privacidad en la información que viaja en la red.

Con la transición del protocolo IPv6 las compañías podrán lograr un buen servicio, ofreciendo navegación, seguridad, mayor velocidad en la conexión y transferencia en la información, además mejores tiempos de respuesta que contribuirán en el desarrollo tecnológico a nivel Nacional.

Por último, este proceso de investigación se realiza una comparación entre los aspectos técnicos de ambos protocolos generando importantes ventajas para realizar la transición.

Palabras clave: IPV4-IPV6, transición, mintic, migración, protocolo, resolución, normas, seguridad

Abstract

The technology progresses enormous steps, this makes thousands of applications in production every day and in the same way, thousands of devices require access to these applications, as well as the network. The Internet is one of the developments in technology that has the greatest relevance in the connectivity service, since these new devices request an IP or unique identifier, but unfortunately the existing protocol does not provide such coverage demands.

It is very important that all entities implement and put into operation the transition process for the coexistence of the IPv4 - IPv6 protocol, as well as the verification of the operation of these by carrying out the respective tests.

The implementation of the IPV6 Protocol, will provide better communication on any computer, greater volume of addressing, security, self-configuration, mobility and privacy in the information traveling on the network.

With the IPv6 protocol transition, companies will be able to achieve a good service, offering navigation, security, faster connection and information transfer, as well as better response times that will contribute to technological development at a national level.

Finally, this research process makes a comparison between the technical aspects of both protocols, generating important advantages to make the transition.

Keywords: IPV4-IPV6, transition, mintic, migration, protocol, resolution, standars, security

1 Introducción

Esta monografía nos permitirá identificar la importancia de la migración Ipv4 a Ipv6 según las normas emitidas por el MINTIC donde se debe garantizar el desarrollo de los principios orientadores de la ley 1341 de 2009, donde es función del ministerio trazar, acoger e impulsar las políticas, procedimientos, temas y propuestas del sector de las TIC, así como organizar y expedir los hechos administrativamente para el cumplimiento de los fines de intervención del Estado en materia de las TIC. Es preciso resaltar que la versión IPv4 más usada ha entrado en su fase de agotamiento de entrega de direccionamiento restringiendo las posibilidades de conexión ya que supero su capacidad debido incremento de usuarios y dispositivos que utilizan Internet.

Es de gran importancia reconocer los procesos determinados para la migración del protocolo IPv4 a IPv6 de acuerdo a los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el desarrollo de esta investigación se basa en la recolección de información definida por diferentes autores de acuerdo a la transición del protocolo Ipv4 a Ipv6, reconociendo ventajas y posibles inconvenientes que se puedan presentar en la transición al protocolo IPv6 en coexistencia del protocolo IPv4.

Finalmente se desarrolló la migración del direccionamiento IP de su versión 4 a la versión 6 con todas las consideraciones que conlleva la migración:

Implementación del protocolo GRE para gestionar las peticiones que vienen de la nube por los clientes y demás usuarios de las plataformas y servicios.

2 Definición del problema

2.1 Antecedentes

La migración de IPv4 a IPv6 la cual está siendo promovida por el ministerio de las TIC de acuerdo con la circular emitida en el año 2011, desde aquel instante se ha liderado un proceso de compañía a empresas públicas en cada uno de los períodos del proceso de migración, también cabe mencionar que las direcciones IPv4 se acabaron y hay que migrar por razones técnicas.

Como no se evidencia numerosa documentación de este tipo de procesos realizados por el MINTIC, hay evidencias de migraciones a IPv6 ejecutados de manera autónoma en varias instituciones educativas y otras empresas particulares. Tomé como evidencia una monografía la cual me sirvió como guía de transición.

2.2 Formulación del problema

¿Es importante Esquematizar el proceso establecido para la migración del protocolo IPv4 a IPv6 de acuerdo con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) para una organización?

Debido a sus limitaciones de direccionamiento, conectividad de extremo a extremo y enrutamiento, dado que cada computadora, teléfono móvil y otro dispositivo conectado a Internet necesita una dirección IP para comunicarse con otros dispositivos; en vista que casi la totalidad de los 4,3 mil millones de direcciones IPv4 ya están asignadas globalmente, la transición de IPv6, que tiene un número inimaginablemente grande de 340 deciles o 340 billones de billones de direcciones únicas, es clave para la prestación de servicios eficientes en consonancia con la estrategia de masificación del gobierno en línea, Para comunicar las máquinas IPv4 con las máquinas IPv6, es necesario implementar mecanismos de traducción o conversión de paquetes. Dado que existen diferencias entre IPv4 e IPv6, estos mecanismos no pueden funcionar en todas las circunstancias. Es posible que algunos protocolos y opciones (movilidad, calidad y servicio) no funcionen (o se degraden) con los mecanismos de traducción. Se espera que la transición de una red IPv4 a una red IPv6 dure mucho tiempo. Por lo tanto, durante este período de transición es necesario permitir que las máquinas IPv4 e IPv6 coexistan y se comuniquen entre sí.

Para abordar los problemas de la migración de IPv6 en la organización, se debe reunir un equipo multifuncional. Este equipo debe representar a las partes interesadas clave en la organización y ser responsable de liderar la planificación y entrega de IPv6 con una red sólida, segura, sistemática, aplicable a las terminales, a los servicios de asistencia y al equipo de administración.

Casi ningún experto en IPv6 se puede encontrar en el mercado global de TI. En la mayoría de las organizaciones, el personal de TI no ha dedicado mucho tiempo a familiarizarse con IPv6. Por estas razones, todavía hay grandes lagunas en el conocimiento de IPv6 entre los administradores e incluso en los desarrolladores. Por esta razón, es importante comenzar a acumular experiencia interna antes de iniciar un IPv6 para ello, se debe desarrollar un plan de capacitación correspondiente en las empresas.

2.3 Descripción del problema

En la actualidad ha surgido una problemática ya que las direcciones IPv4 se encuentran al límite debido al gran número de usuarios que utilizan Internet a nivel mundial a través de dispositivos tecnológicos, esta investigación está basada en identificar aspectos relevantes en la migración de IPv4 a IPv6 teniendo en cuenta la directriz establecida por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTic), es importante que todas las compañías implementen la tecnología IPv4 en coexistencia con IPv4, es de suma importancia cumplir con los protocolos establecidos con el fin de velar por la seguridad de la información.

De acuerdo con la circular 002 del 6 de junio de 2011, dada la presente fase de agotamiento final de direcciones IPv4, el estado colombiano ha creado espacios encaminados al avance de la adopción del protocolo ipv6. Pero existen en la actualidad empresas públicas que todavía no han cumplido con la circular expuesta por el MinTic para realizar la transición efectiva entre los protocolos.

3 Justificación

En cumplimiento del objetivo de realizar la transición del direccionamiento IPv4 a IPv6 según la circular 00002 del 6 de julio de 2011 y la Resolución 0002710 del 3 de octubre de 2017, normas emitidas por el MINTIC donde se debe garantizar el desarrollo de los principios orientadores de la ley 1341 de 2009, donde es función del ministerio trazar, acoger e impulsar las políticas, procedimientos, temas y propuestas del sector de las TIC, así como organizar y expedir los hechos administrativamente para el cumplimiento de los fines de intervención del Estado en materia de las TIC. Es preciso resaltar que la versión IPv4 más usada ha entrado en su fase de agotamiento de entrega de direccionamiento restringiendo las posibilidades de conexión, eso disminuye el desarrollo de nuevas redes y la interacción de los usuarios y su adecuación a las nuevas aplicaciones.

En este momento se requiere de un nuevo protocolo con características apropiadas a los tipos de tráfico de datos, ya que el número de usuarios que entran a la red desde diversos dispositivos móviles, a elevado significativamente.

“Esta estrategia, que se plasma en el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones 1078 de 2015, comprende cuatro grandes propósitos: lograr que los ciudadanos cuenten con servicios en línea de muy alta calidad, impulsar el empoderamiento y la colaboración de los ciudadanos con el Gobierno, encontrar diferentes formas para que la gestión en las entidades públicas sea óptima gracias al uso estratégico de la tecnología y garantizar la seguridad y la privacidad de la información.”¹

¹ RIVERO MALDONADO, Javier. TIC TIC TIC Seguridad y Privacidad de la Información para Gobierno Abierto para Servicio para la gestión manual. Estrategia de Gobierno en Línea. Disponible en: <http://docplayer.es/11095102-Tic-tic-tic-seguridad-y-privacidad-de-la-informacion-para-gobierno-abierto-para-servicio-para-la-gestion-manual-estrategia-de-gobierno-en-linea.html>

4 Objetivo General

- Esquematizar el proceso establecidos para la migración del protocolo IPv4 a IPv6 de acuerdo con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)

5 Objetivos Específicos

- Recopilar información acerca del protocolo IPv4 determinando la importancia de la migración a IPv6, como documentos, directrices y procesos de seguridad requeridos para la planificación y operación que ya hayan sido adaptados a los requisitos de IPv6.
- Analizar aspectos que se deben tener en cuenta para la implementación de IPv6, informando a los empleados de seguridad de TI sobre los posibles problemas y desafíos relacionados con la seguridad informática.
- Describir las pruebas que se deben tener en cuenta posterior a la migración de IPv4 a IPv6, identificando el correcto funcionamiento.
- Presentar un documento de buenas prácticas para la migración de IPv4 a Ipv6.

6 Marco Referencial

6.1 Marco Conceptual y Teórico

6.2 Protocolos TCP/IP

“Los protocolos IP (Protocolo de Internet) y TCP (Protocolo de Control de Transmisión) se originaron a principios de 1980 y fueron adoptados por la red ARPANET en 1983, que estaba integrada por cientos de computadoras de universidades, centros de investigación militar y algunas empresas. El e-mail (electronic mail) fue el servicio más comúnmente utilizado entonces, mientras que el sistema operativo más empleado era UNIX, en su versión BSD UNIX, desarrollada por la Universidad de California. Fue a mediados de los ochenta cuando fue creado el protocolo TCP/IP con la finalidad de contar con un lenguaje común a todas las computadoras conectadas a Internet, ya con la unión de las redes ARPANET, CSNET y MILNET. El protocolo TCP/IP representa, entonces, las reglas que hacen posible la conexión de computadoras de marcas y tecnología diferentes. TCP e IP son los protocolos más importantes. Su nombre representa al conjunto de protocolos que conforman la arquitectura formada por cinco niveles o capas:

1. Aplicación. Están contenidos los protocolos SMTP, para el correo electrónico; FTP, para las transferencias de archivos; TELNET, para la conexión remota, y HTTP, Hypertext Transfer Protocol.
2. Transporte. Se comprende a los protocolos TCP y UDP, que se ocupan del manejo y el transporte de los datos.

3. Internet. Se ubica en el nivel de la red para enviar los paquetes de información.
4. Físico. Es el análogo al nivel físico del OSI.
5. Red. Es el correspondiente a la interfaz de la red”²

6.3 Protocolo IPV4

“IPv4 es la versión 4 del protocolo IP (Internet Protocol). Es el estándar actual de Internet para identificar dispositivos conectados a esta red. Es uno de los protocolos más importantes para el funcionamiento de internet y fue implementado en ARPANET en 1983. Es el protocolo que más enruta datos en internet en la actualidad, a pesar de que ya se ha lanzado hace unos años (2006) su sucesor, la versión IPv6. Ambos conviven en internet”³

“La estructura y funcionamiento de IPv4 está descrito en la publicación RFC 791 (septiembre de 1981) de la IETF, en reemplazo de la definición anterior (RFC 760 de enero 1980). IPv4 utiliza direcciones IP de 32 bits (4 bytes), lo cual limita la cantidad de direcciones a 4.294.967.296 (2 elevado a 32). Esto crea un evidente problema, la escasez de direcciones. Cada dispositivo que se conecta a internet debe tener una dirección IP para ser identificado y 4 mil direcciones IP diferentes no son suficientes. Por lo que se lanzó la versión 6 (IPv6) que permite muchísimas más direcciones, comenzando su despliegue en 2006. La cantidad de direcciones

² QUIROZ CEBALLOS, Maria Jose y VEGA ZAMBRANO Silvio Andres. Servicios web, mensajería y transferencia de archivos en una intranet en el colegio nacional técnico tosagua provincia de Manabí. Calceta, 2013, 15
p. Trabajo de grado (Ingeniero de Informática). Escuela superior politécnica agropecuaria de Manabí Manuel Félix López. Carrera Informática.

³ ALEGSA, Leandro. Definición de IPv4. Argentina. (junio 5 de 2018). [Consultado: junio 5 de 2018]. Disponible en: <http://www.alegsa.com.ar/Dic/ipv4.php>

IPv4 se terminaron el 3 de febrero de 2011, luego de haber sido esto retrasado empleando varios métodos como Classful network, CIDR y NAT. IPv4 reserva bloques de direcciones especiales para redes privadas (aproximadamente 18 millones de direcciones) y direcciones de multidifusión (aproximadamente 270 millones de direcciones)".⁴

6.4 Direcciones IPV4

“Para entender el por qué el espacio de direcciones IPv4 es limitado a 4.3 mil millones de direcciones, podemos descomponer una dirección IPv4. Una dirección IPv4 es un número de 32 bits formado por cuatro octetos (números de 8 bits) en una notación decimal, separados por puntos. Un bit puede ser tanto un 1 como un 0 (2 posibilidades), por lo tanto, la notación decimal de un octeto tendría 2 elevado a la 8va potencia de distintas posibilidades (256 de ellas para ser exactos). Ya que nosotros empezamos a contar desde el 0, los posibles valores de un octeto en una dirección IP van de 0 a 255.

Ejemplos de direcciones IPv4: 192.168.0.1, 66.228.118.51, 173.194.33.16

Si una dirección IPv4 está hecha de cuatro secciones con 256 posibilidades en cada sección, para encontrar el número de total de direcciones IPv4, solo debes de multiplicar $256*256*256*256$ para encontrar como resultado 4,294,967,296

⁴ ALEGSA, Leandro. Definición de IPv4. Argentina. (junio 5 de 2018). [Consultado: junio 5 de 2018]. Disponible en: <http://www.alegsa.com.ar/Dic/ipv4.php>

direcciones. Para ponerlo de otra forma, tenemos 32 bits entonces, 2 elevado a la 32va potencia te dará el mismo número obtenido”.⁵

6.5 Desventajas IPv4

- Elevada demanda de direcciones ip
- No posee seguridad
- Limita el crecimiento a internet

6.6 Formato de dirección

“En una red TCP/IP a cada computadora se le asigna una dirección lógica de 32-bits que se divide en dos partes: el número de red y el número de computadora. Los 32 bits son divididos en 4 grupos de 8 bits, separados por puntos, y son representados en formato decimal.

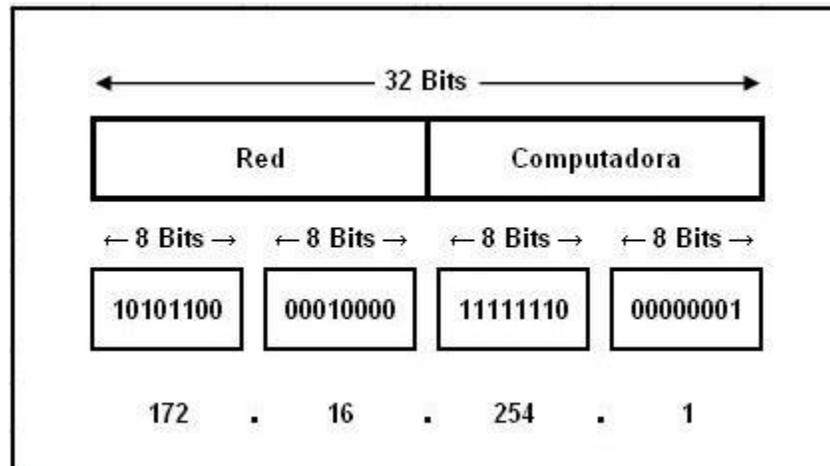
Cada bit en el octeto tiene un peso binario. El valor mínimo para un octeto es 0 y el valor máximo es 255. En la figura 1 se muestra el formato básico de una dirección IP con sus 32 bits agrupados en 4 octetos”.⁶

⁵ DIAZ, Jhonathan. Tantas IP como granos de arena [blog]. ¿Todos somos un número en la red mundial? (9 de abril de 2015). [Consultado: 9 de abril de 2015]. Disponible en: <http://usuariosinfinitosipv6.blogspot.com/2015/04/todos-somos-un-numero-en-la-red-mundial.html>

⁶ ESPINOZA, Alfonso. Diseño de una estructura de redes de computadoras IPv4 e IPv6 en modalidad de pila doble (dual stack) para el inces sede de la nueva granada Caracas-Venezuela. Caracas, 2014, 55 p.

Universidad Nacional Experimental.

Figura 1. Formato de direccion IPv4



Fuente: Fundamentos de IPv4. (2 de mayo de 2013). Recuperado de:

<http://www.ipv6.mx/index.php/informacion/fundamentos/ipv4>

6.7 Clases de direcciones ip

“Esta es utilizada para identificar un dispositivo dentro de una red privada, por ejemplo, la que creas al conectar tu smartphone, la impresora, la Tablet, y la laptop a una misma red de Wifi en tu hogar, o bien, las redes utilizadas a nivel empresarial.”⁷

En la figura 2 encontraremos las clases de direcciones IPs;

⁷ COMPARA HOSTING. ¿qué es una dirección ip y que tipos existen? [en línea]. [Consultado: 2 de marzo de 2020]. Disponible en: <https://www.comparahosting.com/p/que-es-una-direccion-ip/>

Figura 2. Clases Direcciones IP



Fuente: Tipos de clases IP. (s,f). Recuperado de

<https://sites.google.com/site/direccionamientosipredes/home/tipos-de-clases-ip>

Existen 3 rangos de direcciones que son las más utilizadas:

Clase A: “10.0.0.0 a 10.255.255.255 (8 bits red, 24 bits hosts), Esta clase es para las redes muy grandes, tales como las de una gran compañía internacional. Del IP con un primer octeto a partir de 0 al 127 son parte de esta clase. Los otros tres octetos son usados para identificar cada anfitrión. Esto significa que hay 126 redes de la clase A con 16,777,214 ($2^{24} - 2$) posibles anfitriones para un total de 2,147,483,648 (2^{31}) direcciones únicas del IP. Las redes de la clase A totalizan la mitad de las direcciones disponibles totales del IP.”⁸

Clase B: “De 172.16.0.0 a 172.31.255.255, que son usadas para redes medianas, como de alguna empresa local, escuela o universidad.

⁸ PACHECO, Alejandro. Redes de Comunicación en la UDI [en línea]. Rangos y Clases de la IP. (5 de abril de 2016). Disponible en: <https://sites.google.com/site/redesdecomunicacionenlaudi/rangos-y-clases-de-la-ip>

Clase C: “192.168.0.0 a 192.168.255.255, que son usadas para las redes más pequeñas, como redes domésticas”⁹

6.8 Protocolo IPv5

Un protocolo de Internet es el conjunto de reglas que rigen cómo se transmiten los paquetes a través de una red. IPv5 es una versión del protocolo de Internet (IP) que nunca se adoptó formalmente como estándar. El v5 representa la versión 5 del protocolo de internet. Las redes de computadoras usan la versión 4, típicamente llamada IPv4, o una versión más nueva de IP llamada IPv6.

RFC 1819 menciona que la versión 5 de IP estaba reservada para el protocolo experimental ST2, que era solo un complemento de transmisión de IPv4, nunca se lanzó para uso público, pero fue una inspiración para algunos componentes de IPv6. Al igual que IPv4 usa 0100 (4 en binario) para el campo de versión de IP (los primeros cuatro bytes de cada paquete de IP) e IPv6 usa 0110 (6), ST2 usa 0101 (5) para el campo de versión de IP.

⁹ COMPARA HOSTING. ¿qué es una dirección ip y que tipos existen? [en línea]. [Consultado: 2 de marzo de 2020]. Disponible en: <https://www.comparahosting.com/p/que-es-una-direccion-ip/>

6.9 Protocolo IPv6

El Protocolo de Internet versión 6 (IPv6) es un protocolo de capa de red que permite la comunicación de datos a través de una red de paquetes conmutados. La conmutación de paquetes implica el envío y la recepción de datos en paquetes entre dos nodos en una red. El estándar de trabajo para el protocolo IPv6 fue publicado por Internet Engineering Task Force (IETF) en 1998. La especificación IETF para IPv6 es RFC 2460. IPv6 tenía la intención de reemplazar el Protocolo de Internet Versión 4 (IPv4) que se considera la columna vertebral de la internet moderna. IPv6 a menudo se conoce como la "próxima generación de Internet" debido a sus capacidades ampliadas y su crecimiento a través de implementaciones recientes a gran escala. En 2004, Japón y Corea fueron reconocidos por tener los primeros despliegues públicos de IPv6.

El crecimiento explosivo en dispositivos móviles, incluidos teléfonos móviles, computadoras portátiles y dispositivos inalámbricos de mano ha creado la necesidad de bloques adicionales de direcciones IP. IPv4 actualmente admite un máximo de aproximadamente 4.300 millones de direcciones IP únicas. IPv6 admite un máximo teórico de 2128 direcciones (340,282,366,920,938,463,463,374,607,431,768,211,456 para ser exactos). Los avances recientes en la tecnología de red, incluida la traducción de direcciones de red (NAT), han disminuido temporalmente la urgencia de nuevas direcciones IP, sin embargo, estimaciones recientes indican que las direcciones IPv4 podrían agotarse en 2012.

6.10 Cabecera IPv6 vs IPv4

“Lo importante de implementar un nuevo direccionamiento es hacerlo retro compatible con los protocolos anteriores y operando en otras capas. El uso de IPv6 se puede utilizar con los demás protocolos de las capas de aplicación y transporte sin apenas hacer modificaciones en las cabeceras, excepto FTP o NTP por integrar en ellos las direcciones de la capa de red.

También se ha estudiado la forma de simplificar la cabecera del protocolo, haciéndola más sencilla que en IPv4 y de longitud fija, lo que ayuda mucha a la velocidad de su procesado e identificación del datagrama. Esto quiere decir que debemos enviar la información con IPv4 o IPv6, pero no con ambos mezclados.”¹⁰

En la figura 3 podemos ver la estructura de la cabecera IPv6:

Figura 3. Cabecera IPv6

Bits	0-7	8-15	16-23	24-31
Primeros	Versión	Clase de tráfico	Etiqueta de flujo	
	Longitud de datos		Cabecera siguiente	Límite de saltos
40	IP de origen			
Bytes	IP de destino			

CASTILLO, Jose Antonio. IPv4 vs IPv6 – Qué es y para qué se utiliza en redes [en línea]. (29 de febrero de 2020). Disponible en: https://www.profesionalreview.com/2020/02/29/ipv4-vs-ipv6/#Cabecera_IPv6_vs_IPv4_y_otras_novedades

¹⁰ CASTILLO, Jose Antonio. IPv4 vs IPv6 – Qué es y para qué se utiliza en redes [en línea]. (29 de febrero de 2020). Disponible en: https://www.profesionalreview.com/2020/02/29/ipv4-vs-ipv6/#Cabecera_IPv6_vs_IPv4_y_otras_novedades

6.11 Direcciones IPv6

“Las direcciones IPv6 están basadas en 128 bits. Usando la misma matemática anterior, nosotros tenemos 2 elevado a la 128va potencia para encontrar el total de direcciones IPv6 totales, mismo que se mencionó anteriormente. Ya que el espacio en IPv6 es mucho más extenso que el IPv4 sería muy difícil definir el espacio con notación decimal... se tendría 2 elevado a la 32va potencia en cada sección.

Para permitir el uso de esa gran cantidad de direcciones IPv6 más fácilmente, IPv6 está compuesto por ocho secciones de 16 bits, separadas por dos puntos (:). Ya que cada sección es de 16 bits, tenemos 2 elevado a la 16 de variaciones (las cuales son 65,536 distintas posibilidades). Usando números decimales de 0 a 65,535, tendríamos representada una dirección bastante larga, y para facilitar es que las direcciones IPv6 están expresadas con notación hexadecimal (16 diferentes caracteres: 0-9 y a-f).

Ejemplo de una dirección IPv6: 2607: f0d0: 4545: 3: 200: f8ff: fe21: 67cf

que sigue siendo una expresión muy larga, pero es más manejable que hacerlo con alternativas decimales”.¹¹

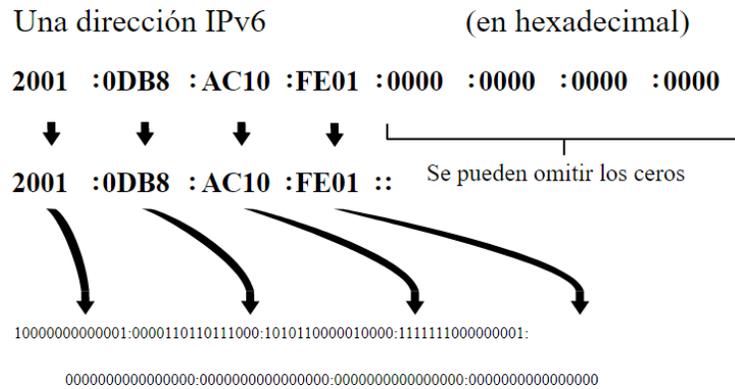
En la figura 4 veremos las direcciones IPv6;

¹¹ DIAZ, Jhonathan. Tantas IP como granos de arena [blog]. ¿Todos somos un número en la red mundial? (9 de abril de 2015). [Consultado: 9 de abril de 2015]. Disponible en: <http://usuariosinfinitosipv6.blogspot.com/2015/04/todos-somos-un-numero-en-la-red->

[mundial.html](#)



Figura 4. Direcciones IPv6



Fuente: Wikipedia. (s, f). Dirección IPv6. Obtenido de:
https://es.wikipedia.org/wiki/Direcci%C3%B3n_IPv6

6.12 Características de la IPV6

“Quizás las principales características de la IPv6 se sintetizan en el mayor espacio de direccionamiento, seguridad, autoconfiguración y movilidad. Pero también hay otras que son importantes mencionar:

- Infraestructura de direcciones y enrutamiento eficaz y jerárquica.
- Mejora de compatibilidad para Calidad de Servicio (QoS) y Clase de Servicio (CoS).
- Multicast: envío de un mismo paquete a un grupo de receptores.
- Anycast: envío de un paquete a un receptor dentro de un grupo.

- Movilidad: una de las características obligatorias de IPv6 es la posibilidad de conexión y desconexión de nuestro ordenador de redes IPv6 y, por tanto, el poder viajar con él sin necesitar otra aplicación que nos permita que ese enchufe/desenchufe se pueda hacer directamente.
- Seguridad Integrada (IPsec): IPv6 incluye IPsec, que permite autenticación y encriptación del propio protocolo base, de forma que todas las aplicaciones se pueden beneficiar de ello.
- Capacidad de ampliación.
- Calidad del servicio.
- Velocidad.”¹²

6.13 Para el desarrollo de esta monografía se tendrán en cuenta 3 variables planteadas en el objetivo general:

- **Migración:** Es una adaptación de los sistemas y una evolución en la innovación empresarial. Traen consigo cuantiosos privilegios que implican directamente en la producción de las compañías: mejora los procesos de negocio, la colaboración, el rendimiento y la optimización del puesto de trabajo.
- **Protocolo IPV4:** Una dirección IPv4 es una dirección de 32 bits que generalmente se representa en notación decimal con puntos, con un valor

¹² BARRIUSO, Héctor. IPv6 (Héctor Barriuso) [Blog]. 15 de diciembre de 2010. Disponible en: <http://httpwwwbloggercomhectorbarriuso.blogspot.com/2010/>

decimal que representa cada uno de los cuatro octetos (bytes) que conforman la dirección. Por ejemplo:

00001001010000110110000100000010 32-bit address

00001001 01000011 01100001 00000010 4 octets

9 67 97 2 dotted decimal notation (9.67.97.2)

- La dirección IPv4 consta de una dirección de red y una dirección de host. Dentro de Internet, las direcciones de red son asignadas por una autoridad central, el Centro de información de red (NIC). La parte de la dirección IPv4 que se usa para cada una de estas direcciones está determinada por la clase de dirección. Hay tres clases de dirección que son clase A, clase B y clase C.
- **Protocolo IPv6:** El Protocolo de Internet versión 6 (IPv6) es un protocolo de capa de red que permite la comunicación de datos a través de una red de paquetes conmutados. La conmutación de paquetes implica el envío y la recepción de datos en paquetes entre dos nodos en una red.

6.14 Diferencias

Tabla 1. Diferencias IPv4 IPv6

IPv4	IPv6
Seguridad Opcional	Seguridad Obligatoria
Broadcast	Unicast, Anycast, Multicast
Direcciones de 32 bits (4 bytes)	Direcciones de 128 bits (16 bytes)
Sin identificaciones QoS	Identificación QoS
Arquitectura jerárquica	Arquitectura plana

Fuente: Elaboración propia

6.15 ¿Es IPv6 más seguro que IPv4?

Cuando se lanzó IPv6 por primera vez, requería que las empresas encriptaran el tráfico de Internet con IPSec, un estándar de encriptación bastante común (pero no tan común como SSL). El cifrado codifica el contenido del tráfico de Internet para que cualquiera que lo intercepte no pueda leerlo.

Pero para lograr que más compañías se unan, ese requisito se transformó en una sugerencia más fuerte. Cifrar y descifrar datos requiere recursos informáticos, lo que requiere más dinero. IPSec también se puede implementar en IPv4, lo que en

teoría significa que IPv6 es igual de seguro que IPv4. Probablemente veremos un aumento en el uso de IPSec en general a medida que hacemos la transición, pero no es obligatorio para todos.

Mientras estamos en la fase de transición, algunos expertos sostienen que los usuarios de IPv6 están en mayor riesgo que aquellos que se adhieren a IPv4. Algunos ISP utilizan tecnologías de transición (túneles IPv6, en particular) que hacen que los usuarios sean más vulnerables a los ataques. Los ISP utilizan normalmente un intermediario de túnel para dar a los usuarios de sus redes IPv4 acceso al contenido de IPv6. Los hackers pueden atacar a los usuarios del túnel IPv6 con inyección de paquetes y ataques de reflexión. Hay que tener en cuenta que algunos corredores de túnel ofrecen una mayor seguridad que otros.

Se espera que la transición tome varios años más antes de que se complete, por lo que estos métodos de transición permanecerán vigentes durante algún tiempo.

Otro posible problema de seguridad viene con una nueva característica de IPv6: configuración automática. Esto permite que los dispositivos se asignen direcciones IP sin la necesidad de un servidor. Estas direcciones se generan utilizando la dirección MAC única de un dispositivo, que tiene cada teléfono, computadora y enrutador. Esto crea un identificador único que terceros podrían usar para rastrear usuarios específicos e identificar su hardware. Los dispositivos Windows, Mac OSX e iOS ya tienen extensiones de privacidad instaladas y habilitadas de manera predeterminada, por lo que esto no será un problema para la mayoría de las personas.

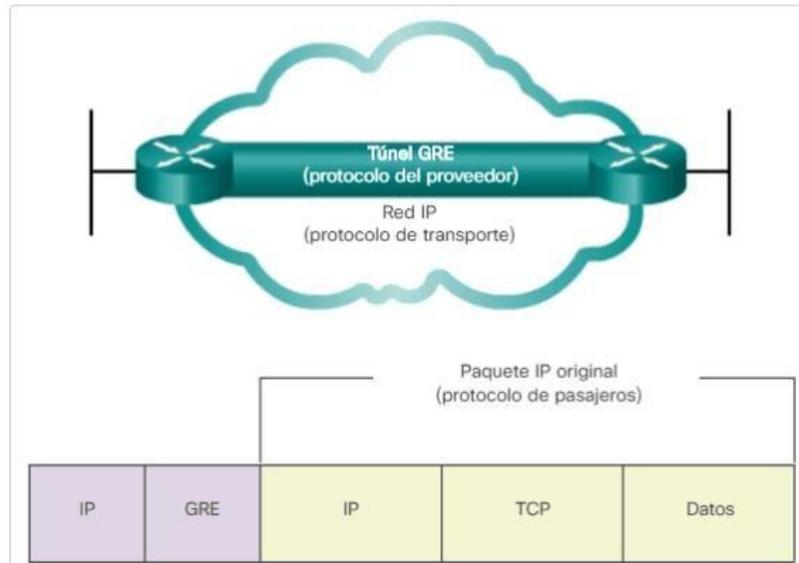
6.16 Protocolo GRE

Los túneles GRE son enlaces entre dos puntos, con un túnel separado para cada enlace. Los túneles no están atados a un protocolo específico de pasajero o transporte, pero en este caso llevar IPv6 como protocolo de pasajero con el GRE como protocolo de operador e IPv4 o IPv6 como protocolo de transporte.

El tráfico IPv6 se puede transportar a través de túneles IPv4 GRE utilizando la técnica de túnel GRE estándar diseñada para proporcionar los servicios para implementar cualquier esquema estándar de encapsulación punto a punto. Como en IPv6 manualmente túneles configurados, los túneles GRE son enlaces entre dos puntos, con un túnel separado para cada enlace. Los túneles no están vinculados a un protocolo específico de pasajeros o transporte, pero, en este caso, llevan IPv6 como protocolo de pasajeros con el GRE como protocolo de operador e IPv4 o IPv6 como protocolo de transporte.

El uso principal de los túneles GRE es para conexiones estables que requieren una comunicación segura regular entre dos dispositivos de borde o entre un dispositivo de borde y un sistema final. Los dispositivos de borde y los sistemas finales deben ser implementaciones de doble pila. A continuación, en la figura 5 se muestra la encapsulación de enrutamiento GRE.

Figura 5. Encapsulación de enrutamiento genérico GRE



Fuente: Walton, A. (s.f.). Túneles GRE: Características y Configuración. Obtenido de <https://ccnadesdecero.es/tuneles-gre-caracteristicas-y-configuracion/>

6.17 Protocolo de Enrutamiento

Un protocolo de enrutamiento utiliza software y algoritmos de enrutamiento para determinar la transferencia óptima de datos de red y las rutas de comunicación entre los nodos de la red. Los protocolos de enrutamiento facilitan la comunicación del enrutador y la comprensión general de la topología de la red.

Un protocolo de enrutamiento también se conoce como política de enrutamiento.

Existen protocolos de enrutamiento estático y dinámicos.

Protocolo de Enrutamiento Estático: “Es generado por el propio administrador, todas las rutas estáticas que se le ingresen son las que el router “conocerá”, por lo tanto, sabrá enrutar paquetes hacia dichas redes”¹³.

Protocolos de Enrutamiento Dinámico: Todos los protocolos de enrutamiento dinámico tienen un único propósito: dirigir el tráfico de datos por la ruta óptima hacia un destino cuando se les da la opción de elegir entre múltiples rutas. La parte "dinámica" se refiere a la capacidad del protocolo para recalcularse y redirigir el tráfico cuando hay rutas óptimas disponibles o cuando fallan los enlaces a lo largo de la ruta óptima. Dicho esto, no todos los protocolos de enrutamiento dinámico son iguales. Estos son los cuatro protocolos de enrutamiento más populares utilizados en las empresas de hoy para ver cómo difieren y dónde se utilizan mejor dentro de las infraestructuras de red.

RIPv2: El Protocolo de información de enrutamiento versión 2 (RIPv2) era un protocolo de enrutamiento LAN común en los años 90, pero se está desvaneciendo rápidamente en las redes de producción. RIPv2 sufrió problemas de escalabilidad debido a un recuento de saltos máximo relativamente bajo de 15 dispositivos de enrutamiento. En comparación con los protocolos de enrutamiento dinámico más modernos, los métodos de RIPv2 para seleccionar rutas óptimas y el tiempo de convergencia sustancial que lleva recalcularse las rutas la vuelven casi obsoleta. Hoy en día, la única razón por la que podría ejecutarse una red que ejecuta RIPv2 es porque la red es muy antigua y necesita una actualización seria o la red está ejecutando un hardware de enrutamiento más barato y apto para el consumidor que solo puede admitir RIP.

EIGRP: “Protocolo de enrutamiento de Gateway Interior por vector distancia, es una versión mejorada de IGRP.

OSPF: Protocolo de enrutamiento de Gateway Interior por estado de enlace.

¹³ ANONYMOUS. Redes Avanzadas [en línea]. Seguridad en TIC. (17 de junio de 2016).
Disponible en: <http://ingredesavanzadas.blogspot.com/2016/06/enrutamiento-estatico-y-dinamico.html>

(Open shortest path first, El camino más corto primero)

OSPF se usa, como RIP, en la parte interna de las redes, su forma de funcionar es bastante sencilla. Cada router conoce los routers cercanos y las direcciones que posee cada router de los cercanos. Además de esto cada router sabe a qué distancia (medida en routers) está cada router. Así cuando tiene que enviar un paquete lo envía por la ruta por la que tenga que dar menos saltos.

Así por ejemplo un router que tenga tres conexiones a red, una a una red local en la que hay puesto de trabajo, otra (A) una red rápida frame relay de 48Mbps y una línea (B) RDSI de 64Kbps. Desde la red local va un paquete a W que esta por A, a tres saltos y por B a dos saltos. El paquete iría por B sin tener en cuenta la saturación de la línea o el ancho de banda de la línea.

La O de OSPF viene de abierto, en este caso significa que los algoritmos que usa son de disposición pública.

BGP: Protocolo de enrutamiento de Gateway exterior por vector distancia.

El concepto de Gateway Interior o Exterior se refiere a que si opera dentro de un sistema Autónomo o fuera de él. Un sistema Autónomo, puede ser una organización que tiene el todo el control de su red, a estos sistemas autónomos se le asigna un número de Identificación por el ARIN (Registro Estadounidense de números de Internet), o por un proveedor de servicios. Los protocolos de enrutamiento como IGRP y EIGRP, necesitan de este número al momento de configurarse.

El protocolo BGP es de Gateway exterior, es decir se encuentra fuera de los sistemas autónomos, generalmente entre los que se les llama routers fronterizos entre ISP's, o entre una compañía y un ISP, o entre redes que interconectan países".¹⁴

¹⁴ VILLARREAL, Joanna. Proyecto de investigación 3 [en línea]. (26 de septiembre de 2016). Disponible en: <https://www.slideshare.net/JoannaVillarreal1/proyecto-de-investigacin-3>

6.18 Marco Histórico

El Protocolo de Internet versión 4 (IPv4) es el primer protocolo de capa de red estándar dominante en uso por computadoras y dispositivos electrónicos para intercambiar datos a través de Internet. IPv4 usa direcciones de 32 bits (por ejemplo, 144.214.32.4 en notación decimal), lo que limita el número de direcciones únicas a 4,3 mil millones. Ese espacio de direcciones no es suficiente para que cada persona viva en la tierra se conecte a Internet con una dirección IPv4 global. A partir de hoy, el espacio de direcciones gratuito que queda disponible para la asignación es de alrededor del 16% del total. Basado en el rápido consumo de direcciones en los últimos años a pesar de los esfuerzos intensos que se han realizado (como el uso de la traducción de direcciones de red y las direcciones IP privadas) para reducir la tasa de agotamiento, se predijo que no habría más direcciones disponibles para la asignación para el año 2011. Como tal, el Protocolo de Internet versión 6 (IPv6), anteriormente conocido como IPng (IP Next Generation), es el protocolo estándar de capa de red diseñado como sucesor de IPv4. Tiene una serie de ventajas sobre IPv4 además de una mayor escalabilidad y un mayor espacio de direcciones, como seguridad adicional, extensión de movilidad, capacidades mejoradas de calidad de servicio y mayor rendimiento, etc. IPv6 utiliza direcciones de 128 bits (por ejemplo, 2001: ce0: 5: 80: 35b0: 6e91: 2fe0:

IPv6 se ha desarrollado durante 10 años, mientras que IPv4 tiene una historia de más de 30 años. No hay fecha límite para migrar de IPv4 a IPv6. El plan inicial para la transición de IPv4 a IPv6 es que todos los sistemas conectados a Internet admitan la pila dual (ejecutando protocolos IPv4 e IPv6 nativos) gradualmente durante un período de muchos años, con el supuesto de que las direcciones IPv4 no se agotarán durante el período de transición. Sin embargo, ejecutar dual-stack ya no será factible, cuando ya no habrá direcciones IPv4 gratuitas disponibles para

la pila de protocolos IPv4. Por lo tanto, se deben buscar soluciones alternativas para permitir que los sistemas IPv4 e IPv6 se comuniquen entre sí durante el período de transición. Actualmente, el IETF (Grupo de trabajo de ingeniería de Internet) está considerando utilizar NAT (traducción de direcciones de red) como mecanismo para traducir entre direcciones IPv4 e IPv6. Las puertas de enlace capaces de hacer NAT bidireccional (IPv4 a IPv6 e IPv6 a IPv4) permitirán que los sistemas solo IPv4 y los sistemas solo IPv6 se comuniquen entre sí.

6.19 Estado del arte

Tabla 2. Propuesta de métrica para evaluar los protocolos de enrutamientos y direccionamiento IP

Autores	Joel Carroll Vargas, Santiago Salazar Fajardo, Edwar Jacinto Gomez
Título	Propuesta de métrica para evaluar los protocolos de enrutamientos y direccionamiento IP
Resumen	En este artículo mostraron el rendimiento de los direccionamientos IPv4 – IPv6, usaron protocolos de enrutamiento OSPF, RIP Y BGP, el primero empleando la métrica propuesta del artículo y el segundo utilizaron la herramienta Jmeter., todo esto para demostrar su rendimiento. Los resultados que hicieron fue que el rendimiento de IPv4 es magnífico en ambientes en tiempo real, por otro lado, IPv6 mostro buen rendimiento utilizando los protocolos OSPF y RIP
Año	2019
País	Colombia

Fuente: Elaboración propia

Tabla 3. La transición del protocolo ipv4 a ipv6 en una empresa: revisión y caso

Autores	Jeisson D. Novoa, Luis A. Gamboa, Gustavo A. Higuera
Título	La transición del protocolo ipv4 a ipv6 en una empresa: revisión y caso
Resumen	Este artículo tuvo con finalidad enseñar un manual que permita ejecutar la transición y aprovisionamiento de IPv6 dentro de las empresas. Dieron detalles de los métodos de transición IPv4 – IPv6, del direccionamiento, de la asignación de ip's y de los protocolos de enrutamiento. Concluyeron que la red y el resto de los servicios trabajaron correctamente y desde que se cuente con una buena estructura de red se puede aplicar la metodología.
Año	2018
País	Colombia

Fuente: Elaboración propia

Tabla 4. Transición de ipv4 a ipv6: revisión

Autores	Yesica María Pérez Pérez, Andrés Mauricio Puentes Velásquez
Título	Transición de IPv4 a IPv6: revisión
Resumen	Para este trabajo dejaron claro que el tema de transición de IPv4 a IPv6 parece complejo ya que hasta este instante no tienen claro cuando harán la migración, porque no han percibido los beneficios de implementar hacia la nueva versión, a parte, revisaron las metodologías, modelos y prácticas seguras para la transición de IPv4 a IPv6 de acuerdo con la escasez de ip's.
Año	2018

Autores	<i>Yesica Maria Pérez Pérez, Andrés Mauricio Puentes Velásquez</i>
País	Colombia

Fuente: Elaboración propia

Tabla 5. Metodología para hacer una transición en una red IPv4 a IPv6

Autores	Edwin Alexander Segura Cruz, Edwin Vargas
Título	Metodología para hacer una transición en una red IPv4 a IPv6
Resumen	De acuerdo con este trabajo, mediante el método de Dual Stack, aplicaron una metodología diseñada para realizar la migración de IPv4 a IPv6 en una red que estuviese en funcionamiento, en esta migración buscaron entre los dos protocolos un funcionamiento paralelo que logren convivir funcionalidades de los dos modelos de direccionamiento.
Año	2017
País	Colombia

Fuente: Elaboración propia

Tabla 6. Planeación para adoptar el protocolo de internet versión 6 (IPv6) en la alcaldía de Acacías (meta)

Autores	Christian Víctor Salazar Hernández Edilberto Romero Trujillo
Título	Planeación para adoptar el protocolo de internet versión 6 (IPv6) en

Autores	Christian Víctor Salazar Hernández Edilberto Romero Trujillo
	la alcaldía de Acacias (meta)
Resumen	En este proyecto, mostraron que de acuerdo al agotamiento de direccionamiento IP ya que el protocolo IPv4 realiza la conexión de dispositivos a internet y la transferencia de información, la alcaldía de Acacias Meta, tomo la decisión de hacer la transición a IPv6, esto en base para migrar a un protocolo que permita continuar con el aumento de la red y claro está, para que les permita el buen trabajo del software y hardware respecto al canje de información tanto a nivel local como a nivel global y como el protocolo IPv6 por su capacidad de direccionamiento, lo eligieron para sustituir al protocolo IPv4
Año	2018
País	Colombia

Fuente: Elaboración propia

6.20 IPv6, posibles problemas y desafíos con la seguridad informática

El aumento de IPv6 podría darle algunos dolores de cabeza de seguridad severos, incluso si no se tiene planes actuales para implementar el nuevo protocolo de red.

Se han visto malware generalizado con capacidades de comando y control basadas en IPv6. Entonces, si su servidor habilita IPv6 de manera predeterminada pero su firewall no lo hace, lo que puede ser el caso para muchos, inevitablemente veremos más abusos para fines maliciosos. La implementación y configuración adecuadas es un problema grave, intentar implementar IPv6 de la misma manera que se hizo IPv4 garantiza problemas, los administradores de TI deben aprender un enfoque completamente nuevo para las redes, desde la simple solución de problemas de red hasta la configuración de firewalls y el monitoreo de registros de seguridad, hay muchas oportunidades para la confusión y los errores.

No hay un cambio instantáneo para cambiar de IPv4 a IPv6, por lo que la adopción parcial implica el uso de tecnologías de túnel para transportar IPv6 sobre IPv4. Este tipo de solución es otra fuente potencial de confusión, configuración errónea y brechas de seguridad. A medida que aumente la adopción de IPv6 y los cibercriminales pasen más tiempo y esfuerzo analizando cómo subvertir su seguridad incorporada, es probable que veamos más problemas. A medida que se descubran nuevos problemas, necesitaremos nuevos métodos y herramientas para superarlos.

Los beneficios de seguridad IPv6 es que pueden ejecutar cifrado de extremo a extremo. Si bien esta tecnología se actualizó en IPv4, sigue siendo un extra opcional que no se usa universalmente. El cifrado y la verificación de integridad utilizados en las VPN actuales es un componente estándar en IPv6, disponible para todas las conexiones, compatible con todos los dispositivos y sistemas.

IPv6 también admite una resolución de nombre más segura. El protocolo Secure Neighbor Discovery (SEND) es capaz de permitir la confirmación criptográfica de que un host es quien dice ser en el momento de la conexión. Esto hace que el envenenamiento del Protocolo de resolución de direcciones (ARP) y otros ataques basados en nombres sean más difíciles. Y aunque no es un reemplazo para la verificación de la capa de servicio o aplicación, todavía ofrece un nivel mejorado de confianza en las conexiones. Con IPv4 es bastante fácil para un atacante redirigir el tráfico entre dos hosts legítimos y manipular la conversación o al menos observarla. IPv6 hace esto muy difícil. Esta seguridad adicional depende completamente del diseño, una implementación adecuada, la infraestructura más compleja y flexible de IPv6 hace más trabajo. Sin embargo, configurada correctamente, la red IPv6 será significativamente más segura que su predecesora.

7 Marco Legal

7.1 Resolución 2710 de 2017

“En respuesta a la masiva conexión de dispositivos a Internet y el agotamiento inminente de las direcciones IPv4, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) expidió la Resolución 2710 de 2017, "Por la cual se establecen lineamientos para la adopción del protocolo IPv6" en el país.

Con esta resolución se busca básicamente que las entidades del Estado adopten el IPv6 en sus infraestructuras tecnológicas, lo cual permite que más dispositivos puedan ser conectados a Internet, abonando el camino para la implementación de redes de nueva generación.

Entre los aspectos más importantes a resaltar de la resolución, está que las entidades del Estado de orden nacional, por tarde, el 31 de diciembre del 2019 deben implementar la tecnología IPv6, en coexistencia con el IPv4. Para entes territoriales, el plazo máximo es el 31 de diciembre del 2020.”¹⁵

¹⁵ COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto

0002710 (03, octubre, 2017). Por el cual se establecen lineamientos para la adopción del protocolo IPv6 [en línea]. Santa Fe de Bogotá, D.C.: El Ministerio, 2017. 4 p. Disponible en: https://www.mintic.gov.co/portal/604/articles-61192_recurso_1.pdf

7.2 Circular Numero 00002 de 2011 MinTIC

“Que en la Circular No. 0002 del 6 de julio de 2011, el Ministerio TIC convocó a las entidades de la Administración Pública, Ramas y Organismos del Estado y al sector TIC, para que en sus compras de infraestructura de TIC (Hardware, Software y Almacenamiento) se exija que soporten el protocolo IPv6 y que sean compatibles con IPv4, además les instó a incluir en sus administraciones un “Plan de transición para la Adopción de IPv6 en coexistencia con IPv4”, que permita una transición segura y sin traumatismos.”¹⁶

7.3 Resolución 180 de 2010 UIT

En la “Resolución 180 de 2010, la Unión Internacional de Telecomunicaciones (UIT), de la cual forma parte Colombia, reconoce que la adopción temprana del IPv6 es la mejor forma de evitar escasez de direcciones y las consecuencias del agotamiento de las direcciones IPv4 pueda implicar para el País, incluidos altos costes, además de resaltar el importante rol que los gobiernos desempeñan como catalizadores de la transición hacia el IPv6; por lo tanto, hace un llamado al fomento y despliegue de IPv6 en las administraciones públicas.”¹⁷

¹⁶ COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 00002

(06, julio, 2011) Promoción de la adopción del IPv6 en Colombia [en línea]. Santa Fe de Bogota, D.C.: El Ministerio, 2011. 4 p. Disponible en Internet: <http://www.mintic.gov.co/portal/604/w3-article-5932.html>

¹⁷ COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.
Decreto
0002710 (03, octubre, 2017). Por el cual se establecen lineamientos para la adopción del protocolo
IPv6

7.4 Ley 1341 de 2009.

"Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones"

“Neutralidad Tecnológica: El Estado garantizará la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones y garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible.

Artículo 4: En desarrollo de los principios de intervención contenidos en la Constitución Política, el Estado intervendrá en el sector las Tecnologías de la Información y las Comunicaciones para lograr los siguientes fines; proteger los derechos de los usuarios, velando por la calidad, eficiencia y adecuada provisión de los servicios, promover el acceso a las Tecnologías de la Información y las Comunicaciones, teniendo como fin último el servicio universal, promover el desarrollo de contenidos y aplicaciones, la prestación de servicios que usen Tecnologías de la Información y las Comunicaciones y la masificación del Gobierno en Línea.”¹⁸

[en línea]. Santa Fe de Bogota, D.C.: El Ministerio, 2017. 4 p.
Disponble en: https://www.mintic.gov.co/portal/604/articles-61192_recurso_1.pdf

¹⁸ COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 1341

(30, julio, 2009) Por lo cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones. [en línea]. Santa Fe de Bogota, D.C.: El Ministerio, 2009. 34 p. Disponible en Internet:

https://www.mintic.gov.co/portal/604/articles-3707_documento.pdf

8 Diseño Metodológico

8.1 Metodología

El plan de trabajo del presente proyecto incluyó tres etapas, comenzando con la realización de un fuerte marco teórico, avanzando hacia la instrumentación de técnicas para el manejo de personal y mitigación de posibles vulnerabilidades que se presente; luego la implementación de pruebas y validaciones técnicas y posibles contingencias que se presentaran durante la migración. Estas etapas están en total correspondencia con los objetivos trazados en el proyecto, y se pueden superponer en el tiempo en algunas ocasiones. El siguiente es la metodología específica para cada uno de los objetivos propuestos.

8.2 Etapa 1 – Revisión del estado del arte

Recopilar información acerca del protocolo ipv4 determinando la importancia de la migración a IPv6, como documentos, directrices y procesos de seguridad requeridos para la planificación y operación que ya hayan sido adaptados a los requisitos de IPv6.

Revisión del estado del arte: estudios de los avances realizados hasta el momento de las migraciones IPv4 – IPv6.

8.3 Etapa 2 – Simulación de la migración ipv4 – ipv6

En esta etapa se realiza el diseño y la simulación de la migración a realizar comprendiendo las siguientes actividades:

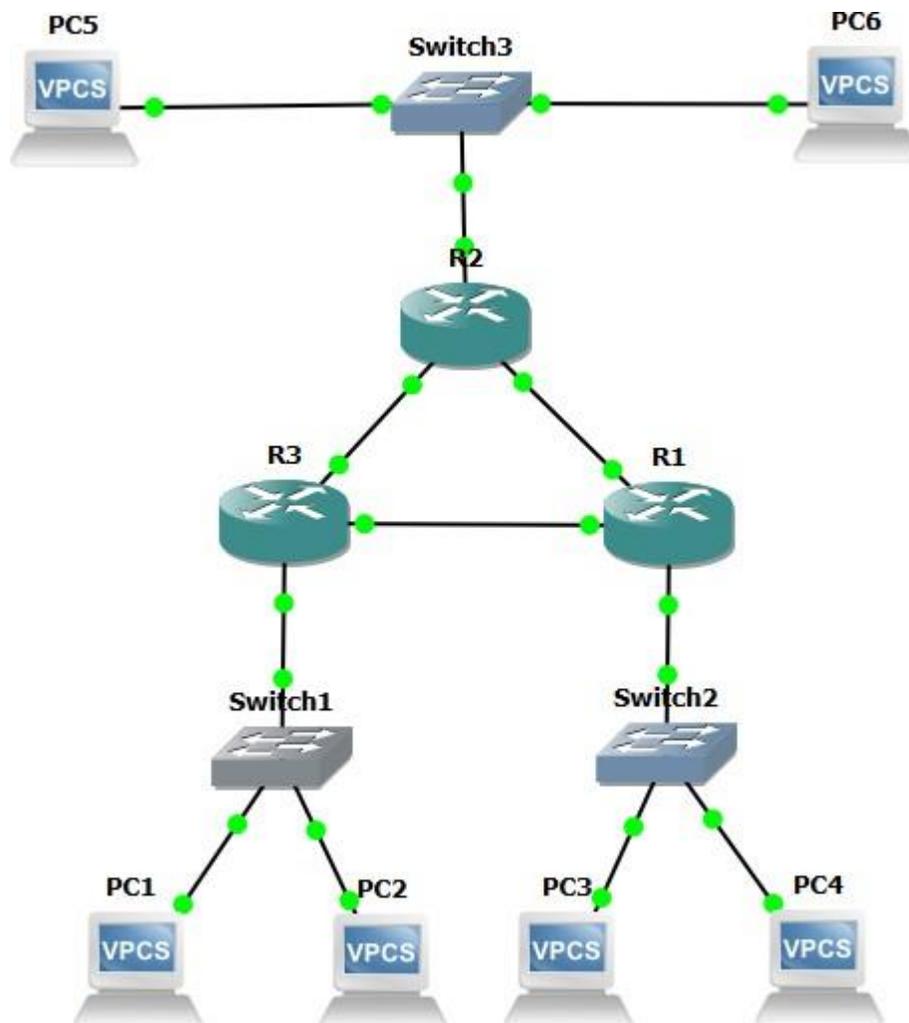
- Elaboración de topología Gns3
- Pruebas y validación de la implementación

8.4 Etapa 3 – Construcción de la monografía

9.1 Pruebas migración ipv6

Como podemos apreciar, en la figura 7 se muestra la topología la cual se hizo la simulación con 5 pc, 3 switches y 3 router. Procedo a realizar la configuración y a conectar los dispositivos.

Figura 7. Interfaz



Fuente: Elaboración propia

9.2 Configuración direcciones IPv6

A continuación, en la figura 8 relaciono la configuración de 6 PCs

Figura 8. Configuración IPv6 en los pc 6 PCs



The figure displays six terminal windows, each representing the configuration of a different PC (PC1 to PC6). Each window shows the following steps: setting the IPv6 address, saving the configuration, and displaying the configuration details. The details include the name, link-local scope, global scope, router link-layer, MAC address, LPORT, RHOST:PORT, and MTU.

```
PC1> ip 2001:db8:1::2
PC1 : 2001:db8:1::2/64

PC1> save
Saving startup configuration to startup.vpc
. done

PC1> show ipv6

NAME           : PC1[1]
LINK-LOCAL SCOPE : fe80::250:79ff:fe66:6800/64
GLOBAL SCOPE    : 2001:db8:1::2/64
ROUTER LINK-LAYER :
MAC            : 00:50:79:66:68:00
LPORT          : 10004
RHOST:PORT     : 127.0.0.1:10005
MTU            : 1500

PC2> ip 2001:db8:2::2
PC2 : 2001:db8:2::2/64

PC2> save
Saving startup configuration to startup.vpc
. done

PC2> show ipv6

NAME           : PC2[1]
LINK-LOCAL SCOPE : fe80::250:79ff:fe66:6801/64
GLOBAL SCOPE    : 2001:db8:2::2/64
ROUTER LINK-LAYER :
MAC            : 00:50:79:66:68:01
LPORT          : 10022
RHOST:PORT     : 127.0.0.1:10023
MTU            : 1500

PC3> ip 2001:db8:3::2
PC3 : 2001:db8:3::2/64

PC3> save
Saving startup configuration to startup.vpc
. done

PC3> show ipv6

NAME           : PC3[1]
LINK-LOCAL SCOPE : fe80::250:79ff:fe66:6802/64
GLOBAL SCOPE    : 2001:db8:3::2/64
ROUTER LINK-LAYER :
MAC            : 00:50:79:66:68:02
LPORT          : 10008
RHOST:PORT     : 127.0.0.1:10009
MTU            : 1500

PC4> ip 2001:db8:4::2
PC4 : 2001:db8:4::2/64

PC4> save
Saving startup configuration to startup.vpc
. done

PC4> show ipv6

NAME           : PC4[1]
LINK-LOCAL SCOPE : fe80::250:79ff:fe66:6803/64
GLOBAL SCOPE    : 2001:db8:4::2/64
ROUTER LINK-LAYER :
MAC            : 00:50:79:66:68:03
LPORT          : 10010
RHOST:PORT     : 127.0.0.1:10011
MTU            : 1500

PC5> ip 2001:db8:5::2
PC5 : 2001:db8:5::2/64

PC5> save
Saving startup configuration to startup.vpc
. done

PC5> show ipv6

NAME           : PC5[1]
LINK-LOCAL SCOPE : fe80::250:79ff:fe66:6804/64
GLOBAL SCOPE    : 2001:db8:5::2/64
ROUTER LINK-LAYER :
MAC            : 00:50:79:66:68:04
LPORT          : 10012
RHOST:PORT     : 127.0.0.1:10013
MTU            : 1500

PC6> ip 2001:db8:6::2
PC6 : 2001:db8:6::2/64

PC6> save
Saving startup configuration to startup.vpc
. done

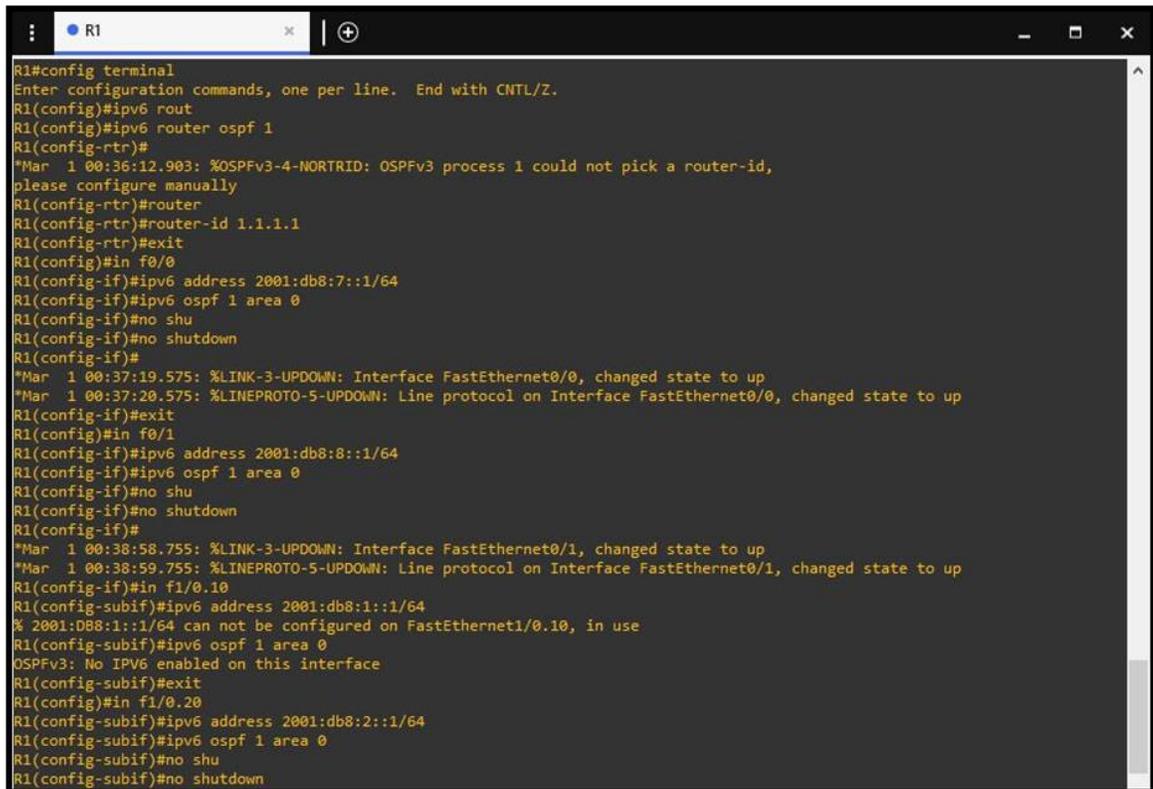
PC6> show ipv6

NAME           : PC6[1]
LINK-LOCAL SCOPE : fe80::250:79ff:fe66:6805/64
GLOBAL SCOPE    : 2001:db8:6::2/64
ROUTER LINK-LAYER :
MAC            : 00:50:79:66:68:05
LPORT          : 10014
RHOST:PORT     : 127.0.0.1:10015
MTU            : 1500
```

Fuente: Elaboración propia

Para realizar la configuración en los switch y en las interfaces de los routers, todo eso se hizo en él putty. En la figura 9 se muestra la interfaz.

Figura 9. Interfaz Gigabit Ethernet



```
R1#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 rout
R1(config)#ipv6 router ospf 1
R1(config-rtr)#
*Mar 1 00:36:12.903: %OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,
please configure manually
R1(config-rtr)#router
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#exit
R1(config)#in f0/0
R1(config-if)#ipv6 address 2001:db8:7::1/64
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#no shu
R1(config-if)#no shutdown
R1(config-if)#
*Mar 1 00:37:19.575: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:37:20.575: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#exit
R1(config)#in f0/1
R1(config-if)#ipv6 address 2001:db8:8::1/64
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#no shu
R1(config-if)#no shutdown
R1(config-if)#
*Mar 1 00:38:58.755: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar 1 00:38:59.755: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R1(config-if)#in f1/0.10
R1(config-subif)#ipv6 address 2001:db8:1::1/64
% 2001:DB8:1::1/64 can not be configured on FastEthernet1/0.10, in use
R1(config-subif)#ipv6 ospf 1 area 0
OSPFv3: No IPV6 enabled on this interface
R1(config-subif)#exit
R1(config)#in f1/0.20
R1(config-subif)#ipv6 address 2001:db8:2::1/64
R1(config-subif)#ipv6 ospf 1 area 0
R1(config-subif)#no shu
R1(config-subif)#no shutdown
```

Fuente: Elaboración propia

Ejecutando los comandos `show ipv6 interface brief` y `show ipv6 route` podremos validar las rutas conectadas a cada uno de los router. En la figura 10 mostramos la configuración de la interfaz

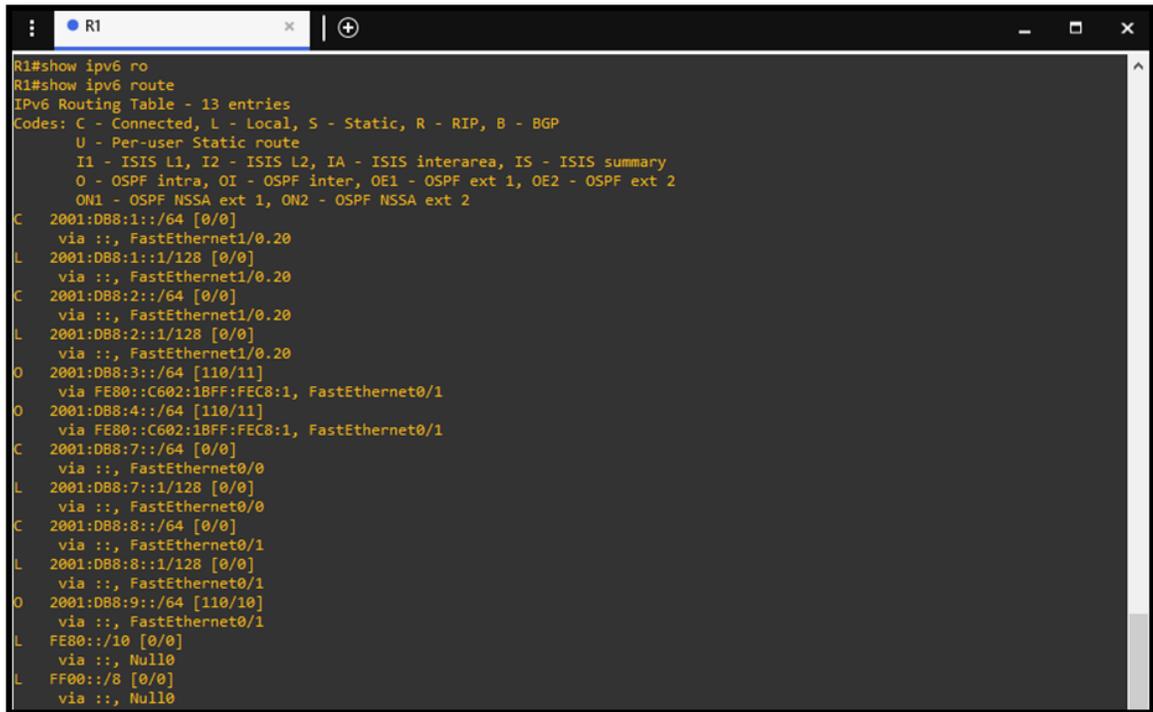
Figura 10. Show IPv6 interface brief



```
R2#show ipv6 interface brief
FastEthernet0/0      [up/up]
  FE80::C602:1BFF:FEC8:0
  2001:DB8:8::2
Serial0/0            [administratively down/down]
FastEthernet0/1      [up/up]
  FE80::C602:1BFF:FEC8:1
  2001:DB8:9::1
Serial0/1            [administratively down/down]
Serial0/2            [administratively down/down]
FastEthernet1/0      [up/up]
FastEthernet1/0.10   [up/up]
  FE80::C602:1BFF:FEC8:10
  2001:DB8:3::1
FastEthernet1/0.20   [up/up]
  FE80::C602:1BFF:FEC8:10
  2001:DB8:4::1
```

Fuente: Elaboración propia

Figura 11. Show ip route



```
R1#show ip route
R1#show ip route
IPv6 Routing Table - 13 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C 2001:D88:1::/64 [0/0]
  via ::, FastEthernet1/0.20
L 2001:D88:1::1/128 [0/0]
  via ::, FastEthernet1/0.20
C 2001:D88:2::/64 [0/0]
  via ::, FastEthernet1/0.20
L 2001:D88:2::1/128 [0/0]
  via ::, FastEthernet1/0.20
O 2001:D88:3::/64 [110/11]
  via FE80::C602:1BFF:FEC8:1, FastEthernet0/1
O 2001:D88:4::/64 [110/11]
  via FE80::C602:1BFF:FEC8:1, FastEthernet0/1
C 2001:D88:7::/64 [0/0]
  via ::, FastEthernet0/0
L 2001:D88:7::1/128 [0/0]
  via ::, FastEthernet0/0
C 2001:D88:8::/64 [0/0]
  via ::, FastEthernet0/1
L 2001:D88:8::1/128 [0/0]
  via ::, FastEthernet0/1
O 2001:D88:9::/64 [110/10]
  via ::, FastEthernet0/1
L FE80::/10 [0/0]
  via ::, Null0
L FF00::/8 [0/0]
  via ::, Null0
```

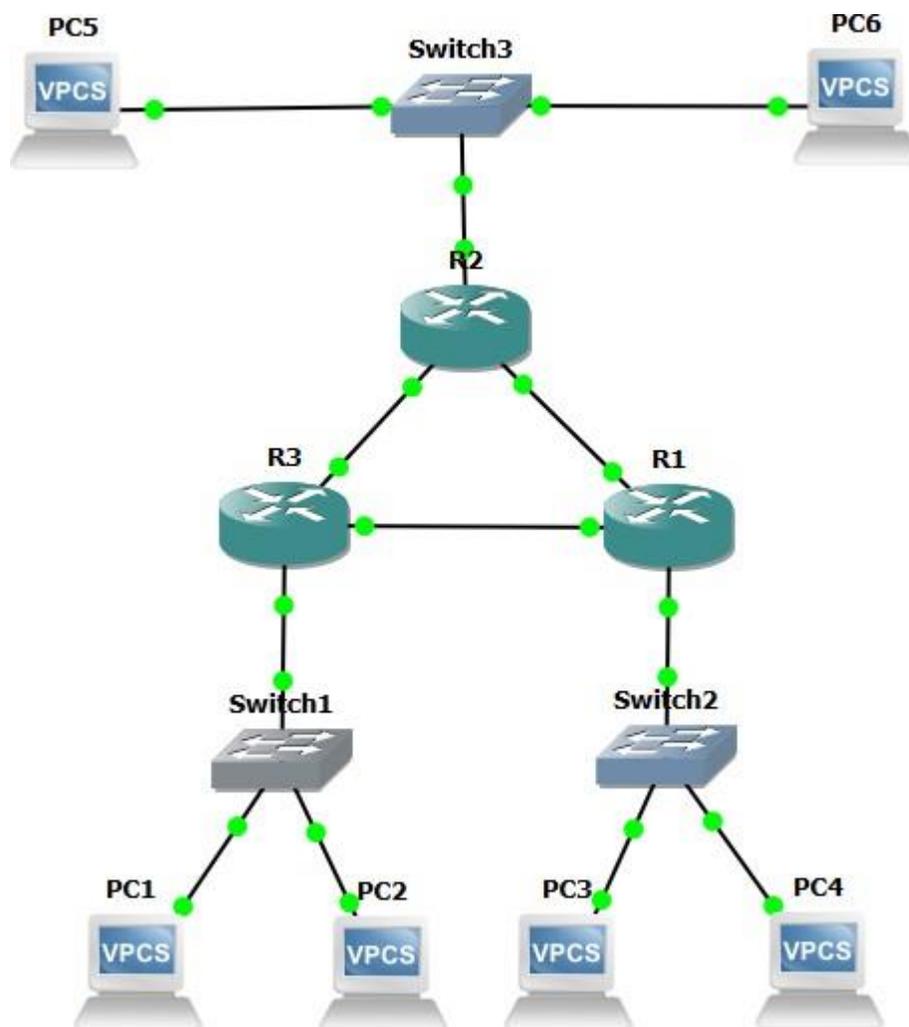
Fuente: Elaboración propia

Ya culminada la configuración de las interfaces, como podremos evidenciar en la siguiente imagen, cuando en el packet tracer todos los enlaces estén en color verde, eso quiere decir, que los paquetes se encuentran listos para transmitir y que los enlaces están activos.

9.2.1 Implementación Red IPv6

En la figura 12 se muestra la implementación de la red IPv6

Figura 12. Implementación Red IPv6



Fuente: Elaboración propia

9.2.2 Pruebas de conexión

A continuación, en la figura 13 se muestra las pruebas de conexión de los pc's, los cuales se hizo un ping desde el PC1 con IPv6 2001:DB8:1::2 al PC6 con IPv6 2001:DB8:6::2

Figura 13. Ping PC1 a PC6



```
PC1> ping 2001:db8:6::2
2001:db8:6::2 icmp_seq=1 ttl=64 time=0.001 ms
2001:db8:6::2 icmp_seq=2 ttl=64 time=0.001 ms
2001:db8:6::2 icmp_seq=3 ttl=64 time=0.001 ms
2001:db8:6::2 icmp_seq=4 ttl=64 time=0.001 ms
2001:db8:6::2 icmp_seq=5 ttl=64 time=0.001 ms
```

Fuente: Elaboración propia

Ahora, como se muestra en la figura 14, se ejecutó el comando tracert desde el PC1 al PC6 para así darnos cuenta si existe algún problema entre ambos y cómo podemos apreciar en la imagen que se identificó el número de saltos que realizó el paquete hasta completar la traza satisfactoriamente.

Figura 14. Comando Tracert

```
C:\>tracert 2001:DB8:6::2

Tracing route to 2001:DB8:6::2 over a maximum of 30 hops:

  1  3 ms      0 ms      0 ms      2001:DB8:1::1
  2  0 ms      0 ms      0 ms      2001:DB8:7::2
  3  0 ms      0 ms      0 ms      2001:DB8:6::2

Trace complete.
```

Fuente: Elaboración propia

10 Buenas practicas

- IPv6 tiene algunos componentes fundamentales que son completamente diferentes de IPv4, IT necesita hacer su tarea y aprender sobre el nuevo protocolo y cómo afectará la infraestructura y las aplicaciones.
- La capacitación en IPv6 debería extenderse al personal de TI más allá del equipo de redes, se debe entrenar a todos en todos los ámbitos y educarlos sobre lo que está sucediendo.
- Se debe realizar un inventario de la infraestructura existente. Esto incluirá una lista de todas las direcciones IPv4 de infraestructura en la red, una lista de dónde se hace referencia en todas las aplicaciones y una lista de todas las asignaciones de DNS. Esta evaluación verificaría si el proveedor de DNS externo actual es compatible con IPv6 y si los dispositivos de infraestructura son compatibles con IPv6.
- Todas las aplicaciones y dispositivos de infraestructura que no sean compatibles con IPv6 deben documentarse. El proceso y el costo necesarios para actualizarlos para admitir IPv6 deben documentarse y presentarse a la gerencia. Se debe tomar una decisión sobre si estos dispositivos y aplicaciones se deben actualizar de inmediato para admitir IPv6. Este es un paso crítico para definir el alcance de una migración IPv6.

- Los usuarios no deben observar ningún cambio significativo cuando estén trabajando sobre IPv6 o cuando están sobre IPv4, a salvo que esto suministre un beneficio claro sobre IPv6.
- La configuración remota o local deberán soportar IPv6
- Todo software tiene que soportar IPv4 e IPv6 tiene que ser lo suficientemente competente de gestionar la comunicación solo con IPv4.
- En el REC-3484 se contempla una práctica mala emplear el uso de direcciones en el código fuente.
- Exigir pruebas en diferentes entornos (IPv4, IPv6 o mixto)
- Se recomienda que las organizaciones construyan un laboratorio de pruebas que emule las operaciones fundamentales. El personal puede habilitar IPv6 en ese entorno de prueba y ver qué sucede, IPv6 a veces genera problemas inesperados con aplicaciones o hardware.
- Con base en la información que han aprendido de su capacitación, evaluaciones y pruebas, las organizaciones pueden planificar cómo desean implementar el nuevo protocolo en su entorno.

- Cuando llega el momento de desplegar IPv6 en producción se deberían hacer en pequeñas piezas donde sea un poco mas manejable. Una implementación gradual puede hacer que sea mucho más fácil lidiar con cualquier problema que ocurra, por tal motivo, la migración de IPv4 a IPv6 no es tan dolorosa y no es tan desalentadora como todo el mundo parece pensar.

Después de decidir qué enfoque usar, la organización debe desarrollar un plan de implementación de IPv6 que considere la logística de mover, convertir los dispositivos y aplicaciones a IPv6 o instalar nuevos equipos. La planificación adecuada debe reconocer el impacto potencial que la migración tendrá en los usuarios finales e identificar una estrategia para mitigar esos impactos en caso de que surjan problemas después de los cambios.

Es importante que las organizaciones sepan que esperar para abordar IPv6 conlleva un riesgo para ellos en la pérdida de comunicación y la pérdida potencial de ingresos y clientes. Es prudente comenzar a planificar ahora en preparación para el futuro. Afortunadamente, no es tan difícil como parece, y con una planificación cuidadosa, una migración de IPv6 puede ser sencilla y sin problemas para sus usuarios finales y clientes.

11 Resultado y Discusión

- Después de finalizado el proceso de transición de IPv4 a IPv6, y cumpliendo con el objetivo de realizar la transición del direccionamiento IPv4 a IPv6 según la circular 00002 del 6 de julio de 2011 y la Resolución 0002710 del 3 de octubre de 2017, normas emitidas por el MINTIC, no tendremos que preocuparnos por el agotamiento de las direcciones IP (Internet Protocol) ya que cuenta con la coexistencia de los protocolos IPv4 e IPv6 garantizando la navegación de las plataformas y servicios.
- Debido a que existen equipos que aún no son compatibles con el protocolo IPv6, es necesario mantener la coexistencia de los dos protocolos para ofrecer un servicio adecuado.
- Con la transición del protocolo IPv6 se podrá seguir manteniendo un buen servicio, ofreciendo navegación, seguridad, mayor velocidad en la conexión y transferencia en la información, mejores tiempos de respuesta, en resumen, ofrecer un mejor servicio.

12 Conclusiones

A través de esta monografía, se concluyó que, aunque la implementación de IPv6 es una necesidad, es todavía una transición gradual a pesar de las diversas ventajas asociadas con la nueva versión. IPv4 e IPv6 coexistirá durante mucho tiempo, ahora está bastante bien aceptado que la llegada de IPv6 a Internet realmente sucederá. Los defensores admiten que el progreso en la adopción de este nuevo protocolo ha sido más lento de lo que inicialmente se esperaba. Creo que la razón clave de esto es que IPv6 es evolutivo, no revolucionario, hasta que Internet realmente se quede sin espacio de direcciones, o la demanda de seguridad se vuelva más importante, la tecnología IPv6 se considerará un lujo. Sin embargo, la aceptación de IPv6 está aumentando constantemente, principalmente debido a la constatación de que los problemas que surgen en el Internet IPv4 actual deberán resolverse tarde o temprano, y que abordar estos problemas más pronto es probable que resulte en un gasto general menor. Además, IPv6 es la única solución real que tenemos para este problema inminente, ganando madurez y ampliando la comprensión.

Debido a que existen equipos que aún no son compatibles con el protocolo IPv6, como por ejemplo impresoras, servidores, aplicaciones, telefonía IP, es necesario mantener la coexistencia de los dos protocolos para ofrecer un servicio adecuado. Con la transición del protocolo IPv6 se podrá seguir manteniendo un buen servicio, ofreciendo navegación, seguridad, mayor velocidad en la conexión y transferencia en la información, mejores tiempos de respuesta, en resumen, ofrecer un mejor servicio.

En las organizaciones se deben establecer capacitaciones en IPv6 no solo al personal de TI sino a todos en los ámbitos y educarlos sobre lo que está sucediendo, IPv6 tiene algunos componentes fundamentales que son completamente diferentes de IPv4, por eso, TI necesita hacer su tarea y aprender sobre el nuevo protocolo y cómo afectará la infraestructura y las aplicaciones, por tal motivo, los usuarios no deben observar ningún cambio significativo cuando estén trabajando sobre IPv6 o cuando están sobre IPv4, a salvo, que esto suministre un beneficio claro sobre IPv6.

13 Bibliografía

RIVERO MALDONADO, Javier. TIC TIC TIC Seguridad y Privacidad de la Información para Gobierno Abierto para Servicio para la gestión manual. Estrategia de Gobierno en Línea. Disponible en: <http://docplayer.es/11095102-Tic-tic-tic-seguridad-y-privacidad-de-la-informacion-para-gobierno-abierto-para-servicio-para-la-gestion-manual-estrategia-de-gobierno-en-linea.html>

QUIROZ CEBALLOS, Maria Jose y VEGA ZAMBRANO Silvio Andres. Servicios web, mensajería y transferencia de archivos en una intranet en el colegio nacional técnico tosagua provincia de Manabí. Calceta, 2013, 15 p. Trabajo de grado (Ingeniero de Informática). Escuela superior politécnica agropecuaria de Manabí Manuel Félix López. Carrera Informática.

ALEGSA, Leandro. Definición de IPv4. Argentina. (junio 5 de 2018). [Consultado: junio 5 de 2018]. Disponible en: <http://www.alegsa.com.ar/Dic/ipv4.php>

DIAZ, Jhonathan. Tantas IP como granos de arena [blog]. ¿Todos somos un número en la red mundial? (9 de abril de 2015). [Consultado: 9 de abril de 2015]. Disponible en: <http://usuariosinfinitosipv6.blogspot.com/2015/04/todos-somos-un-numero-en-la-red-mundial.html>

ESPINOZA, Alfonso. Diseño de una estructura de redes de computadoras IPv4 e IPv6 en modalidad de pila doble (dual stack) para el inces sede de la nueva granada Caracas-Venezuela. Caracas, 2014, 55 p. Universidad Nacional Experimental.

COMPARA HOSTING. ¿qué es una dirección ip y que tipos existen? [en línea]. [Consultado: 2 de marzo de 2020]. Disponible en: <https://www.comparahosting.com/p/que-es-una-direccion-ip/>

PACHECO, Alejandro. Redes de Comunicación en la UDI [en línea]. Rangos y Clases de la IP. (5 de abril de 2016). Disponible en: <https://sites.google.com/site/redesdecomunicacionenlaudi/rangos-y-clases-de-la-ip>

CASTILLO, Jose Antonio. IPv4 vs IPv6 – Qué es y para qué se utiliza en redes [en línea]. (29 de febrero de 2020). Disponible en: <https://www.profesionalreview.com/2020/02/29/ipv4-vsipv6/#Cabecera IPv6 vs IPv4 y otras novedades>

BARRIUSO, Héctor. IPv6 (Héctor Barriuso) [Blog]. 15 de diciembre de 2010. Disponible en: <http://httpwwwbloggercomhectorbarriuso.blogspot.com/2010/>

PACHECO, Alejandro. Redes de Comunicación en la UDI [en línea]. Rangos y Clases de la IP. (5 de abril de 2016). Disponible en: <https://sites.google.com/site/redesdecomunicacionenlaudi/rangos-y-clases-de-la-ip>

VILLARREAL, Joanna. Proyecto de investigación 3 [en línea]. (26 de septiembre de 2016). Disponible en: <https://www.slideshare.net/JoannaVillarreal1/proyecto-de-investigacin-3>

ANONYMOUS. Redes Avanzadas [en línea]. Seguridad en TIC. (17 de junio de 2016). Disponible en: <http://ingredesavanzadas.blogspot.com/2016/06/enrutamiento-estatico-y-dinamico.html>

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 0002710 (03, octubre, 2017). Por el cual se establecen lineamientos para la adopción del protocolo IPv6 [en línea]. Santa Fe de Bogota, D.C.: El ministerio, 2017. 4 p. Disponible en: https://www.mintic.gov.co/portal/604/articles-61000_documento.pdf

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 00002 (06, julio, 2011) Promoción de la adopción del IPv6 en Colombia [en línea]. Santa Fe de Bogota, D.C.: El Ministerio, 2011. 4 p. Disponible en Internet: <http://www.mintic.gov.co/portal/604/w3-article-5932.html>

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 1341 (30, julio, 2009) Por lo cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones. [en línea]. Santa Fe de Bogota, D.C.: El Ministerio, 2009. 34 p. Disponible en Internet: https://www.mintic.gov.co/portal/604/articles-3707_documento.pdf

Carroll Vargas, J., Salazar Fajardo, S., & Gomez, E. J. (2019). Propuesta de métrica para evaluar los protocolos de enrutamiento y direccionamiento ip. Recuperado de: <https://revistas.unilibre.edu.co/index.php/avances/article/view/5046>

Salazar Hernandez, C., Romero Trujillo, E. (17 de septiembre de 2018). PLANEACIÓN PARA ADOPTAR EL PROTOCOLO DE INTERNET VERSIÓN 6 (IPV6) EN LA ALCALDÍA DE ACACÍAS (META). Recuperado de <http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4689/00004871.pdf?sequence=1&isAllowed=y>

14 ANEXOS

14.1 Anexos 1 (Formato RAE)

1.Información General	
Tipo de documento	Monografía Proyecto de Grado
Acceso al documento	Universidad Nacional Abierta y a Distancia UNAD
Título del documento	Esquema de transición del proceso establecido para la migración del protocolo IPv4 a IPv6 de acuerdo con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
Autor(es)	Henry Fabian Espejo Guerrero
Director	Ing. Joel Carroll
Publicación	Digitado en computador
Unidad Patrocinante	Universidad Nacional Abierta y a Distancia UNAD Programa de Especialización en Seguridad Informática
Palabras Claves	IPV4-IPV6, transición, mintic, migración, protocolo, resolución, normas, seguridad

2.Descripción
En la actualidad ha surgido una problemática ya que las direcciones IPv4 se encuentran al límite debido al gran número de usuarios que utilizan Internet a nivel mundial a través de dispositivos tecnológicos, esta investigación está basada en

identificar aspectos relevantes en la migración de IPv4 a IPv6 teniendo en cuenta la directriz establecida por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTic), es importante que todas las compañías implementen la tecnología IPv4 en coexistencia con IPv4, es de suma importancia cumplir con los protocolos establecidos con el fin de velar por la seguridad de la información.

3.Fuentes

- Salazar Hernandez, C., Romero Trujillo, E. (17 de septiembre de 2018). PLANEACIÓN PARA ADOPTAR EL PROTOCOLO DE INTERNET VERSIÓN 6 (IPV6) EN LA ALCALDÍA DE ACACÍAS (META). Recuperado de <http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4689/00004871.pdf?sequence=1&isAllowed=y>
- Carroll Vargas, J., Salazar Fajardo, S., & Gomez, E. J. (2019). Propuesta de métrica para evaluar los protocolos de enrutamiento y direccionamiento ip. Recuperado de: <https://revistas.unilibre.edu.co/index.php/avances/article/view/5046>
- Estrategia.gobiernoenlinea.gov.co. (2015). Manual de Estrategia de Gobierno en Línea. Recuperado de: http://estrategia.gobiernoenlinea.gov.co/623/propertyvalues-7751_archivo_pdf_manual.pdf
- IPv4 vs IPv6 ¿Cuál es la diferencia? (s.f). Recuperado de: <http://www.ipv6.mx/index.php/component/content/article/189-ipv4-vs-ipv6-icual-es-la-diferencia>

- Transición a IPv6. Protocolo de Internet versión 6. Ministerio de industria, tecnología y turismo de España. Consultado el 2 de noviembre de 2016.
- IPv4 vs IPv6 ¿Cuál es la diferencia? (s.f). Recuperado de:
<http://www.ipv6.mx/index.php/component/content/article/189-ipv4-vs-ipv6-icual-es-la-diferencia>
- Mintic.gov.co. (23 de octubre de 2017). Entró en vigencia la resolución 2710 del 2017 para la implementación del protocolo IPv en Colombia. Recuperado de:
<https://www.mintic.gov.co/portal/604/w3-article-61192.html> Online:
https://www.mintic.gov.co/portal/604/articles-61000_documento.pdf
- Mintic.gov.co. (2017). Circular 00002 de 2011 - Ministerio de Tecnologías de la Información y las Comunicaciones. [online] Disponible en Internet:
<http://www.mintic.gov.co/portal/604/w3-article-5932.html> [Consultado en 25 oct. 2017]

4.Contenidos

Esta monografía nos permitirá identificar la importancia de la migración Ipv4 a Ipv6 según las normas emitidas por el MINTIC donde se debe garantizar el desarrollo de los principios orientadores de la ley 1341 de 2009, donde es función del ministerio diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las tecnologías de la información y las comunicaciones, así como preparar y expedir los actos administrativos para el cumplimiento de los fines de intervención del Estado en materia de TIC. Es preciso resaltar que la versión IPv4 más usada ha entrado en su fase de agotamiento de entrega de direccionamiento restringiendo las posibilidades de conexión ya que supero su capacidad debido incremento de usuarios y dispositivos que utilizan Internet.

Esta monografía se divide en:

- Portadas, dedicatorias, aceptación, tablas de contenido
- Título
- Introducción
- Definición del problema
- Justificación
- Objetivos generales y específicos
- Marco referencial
- Resultado y discusión
- Bibliografía
- Anexos Formato RAE

5. Metodología

El plan de trabajo del presente proyecto incluyó tres etapas, comenzando con la realización de un fuerte marco teórico, avanzando hacia la instrumentación de técnicas para el manejo de personal y mitigación de posibles vulnerabilidades que se presente; luego la implementación de pruebas y validaciones técnicas y posibles contingencias que se presentaran durante la migración. Estas etapas están en total correspondencia con los objetivos trazados en el proyecto, y se pueden superponer en el tiempo en algunas ocasiones. El siguiente es la metodología específica para cada uno de los objetivos propuestos.

14.2 Etapa 1 – Revisión del estado del arte

Recopilar información acerca del protocolo ipv4 determinando la importancia de la migración a ipv6, como documentos, directrices y procesos de seguridad requeridos para la planificación y operación que ya hayan sido adaptados a los requisitos de IPv6.

Revisión del estado del arte: estudios de los avances realizados hasta el momento de las migraciones ipv4 – ipv6

14.3 Etapa 2 – Simulación de la migración ipv4 – ipv6

En esta etapa se realiza el diseño y la simulación de la migración a realizar comprendiendo las siguientes actividades:

- Elaboración de topología Gns3
- Pruebas y validación de la implementación

14.4 Etapa 3 – Construcción de la monografía



6.Conclusiones

A través de esta monografía, se concluyó que, aunque la implementación de IPv6 es una necesidad, es todavía una transición gradual a pesar de las diversas ventajas asociadas con la nueva versión. IPv4 e IPv6 coexistirá durante mucho tiempo, ahora está bastante bien aceptado que la llegada de IPv6 a Internet realmente sucederá. Los defensores admiten que el progreso en la adopción de este nuevo protocolo ha sido más lento de lo que inicialmente se esperaba. Creo que la razón clave de esto es que IPv6 es evolutivo, no revolucionario, hasta que Internet realmente se quede sin espacio de direcciones, o la demanda de seguridad se vuelva más importante, la tecnología IPv6 se considerará un lujo. Sin embargo, la aceptación de IPv6 está aumentando constantemente, principalmente debido a la constatación de que los problemas que surgen en el Internet IPv4 actual deberán resolverse tarde o temprano, y que abordar estos problemas más pronto es probable que resulte en un gasto general menor. Además, IPv6 es la única solución real que tenemos para este problema inminente, ganando madurez y ampliando la comprensión.

Debido a que existen equipos que aún no son compatibles con el protocolo IPv6, como por ejemplo impresoras, servidores, aplicaciones, telefonía IP, es necesario mantener la coexistencia de los dos protocolos para ofrecer un servicio adecuado. Con la transición del protocolo IPv6 se podrá seguir manteniendo un buen servicio, ofreciendo navegación, seguridad, mayor velocidad en la conexión y transferencia en la información, mejores tiempos de respuesta, en resumen, ofrecer un mejor servicio.

En las organizaciones se deben establecer capacitaciones en IPv6 no solo al personal de TI sino a todos en los ámbitos y educarlos sobre lo que está sucediendo, IPv6 tiene algunos componentes fundamentales que son

completamente diferentes de IPv4, por eso, TI necesita hacer su tarea y aprender sobre el nuevo protocolo y cómo afectará la infraestructura y las aplicaciones, por tal motivo, los usuarios no deben observar ningún cambio significativo cuando estén trabajando sobre IPv6 o cuando están sobre IPv4, a salvo, que esto suministre un beneficio claro sobre IPv6

Elaborado por:	Henry Fabian Espejo Guerrero
Revisado por:	

Fecha de elaboración del Resumen:	16	10	2019
--	----	----	------

14.5 ANEXO 2

14.5.1 Configuración topología de red

Configuración Switch 0

```
Switch>en
```

```
Switch#configure
```

```
Switch(config)#vlan 0
```

```
Switch(config)#vlan 3
```

```
Switch(config-vlan)#name CCA
```

```
Switch(config-vlan)#exit
```

```
Switch(config)#vlan 4
```

```
Switch(config-vlan)#name CCB
```

```
Switch(config-vlan)#exit
```

```
Switch(config)#in f0/1
```

```
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)#switchport trunk allowed vlan 3,4
```

```
Switch(config-if)#exit
```

```
Switch(config)#in f0/2
```

```
Switch(config-if)#switchport mode access
```

```
Switch(config-if)#switchport access vlan 3
```

```
Switch(config-if)#exit
```

```
Switch(config)#in          f0/3
Switch(config-if)#switchport access
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 4
Switch(config-if)#exit
Switch(config)#exit
wr
```

Configuración Switch1

```
Switch>en
Switch#configure terminal
Switch(config)#vlan 3
Switch(config-vlan)#name CCA
Switch(config-vlan)#exit
Switch(config)#vlan 4
Switch(config-vlan)#name CCB
Switch(config-vlan)#exit
Switch(config)#in f0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 3,4
Switch(config-if)#exit
Switch(config)#in f0/2
```

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#in f0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 4
Switch(config-if)#exit
Switch(config)#exit
wr
```

Configuración Switch2

```
Switch>en
Switch#configure terminal
Switch(config)#vlan 3
Switch(config-vlan)#name CCA
Switch(config-vlan)#exit
Switch(config)#vlan 4
Switch(config-vlan)#name CCB
Switch(config-vlan)#exit
Switch(config)#in f0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 3
```

```
Switch(config-if)#switchport trunk allowed vlan 4
Switch(config-if)#exit
Switch(config)#in f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#in f0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 4
Switch(config-if)#exit
Switch(config)#exit
Switch#wr
```

Router 1 Configuración

```
Router>en
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)#in g0/2
Router(config-if)#no ip address
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#in g0/0.3
Router(config-subif)#exit
Router(config)#in g0/2.3
```

```
Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ipv6 address 2001:db8:1::1/64
Router(config-subif)#ipv6 enable
Router(config-subif)#exit
Router(config)#in g0/2.4
Router(config-subif)#encapsulation dot1Q 4
Router(config-subif)#ipv6 address 2001:db8:2::1/64
Router(config-subif)#ipv6 enable
Router(config-subif)#exit
Router(config)#exit
Router#wr
```

Router 2 Configuración

```
Router>en
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)#in g0/2
Router(config-if)#no ip address
Router(config-if)#no sh
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#in g0/2.3
Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ipv6 address 2001:db8:3::1/64
Router(config-subif)#ipv6 enable
Router(config-subif)#exit
Router(config)#in g0/2.4
Router(config-subif)#encapsulation dot1Q 4
Router(config-subif)#ipv6 address 2001:db8:4::1/64
```

```
Router(config-subif)#ipv6 enable
Router(config-subif)#exit
Router(config)#exit
Router#wr
```

Router 0 Configuración

```
Router>en
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)#in g0/2
Router(config-if)#no ip address
Router(config-if)#no sh

Router(config-if)#exit
Router(config)#in g0/2.3
Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ipv6 address 2001:db8:5::1/64
Router(config-subif)#ipv6 enable
Router(config-subif)#exit
Router(config)#in g0/2.4
Router(config-subif)#encapsulation dot1Q 4
Router(config-subif)#ipv6 address 2001:db8:4::1/64
Router(config-subif)#ipv6 enable
Router(config-subif)#exit
Router(config)#exit
Router#wr mem
Router#wr memory
```

