

**PROPUESTA PARA LA MIGRACIÓN DEL PROTOCOLO IPV4 A PROTOCOLO
IPV6 PARA LA SECRETARIA DEL SISBEN DE LA ALCALDIA DE TUNJA**

JUAN PABLO MONTAÑEZ PRIETO

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESPECIALIZACION EN SEGURIDAD INFORMATICA - ECBTI**

**TUNJA
2018**

**PROPUESTA PARA LA MIGRACIÓN DEL PROTOCOLO IPV4 A PROTOCOLO
IPV6 PARA LA SECRETARIA DEL SISBEN DE LA ALCALDIA DE TUNJA**

**PRESENTADO POR
JUAN PABLO MONTAÑEZ PRIETO**

Proyecto Aplicado: Proyecto de desarrollo Tecnológico

ING. FRANCISCO NICOLAS SOLARTE

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESPECIALIZACION EN SEGURIDAD INFORMATICA - ECBTI**

TUNJA

2018

Nota de Aceptación

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

DEDICATORIA

A Dios quien todo este tiempo me dio la gracia y la licencia de terminar mi carrera universitaria y graduarme como Ingeniero de Sistemas, ya que en muchos momentos quise dejar mi universidad. Él con su gracia y misericordia siempre me dio el valor de seguir hoy soy profesional de mi prestigiosa Universidad Nacional Abierta y a Distancia UNAD sede Tunja. A la virgen Santísima del Milagro de Tunja, quien es mi guía espiritual y a la cual siempre le pido con devoción ya que nunca me ha abandonado, a ella siempre acudo y ella me escucha y me guía dándome fortaleza sin dejarme desfallecer.

A mi familia quien es mi norte y mi sur, son la razón de ser, quienes todos los días me apoyan y me dan mucho valor para seguir adelante con mis estudios y trabajo siempre están conmigo dándome moral y entusiasmo.

Dedico esta especialización a la Alcaldía Mayor de la ciudad de Tunja ya que con mi cargo de celador tuve los recursos económicos para matricularme y poder realizar mis estudios. Sin mi trabajo y el tiempo que pude sacar para estudiar no hubiera sido posible terminar mi carrera.

Dedico este título de especialización a las directivas directores, tutores y compañeros quienes siempre me están retroalimentando mis aportes y dedican su valioso tiempo a explicar y corregir cada uno de los diferentes cursos buscando siempre llegar a los estudiantes con sus enseñanzas.

A las personas que trabajan en la oficina de consejería ya que aparte de ayudar académicamente siempre están al pendiente de los estudiantes cuando estuvimos tristes y en ocasiones con problemas sus consejos siempre fueron una voz de aliento cuando más lo necesite.

Juan Pablo Montañez Prieto.

AGRADECIMIENTOS

A mi Dios y a la Santísima Virgen de Milagro de Tunja por darme la salud ante todo y la gracia de terminar mi especialización. Gracias a mi familia y seres queridos por apoyarme en toda esta etapa de estudios ya sea en la carrera de ingeniería como en la especialización de una u otra forma siempre estuvieron conmigo sin dejarme desfallecer y siempre motivándome para no abandonar mis estudios.

Agradezco a la universidad Nacional Abierta y a Distancia UNAD que fue la institución que me dio la oportunidad de realizar mi carrera con su programa en mediación virtual y me permitió la oportunidad de trabajar y estudiar al mismo tiempo. A todas las personas que estuvieron involucradas de manera directa e indirecta con la realización de mi proyecto de grado por darme moral y entusiasmo para no dejar mis estudios a mitad de camino si no terminarlos con gran éxito.

A la alcaldía Mayor de Tunja por facilitarme sus instalaciones e infraestructura y darme las herramientas para poder desarrollar mi propuesta en la Secretaria del Sisbén ya que fue de mucha ayuda para realizar mi Proyecto.

Gracias a mis directores, decanos y tutores; agradezco al director de mi proyecto Doctor Salomón González por estar siempre revisando mi proyecto y es mi guía para culminar mi especialización con gran éxito.

Agradezco a todas las personas que de una u forma me ayudaron en este proceso y a culminar mis estudios. Siempre quise terminar una carrera universitaria con

todos los reconocimientos, pero no era posible ya que la mayoría de las universidades los programas tienen una mediación presencial y por mi trabajo me quedaba imposible estudiar. Un día en el 2011, alguien me comento de la Universidad Nacional Abierta y a Distancia UNAD, me dirigí a registro y control donde en ese momento fui asesorado por una persona muy amable quien me ilustro de los programas que dicta dicha universidad. Yo no lo pensé 2 veces y tome los primeros pasos e inscribí cursos intersemestrales. Hoy en día le agradezco a Dios y a la universidad ya que termine mi carrera y me encuentro terminando mi especialización en Seguridad Informática.

CONTENIDO

	Pág.
CONTENIDO	8
INTRODUCCIÓN	15
DEFINICIÓN DEL PROBLEMA	16
1.1. DESCRIPCIÓN DEL PROBLEMA	16
1.2. FORMULACIÓN DEL PROBLEMA	17
JUSTIFICACIÓN.....	18
OBJETIVOS DEL PROYECTO.....	20
1.3. OBJETIVOS GENERAL	20
1.4. OBJETIVOS ESPECÍFICOS	20
MARCO DE REFERENCIA	21
1.5. MARCO DE ANTECEDENTES DE INVESTIGACIÓN	22
1.6. MARCO TEORICO	26
1.6.1. Internet.	26
1.6.2. Protocolo TCP/IP.....	27
1.6.3. Protocolo IPv4.....	27
1.6.4. Direcciones IPv4.	29
1.6.5. Protocolo IPv6.....	30
1.6.6. Direcciones IPv6.	31
1.6.7. Características de Ipv6.....	32
1.6.8. Mecanismos de Transición Ipv6.....	33

1.6.9. Dual Stack.....	33
1.6.10. Túneles.....	34
1.6.11. Traducción.....	35
1.6.12. Guía de Transición de IPv4 a IPv6 para Colombia.....	36
1.6.13. Guía de aseguramiento del Protocolo IPv6.	39
1.6.14. La Seguridad en las Redes.	40
1.6.15. Consideraciones de Seguridad en IPv4 e IPV6.....	42
1.6.16. IPSec.....	43
1.7. MARCO CONCEPTUAL.....	44
1.8. MARCO LEGAL.....	47
1.8.1. Resolución 2710 de 2017.....	47
1.8.2. Circular Numero 00002 de 2011 MinTIC.....	48
1.8.3. Resolución 180 de 2010 UIT.....	49
1.8.4. Ley 1341 de 2009.....	49
1.9. MARCO METODOLÓGICO.....	50
1.9.1. TIPO DE INVESTIGACIÓN	50
1.9.2. ETAPAS DE LA INVESTIGACIÓN.....	51
Fase I. Planeación de IPv6	51
Fase II. Implementación del protocolo IPv6	51
Fase III. Pruebas de funcionalidad de IPv6	52
1.9.3. RECOLECCIÓN DE INFORMACIÓN.....	52
DESARROLLO DEL PROYECTO	53
1.10. INVENTARIO ACTUAL.....	53

1.11.	IMPLEMENTACIÓN DE DIRECCIONAMIENTO IPV6.....	67
1.12.	PROPUESTA DIRECCIONAMIENTO IPV6 PARA RUTAS ESTÁTICAS .	68
1.13.	PREPARACIÓN DEL LA MIGRACION A IPV6 ESCENARIO EN EL SIMULADOR PACKET TRACER.....	69
1.14.	CONFIGURACIÓN DE DIRECCIONES IPV6 EN CADA UNO DE LOS DISPOSITIVOS.....	72
1.15.	PRUEBA DE CONECTIVIDAD POR MEDIO DEL COMANDO PING	77
1.16.	CONFIGURACIÓN RUTA ESTÁTICA IPV6 DE SIGUIENTE SALTO.....	79
1.17.	COMANDO TRACERT	84
	RESULTADOS DE LA MIGRACION PROTOCOLO IPV4 A IPV6	86
1.18.	HABILITACIÓN DE PROTOCOLOS IPV4 E IPV6.....	86
1.19.	CONFIGURACIÓN AVANZADA DE IPV6	88
1.20.	PRUEBAS DE CONECTIVIDAD.....	92
1.21.	HOJA DE RUTA PARA LA IMPLEMENTACION DE IPv6	94
	CONCLUSIONES	98
	RECOMENDACIONES.....	100
	BIBLIOGRAFÍA.....	101
	ANEXOS	105

Lista de Figuras

	Pág.
Figura 1. Clases de Direcciones IPv4	30
Figura 2. Formato básico de las direcciones IPv6	31
Figura 3. Dual Stack	34
Figura 4. Túneles	35
Figura 5. Traducción	36
Figura 6. Fases de Transición. Guía de Transición de IPv4 a	38
Figura 7. Pilares de La Seguridad de la Información en Ipv6. Guía de aseguramiento del Protocolo IPv6 MinTIC.....	39
Figura 8. Ciclo de Vida de la Seguridad en Redes	41
Figura 9. ¿Porque se debe migrar a IPv6?	44
Figura 10. Inventario equipos activos con ayuda de SW Network Inventory Advisor	55
Figura 11. Inventario de direcciones IPv4. SW Network Inventory Advisor	56
Figura 12. Inventario de Hardware equipos. SW Network Inventory Advisor.....	56
Figura 13. Inventario de Sistemas Operativos. SW Network Inventory Advisor	57
Figura 14. Inventario de Grupos de Trabajo y Subredes. SW Network Inventory Advisor.....	58
Figura 15. Dependencia Secretaria Del Sisben Que Pertenece A La Alcaldía Mayor De Tunja	61
Figura 16. Dependencias Secretaria Del Sisben Que Pertenece A La Alcaldía Mayor De Tunja. Oficina de Aseguramiento y Ventanilla.....	62
Figura 17. Equipos Físicos con Protocolo de Seguridad Ipv4.....	63
Figura 18. Topología Física actual Secretaria de Sisben Alcaldía Tunja	64
Figura 19. Topología Física. Equipos Networking Secretaria Sisben Alcaldía Tunja	65

Figura 20. Topología Física actual Secretaria de Sisben Alcaldía Tunja Packet Tracert	66
Figura 21. Tipos de Rutas Estáticas IPv6	67
Figura 22. Definición de Dispositivos en Packet Tracert.....	69
Figura 23. Configuración de adaptadores de Red - Routers.....	70
Figura 24. Configuración de Interfaz.....	71
Figura 25. Configuración de IPV6 en los PC	72
Figura 26. Configuración IPv6 Intefaz GigabitEthernet	73
Figura 27. Comando show ip route	75
Figura 28. Implementación Segmentos de Red IPv6.....	76
Figura 29. Prueba de conectividad IPv6	79
Figura 30. Configuración ruta estatica proximo salto (IPv6)	80
Figura 31. Comprobación de Rutas Estáticas R1	81
Figura 32. Comprobación rutas Estáticas R2 R3.....	82
Figura 33. Comprobación de conectividad PC1 PC2.....	83
Figura 34. Envío de paquetes IPv6.....	84
Figura 35. Comando Tracert.....	85
Figura 36. Propiedades del adaptadores de Red.....	86
Figura 37. Propiedades de los Protocolos IPv4 IPv6	87
Figura 38. Verificación de dirección IP.....	87
Figura 39. Configuración avanzada TCP/IP	88
Figura 40. Configuración manual de IPv6.....	88
Figura 41. Comprobación de conectividad IPv6 comando Ping.....	90
Figura 42. Configuración DNS Protocolo IPv6	91
Figura 43. Pruebas DNS equipos IPv6 Secretaria Sisben	92
Figura 44. Coexistencia del protocolo IPv4 IPv6 Secretaria Sisben	93
Figura 45. Pruebas de migración IPv4 a IPv6 Secretaria Sisben.....	93
Figura 46. Pruebas de migración IPv4 a IPv6 Secretaria Sisben (parte 2)	94
Figura 47. Guía de Implementación Ipv6	95

Lista de Tablas

	Pág.
Tabla 1. Diagnostico Uno.....	53
Tabla 2. Diagnostico Dos.....	58
Tabla 3. Diagnostico Tres.....	59
Tabla 4. Propuesta de Direccionamiento IPv6.....	68

TITULO

**“PROPUESTA PARA LA MIGRACIÓN DEL PROTOCOLO IPV4 A PROTOCOLO
IPV6 PARA LA SECRETARIA DEL SISBEN DE LA ALCALDIA DE TUNJA”**

INTRODUCCIÓN

La tecnología avanza a grandes pasos esto hace que coloquen 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 avances de la tecnología que tiene la mayor relevancia en el servicio de la conectividad, ya que estos nuevos dispositivos requieren una IP o identificador único pero desafortunadamente el protocolo actual no abastece dichas demandas de cobertura.

Desde 1981 se viene utilizando la versión 4 del protocolo (o IPv4), donde operan la mayoría de las comunicaciones de internet. IPv4 usa direcciones de 32 bit, que permite un total de 2^{32} direcciones (o 4.294.967.296 direcciones en total), pero con el desarrollo de la web, las direcciones IPv4 ya se agotaron prácticamente¹.

El Protocolo IPV4 que actualmente está implementado en la secretaria del Sisben de la Alcaldía Mayor de Tunja está requiriendo de una renovación y actualización, el motivo es la cobertura, ya que los ordenadores y dispositivos se vuelvan más lentos requieren de una mejor administración y cubrir las necesidades de seguridad de prevención de amenazas y vulnerabilidades en las redes.

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

¹IBM Knowledge Center. (2016). Comparación de IPv4 y IPv6. [online] Available at: https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_73/rzai2/rzai2compipv4ip6.htm [Revisado 16 May. 2018].

DEFINICIÓN DEL PROBLEMA

1.1. DESCRIPCIÓN DEL PROBLEMA

Existe una gran problemática en las organizaciones públicas y privadas y es el agotamiento de direcciones IPv4 debido a la gran cantidad de usuarios que ahora recurren al internet esto ha aumentado de forma considerable, ya no solo se ven comprometidos los computadores o equipos de oficina, sino muchos más dispositivos tecnológicos como son todos los dispositivos móviles, los celulares entre muchos más dispositivos.

Este fenómeno se presenta también en la Secretaria de Protección Social y en especial a la oficina del Sisben de la Alcaldía Mayor de Tunja. Esta oficina tiene las funciones de vincular a los programas sociales en un porcentaje muy alto en la población Tunjana. Las familias que son vinculadas a los programas sociales se encuentran en alto grado de vulnerabilidades y no cuenta con los recursos necesarios para vivir. Esto trae mucha consecuencia en especial las personas que son más indefensas que son los niños ellos los que sufren más con la falta de recursos por parte de sus padres. Así mismo esta dependencia maneja una gran base de datos que requiere de un acceso contante de consulta de usuarios internos y externos lo que demanda de la misma manera una gran administración de la red.

En Colombia las pequeñas empresas no cuentan con una metodología clara de implementacion del protocolo IPV6 siguen trabajando con el protocolo IPV4 esto hace que los a administradores de red no cuente con los recursos necesarios para darle seguridad a las redes de sus empresa, esto está llevando a que los directivos busquen una solución para mitigar estos inconvenientes de seguridad.

Del mismo modo la masiva conexión de dispositivos a Internet y el agotamiento inminente de las direcciones IPv4, han hecho que se generen estrategias desde los entes de control como por ejemplo el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) que expidió la Resolución 2710 de 2017, "Por la cual se establecen lineamientos para la adopción del protocolo IPv6" en el país².

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.

Es por esto que las organizaciones en particular las oficinas como el SISBEN, tienen la necesidad de migrar en particular de IPV4 A IPV6, el mayor problema es que se desconoce cómo es realmente el procedimiento en la nueva nomenclatura y la compatibilidad con los protocolos de conexión y los procedimientos que se deben llevar acabo para no descuidar la parte de seguridad en la información o tener el inconveniente de ser desconectados. Es por esto, que algunas empresas se privan de dar este paso a nuevos cambios en la tecnología, siendo causa principal la falta de personal experto que pueda llevar a cabo una migración no traumática entre ambos protocolos

1.2. FORMULACIÓN DEL PROBLEMA

¿Cómo la migración del protocolo IPv4 a IPv6 ayudará o mejorar administración y la seguridad de la red en la secretaría del SISBEN de la ciudad de Tunja?

² [www.mintic.gov.co](http://www.mintic.gov.co/portal/604/w3-article-61192.html). (2017). Resolución 2710 del 2017. [online] Disponible en Internet: <http://www.mintic.gov.co/portal/604/w3-article-61192.html> [Consultado en 15 May. 2018].

JUSTIFICACIÓN

Desde los orígenes de Internet, IPv4 se convierte en el primer protocolo para su uso. Las direcciones IP se han agotado en los últimos años, lo que limita el crecimiento de nuevas redes y la interacción de los usuarios y su adecuación a las nuevas aplicaciones. La gran limitante es la asignación de nuevas IP públicas a los usuarios de diferentes organizaciones en todos los entornos, productivos, sociales y comerciales.

En la actualidad, se necesitan de un nuevo protocolo con características adecuadas a los tipos de tráfico de datos, ya que el número de usuarios que acceden a la red desde diversos dispositivos móviles principalmente aumenta exponencialmente.

Gracias al interés de todos los sectores que interactúan en la Web, surge el protocolo IPV6 o IPng (Protocolo de Internet de Nueva generación), el cual tiene como principal función eliminar las barreras presentadas en el protocolo IPv4, agotamiento de direcciones IP, la seguridad de la información, lo que permite mantener una transmisión más confiable y segura con mayor calidad del servicio³.

Esta labor está siendo incentivada desde el Ministerio de las TIC quien emitió la circular 002/2011, mediante la cual busca que todas las entidades que hagan parte del programa de Gobierno en línea, empiecen a llevar a cabo los estudios para la migración al protocolo IPV6. La secretaria del Sisben de la Alcaldía de Tunja no es la excepción.

³ Eveliux.com. (2004). IPv6: El protocolo del Internet de la nueva generación. [online] Disponible en Internet: <http://www.eveliux.com/mx/IPv6-El-protocolo-del-Internet-de-la-nueva-generacion.html>. [Consultado en 16 May. 2018].

También se puede ver que esta nueva 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. Todo esto está concebido en el Manual de Gobierno en Línea⁴.

Con la realización de la propuesta de migración del protocolo IPv4 a IPv6 para mejorar la conectividad en la Secretaría del Sisben se pretende articular sus funciones con el programa de Gobierno en línea, garantizando la articulación con el Ministerio de las TIC y aprovechando la capacidad casi ilimitada de esta nueva versión de protocolo de 128 bits lo cual equivale a tener $2^{128} = 340.283.366.920.938.463.374.607.431.768.211.456$ direcciones de IP, esta cantidad de nuevas direcciones podrán ser utilizadas por millones de usuarios que requieran servicios en las diferentes plataformas que necesiten las diferentes direcciones IP. Como son las páginas WEB, los dispositivos móviles como teléfonos celulares.

El proyecto pretende mejorar la conectividad y seguridad de la red en esta secretaria y con el éxito de la propuesta se pretende ampliar al resto de las secretarías que pertenecen a la Alcaldía Mayor de Tunja.

⁴ estrategia.gobiernoenlinea.gov.co. (2015). Manual de Estrategia de Gobierno en Línea. [online] Disponible en Internet: http://estrategia.gobiernoenlinea.gov.co/623/propertyvalues-7751_archivo_pdf_manual.pdf. [Consultado en 14 May. 2018].

OBJETIVOS DEL PROYECTO

1.3. OBJETIVOS GENERAL

Desarrollar una propuesta para la migración del protocolo de INTERNET IPv4 al protocolo IPv6 y mejorar la seguridad y la administración de la red en la Secretaria del Sisben de la Alcaldía de Tunja.

1.4. OBJETIVOS ESPECÍFICOS

Revisar la información conceptual, el estado actual de los equipos, dispositivos de comunicaciones, características del protocolo actual que es IPv4 y las ventajas de Implementar el protocolo de Internet IPv6 en la Secretaria del Sisben de la Alcaldía del municipio de Tunja.

Diseñar el plan de pruebas de migración del protocolo IPv4 a IPv6 y sus requerimientos de acuerdo a las especificaciones técnicas para realizar el proceso bien configurado.

Elaborar una guía para la migración del protocolo IPv4 a IPv6 que muestre los procesos de instalación, configuración y resultados de pruebas y las ventajas que conllevan a cambiar el direccionamiento.

MARCO DE REFERENCIA

En la actualidad internet ha pasado hacer formar y parte de un medio de comunicación necesario y fundamental en las sociedades, en cualquier espacio, ya sea financiero, económico, telecomunicaciones, académico, etc., es una excelente herramienta para cualquier aplicación o tarea que se desee realizar. El agotamiento de las direcciones IPV4 protocolo actual de Internet, ha sido una preocupación desde los años 80 ya que la cantidad de usuarios que ahora recurren a Internet está en aumento de forma considerable ya que aparte de los computadores hay muchos dispositivos móviles que también necesitan estar conectados.

El nuevo Protocolo de Internet versión 6 (IPv6), es la nueva versión de protocolo diseñada para solucionar esta limitación; dado que el crecimiento de Internet y su uso es continuo a nivel mundial. IPv6 modifica el formato de la cabecera, así como en la forma de direccionar los nodos, ahora los campos ya no serán campos de 8 bits representados en forma decimal, sino que serán campos de 16 bits representados en forma hexadecimal, lo cual cambia la forma de direccionar, así como elimina o cambia algunas herramientas de enrutamiento y gestión que se venían utilizando con IPv4.

El esfuerzo del cambio va a recaer en los proveedores de servicios de Internet, los operadores de red y los grandes portales. Algunas agencias gubernamentales en Estados Unidos ya han implantado IPv6. El usuario doméstico no debería notar nada, aunque a medio plazo tal vez se necesita cambiar el router⁵.

⁵ Genbeta.com. (2017). Las últimas direcciones IPv4 se han agotado, IPv6 es la solución. [online] Available at: <https://www.genbeta.com/actualidad/las-ultimas-direcciones-ipv4-se-han-agotado-ipv6-es-la-solucion> [Revisado 23 Nov. 2017].

1.5. MARCO DE ANTECEDENTES DE INVESTIGACIÓN

- DISEÑO DE LA TRANSICIÓN DEL PROTOCOLO IPV4 HACIA IPV6 EN LA AGENCIA COLOMBIANA PARA LA REINTEGRACIÓN-ACR CON BASE EN CONSIDERACIONES DE SEGURIDAD EN IMPLEMENTACIÓN DE IPV6

Autores: Diego Ferney Ramírez Pulido, Jaime Guzmán Pantoja, Jesús Alirio Beltrán Días⁶. Universidad Católica de Colombia Facultad de ingeniería. Programa de Especialización en Seguridad de la información. Bogotá D.C- 2015.

El objetivo principal de este proyecto fue proponer una guía de transición de IPv4 hacia IPv6 en el segmento de servidores que se exponen a internet en la Agencia Colombiana para la Reintegración (ACR) con base en consideraciones de seguridad en implementaciones realizadas sobre IPv6.

Este proyecto permite identificar la importancia de la implementación de IPv6 en las entidades del estado y su articulación con las políticas de Gobierno en Línea. Así mismo establece políticas de seguridad a nivel de red y de conectividad lo que mejorara los servicios ofrecidos por la entidad.

- MIGRACIÓN DE RED IPV4 A IPV6 SOBRE LA RED DEL EJÉRCITO NACIONAL

Autores: Gómez Prieto, Nancy F.; Torres Rojas, Yudy A⁷.Universidad Nacional Abierta y A Distancia UNAD. 2012

⁶ Repository.ucatolica.edu.co. (2017). Citar un sitio web - Cite This For Me. [online] Disponible en Internet: <http://repository.ucatolica.edu.co/bitstream/10983/2803/1/IPV6.pdf> [Consultado en 7 Nov. 2017].

⁷ Gómez Prieto, N. and Torres Rojas, Y. (2017). Migración de red IPV4 A IPV6 sobre la red del Ejército Nacional. [online] Hdl.handle.net. Disponible en Internet: <http://hdl.handle.net/10596/1570> [Consultado el 7 Dec. 2017].

El proyecto cubre la investigación preliminar de las tecnologías existentes, sus ventajas y desventajas, comparándolas entre sí para justificar la migración de IPv4 a IPv6 realizando un análisis de riesgos en cuanto a tecnología y recursos. El resultado de esta investigación es una propuesta técnica para ser evaluada por los encargados del área de Tecnologías de Información.

Este proyecto permitió evaluar los conocimientos requeridos para lograr los alcances de la migración de protocolo IPv6, presenta una guía básica de los principales requisitos a tener en cuenta en cualquier entidad que desea incorporar funcionalidades que mejoran su comportamiento en aspectos de seguridad y configuración.

- **ESTRATEGIA DE MIGRACIÓN DE IPv4 A IPv6 PARA LAS PYMES EN COLOMBIA**

Autor: Arias Pulgarín, Héctor Fabio⁸. Universidad Católica de Pereira, Programa Ingeniería De Sistemas Y Telecomunicaciones. Pereira 2011.

El proyecto realiza un análisis en Colombia en donde las PYMES se encuentran trabajando hoy en día sobre IPv6, unas porque no han visto la necesidad de la migración de IPv4 a IPv6 y otras porque temen este cambio debido a que no cuentan con personal capacitado. Es por eso que el proyecto busca construir el soporte documental que permita a los administradores de redes de las diferentes PYMES de Colombia, analizar los aspectos teóricos y técnicos asociados a la migración hacia el nuevo protocolo de internet, aportando además, un estudio y análisis acerca de la nueva nomenclatura del protocolo "IPV6", con el fin de garantizar un manejo adecuado a la información de las organizaciones.

⁸ Repositorio.ucp.edu.co. (2017). Citar un sitio web - Cite This For Me. [online] Disponible en Internet: <http://repositorio.ucp.edu.co:8080/jspui/bitstream/10785/958/1/CDMIST45.pdf> [Revisado 7 Dec. 2017].

Este trabajo de investigación aporta al proyecto, que la implementación de IPv6 es muy importante ya que permite manejar múltiples direcciones por interfaz de dispositivo haciendo la ruta simple y eficiente. En el caso de Ipv4, las direcciones tienen muy poca o ninguna conexión con los caminos de enrutamiento, por lo tanto, los enrutadores deben mantener enormes tablas de caminos de enrutamiento, mientras que en Ipv6 los enrutadores mantienen pequeñas tablas de prefijos que permiten que la fuente envíe los paquetes al destino correcto.

- MECANISMOS DE TRANSICIÓN DE IPV4 A IPV6

Autores: Correa, Adelaida. Candamil, Martha Lucia⁹. Universidad Libre Facultad De Ingeniería De Sistemas. Bogotá 2010

El objetivo general de este proyecto fue planificar, implementar y emular los mecanismos de transición del protocolo IPV4 a IPV6 configurando y verificando los servicios de red sobre la plataforma 2003 Server Enterprise Edition Windows XP, y planificar los servicios de red utilizando los protocolos IPV4 e IPV6 que se puedan implementar en una red empresarial estándar.

Este proyecto muestra de manera detallada la configuración de IPv6 en entornos multiusuarios, redes de cobertura WAN y la implementación del (Network address translation-protocols translation) es un mecanismo que permite que los nodos IPv6 se comuniquen con nodos IPv4 de forma transparente utilizando una única dirección IPv4. También muestra la configuración de DNS IPv6 tanto en Cliente como Servidor. También permite identificar características propias de los túneles que proporcionan un mecanismo para utilizar la infraestructura IPv4 mientras la infraestructura IPv6 está siendo implantada. Este mecanismo consiste en enviar datagramas IPv6 encapsulados en paquetes IPv4.

⁹ Repository.unilibre.edu.co. (2017). Citar un sitio web - Cite This For Me. [online] Disponible en Internet: <http://repository.unilibre.edu.co/bitstream/handle/10901/8797/MONOGRAFIA%20MECANISMOS%20DE%20TRANSICIÓN%20DE%20IPV4%20A%20IPV6.pdf?sequence=1> [Revisado 7 Dec. 2017].

- ELABORACIÓN DE UNA GUÍA ABIERTA PARA LA ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD EN EL PROTOCOLO DE INTERNET IPv6 SOBRE ESTÁNDARES DE ENRUTAMIENTO DINÁMICO EN EQUIPOS CON PLATAFORMA CISCO

Autor: Sabogal Ortiz, Arth Grossy¹⁰.Universidad Nacional Abierta y A Distancia UNAD. 2017.

Este proyecto permite identificar y estructurar las técnicas y mejoras para la administración de seguridad sobre estándares de enrutamiento dinámico ejecutado en equipos con plataforma CISCO, mediante la elaboración de una guía abierta de seguridad basada en el análisis de riesgo en el protocolo de internet IPV6.

Como aporte a la investigación este proyecto muestra de manera detallada los aspectos de la Seguridad por defecto en IPv6, así como las vulnerabilidades y el uso de la autenticación de origen de datos, confidencialidad, integridad en un esquema no orientado a la conexión. Permite establecer los requisitos mínimos para la creación de una guía rápida que determine múltiples vulnerabilidades en IPv6, análisis y tratamiento de mitigación del riesgo, junto con múltiples recomendaciones útiles para los administradores de red.

¹⁰ Stadium.unad.edu.co. (2017). Citar un sitio web - Cite This For Me. [online] Disponible en Internet: <http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/12015/1/14703624.pdf> [Revisado 7 Dec. 2017].

1.6. MARCO TEORICO

1.6.1. Internet.

El nombre Internet¹¹ procede de las palabras en inglés Interconnected Networks, que significa “redes interconectadas”. Internet es la unión de todas las redes y computadoras distribuidas por todo el mundo, por lo que se podría definir como una red global en la que se conjuntan todas las redes que utilizan protocolos TCP/IP y que son compatibles entre sí.

En esta “red de redes” como también es conocida, participan computadores de todo tipo, desde grandes sistemas hasta modelos personales. En la red se dan citas instituciones oficiales, gubernamentales, educativas, científicas y empresariales que ponen a disposición de millones de personas su información.

Internet¹² fue el resultado de un experimento del Departamento de Defensa de Estados Unidos, en el año 1969, que se materializó en el desarrollo de arpanet, una red que enlazaba universidades y centros de alta tecnología con contratistas de dicho departamento. Tenía como fin el intercambio de datos entre científicos y militares. A la red se unieron nodos de Europa y del resto del mundo, formando lo que se conoce como la gran telaraña mundial (World Wide Web). En 1990 ARPAnet dejó de existir.

¹¹ Definista (2017). ¿Qué es Internet? - Su Definición, Concepto y Significado. [online] Conceptodefinicion.de. Disponible en Internet: <http://conceptodefinicion.de/internet/> [Revisado 23 Nov. 2017].

¹² Ibid.

1.6.2. Protocolo TCP/IP.

TCP/IP¹³ (Transmission Control Protocol/Internet Protocol), más que un protocolo, TCP/IP es un conjunto de protocolos de red, capaces de soportar las comunicaciones entre equipos conectados a gran número de redes heterogéneas, independientes de un vendedor. Su origen es: solucionar las comunicaciones a través de la red ARPANET para el Departamento de Defensa de USA (Department of Defense 1.972). Comienza su utilización en DARPA (Agencia de proyectos de investigación avanzada para la defensa). En 1983 se convierte en estándar para DoD (ARPANET + MILNET) (Defense Data Network DDN). Sus principales características son:

- Utiliza conmutación de paquetes.
- Proporciona una conexión fiable entre dos máquinas en cualquier punto de la red.
- Ofrece la posibilidad de interconectar redes de diferentes arquitecturas y con diferentes sistemas operativos.
- Se apoya en los protocolos de más bajo nivel para acceder a la red física (Ethernet, Token-Ring).

1.6.3. Protocolo IPv4.

IPv4 es la versión 4 del Protocolo de Internet (IP o Internet Protocol)¹⁴ y constituye la primera versión de IP que es implementada de forma extensiva. IPv4 es el principal protocolo utilizado en el Nivel de Red del Modelo TCP/IP para Internet.

¹³ Rodin.uca.es. (2017). Cite a Website - Cite This For Me. [online] Disponible en Internet: http://rodin.uca.es/xmlui/bitstream/handle/10498/16833/temaII_tcpip.pdf [Revisado 23 Nov. 2017].

¹⁴ Alcancelibre.org. (2017). Introducción a IP versión 4. - Alcance Libre. [online] Disponible en Internet: <http://www.alcancelibre.org/staticpages/index.php/introduccion-ipv4> [Revisado 23 Nov. 2017].

Fue descrito inicialmente en el RFC 791 elaborado por la Fuerza de Trabajo en Ingeniería de Internet (IETF o Internet Engineering Task Force) en Septiembre de 1981, documento que dejó obsoleto al RFC 760 de Enero de 1980.

IPv4 es un protocolo orientado hacia datos que se utiliza para comunicación entre redes a través de interrupciones (switches) de paquetes (por ejemplo a través de Ethernet), el propósito principal de IP es proveer una dirección única a cada sistema para asegurar que una computadora en Internet pueda identificar a otra. Tiene algunas de las siguientes características:

- Es un protocolo de un servicio de datagramas no fiable (también referido como de mejor esfuerzo).
- No proporciona garantía en la entrega de datos.
- No proporciona ni garantías sobre la corrección de los datos.
- Puede resultar en paquetes duplicados o en desorden.

IPv4 utiliza direcciones de 32 bits (4 bytes) que limita el número de direcciones posibles a utilizar a 4, 294, 967,295 direcciones únicas. Sin embargo, muchas de estas están reservadas para propósitos especiales como redes privadas, Multidifusión, etc. Debido a esto se reduce el número de direcciones IP que realmente se pueden utilizar, es esto mismo lo que ha impulsado la creación de IPv6 (actualmente en desarrollo) como reemplazo eventual dentro de algunos años para IPv4.

1.6.4. Direcciones IPv4.

Como referencia¹⁵ para entender el por qué el espacio de direcciones IPv4 es limitado a 4.3 mil millones de direcciones, se puede 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 se empieza 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 direcciones. Para ponerlo de otra forma, se tienen 32 bits entonces, 2 elevado a la 32va potencia te dará el mismo número obtenido.

Las direcciones IP se clasifican en 5 clases: A, B, C, D y E. El factor que va a determinar la clase de una IP va a ser el octeto 1. En la actualidad se usan sólo las clases A, B y C, las clases D y E, se usan sólo para fines de estudio e investigación (Figura 1).

¹⁵ Cantu, D. (2017). IPv4 vs IPv6 - ¿Cuál es la diferencia?. [online] ipv6.mx. Disponible en Internet: <http://ipv6.mx/index.php/component/content/article/189-ipv4-vs-ipv6-icual-es-la-diferencia> [Revisado 23 Nov. 2017].

Figura 1. Clases de Direcciones IPv4



Fuente: Lordratita.files.wordpress.com. (2017). Cite a Website - Cite This For Me. [en línea] Available at: <https://lordratita.files.wordpress.com/2012/06/sin-tc3adtulo5.jpg>.

1.6.5. Protocolo IPv6.

El Protocolo de Internet versión 6 (Internet Protocol version 6, IPv6)¹⁶, se constituye en la nueva alternativa al agotamiento de direcciones disponibles a nivel mundial del protocolo IPv4. Debido al crecimiento del Internet y la sofisticación de los dispositivos electrónicos, las soluciones propuestas con el fin de escalar el espacio de direccionamiento de Internet IPv4, no serán suficientes para cubrir la necesidad de las mismas en los próximos años. Como consecuencia de este escenario, el Grupo Especial sobre Ingeniería de Internet (Internet Engineering Task Force o IETF, por sus siglas en inglés) elaboró una serie de especificaciones para definir un protocolo IP de Siguiete Generación (IP Next Generation, IPng) que actualmente se conoce como Protocolo de Internet versión 6.

¹⁶ Ipv6.mx. (2017). Fundamentos IPv6. [online] Disponible en Internet: <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6> [Revisado 23 Nov. 2017].

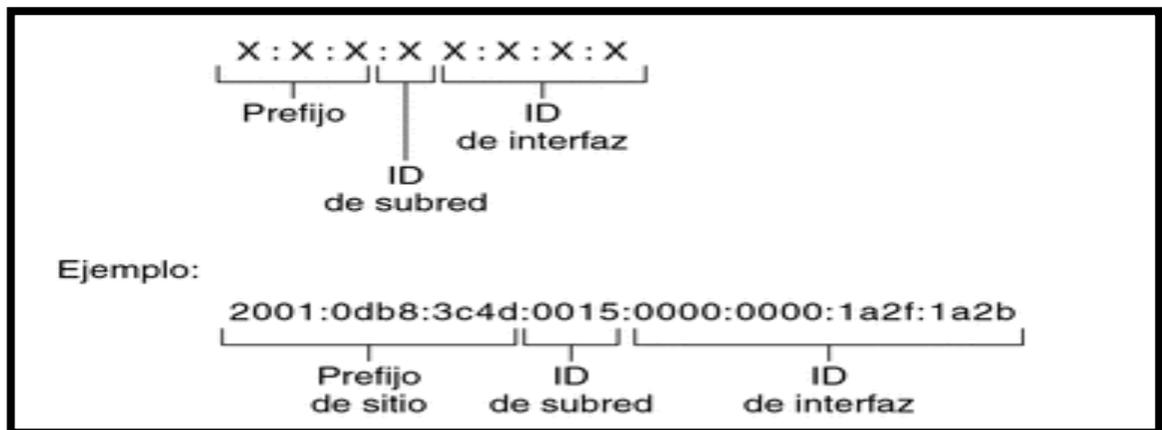
1.6.6. Direcciones IPv6.

Las direcciones IPv6 están basadas en 128 bits¹⁷. Se tiene 2 elevado a la 128va potencia para encontrar el total de direcciones IPv6 totales. 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, tendríamos 2 elevado a la 16 de variaciones (las cuales son 65,536 distintas posibilidades) (Figura 2). Usando números decimales de 0 a 65,535, tendríamos representada una dirección bastante larga, y para facilitararlo 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**

Figura 2. Formato básico de las direcciones IPv6



Fuente: Docs.oracle.com. (2017). Descripción general de las direcciones IPv6 (Guía de

¹⁷ ipv6.mx. (2017). Fundamentos IPv6. [online] Disponible en Internet: <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6> [Revisado 23 Nov. 2017].

administración del sistema: servicios IP). [en línea] Disponible en Internet: <https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-10/index.html>.

1.6.7. Características de Ipv6. Las direcciones IPv6 tienen características particulares que las hacen ser una nueva alternativa para la nueva etapa de la Internet¹⁸:

- El esquema de direcciones de 128 bits provee una gran cantidad de direcciones IP, con la posibilidad de asignar direcciones únicas globales a nuevos dispositivos.
- Los múltiples niveles de jerarquía permiten juntar rutas, promoviendo un enrutamiento eficiente y escalable al Internet.
- El proceso de autoconfiguración permite que los nodos de la red IPv6 configuren sus propias direcciones IPv6, facilitando su uso.
- La transición entre proveedores de IPv6 es transparente para los usuarios finales con el mecanismo de reenumerado.
- La difusión ARP es reemplazada por el uso de multicast en el link local.
- El encabezado de IPv6 es más eficiente que el de IPv4: tiene menos campos y se elimina la suma de verificación del encabezado.
- Puede hacerse diferenciación de tráfico utilizando los campos del encabezado.
- Las nuevas extensiones de encabezado reemplazan el campo Opciones de IPv4 y proveen mayor flexibilidad.
- IPv6 fue esbozado para manejar mecanismos de movilidad y seguridad de manera más eficiente que el protocolo IPv4.
- Se crearon varios mecanismos junto con el protocolo para tener una transición sin problemas de las redes IPv4 a las IPv6.

¹⁸ CCM. (2017). Protocolo IPv6. [online] Disponible en Internet: <http://es.ccm.net/contents/268-protocolo-ipv6> [Revisado 23 Nov. 2017].

- La autenticación y confidencialidad constituyen las funciones de seguridad más importantes del protocolo IPv6.

1.6.8. Mecanismos de Transición Ipv6. Ante el agotamiento de las direcciones IPv4 a nivel mundial, se han presentado múltiples problemas que está ocasionando, que países como Asia como India o China, hayan dado inicio al cambio a IPv6. La literatura de esta temática indicaba que en el 2012 este proceso ya debía estar en marcha, pues las direcciones IPv4 se terminan.

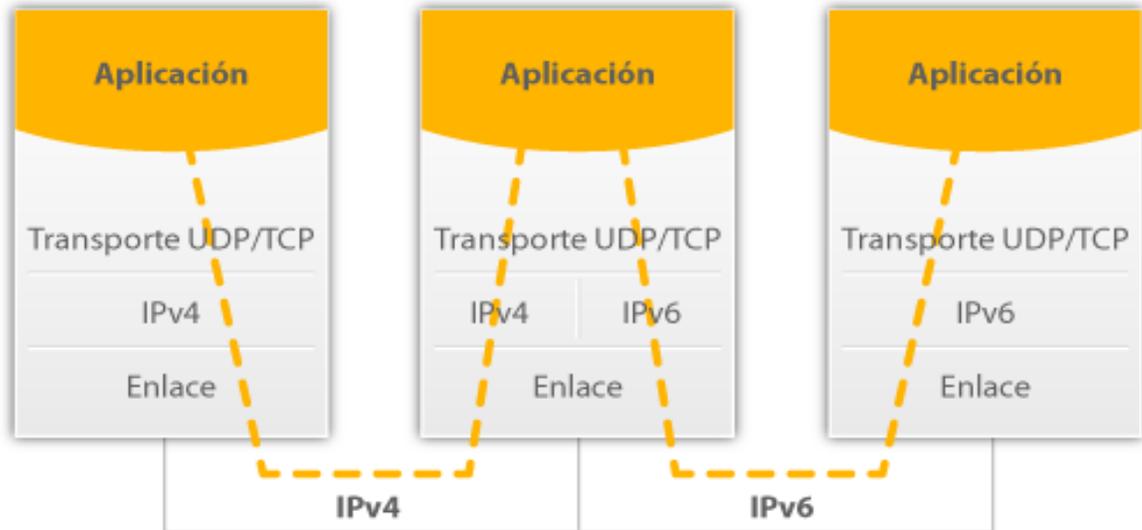
Existe una serie de mecanismos que permitirán la convivencia y la migración progresiva tanto de las redes como de los equipos de usuario¹⁹, se puede hacer una clasificación general entre los mecanismos de transición de acuerdo al tipo de técnica que se utilizan: **Dual Stack, Túneles y Traducción.**

1.6.9. Dual Stack. Es el método propuesto originalmente para tener una transición suave hacia IPv6. En este caso se necesita contar con suficiente cantidad de direcciones IPv4 para poder desplegar las dos versiones del protocolo en simultáneo en toda la red (Figura 3). De esta forma, cuando se establece una conexión hacia un destino sólo IPv4, se utilizará la conectividad IPv4 y si es hacia una dirección IPv6, se utilizará la red IPv6. En caso que el destino tenga ambos protocolos, normalmente se preferirá intentar conectar primero por IPv6 y en segunda instancia por IPv4²⁰.

¹⁹ Portalipv6.lacnic.net. (2017). Portal IPv6 - LACNIC. [online] Disponible en Internet: <http://portalipv6.lacnic.net/mecanismos-de-transicion/> [Revisado 10 Nov. 2017].

²⁰ Portalipv6.lacnic.net. (2017). Portal IPv6 - LACNIC. [online] Disponible en Internet: <http://portalipv6.lacnic.net/mecanismos-de-transicion/> [Revisado 10 Nov. 2017].

Figura 3. Dual Stack

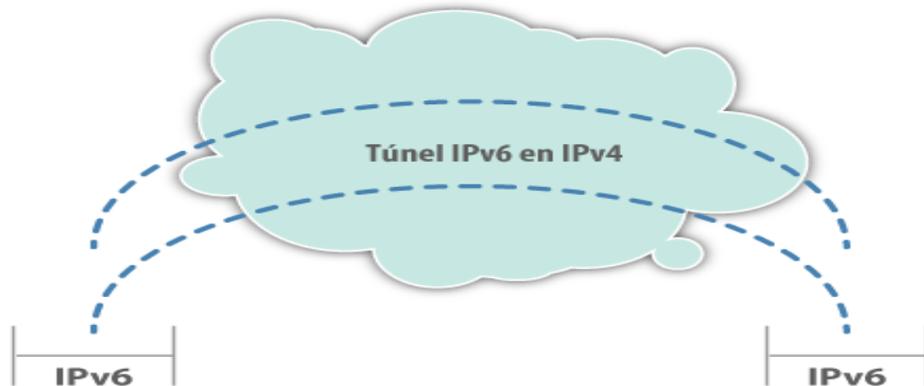


Fuente: Portalipv6.lacnic.net. (2017). Portal IPv6 - LACNIC. [en línea] Disponible en Internet: <http://portalipv6.lacnic.net/dual-stack-o-pila-doble/>.

1.6.10. Túneles. Es uno de los mecanismos más antiguos para poder atravesar redes que no tienen soporte nativo del protocolo que se está utilizando (Figura 4). En general se utilizan túneles encapsulando IPv6 dentro de IPv4, permitiendo de esta forma atravesar redes que no manejan IPv6. Los paquetes originales son transportados hasta un punto de la red por medio del protocolo original, luego encapsulados para atravesar la porción de red que no lo soporta y luego des-encapsulados en el otro extremo para ser enviados al destino final en forma nativa. Los túneles más habituales son los túneles manuales y los túneles automáticos. Los túneles manuales se deben configurar explícitamente en algún equipo de la red, mientras que los automáticos se configuran automáticamente en algunos sistemas operativos. En el caso de los primeros, se puede citar los túneles

manuales entre dos equipos o mediante “tunnel brokers”. En el segundo caso, los más conocidos son 6to4 y Teredo²¹.

Figura 4. Túneles



Fuente: Portalipv6.lacnic.net. (2017). Portal IPv6 - LACNIC. [en línea] Disponible en Internet: <http://portalipv6.lacnic.net/tunelesencapsulamiento/>

1.6.11. Traducción.

Esta técnica consiste en utilizar algún dispositivo en la red que convierta los paquetes de IPv4 a IPv6 y viceversa. Ese dispositivo tiene que ser capaz de realizar la traducción en los dos sentidos de forma de permitir la comunicación (Figura 5).

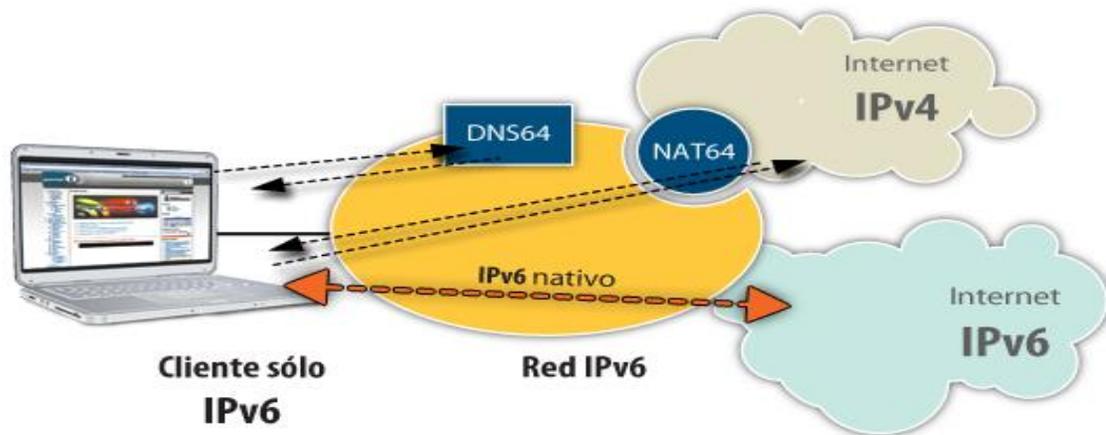
Dentro de esta clasificación se menciona NAT64/DNS64: la red es IPv6 nativa y para llegar a sitios que son sólo IPv4 se realiza una traducción al estilo NAT²², mediante un mapeo entre los paquetes IPv6 e IPv4. Se utiliza un prefijo especial

²¹ Portalipv6.lacnic.net. (2017). Portal IPv6 - LACNIC. [online] Disponible en Internet: <http://portalipv6.lacnic.net/tunelesencapsulamiento/> [Revisado 23 Nov. 2017].

²² Ibid.

para mapear direcciones IPv4 a IPv6: 64:ff9b::/96. Es necesario también utilizar una modificación al DNS, llamada DNS64, que permite generar un registro AAAA aun cuando el destino no tenga dirección IPv6 (es decir, el DNS responde sólo con registros de tipo A).

Figura 5. Traducción



Fuente: Portalipv6.lacnic.net. (2017). Portal IPv6 - LACNIC. [en línea] Disponible en Internet: <http://portalipv6.lacnic.net/traduccion/>.

Los antecedentes de la investigación se refieren a la revisión de trabajos previos sobre el tema en estudio, para el caso particular, se tomó como base la documentación del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, que es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

1.6.12. Guía de Transición de IPv4 a IPv6 para Colombia.

El Ministerio de las Tecnologías de la Información y las Comunicaciones, función de lo dispuesto en el Marco de Referencia de Arquitectura Empresarial, la Estrategia

de Gobierno en Línea y la Subdirección de Seguridad y Privacidad de TI, pone a disposición de las entidades, una guía, la cual permite a las entidades contar con una línea base para el análisis de la implementación del protocolo IPv6, de esta manera ayudar a proteger los bienes, activos, servicios, derechos y libertades dependientes del Estado²³.

Este documento presenta los lineamientos técnicos que se requieren tener en cuenta para seguir el proceso de transición de IPv4 a IPv6, en las distintas organizaciones del Estado, teniendo en cuenta su aplicación para todo el ciclo de desarrollo por fases que requiere el nuevo protocolo, en un ambiente controlado y seguro que permita consolidar una adopción del protocolo IPv6 con éxito en el país. El protocolo IPv6²⁴, permitirá que todos los dispositivos tecnológicos usados para la conexión a internet, tengan una dirección en IPv6, la cual facilitará la conectividad en banda ancha, ofreciendo mejores servicios poniéndolos al alcance de toda la población a fin de estimular y ofrecer mejores oportunidades para el desarrollo mundial.

El objetivo principal es presentar un marco de referencia para facilitar el proceso de transición de IPv4 a IPv6, que permita orientar a las Entidades del Gobierno y a la sociedad en general, en el análisis, la planeación, la implementación y las pruebas de funcionalidad del protocolo IPv6, con el fin de incentivar el proceso de adopción y despliegue del protocolo IPv6 en el país.

La guía establece los beneficios de la transición y las fases de la transición así como los requerimientos y entregables que se deben tener en cuenta a la hora de tomar la decisión de realizar una migración de IPv4 a IPv6 (Figura 6).

²³ Mintic.gov.co. (2017). Citar un sitio web - Cite This For Me. [online] Available at: http://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf [Revisado 10 Oct. 2017].

²⁴ Ibid.

Figura 6. Fases de Transición. Guía de Transición de IPv4 a



Fuente: del Autor.

Como conclusiones principales de esta guía nacional se puede resaltar que:

- Una vez culminado el proceso de transición de IPv4 a IPv6, las Entidades no tendrán que preocuparse por el agotamiento de las direcciones IP (Internet Protocol) pues se garantizará que las infraestructuras de TI, deben seguir conectadas con los dos protocolos coexistentes, ofreciendo a los usuarios múltiples oportunidades de seguir conectados y apuntar a los nuevos mercados y servicios que surgen alrededor de IPv6.
- El nuevo protocolo IPv6 permitirá a las entidades, introducir nuevas funciones que mejorarán aspectos tales como la seguridad informática, vista desde el escenario del funcionamiento del protocolo mismo, la facilidad para conectar una gran variedad de dispositivos de comunicaciones, de computación y de almacenamiento, produciendo un cambio gradual en el funcionamiento tanto de las redes de comunicaciones como de las aplicaciones que producirá resultados exitosos a mediano plazo en la medida en que este nuevo protocolo se afiance en el medio.

1.6.13. Guía de aseguramiento del Protocolo IPv6.

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones²⁵.

En este documento se presentan los lineamientos y políticas que se requieren tener en cuenta para la seguridad del protocolo IPv6, en las distintas infraestructuras de Tecnologías de la Información y las Comunicaciones que las Entidades del Estado, teniendo en cuenta su aplicación en todo el ciclo de desarrollo que sigue el nuevo protocolo, en un ambiente controlado y seguro que permita consolidar el proceso de adopción de IPv6 con seguridad y con un nivel de impacto altamente positivo para todas las organizaciones del país.

Presentar un marco de referencia sobre lineamientos de seguridad en IPv6, que sea referente para abordar el plan de diagnóstico, plan de implementación y monitoreo del proceso de transición de IPv4 a IPv6 en cada una de las Entidades del Estado, para adoptar el protocolo IPv6 con base en las características de Confidencialidad, Integridad, Disponibilidad y Privacidad de la información; a fin de generar mecanismos de direccionamiento IP de acceso seguro y uso eficiente de las infraestructuras de información y comunicación de los diferentes organismos del Estado. (Figura 7).

Figura 7. Pilares de La Seguridad de la Información en Ipv6. Guía de aseguramiento del Protocolo IPv6 MinTIC

²⁵ Mintic.gov.co. (2017). Documentos IPv6 - Ministerio de Tecnologías de la Información y las Comunicaciones. [online] Disponible en Internet: <http://www.mintic.gov.co/portal/604/w3-article-5903.html> [Revisado 23 Nov. 2017].



Fuente: del Autor.

1.6.14. La Seguridad en las Redes.

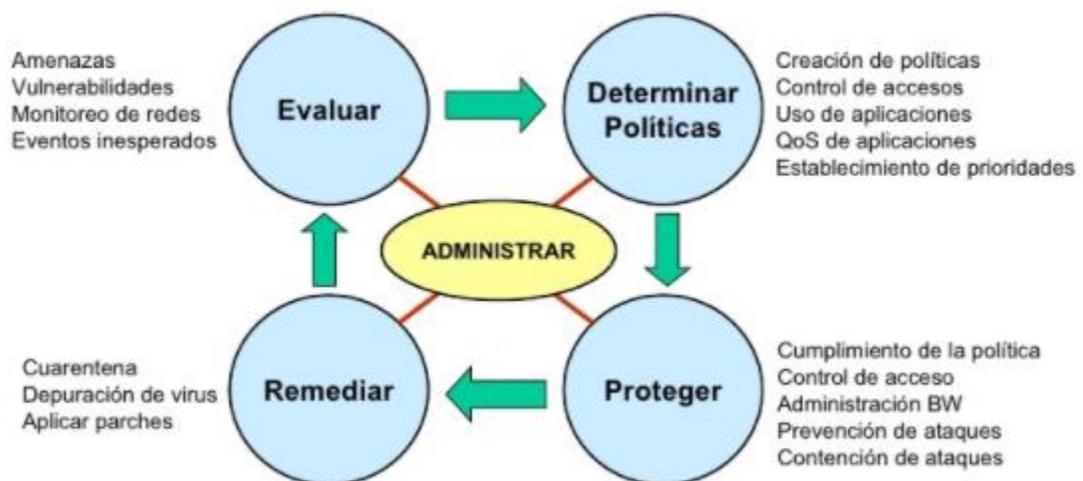
La seguridad en redes tiene el objetivo de mantener el intercambio de información libre de riesgo y proteger los recursos informáticos de los usuarios y las Organizaciones. Generalmente, se encuentra amenazada por riesgos que van de la mano con el aumento del uso de Internet en las Instituciones de todos los ámbitos. De esta forma, la Seguridad en redes es la clave para conseguir la confianza de los visitantes web y está avalada por Autoridades de Confianza como Symantec.²⁶

²⁶ Certsuperior.com. (2017). Seguridad en redes | Cert Superior. [en línea], [Accessed 13 Dec. 2017]. Disponible en Internet: <https://www.certsuperior.com/SeguridadenRedes.aspx>.

Es importante considerar que la Seguridad en redes también puede ser vulnerable desde el interior de las Organizaciones. Es decir, existen dos tipos de amenazas: internas y externas. (Figura 8).

Las amenazas internas pueden ser más serias que las externas porque los IPS y Firewalls son mecanismos no efectivos en amenazas internas, los usuarios conocen la red, saben cómo es su funcionamiento y tienen algún nivel de acceso a ella. Esta situación se presenta debido a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías y porque no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas. El resultado es la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización, lo que puede representar un daño con valor de miles o millones de dólares.

Figura 8. Ciclo de Vida de la Seguridad en Redes



Fuente: <https://www.slideshare.net/wbarriosb/seguridad-informtica-en-redes-de-computadores>

1.6.15. Consideraciones de Seguridad en IPv4 e IPV6.

El nuevo protocolo IPv6 retiene la mayoría de los conceptos básicos de IPv4. Al igual que IPv4, en IPv6 los data grama son no confiables y sin conexión. El formato de los data gramas en IPv6 es muy diferente al de IPv4. IPv6 provee nuevas funcionalidades como autenticación y seguridad. IPv6 organiza cada data grama como una secuencia de encabezados seguida de datos. Un data grama siempre comienza con un encabezado base de 40 octetos, el cual contiene las direcciones fuentes y destino y un identificador de flujo. El encabezado base puede estar seguido de 0 o más encabezados de extensión, seguido de datos. Los encabezados de extensión son opcionales; IPv6 los usa para codificar la mayoría a de las opciones de IPv4²⁷.

La arquitectura de seguridad para IPv6 está definida en RFC 2401. La meta de IP Security (IPSec) es proveer seguridad basada en criptografía, interoperable para IPv4 e IPv6. Como estas funciones de seguridad son ofrecidas en la capa IP, la protección para tanto IP como cualquier capa más alta de protocolos. IPSec habilita a un sistema seleccionar los protocolos de seguridad requeridos, determinar los algoritmos que serán usados para el servicio de seguridad, e implementar cualquier clave criptográfica que sea requerida para proveer estos servicios. IPSec puede ser usado para proteger los caminos de comunicación entre 2 hosts, entre 2 gateways de seguridad o entre un host y un gateway de seguridad.

Definido como estándar de seguridad obligatorio para IPv6 y opcional para IPv4, IPSec (IP Security) ofrece encriptación y autenticación de extremo a extremo haciendo seguras las comunicaciones TCP/IP en redes privadas y públicas.

27 Repositorio.utp.edu.co. (2017). Citar un sitio web - Cite This For Me. [en línea], [Revisado 13 Dec. 2017]. Disponible en Internet: <http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2073/004678E82.pdf;sequence=1>.

1.6.16. IPSec.

IPsec es un conjunto de protocolos abiertos que tienen como fin proporcionar seguridad en las comunicaciones de la capa de red del modelo OSI (a la que pertenece el protocolo IPv6), y de ese modo, a todos los protocolos de capas superiores. En IPv4 la implementación de IPsec se define en una especificación diferente a la del propio protocolo IPv4, por lo que la inclusión del protocolo se hace con mecanismos definidos fuera del mismo, mientras que en IPv6 la propia arquitectura "extensible" del protocolo permite implementar IPsec de forma natural²⁸.

Es importante reseñar que IPv6 habilita la posibilidad de usar IPsec, y no los mecanismos de cifrado y autenticación propios de IPsec. IPsec tiene dos modos de funcionamiento que proporcionan distintos niveles de seguridad:

- **Modo Transporte:** se cifra y/o autentica la carga útil, o payload, pero las cabeceras no se tienen en cuenta. Tiene como ventaja que se puede utilizar de extremo a extremo, pero, por contra, la información de las cabeceras, como la dirección IP de origen y destino, es visible.
- **Modo Túnel:** una plataforma, o pasarela, encapsula el paquete original en otro paquete. Con ello se cifra y/o autentica el paquete original completo, pero se necesita de una plataforma que realice el túnel.

²⁸ Incibe.es. (2017). Implementación De Ipsec. [en línea], [Revisado 13 Dec. 2017] Disponible en Internet: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_implantacion_ipv6.pdf.

1.7. MARCO CONCEPTUAL

Con el fin de desarrollar el presente proyecto se hace indispensable relacionar e identificar los conceptos más relevantes para entender para que se requiere la migración, implementación y medición de la seguridad de la red con el protocolo IPV6. Se parte del hecho de definir como pregunta base la siguiente: ¿Por qué se debe migrar a IPV6?. IPV6 es la última versión del Protocolo de Internet, está llamado a convivir con IPV4, y finalmente a sustituirlo, proporcionando un mayor espacio de direcciones que permita impulsar el crecimiento de internet en los próximos años. (Figura 9).

Figura 9. ¿Porque se debe migrar a IPV6?



Fuente: Del Autor

- **IoT**

Kevin Ashton es la persona que acuñó el término “internet de las cosas” (IoT), que hoy se utiliza para referirse a un mundo en el que todo –la casa, los electrodomésticos, el carro, el mobiliario urbano, las máquinas de las fábricas– estará conectado a internet²⁹. Todo lo que existe va a estar conectado a la Internet, por eso es importante migrar a otro protocolo como lo es IPv6.

- **El agotamiento de las direcciones IP versión 4 (IPv4)**

Después de muchos años el crecimiento de Internet está llegando a su límite, las direcciones IPv4, protocolo origen de Internet, se están acabando³⁰. Surge entonces un nuevo protocolo denominado IPv6 con un número casi infinito de direcciones. Podemos definir entonces que es una dirección IP, todo computador conectado a Internet tiene una dirección IP, que se representa mediante un número binario de 32 bits, dividida en cuatro octetos, por ejemplo, una dirección IPv4 sería: 164.12.123.65. Para poder extender la cantidad de direcciones disponibles, las IPv6 están compuestas por 8 segmentos de 16 bits cada uno, que en total suman 128 bits, que se escriben como ocho grupos de cuatro dígitos hexadecimales, por ejemplo, una dirección IPv6 sería: 2001:0db8:85a3:08 d3:1319:8a2e:0370:7334.

- **La Seguridad de Redes**

²⁹ IoT cosas, L. (2017). La historia detrás de la internet de las cosas. ELESPECTADOR.COM. [en línea], [Revisado 12 Dec. 2017]. ELESPECTADOR.COM. Disponible en Internet: <https://www.elespectador.com/tecnologia/la-historia-detras-de-la-internet-de-las-cosas-articulo-716678>.

³⁰ Dcc.uchile.cl. (2017). Citar un sitio web - Cite This For Me. [en línea], [Accessed 12 Dec. 2017]. Disponible en Internet: https://www.dcc.uchile.cl/sites/default/files/DCC-Inside/FCFM_40_Se_agotan_direcciones_IP.pdf.

La seguridad de redes consiste en las políticas y prácticas adoptadas para prevenir y supervisar el acceso no autorizado, el uso indebido, la modificación o la denegación de una red informática y sus recursos accesibles. La seguridad de redes involucra la autorización del acceso a datos en la red, que es controlada por el administrador de red. Los usuarios eligen o se les asigna una identificación y contraseña u otra información de autenticación que les permite acceder a información y programas dentro de sus autorizaciones³¹.

- **Extremo a Extremo**

El principio de "extremo a extremo" significa que los interlocutores de una comunicación dialogan desde cada extremo de la red para establecer y gestionar su comunicación³². A diferencia de IPv4 que utiliza el NAT, IPv6 tiene la capacidad de asignar una única dirección IP a cualquier equipo que quiera estar conectado a Internet.

- **NAT**

El Network Address Translation (NAT) se diseña para la conservación de IP Address. Habilita las redes de IP privado que utilizan los IP Address no registrados para conectar con el Internet. El NAT actúa encendido a un router, generalmente conectando dos redes juntas, y traduce (privadas a públicas) los direccionamientos

³¹ Es.wikipedia.org. (2017). Seguridad de redes. [en línea], [Revisado 12 Dec. 2017]. . Disponible en Internet: https://es.wikipedia.org/wiki/Seguridad_de_redes

³² Livre.g6.asso.fr. (2017). Introduccion - Livre IPv6. [en línea], [Revisado 12 Dec. 2017] Disponible en Internet: <http://livre.g6.asso.fr/index.php/Introduccion>.

únicos privados en la red interna a las direcciones legales, antes de que los paquetes se remitan a otra red³³.

1.8. MARCO LEGAL

A continuación, se presentan las bases legales que sustentan el desarrollo del proyecto de investigación en lo referente a la implementación del nuevo Protocolo de Internet, todas articuladas con el decreto 2573 de 2014, *"Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea..."*

1.8.1. 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 país³⁴.

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.

³³ Tecnologías, S., Services, I. and Tecnología, P. (2017). Network Address Translation (NAT) FAQ. [en línea] Cisco. [Revisado 12 Dec. 2017]. Disponible en Internet: https://www.cisco.com/c/es_mx/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html.

³⁴ Mintic.gov.co. (2017). Entra en vigencia la resolución 2710 del 2017 para la implementación del protocolo IPv6 en Colombia - Ministerio de Tecnologías de la Información y las Comunicaciones. [online] Disponible en Internet: <http://www.mintic.gov.co/portal/604/w3-article-61192.html> [Revisado 2 Agosto. 2017].

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.

1.8.2. Circular Numero 00002 de 2011 MinTIC.

El Ministerio de las TIC³⁵ convoca las entidades de la Administración Pública, Ramas Organismos del Estado al sector de TIC, para que en sus compras de equipos de TIC (hardware software), aplicaciones, plataformas TIC servicios prestados través de TIC, se exija que estén desarrollados implementados sobre el Protocolo IPv6 con compatibilidad soporte total IPv4; demostrable mediante los RFCs concretos del IETF demás normas que determinan esta compatibilidad.

También invita a la creación de un Plan de Transición para la Adopción de Ipv6 en coexistencia con Ipv4, programado para 3 años partir de la publicación de la presente circular; que permita una transición segura sin traumatismos para la Entidad, sus beneficiarios, usuarios para el administrado. Dicho plan deberá contemplar al menos: diagnóstico, plan de inversión, cronograma de implementación, formación en IPv6 de los funcionarios del área afín, evaluación de resultados los aspectos técnicos que permitan la correcta implementación de mecanismos de transición de IPv4 a IPv6 en sus redes, servicios al ciudadano prestados a través de TIC y en general las Plataformas (hardware software) Informáticas de Comunicaciones.

³⁵ 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].

1.8.3. Resolución 180 de 2010 UIT.

En 2010, la Conferencia Mundial de Desarrollo de las Telecomunicaciones (CMDT-10) adoptó la Resolución 63, “Asignación de direcciones IP y fomento de la implantación de IPv6 en los países en desarrollo”. Posteriormente, la Conferencia de Plenipotenciarios de la UIT (Guadalajara, 2010) adoptó la Resolución 180, “Facilitar la transición de IPv4 a IPv6”. El Grupo IPv6 de la UIT recibió el mandato de proseguir las actividades adicionales destinadas a la aplicación de estas Resoluciones.

Resolución 180 de 210³⁶, de la cual hace parte Colombia, y reconoce que la adopción temprana del IPv6 es la mejor forma de evitar escasez de direcciones IP y las consecuencias del agotamiento pueda implicar para el país. Se hace una convocatoria a todas las entidades públicas para preparar la adopción del nuevo protocolo IPv6.

1.8.4. Ley 1341 de 2009.

Artículo 2, numeral 6, establece la Neutralidad Tecnológica³⁷. 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.

³⁶ Mintic.gov.co. (2017). Citar un sitio web - Cite This For Me. [online] Disponible en Internet: http://www.mintic.gov.co/portal/604/articles-61000_documento.pdf [Revisado 23 Nov. 2017].

³⁷ Alcaldiabogota.gov.co. (2017). Consulta de la Norma:. [online] Disponible en Internet: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913> [Revisado 23 Nov. 2017].

Artículo 4³⁸, 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 y promover el acceso a las Tecnologías de la Información y las Comunicaciones, teniendo como fin último el servicio universal.

1.9. MARCO METODOLÓGICO

1.9.1. Tipo De Investigación .

El tipo de investigación utilizado por el desarrollo del proyecto corresponde a un **estudio descriptivo**, el cual busca especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis, miden o evalúan diversos aspectos, dimensiones o componentes del fenómeno o fenómenos a investigar³⁹. Para el caso de estudio en particular, lo que se desea es identificar las características principales de la red actual de la Secretaria del Sisben de la Alcaldía de Tunja, con el fin de caracterizar los elementos necesarios para el cambio progresivo de la red de comunicaciones y su migración de IPv4 a IPv6, lo anterior implica una evaluación de equipos, identificación y ubicación dentro de la organización, propuesta de diseño topológico (física y lógica) y costos de implementación.

³⁸ Ibid.

³⁹ Psicol.unam.mx. (2017). Métodos de Investigación. [online] Disponible en Internet: <http://www.psicol.unam.mx/Investigacion2/pdf/METO2F.pdf> [Revisado 3 Nov. 2017].

1.9.2. Etapas De La Investigación

Para el desarrollo del presente proyecto se definen tres etapas principales las cuales se fundamentan en la Guía de Transición de IPv4 a IPv6 para Colombia⁴⁰ del Ministerio de las Tic y que permiten dar cumplimiento a los objetivos específicos planteados:

- **Fase I. Planeación de IPv6**

- Recolección de la información acerca de todo lo que tiene que ver con el estado de arte de la migración del protocolo IPV4 a IPV6.
- Realizar un plano en las instalaciones del Sisben donde se pueda identificar los equipos activos y pasivos de la red actual para identificar: el rack principal, cableado, routers, los switch, redes telefónicas, UPS, estabilizadores y demás dispositivos.
- Conocer el estado actual de los equipos para poder establecer si cumplen con los requerimientos necesarios para la implementación del Protocolo IPV6.

- **Fase II. Implementación del protocolo IPv6**

- Identificar las características actuales del protocolo IPv4 implementado en la secretaria del Sisben y generar un plan de migración al protocolo IPv6.
- Desarrollar el plan de diagnóstico de IPv6 en la red con base en lo establecido en el inventario de activos de información.
- Definir e implementar el plan de direccionamiento IPv6.
- Configuración de direcciones IPV6 en cada uno de los dispositivos.

⁴⁰ Mintic.gov.co. (2017). Citar un sitio web - Cite This For Me. [online] Disponible en Internet: http://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf [Revisado 10 Oct. 2017].

- **Fase III. Pruebas de funcionalidad de IPv6**

- Generar un informe en el cual se evidencie todo el proceso que se hizo para realizar la Implementación del protocolo IPV6 en la secretaria del Sisben.
- Establecer los pasos básicos para la implementación de la migración de protocolo IPv4 a Protocolo IPv6.

1.9.3. Recolección De Información

La recolección de datos se refiere al uso de una diversidad de técnicas y herramientas que pueden ser utilizadas por el investigador para desarrollar los sistemas de información, para el desarrollo del proyecto se establecieron los siguientes métodos para la recolección de datos:

- La observación: consiste en realizar una verificación de las personas que actualmente labora en las distintas dependencias del Sisben para determinar que se están haciendo, cómo lo está haciendo, cuando se lleva a cabo, dónde se hace y por qué se hace.
- La entrevista: se utiliza para obtener información en forma verbal a través de preguntas que se generaron directamente a los funcionarios, estas entrevistas se realizaron de manera no estructuradas.
- Inventario Tecnológico: Se realiza un inventario de los equipos actuales de la Secretaria del Sisben de la Alcaldía Mayor de Tunja, soportado mediante Software de Inventario de Pc Network Inventory Advisor⁴¹

⁴¹ Network-inventory-advisor.com. (2017). Network Inventory Advisor: Software de gestión de activos de PC. [online] Disponible en Internet : <https://www.network-inventory-advisor.com/es/> [Consultado en 28 Nov. 2017].

DESARROLLO DEL PROYECTO

1.10. INVENTARIO ACTUAL

Para realizar la recolección de la información actual de los equipos con que cuenta la secretaria del Sisben, se elaboran tablas de valoración para cada uno de los activos de información de la entidad, la cual permite calificar el nivel de criticidad, si es “Alto”, “Medio” o “Bajo”; el impacto del uso de IPv6 de acuerdo al grado de confidencialidad, integridad y disponibilidad, de los equipos de comunicaciones, equipos de cómputo/almacenamiento y aplicaciones de cada una las dependencias (Tabla 1):

Tabla 1. Diagnostico Uno

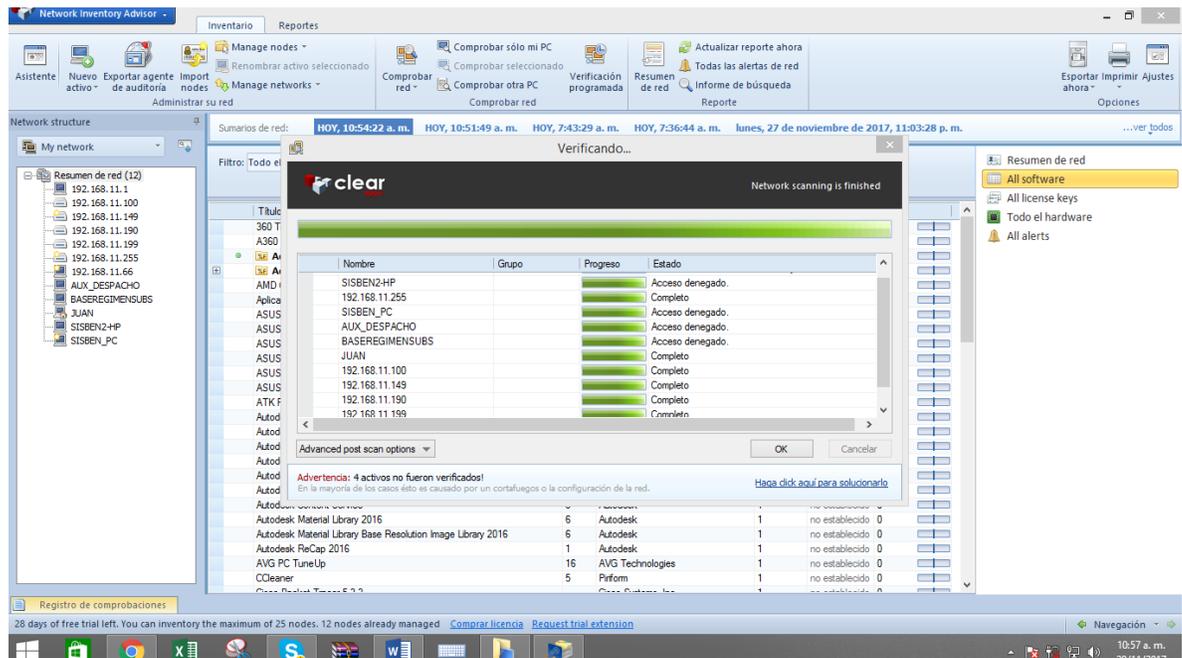
Fase I	Actividades Generales	Tiempo en meses para desarrollar cada actividad
Diagnóstico De La Situación Actual	Inventario de Equipos con que cuenta la secretaria del Sisben (Hardware, Software) los cuales se encuentran actualmente con un Protocolo IPV4.	La secretaria del Sisben cuenta con una red de Internet de Telecom de 10 megas de Velocidad, Se tienen 50 Computadores de distintos Sistemas Operativos, 2 Switch, 8 Impresoras de distintas Tecnologías, 2 Routers
	Análisis de la nueva topología de la	Actualmente la secretaria del Sisben de la Ciudad de Tunja cuenta con una Topología en Estrella donde las comunicaciones se

infraestructura actual y su funcionamiento	conectan a través de un punto en este caso un Enrutador O (LAN). Tiempo en que se analizara si es viable No migrar el protocolo actual por el IPV6
Protocolo de pruebas de validación de aplicativos, comunicaciones, de seguridad y coexistencia de los protocolos	Se solicita permiso a la Empresa prestadora del Servicio de Internet, para realizar las pruebas y verificar si los Equipos y Dispositivos soportan la migración del Protocolo IPV4 a IPV6.
Planeación de la transición de los servicios tecnológicos de la Entidad	Con todo el levantamiento de la Información y realizando un presupuesto de costos se realiza la Propuesta de Migración.
Validación de estado actual de los sistemas de información, sistemas de comunicaciones, interfaces y revisión de los correspondientes.	Con la Actualización de Equipos y ya con la Infraestructura que soporte la migración se realiza la validación de los sistemas de Información, y a la vez la actualización de los Equipos para que soporten el Protocolo IPV6. Esto nos dé como resultado una conectividad más amplia y ante todo más ágil en todos los aspectos.

Fuente: Del Autor

La actividad para la recolección de información sobre el inventario de equipos activos de la Secretaria de Sisben se realiza con ayuda de Sw de inventario de equipos e identificación de características de Red (Figura 10).

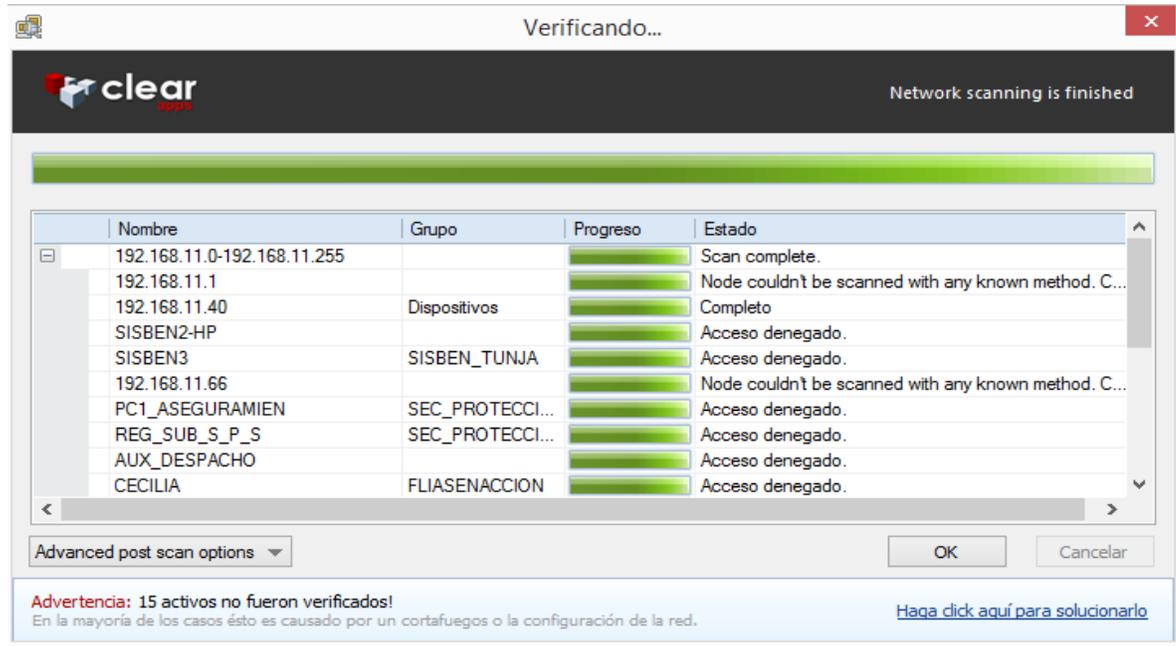
Figura 10. Inventario equipos activos con ayuda de SW Network Inventory Advisor



Fuente: Del Autor

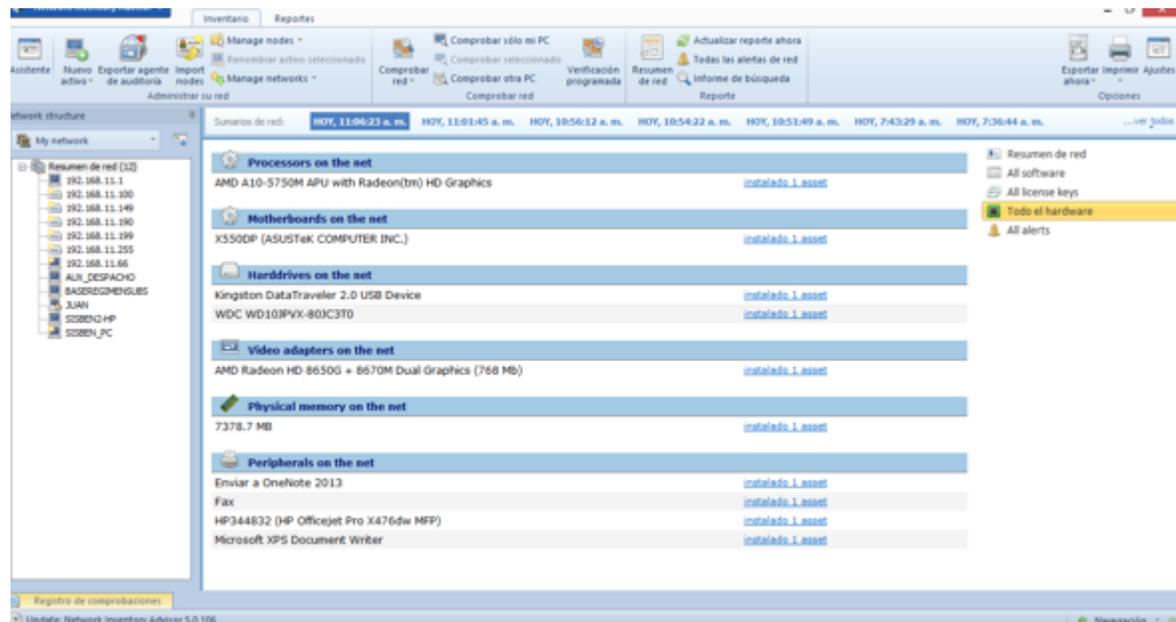
Identificación de direcciones IP segmento de red y distribución de subredes o grupos de dominio. Del mismo modo permite identificar características propias de licenciamiento, identificación de sistemas operativos, características de los dispositivos de red, nombres de equipos, inventario general de hardware entre otros (Figura 11).

Figura 11. Inventario de direcciones IPv4. SW Network Inventory Advisor



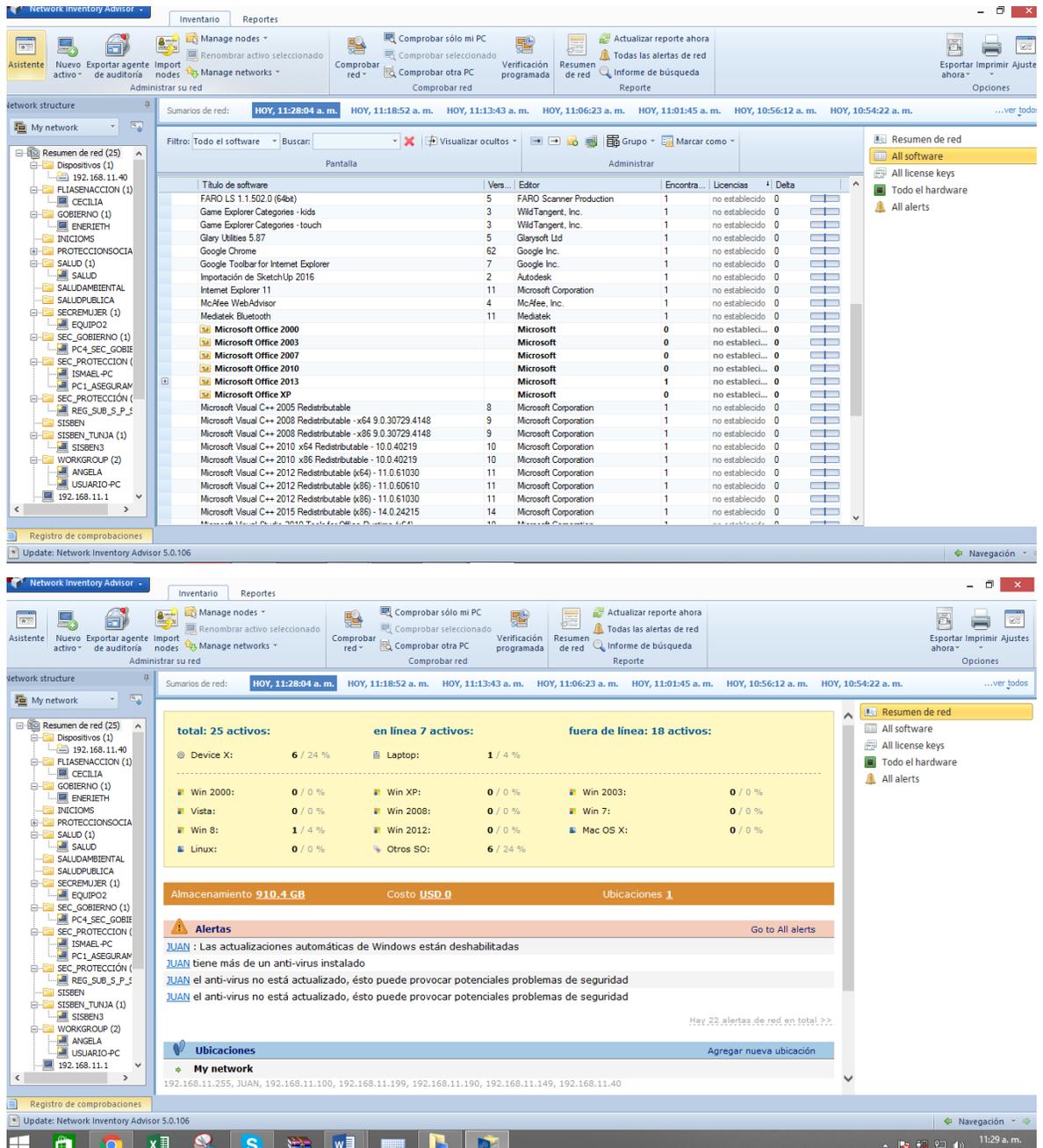
Fuente: Del Autor

Figura 12. Inventario de Hardware equipos. SW Network Inventory Advisor



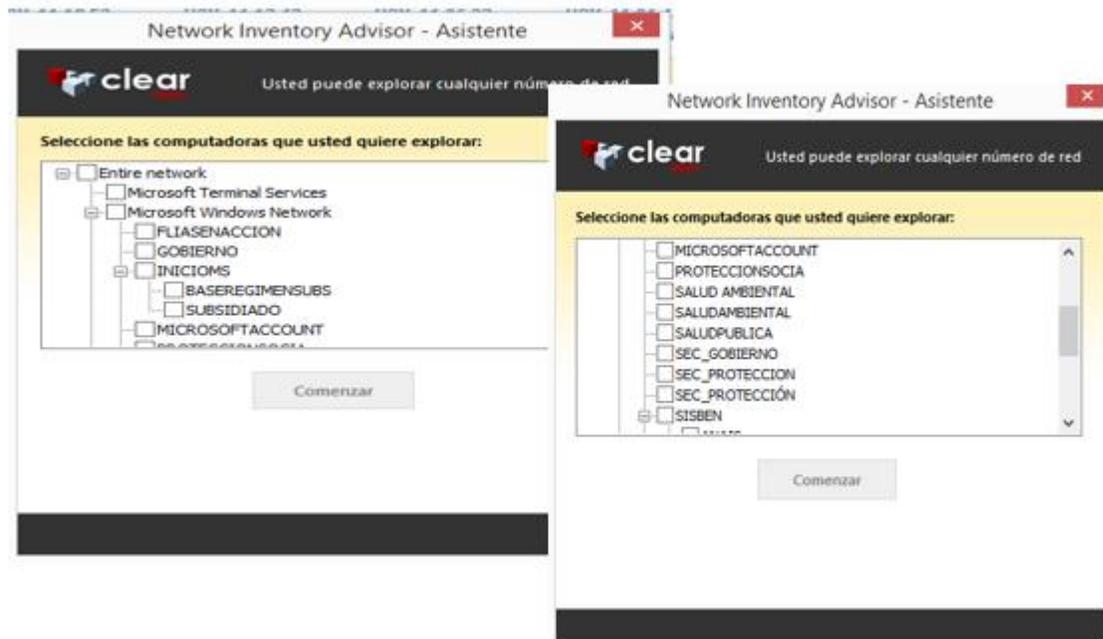
Fuente: Del Autor

Figura 13. Inventario de Sistemas Operativos. SW Network Inventory Advisor



Fuente: Del Autor

Figura 14. Inventario de Grupos de Trabajo y Subredes. SW Network Inventory Advisor



Fuente: Del Autor

Tabla 2. Diagnostico Dos

Activos de Información	Descripción de equipo S.O	Confidencialidad De IPV6	Integridad IPV6	de Disponibilidad de IPV6
Switch 2	HP 25 30-486	Alto	Alto	Alto
Red de Internet Fibra óptica	Telefónica RT 20-15 Fibra óptica 10 Mega bits	Alta	Ata	Alta
Equipos de cómputo 3	HP 5502 SO Windows XP	Bajo	Bajo	Bajo

Equipos de cómputo 15	HP LS 506 SO Windows 7	Medio	Medio	Medio
Equipos de cómputo 20	SONY SO Windows 8.1	Alto	Alto	Alto
Equipos de Cómputo 12	Samsung Windows 10	Alto	Alto	Alto
Impresoras 4	HP Deskjet 2050	Bajo	Bajo	Bajo
Impresoras 4	HP Laser Jet Manajet MFP M630m	Alto	Alto	Alto
Router 2	TP-LINK 1588	Alto	Alto	Alto

Fuente: Del Autor

Tabla 3. Diagnostico Tres

EQUIPO Y CANTIDAD	MARCA	MODELO	SISTEMA OPERATIVO	PUERTOS ETHERNET	ROL	VERSIÓN IP
Computador de Escritorio 15	HP LS 506 SO	LS 506	SO Windows 7 32 bits	2 Puertos	Oficina de Aseguramiento	IPV4/IPV6
Computadores de Escritorio	SONY SO	Sony	Windows 8.1. 64 bits	2 Puertos	Oficinas de Afiliaciones al Sisben, Bases de datos	IPV4/IPV6
Portátiles 5	Asus	K550D Serie hdmi	Windows 8.1. 64 bits	2 Puertos	Funcionarios que realizan las encuestas	IPV4/ IPV6
Computadores	HP	5005	Windows XP 32 bits	1 Puerto de Ethernet	Oficina de Archivo y	IPV4

de Escritori 5						Gestión Documental		
Switch 2 de 48 Puertos	HP	48	25 30- 486	Windows 8.1. 64 bits	48 Puertos	T4odos equipos distintos puertos in	los	IPV4/IPV6 con
Impreso ra 5	HP Jet Manajet	Laser	MFP M630m	Windows 8.1. 64 bits	3 Puertos	Oficina Aseguramient o y Afiliaciones	de	IPV4/IPV6
Router 2	Phicomm		IP 192.168. 0.1	Windows 8.1. 64 bits	4 Puertos	Rack de todos los Equipos		IPV4 a IPV6

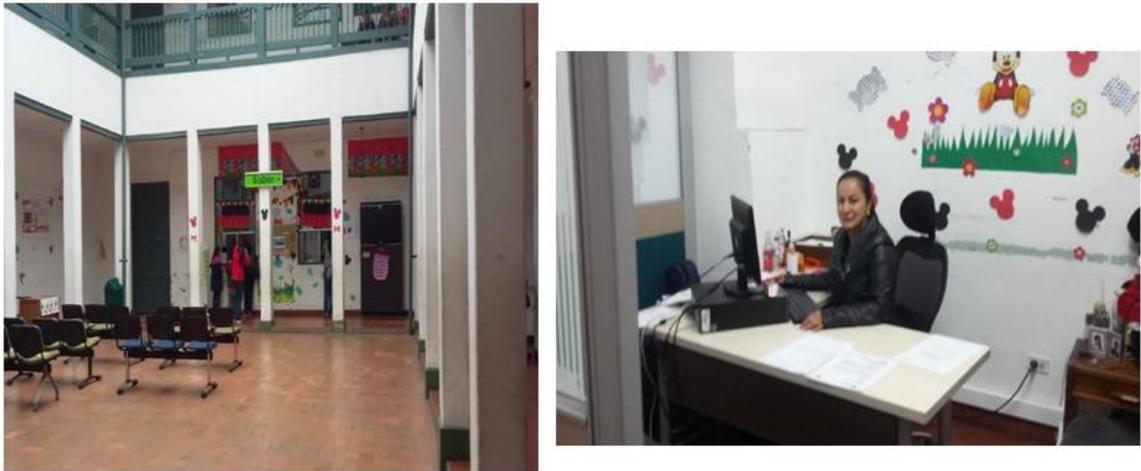
Fuente: Del Autor

La secretaria del Sisben cuenta en la actualidad con una topología en estrella la cual será implementada mediante el simulador Packet Tracer para su mejor entendimiento:

1.10.1. Topología Actual de la Red Secretaria de Sisben Alcaldía Mayor de Tunja

Contando con la autorización correspondiente por parte de la Secretaria del Sisben se precede a realizar una verificación en sitio para identificar la infraestructura actual, la topología física y la topología lógica (Figura 15):

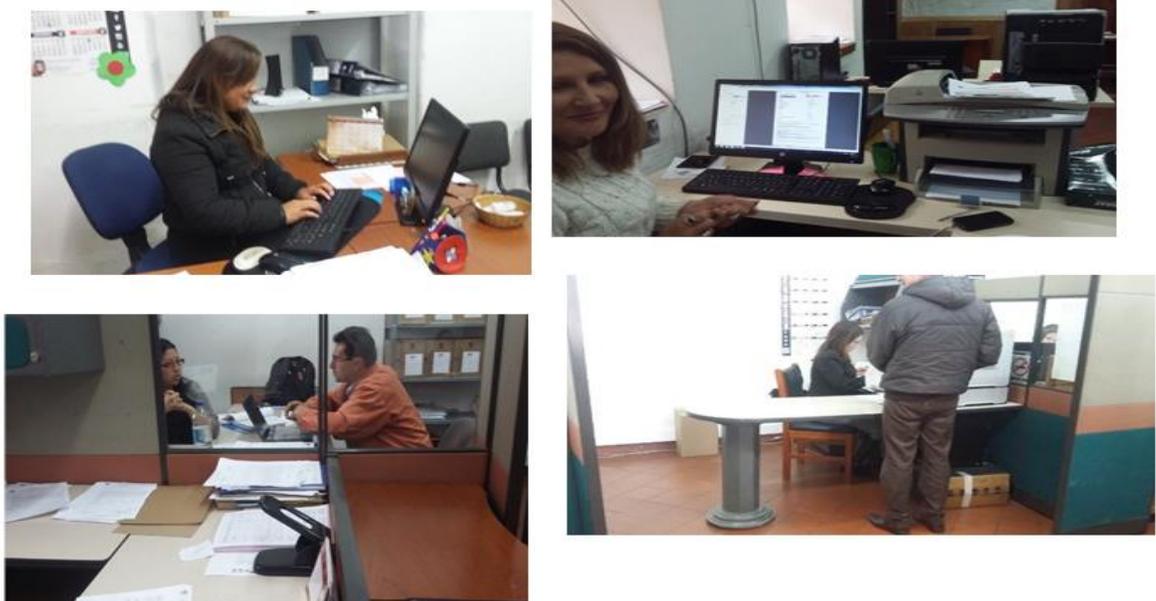
Figura 15. Dependencia Secretaria Del Sisben Que Pertenece A La Alcaldía Mayor De Tunja



Fuente: Del Autor

- Las fotos muestran las diferentes dependencias del Sisben El organigrama como está conformada la red de esta secretaria. La primera foto muestra el edificio donde queda ubicado todas las dependencias con sus respectivos de departamentos Los cuales funcionan con un protocolo de seguridad IPV4.
- La segunda foto muestra la secretaria Principal de esta secretaria La Doctora Luz Nidia Amaya (Figura 16).

Figura 16. Dependencias Secretaria Del Sisben Que Pertenece A La Alcaldía Mayor De Tunja. Oficina de Aseguramiento y Ventanilla

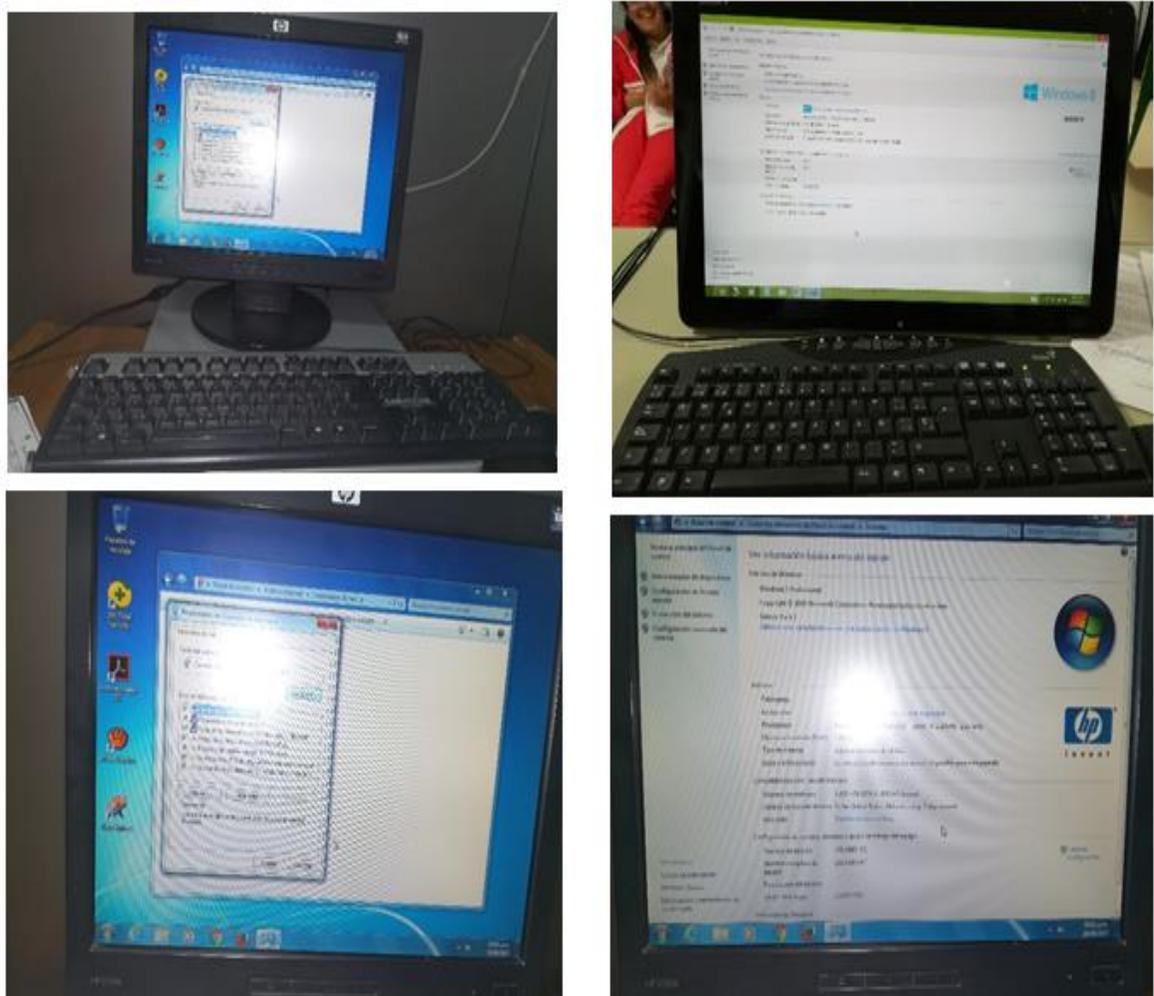


Fuente: Del Autor

- En esta siguiente foto se registra a la señora Patricia Jiménez quien es la encargada de la ventanilla de afiliaciones es la persona que tiene a su cargo revisar en el Sisben que toda la información que ingresa de los usuarios corresponda y corrobora con las demás dependencias.
- La siguiente fotografía muestra la oficina de Aseguramiento la cual tiene a su cargo la señora blanca Sánchez quien es la encargada de afiliar a los usuarios cuando toda la información es correcta.
- La otra foto muestra la oficina del archivo del Sisben esta oficina es muy importante ya que es donde se organiza toda la documentación ya sea en forma física como Digital.

- La ultima foto nos muestra la oficina de datos esta oficina la tiene a su cargo La ingeniera María Consuelo quien es la encargada de manejar la base de datos del Sisben.

Figura 17. Equipos Físicos con Protocolo de Seguridad Ipv4



Fuente: Del Autor

Estas fotos muestran las propiedades de la red, se tomaron para conocer el estado de los equipos con que cuenta actualmente la secretaria del sisben. Esto se hizo para revisar si cumplen con los requerimientos necesarios para la implementación del protocolo IPV6 ya que actualmente tienen el protocolo de seguridad IPV4.

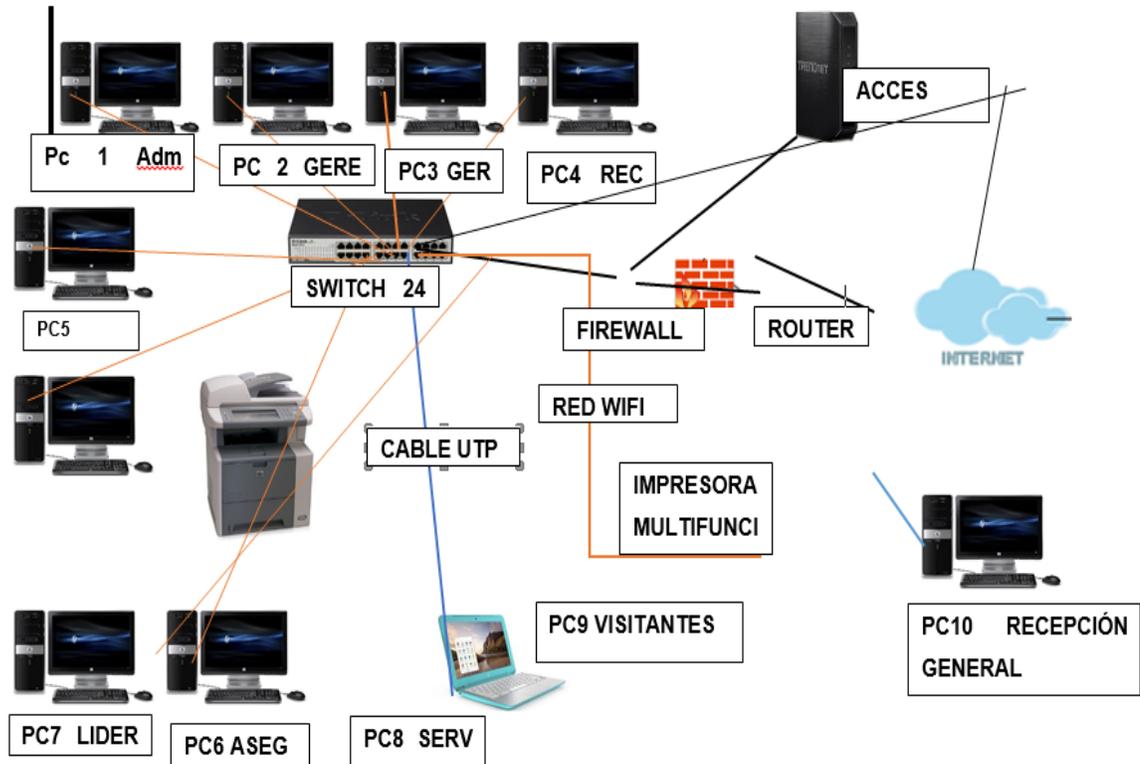
Figura 18. Topología Física actual Secretaria de Sisben Alcaldía Tunja



Fuente: Del Autor

Esta imagen muestra un levantamiento de la información se realizó para poder hacer la topología de las instalaciones del Sisben se hizo para conocer con una forma de plano como está dividido las oficinas del Sisben donde queda cada dependencia, Como primero se ve El cuarto de Sistemas el cual se encuentra dotado con todos los equipos tecnológicos como es un armario gigante dotado con 2 router, 2 Switch, Una UPS, 2Estabilizadores y toda la serie de cableados que alimentan los equipos de esta Secretaria. Las demás dependencias que muestra el plano ya están estipuladas en las fotos anteriores (Figura 19).

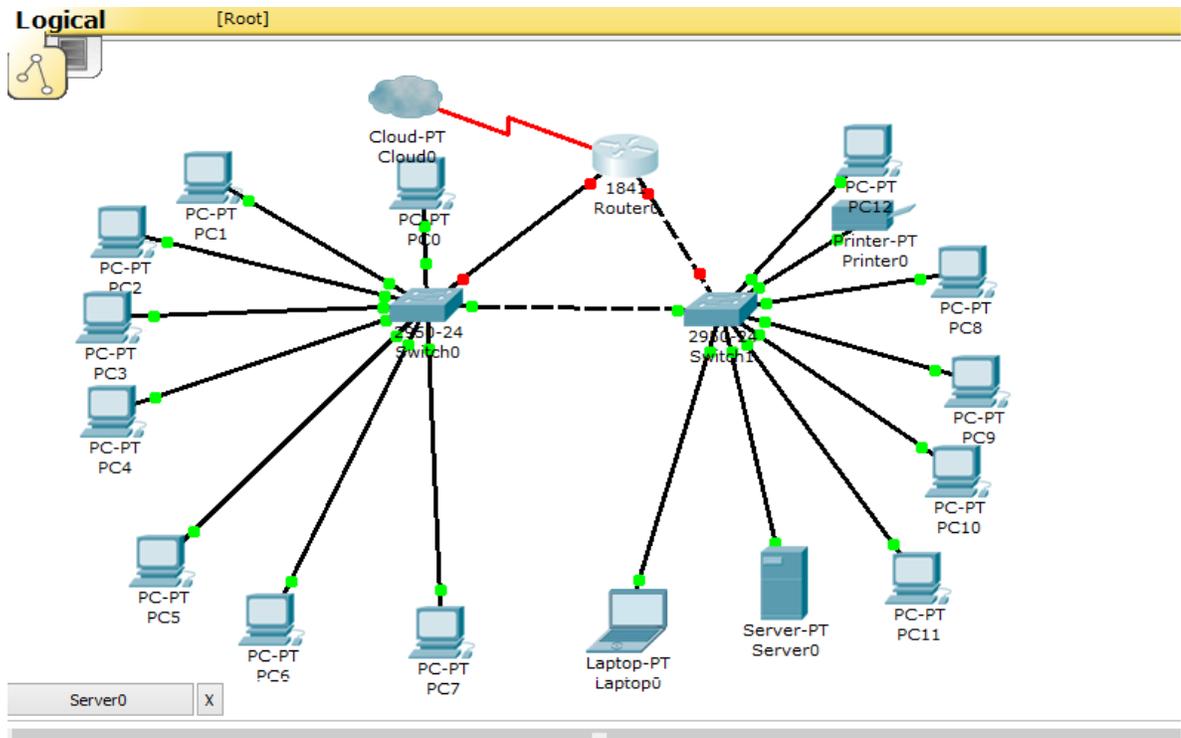
Figura 19. Topología Física. Equipos Networking Secretaria Sisben Alcaldía Tunja



Fuente: Del Autor

En la figura se observa la topología en estrella la cual se encuentra en la secretaria del Sisben. También se realizó para hacer el levantamiento de Información y sacar un inventario de equipos y como está su estructura para verificar si soportan la migración del Protocolo IPV4 A IPV6.(Figura 20).

Figura 20. Topología de Red Secretaria de Sisben Alcaldía Tunja.



Fuente: Del Autor

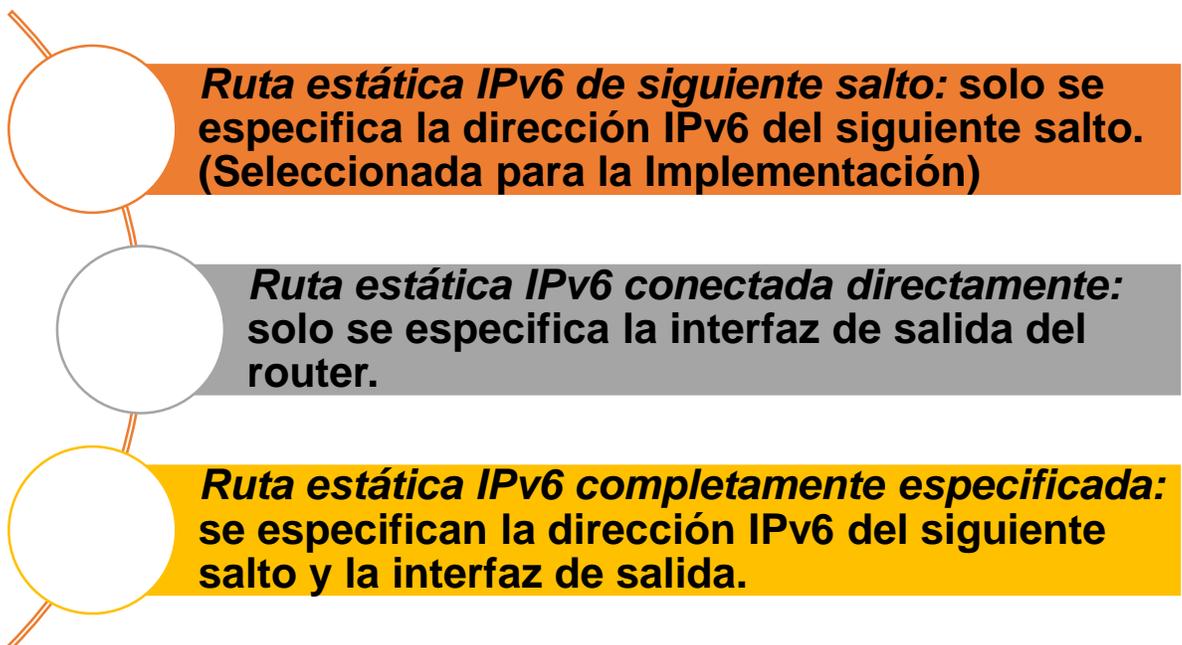
Esta imagen muestra la topología en estrella como está formada la red de la secretaria del Sisben pero ya en el Simulador de Pakert tracer. Muestra donde llega el prestador de Internet que en este caso es Telefónica Movistar, esta res llega al router, este reenvía la señal a los 2 switch cada uno con 48 puestos los cuales alimentan de Internet todos los equipos de la secretaria del Sisben.

1.11. IMPLEMENTACIÓN DE DIRECCIONAMIENTO IPV6

Cada router en una topología tiene entradas solo para redes conectadas directamente y sus direcciones locales asociadas. Ninguno de los router tiene conocimiento de las redes que están fuera de las interfaces conectadas directamente. El siguiente salto de un router se puede identificar mediante una dirección IPv6, una interfaz de salida, o ambas (Figura 21).

El modo en que se especifica el destino genera uno de los siguientes tres tipos de ruta:

Figura 21. Tipos de Rutas Estáticas IPv6



Fuente: Del Autor

Esta imagen muestra la ruta Estática IPV6. Como se hacen los saltos de la interfaz de salida ya con la migración del protocolo IPV6.

1.12. PROPUESTA DIRECCIONAMIENTO IPV6 PARA RUTAS ESTÁTICAS

Se debe construir con anticipación la tabla de direccionamiento para la topología propuesta con el fin de garantizar una óptima implementación (proceso de documentación de la Red):

Tabla 4. Propuesta de Direccionamiento IPv6

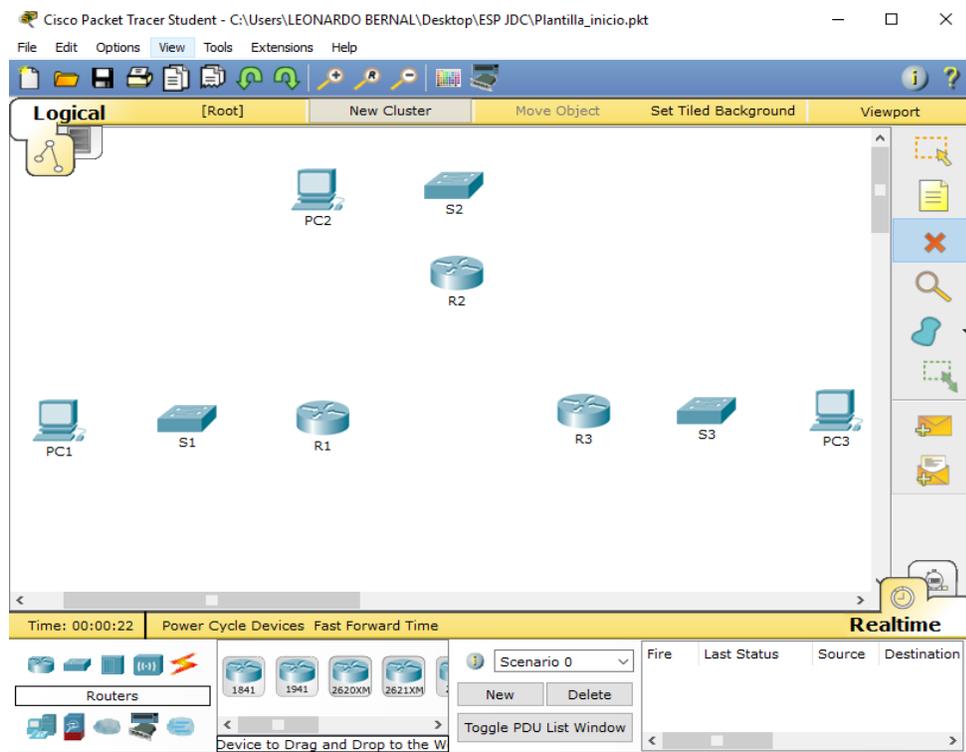
DISPOSITIVO	INTERFAZ	DIRECCIÓN/PREFIJO IPV6	GATEWAY PREDETERMINADO
R1	G0/0	2001:DB8:ACAD:1::1/64	N/A
	S0/0/0	2001:DB8:ACAD:4::1/64	N/A
R2	G0/0	2001:DB8:ACAD:2::1/64	N/A
	S0/0/0	2001:DB8:ACAD:4::2/64	N/A
	S0/0/1	2001:DB8:ACAD:5::2/64	N/A
R3	G0/0	2001:DB8:ACAD:3::1/64	N/A
	S0/0/1	2001:DB8:ACAD:5::1/64	N/A
PC1	NIC	2001:DB8:ACAD:1::F/64	2001:DB8:ACAD:1::1
PC2	NIC	2001:DB8:ACAD:2::F/64	2001:DB8:ACAD:2::1
PC3	NIC	2001:DB8:ACAD:3::F/64	2001:DB8:ACAD:3::1
PCN	NIC	2001:DB8:ACAD:N::F/64	2001:DB8:ACAD:N::1

Fuente: Del Autor

1.13. PREPARACIÓN DEL LA MIGRACION A IPV6 ESCENARIO EN EL SIMULADOR PACKET TRACER

La topología propuesta tiene como elementos activos: 3 PCs, 3 Switches 2950-24 y 3 Routers 1941.

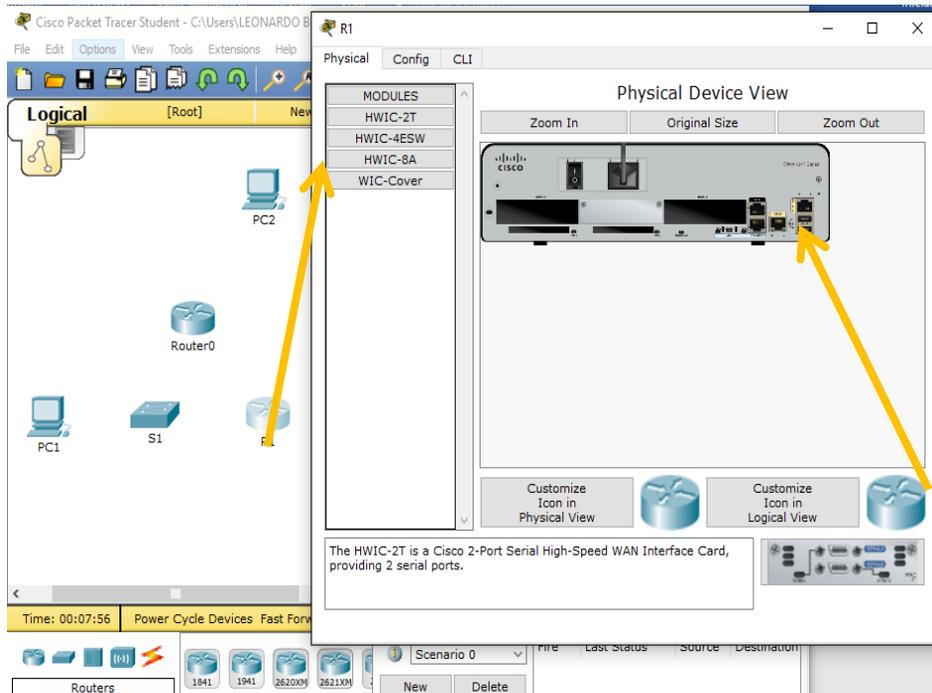
Figura 22. Definición de Dispositivos en Packet Tracert



Fuente: Del Autor

Como los Router 1941 solo cuenta con 2 interfaz GigabitEthernet y no cuentan con puertos seriales instalados se hace necesario ingresar a cada uno de ellos e instalar el módulo HWIC-2T (Cisco 2-Port Serial High-Speed WAN Interface Card, providing 2 serial ports)

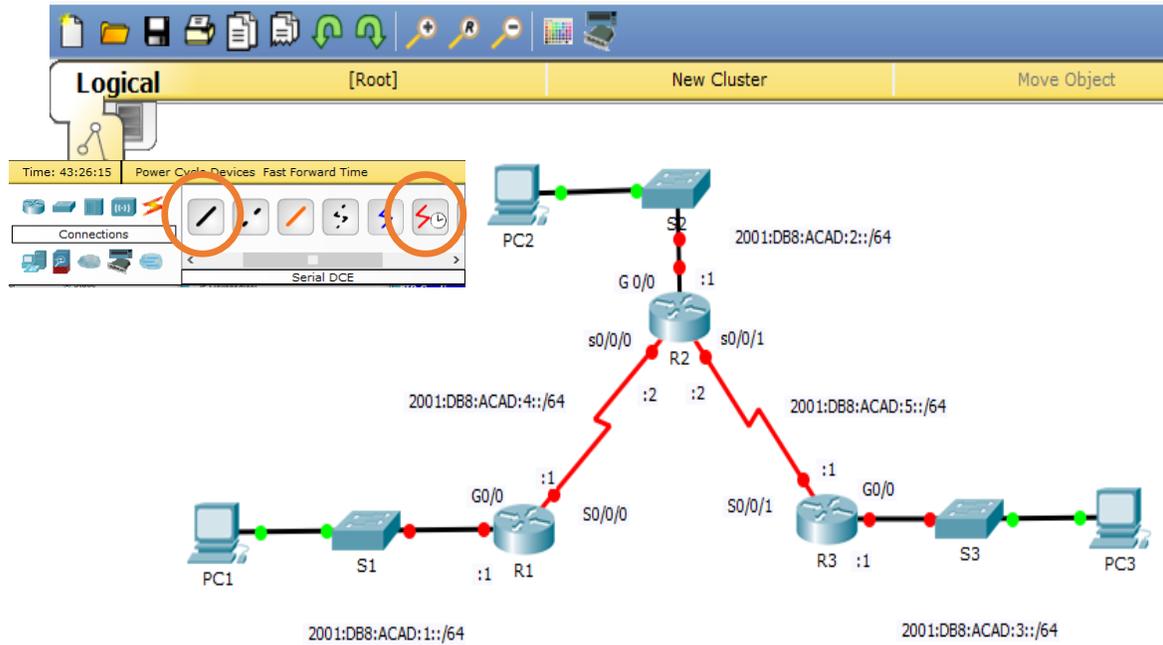
Figura 23. Configuración de adaptadores de Red - Routers



Fuente: Del Autor

Procedo a conectar los dispositivos e identificar los segmentos de red y cada una de la interfaz a ser utilizadas, con el fin de facilitar su configuración.

Figura 24. Configuración de Interfaz



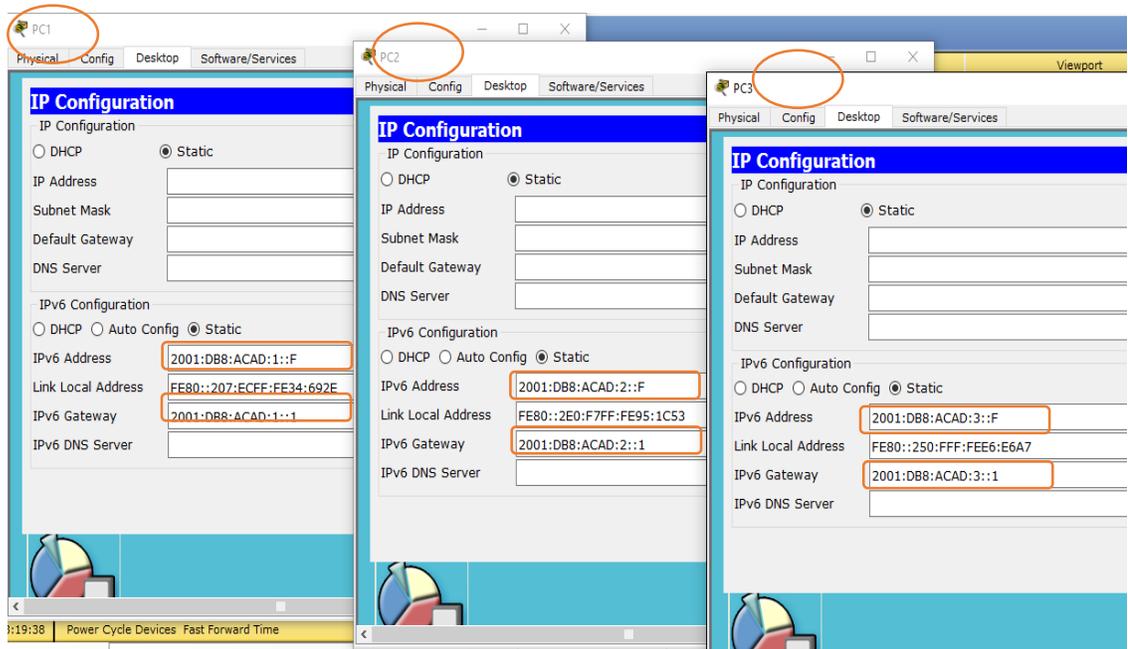
Fuente: Del Autor

Las conexiones entre Pc-Sw y Sw-Router se realizan con cable UTP directo y las conexiones seriales entre los Router deben corresponder a conexiones serial DCE.

1.14. CONFIGURACIÓN DE DIRECCIONES IPV6 EN CADA UNO DE LOS DISPOSITIVOS

Teniendo en la tabla de direccionamiento procedo a la configuración de los 3 PC (Figura 25) (Ipv6 Address y el Ipv6 Gateway el link local Address no se modifica):

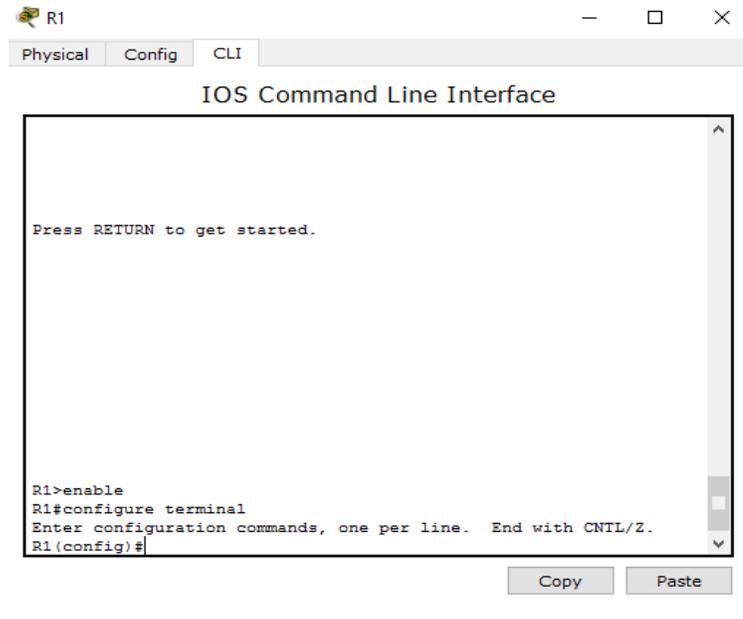
Figura 25. Configuración de IPV6 en los PC



Fuente: Del Autor

El proceso para configurar la interfaz GigabitEthernet y la interfaz Serial de cada uno de los router se debe realizar por medio de CLI (Comand-Line Interfaz de Cisco).(Figura 26).

Figura 26. Configuración IPv6 Intefaz GigabitEthernet



Fuente: Del Autor

Configuración Router 1 (R1) interfaz gigabitEthernet 0/0

```
R1>enable          (Entrar a modo privilegiado)
R1#configure terminal      (Entra en Modo Configuración)
R1(config)#ipv6 unicast-routing
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64
R1(config-if)#no shutdown
```

Configuración Router 1 (R1) interfaz serial 0/0/0

```
R1>enable
R1#configure terminal
R1(config)#ipv6 unicast-routing
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 enable
R1(config-if)#clock rate 9600 (reloj se debe configurar solo en uno de los
extremos de la interfaz )
R1(config-if)#ipv6 address 2001:DB8:ACAD:4::1/64
R1(config-if)#no shutdown
```


Configuración Router 2 (R2) interfaz gigabitEthernet 0/0

```
R2>enable
R2#configure terminal
R2(config)#ipv6 unicast-routing
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
R2(config-if)#no shutdown
```

Configuración Router 2 (R2) interfaz serial 0/0/0 e interfaz serial 0/0/1

```
R2>enable
R2#configure terminal
R2(config)#ipv6 unicast-routing
R2(config)#interface serial0/0/0
R2(config-if)#ipv6 enable
R2(config-if)#ipv6 address 2001:DB8:ACAD:4::2/64
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface serial0/0/1
R2(config-if)#ipv6 enable
R2(config-if)#ipv6 address 2001:DB8:ACAD:5::2/64
R2(config-if)#no shutdown
```


Configuración Router 3 (R3) interfaz gigabitEthernet 0/0

```
R3>enable
R3#configure terminal
R3(config)#ipv6 unicast-routing
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
R3(config-if)#no shutdown
```

Configuración Router 3 (R3) interfaz serial 0/0/1

```
R3>enable
R3#configure terminal
R3(config)#ipv6 unicast-routing
R3(config)#interface serial 0/0/1
R3(config-if)#ipv6 enable
R3(config-if)#clock rate 9600
R3(config-if)#ipv6 address 2001:DB8:ACAD:5::1/64
R3(config-if)#no shutdown
```

Por medio del comando `show ipv6 route` o el comando `show ipv6 interface brief` es posible verificar y comprobar las rutas conectadas localmente (C y L) a cada uno de los router (tabla de ruteo). (Figura 27).

Figura 27. Comando `show ip route`

The image shows two side-by-side screenshots of Cisco IOS Command Line Interface (CLI) windows for routers R1 and R2.

Left Window (R1): Shows the output of the `show ipv6 route` command. The output displays the IPv6 Routing Table with 5 entries. The entries are:

- C 2001:DB8:ACAD:1::/64 [0/0] via GigabitEthernet0/0, directly connected
- L 2001:DB8:ACAD:1::1/128 [0/0] via GigabitEthernet0/0, receive
- C 2001:DB8:ACAD:4::/64 [0/0] via Serial0/0/0, directly connected
- L 2001:DB8:ACAD:4:1/128 [0/0] via Serial0/0/0, receive
- L FF00::/8 [0/0] via Null0, receive

The command `show ipv6 route` is highlighted with an orange box.

Right Window (R2): Shows the output of the `show ipv6 interface brief` command. The output displays the status of the IPv6 interfaces:

- GigabitEthernet0/0 [up/up] FE80::2E0:F7FF:FE50:2401 2001:DB8:ACAD:2::1
- GigabitEthernet0/1 [administratively down/down]
- Serial0/0/0 [up/up] FE80::2E0:F7FF:FE50:2401 2001:DB8:ACAD:4::2
- Serial0/0/1 [up/up] FE80::2E0:F7FF:FE50:2401 2001:DB8:ACAD:5::2
- Vlan1 [administratively down/down]

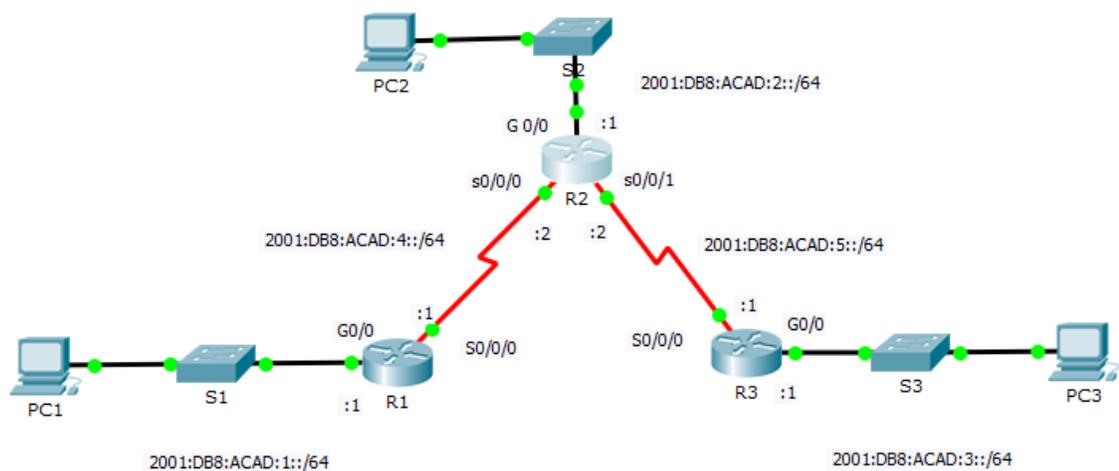
The command `show ipv6 interface brief` is highlighted with an orange box.

Fuente: Del Autor

Una vez terminada la configuración de direccionamiento de la totalidad de las interfaces, la simulación en Packet Tracer permite indicar con color verde que todos los enlaces se encuentran activos y listos para transmitir paquetes de datos.

En esta fase de la implementación solo se podrán transmitir paquetes desde los PC a cada router, no será posible enviar paquetes de extremo a extremo debido a que no se han configurado ningún tipo de enrutamiento ya sea estático o dinámico. (Figura 28).

Figura 28. Implementación Segmentos de Red IPv6



Fuente: Del Autor

1.15. PRUEBA DE CONECTIVIDAD POR MEDIO DEL COMANDO PING

El comando PING sirve para verificar la conectividad IP, el funcionamiento y la disponibilidad de una Red.

Si se aplica el comando Ping desde el PC 1, se puede verificar que únicamente se tiene acceso a la dirección local, a la puerta de enlace y a la interfaz serial 0/0/0 pero no se puede alcanzar ninguno de los demás dispositivos.

```
PC>ping 2001:db8:acad:1::f      (ping a la dirección local del equipo)
```

```
Pinging 2001:db8:acad:1::f with 32 bytes of data:
```

```
Reply from 2001:DB8:ACAD:1::F: bytes=32 time=15ms TTL=128
```

```
Reply from 2001:DB8:ACAD:1::F: bytes=32 time=1ms TTL=128
```

```
Reply from 2001:DB8:ACAD:1::F: bytes=32 time=14ms TTL=128
```

```
Reply from 2001:DB8:ACAD:1::F: bytes=32 time=26ms TTL=128
```

```
Ping statistics for 2001:DB8:ACAD:1::F:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 1ms, Maximum = 26ms, Average = 14ms
```

```
PC>ping 2001:db8:acad:1::1      (ping a la puerta de enlace del equipo)
```

```
Pinging 2001:db8:acad:1::1 with 32 bytes of data:
```

```
Reply from 2001:DB8:ACAD:1::1: bytes=32 time=0ms TTL=255
```

```
Ping statistics for 2001:DB8:ACAD:1::1:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 2001:db8:acad:4::1 (ping a la interfaz serial del router)

Pinging 2001:db8:acad:4::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:4::1: bytes=32 time=0ms TTL=255

Reply from 2001:DB8:ACAD:4::1: bytes=32 time=0ms TTL=255

Reply from 2001:DB8:ACAD:4::1: bytes=32 time=0ms TTL=255

Reply from 2001:DB8:ACAD:4::1: bytes=32 time=3ms TTL=255

Ping statistics for 2001:DB8:ACAD:4::1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 3ms, Average = 0ms

PC>ping 2001:db8:acad:2::F (ping a la interfaz del PC. NO EXISTE COMUNICACIÓN)

Pinging 2001:db8:acad:4::2 with 32 bytes of data:

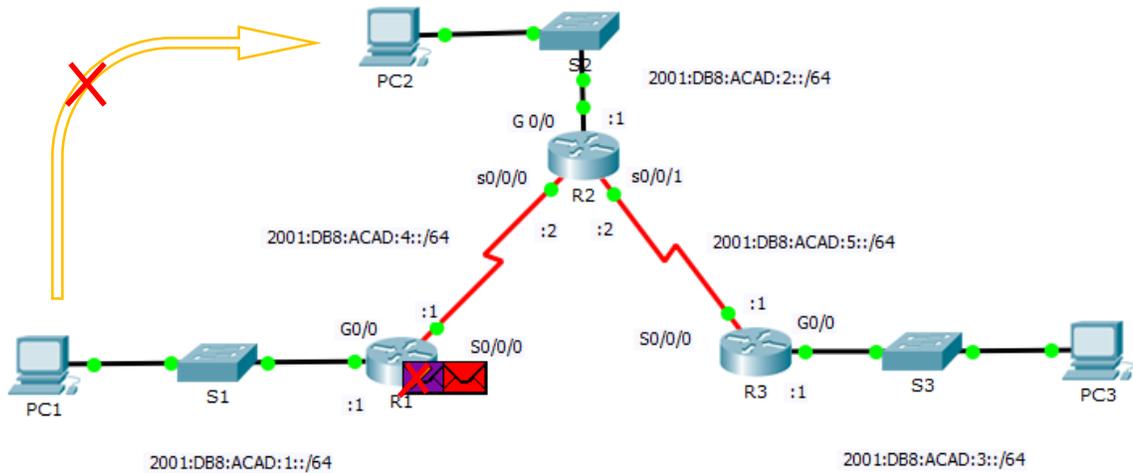
Request timed out.

Request timed out.

Ping statistics for 2001:DB8:ACAD:4::2:

Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),

Figura 29. Prueba de conectividad IPv6



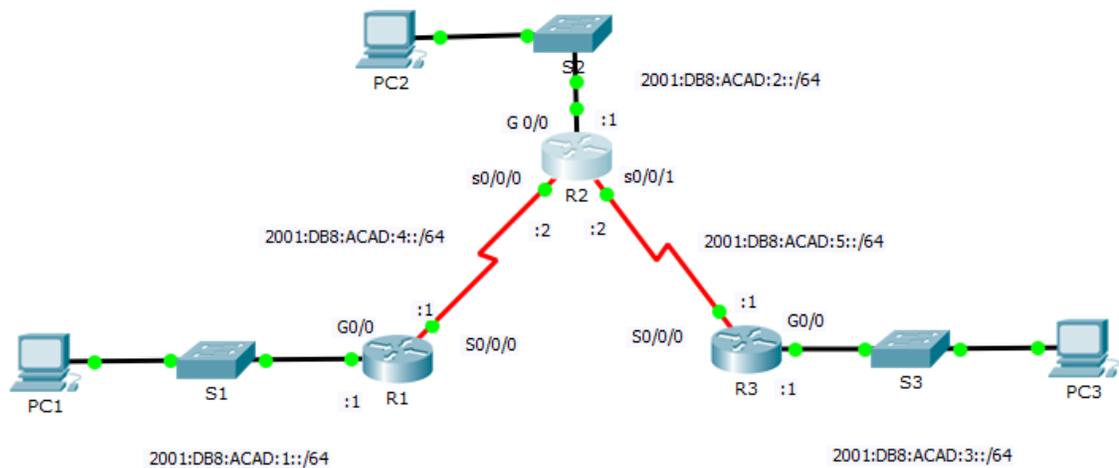
Fuente: Del Autor

1.16. CONFIGURACIÓN RUTA ESTÁTICA IPV6 DE SIGUIENTE SALTO

Cuando un paquete desde el PC1 está destinado a la red 2001:DB8:ACAD:3::/64, el R1 busca una coincidencia en la tabla de routing y encuentra que debe reenviar paquetes a la dirección IPv6 2001:DB8:ACAD:4::2 del siguiente salto (interfaz serial 0/0/0 del R2).

Todas las rutas que hacen referencia solo a la dirección IPv6 del siguiente salto y que no hacen referencia a una interfaz de salida deben resolver la dirección IPv6 del siguiente salto con otra ruta de la tabla de routing que tenga una interfaz de salida.

Figura 30. Configuración ruta estatica proximo salto (IPv6)



Fuente: Del Autor

Configuración próximo salto R1

```
R1>enable
```

```
R1#configure terminal
```

```
R1(config)#ipv6 route 2001:db8:acad:2::/64 2001:db8:acad:4::2
```

```
R1(config)#ipv6 route 2001:db8:acad:5::/64 2001:db8:acad:4::2
```

```
R1(config)#ipv6 route 2001:db8:acad:3::/64 2001:db8:acad:4::2
```

Configuración próximo salto R2

```
R2>enable
```

```
R2#configure terminal
```

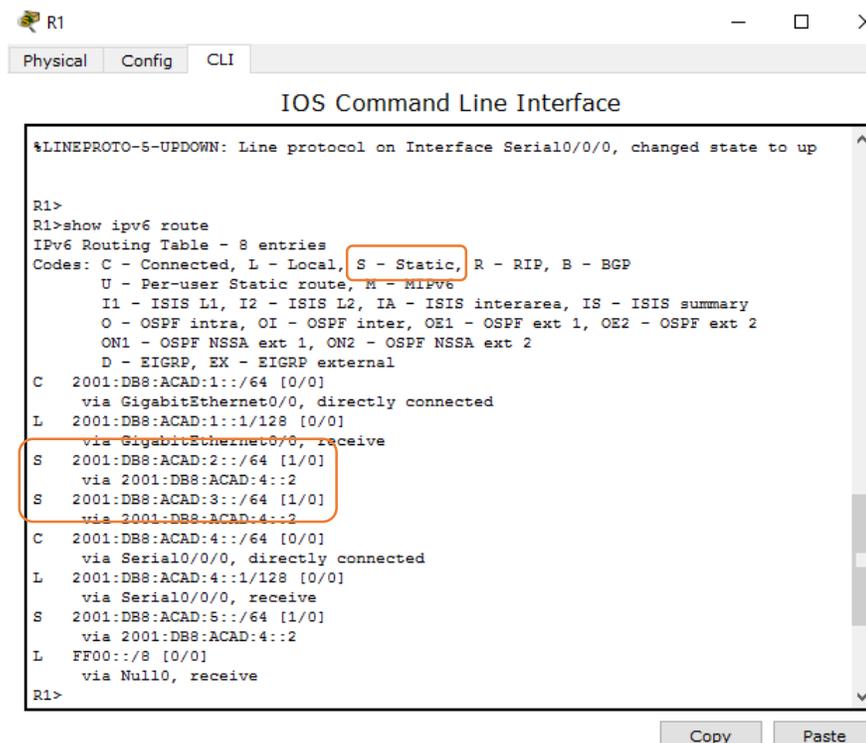
```
R2(config)#ipv6 route 2001:db8:acad:1::/64 2001:db8:acad:4::1
R2(config)#ipv6 route 2001:db8:acad:3::/64 2001:db8:acad:5::1
```

Configuración próximo salto R3

```
R3>enable
R3#configure terminal
R3(config)#ipv6 route 2001:db8:acad:1::/64 2001:db8:acad:5::2
R3(config)#ipv6 route 2001:db8:acad:4::/64 2001:db8:acad:5::2
R3(config)#ipv6 route 2001:db8:acad:2::/64 2001:db8:acad:5::2
```

Por medio del comando show ipv6 route es posible verificar y comprobar las rutas ESTATICAS (S) configuradas en cada router (tabla de ruteo).

Figura 31. Comprobación de Rutas Estáticas R1



```
R1
Physical Config CLI
IOS Command Line Interface

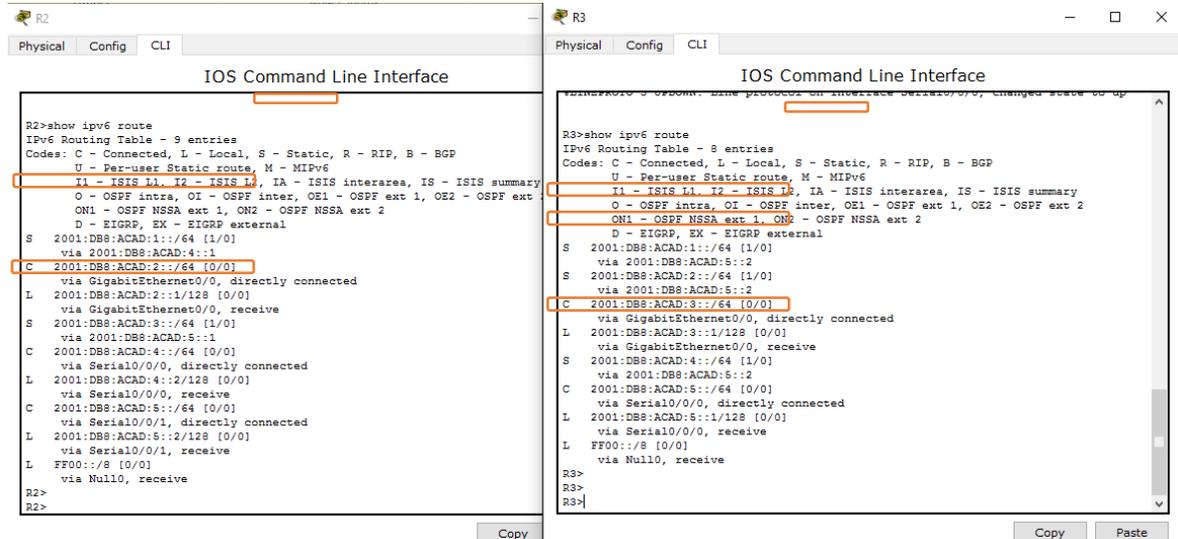
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R1>
R1>show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       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
       D - EIGRP, EX - EIGRP external
C 2001:DB8:ACAD:1::/64 [0/0]
  via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:1::1/128 [0/0]
  via GigabitEthernet0/0, receive
S 2001:DB8:ACAD:2::/64 [1/0]
  via 2001:DB8:ACAD:4::2
S 2001:DB8:ACAD:3::/64 [1/0]
  via 2001:DB8:ACAD:4::2
C 2001:DB8:ACAD:4::/64 [0/0]
  via Serial0/0/0, directly connected
L 2001:DB8:ACAD:4::1/128 [0/0]
  via Serial0/0/0, receive
S 2001:DB8:ACAD:5::/64 [1/0]
  via 2001:DB8:ACAD:4::2
L FF00::/8 [0/0]
  via Null0, receive

R1>
```

Fuente: Del Autor

Figura 32. Comprobación rutas Estáticas R2 R3

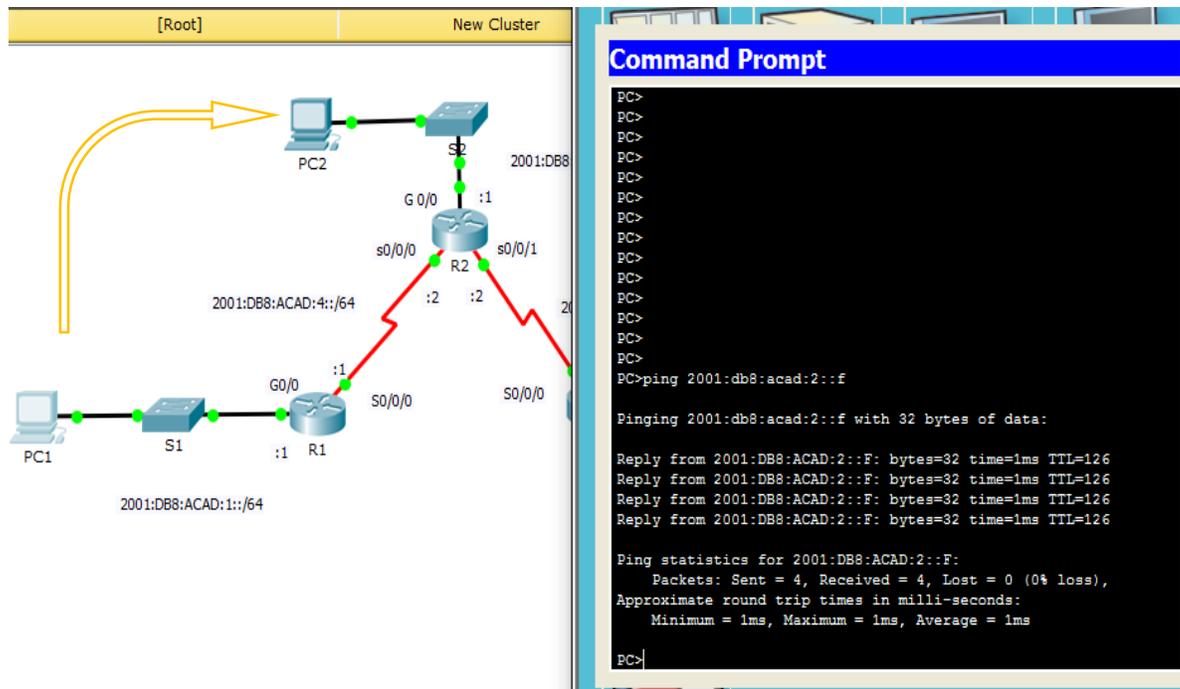


Fuente: Del Autor

Prueba de conectividad por medio del comando Ping (después de configurar la ruta estática de siguiente salto)

Una vez configurada la ruta de siguiente salto y se aplica el comando Ping desde el PC 1 hasta el PC2, se puede verificar que tiene acceso:

Figura 33. Comprobación de conectividad PC1 PC2



Fuente: Del Autor

Prueba de conectividad por medio del modo simulación de Packet Tracer (después de configurar la ruta estática de siguiente salto)

Figura 34. Envío de paquetes IPv6

The screenshot displays a network simulation environment. The main window shows a network topology with routers R1, R2, and R3, switches S1 and S3, and PCs PC1, PC2, and PC3. The routers are interconnected, and the PCs are connected to the switches. The interface includes a 'Simulation Panel' on the right with an 'Event List' table and 'Play Controls' at the bottom. The 'Event List' table shows the following data:

Vis.	Time(sec)	Last Device	At Device	Type	Info
	1.796	S3	PC3	ICMPv6	
	1.797	R3	S3	ICMPv6	
	1.797	R2	R1	ICMPv6	
	1.797	PC3	S3	ICMPv6	
	1.798	S3	PC3	ICMPv6	
	1.798	R1	S1	ICMPv6	
	1.798	S3	R3	ICMPv6	
	1.799	S1	PC1	ICMPv6	
	1.799	R3	R2	ICMPv6	

At the bottom of the interface, there is a 'Simulation' panel with a table showing the results of the simulation:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC3	PC2	ICMPv6		0.000	N	0
	Successful	PC1	PC2	ICMPv6		0.000	N	1
	Successful	PC2	PC3	ICMPv6		0.000	N	2

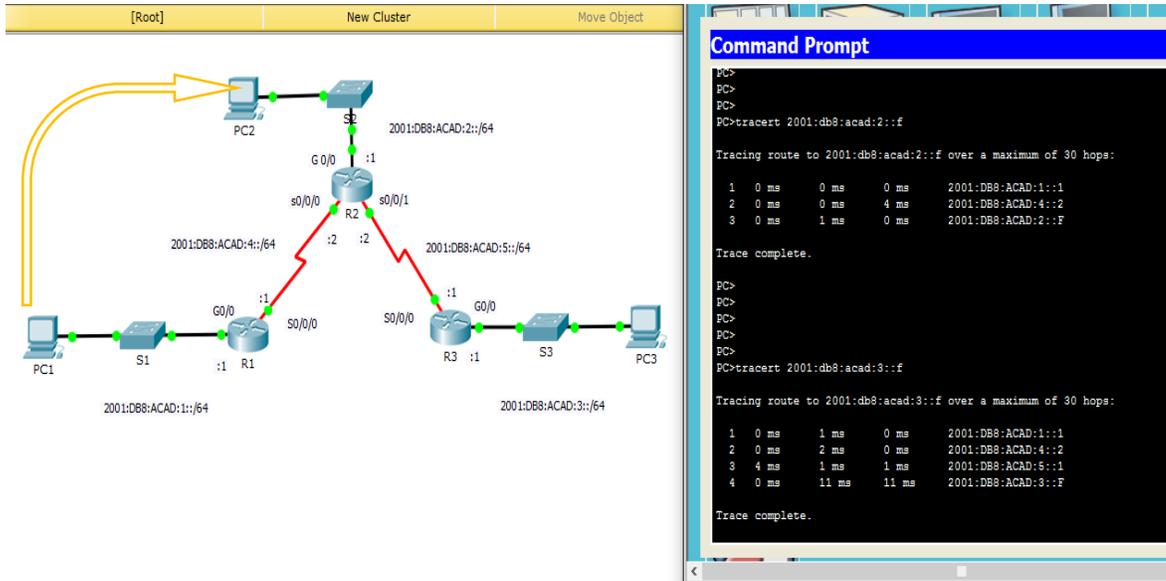
Fuente: Del Autor

1.17. COMANDO TRACERT

Resulta un comando muy útil para determinar el camino que siguen los paquetes de red desde un equipo origen a otro equipo destino y así determinar si existe algún problema en algún momento entre ambos. Permite identificar el número de saltos que realiza un paquete para llegar al destino.

Aplicando el comando tracert desde el PC1 al PC2 y desde PC1 al PC3 se puede verificar los siguientes resultados:

Figura 35. Comando Tracert



Fuente: Del Autor

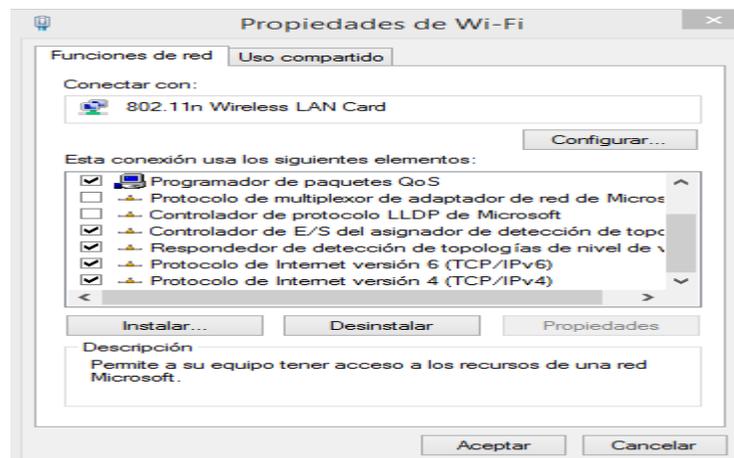
RESULTADOS DE LA MIGRACION PROTOCOLO IPV4 A IPV6

Como etapa final del proyecto se establecen los resultados y los pasos necesarios que se deben tener en cuenta a la hora de realizar la configuración del protocolo IPv4 a IPv6.

1.18. HABILITACIÓN DE PROTOCOLOS IPV4 E IPV6

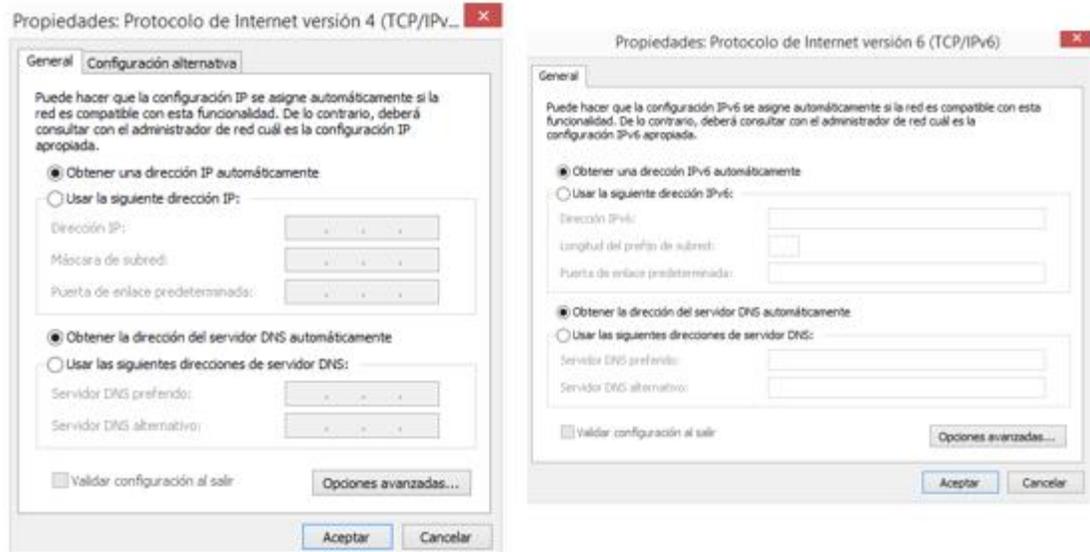
Se debe identificar que los protocolos de internet versión IPV4 y IPV6 estén habilitados para esto hay que dirigirse al centro de redes y recursos compartidos y luego al icono de bandeja del sistema para comprobar las propiedades del adaptador de red (Figura 36).

Figura 36. Propiedades del adaptadores de Red



Fuente: Del Autor

Figura 37. Propiedades de los Protocolos IPv4 IPv6



Fuente: Del Autor

Figura 38. Verificación de dirección IP

```

Dirección física. . . . . : 38-2C-4A-1E-D0-A6
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::3cec:474d:8d8a:2a7a%4<Preferido>
Dirección IPv4. . . . . : 192.168.11.102<Preferido>
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : miércoles, 29 de noviembre de 20
8:10:48 p. m.
La concesión expira . . . . . : miércoles, 29 de noviembre de 20
10:53:34 p. m.
Puerta de enlace predeterminada . . . . . : 192.168.11.1
Servidor DHCP . . . . . : 192.168.11.1
IAID DHCPv6 . . . . . : 154676298
DUID de cliente DHCPv6. . . . . : 00-01-00-01-1B-AE-5A-3F-38-2C-4A
-D0-A6
Servidores DNS. . . . . : 192.168.11.1
NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de LAN inalámbrica Wi-Fi:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . : engineering.c9.com
    
```

Fuente: Del Autor

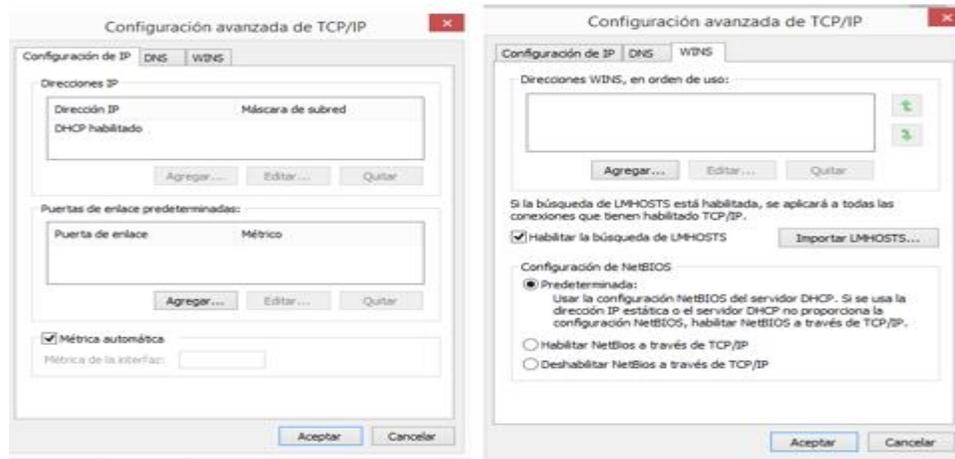
El protocolo de Internet IPv4 se encuentra como IP automática paso a la pestaña WINS en esta opción se ve la configuración de NetBIOS la cual se encuentra como predeterminada, deshabilitar NetBIOS a través de TCP/IP para que NetBIOS no use la configuración del servidor DHCP.

1.19. CONFIGURACIÓN AVANZADA DE IPV6

Se procede a configurar las direcciones IPv6 en los diferentes equipos de cómputo de la Secretaria de Sisben, para lo cual se ingresa al símbolo del sistema y el comando (Figura 39):

```
netsh interface IPv6 add address "Conexión de área local" 2001:DB8:ACAD:1::F/64
```

Figura 39. Configuración avanzada TCP/IP



Fuente: Del Autor

Figura 40. Configuración manual de IPv6

```

C:\Windows\system32>netsh interface ipv6 add address "Conexión de área local" 2001:db8:290c:1291::2
C:\Windows\system32>_

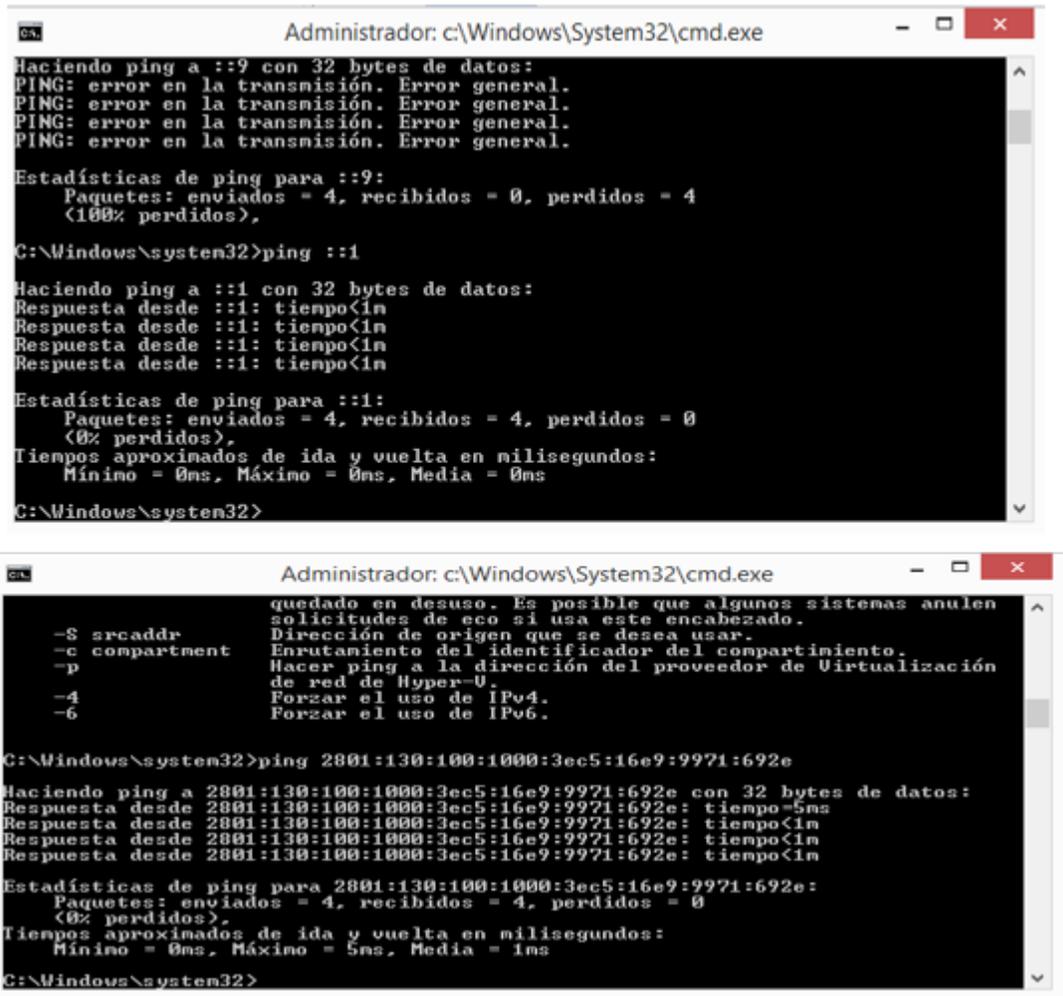
C:\Windows\system32>netsh interface ipv6 show address
Interfaz 1: Loopback Pseudo-Interface 1
Tipo direc. Estado DAD Vigencia válida Vigencia pref. Dirección
-----
Otros Preferido infinite infinite ::1
Interfaz 12: isatap.<EDD09246-727B-4E51-83D6-BAC76E3C0477>
Tipo direc. Estado DAD Vigencia válida Vigencia pref. Dirección
-----
Otros Obsoleto infinite infinite fe80::5efe:192.168.0.15%12
Interfaz 13: Teredo Tunneling Pseudo-Interface
Tipo direc. Estado DAD Vigencia válida Vigencia pref. Dirección
-----
Otros Obsoleto infinite infinite fe80::100:7f:ffffe%13
Interfaz 11: Conexión de área local
Tipo direc. Estado DAD Vigencia válida Vigencia pref. Dirección
-----
Manual Preferido infinite infinite 2001:db8:290c:1291::2
Otros Preferido infinite infinite fe80::e8e0:544c:1875:1c4%11
C:\Windows\system32>

```

Fuente: Del Autor

Siguiendo con la implementación del protocolo IPV6 En la oficina del Sisben que pertenece a la Alcaldía mayor de Tunja se hace la verificación por la consola CMD y se reemplaza con el comando ping a los diferentes equipos (Figura 41).

Figura 41. Comprobación de conectividad IPv6 comando Ping



```
Administrador: c:\Windows\System32\cmd.exe
Haciendo ping a ::9 con 32 bytes de datos:
PING: error en la transmisión. Error general.

Estadísticas de ping para ::9:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

C:\Windows\system32>ping ::1

Haciendo ping a ::1 con 32 bytes de datos:
Respuesta desde ::1: tiempo<1m
Respuesta desde ::1: tiempo<1m
Respuesta desde ::1: tiempo<1m
Respuesta desde ::1: tiempo<1m

Estadísticas de ping para ::1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Windows\system32>

Administrador: c:\Windows\System32\cmd.exe
quedado en desuso. Es posible que algunos sistemas anulen
-s srcaddr      solicitudes de eco si usa este encabezado.
-c compartment  Dirección de origen que se desea usar.
-p             Enrutamiento del identificador del compartimento.
              Hacer ping a la dirección del proveedor de Virtualización
              de red de Hyper-V.
-4            Forzar el uso de IPv4.
-6            Forzar el uso de IPv6.

C:\Windows\system32>ping 2801:130:100:1000:3ec5:16e9:9971:692e

Haciendo ping a 2801:130:100:1000:3ec5:16e9:9971:692e con 32 bytes de datos:
Respuesta desde 2801:130:100:1000:3ec5:16e9:9971:692e: tiempo<5ms
Respuesta desde 2801:130:100:1000:3ec5:16e9:9971:692e: tiempo<1m
Respuesta desde 2801:130:100:1000:3ec5:16e9:9971:692e: tiempo<1m
Respuesta desde 2801:130:100:1000:3ec5:16e9:9971:692e: tiempo<1m

Estadísticas de ping para 2801:130:100:1000:3ec5:16e9:9971:692e:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 5ms, Media = 1ms

C:\Windows\system32>
```

Fuente: Del Autor

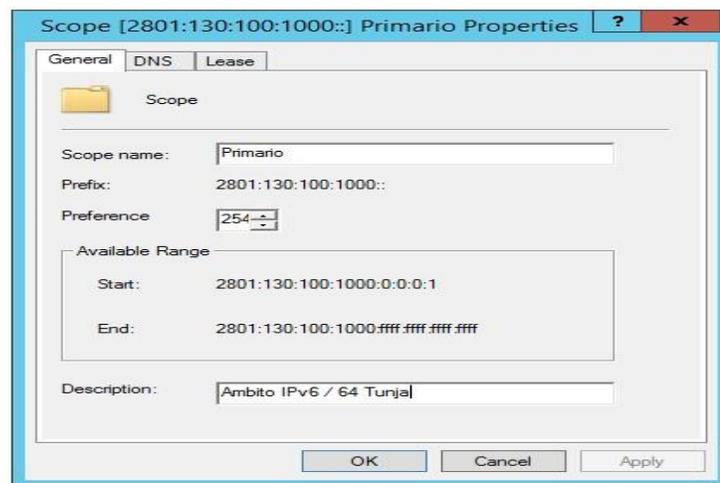
Ya teniendo los quipos de la secretaria del Sisben con protocolo de Seguridad IPV6 se configura el DNS. Que significa sistema de nombre de dominio esto consiste en asignar nombres de dirección IP para poder acceder a diferentes sitios sin tener que recordar valores numéricos.

Siguiendo con la comprobación del DNS para verificar que ya existen más equipos conectados de esta Secretaria del Sisben con el Protocolo IPV6.

Al ser muy tedioso el recordar el número hexadecimal correspondiente a los 8 grupos que constituyen la dirección IPV6 es necesario el uso del DNS el cual constituye una herramienta esencial de administración de redes LAN por lo que puede entregar la dirección según directrices de protocolos establecidos por la misma institución (Figura 42).

Ya establecido el segmento y cantidad de direccionamiento para el ipv6 se establece el inicio o primera dirección IPV6 y el final de las mismas

Figura 42. Configuración DNS Protocolo IPv6



Fuente: Del Autor

Siguiendo el proceso de comprobación voy a realizar el direccionamiento ya con el DNS cargado en los equipos de los diferentes funcionarios de la secretaria del Sisben de Tunja.

1.20. PRUEBAS DE CONECTIVIDAD

Figura 43. Pruebas DNS equipos IPv6 Secretaria Sisben

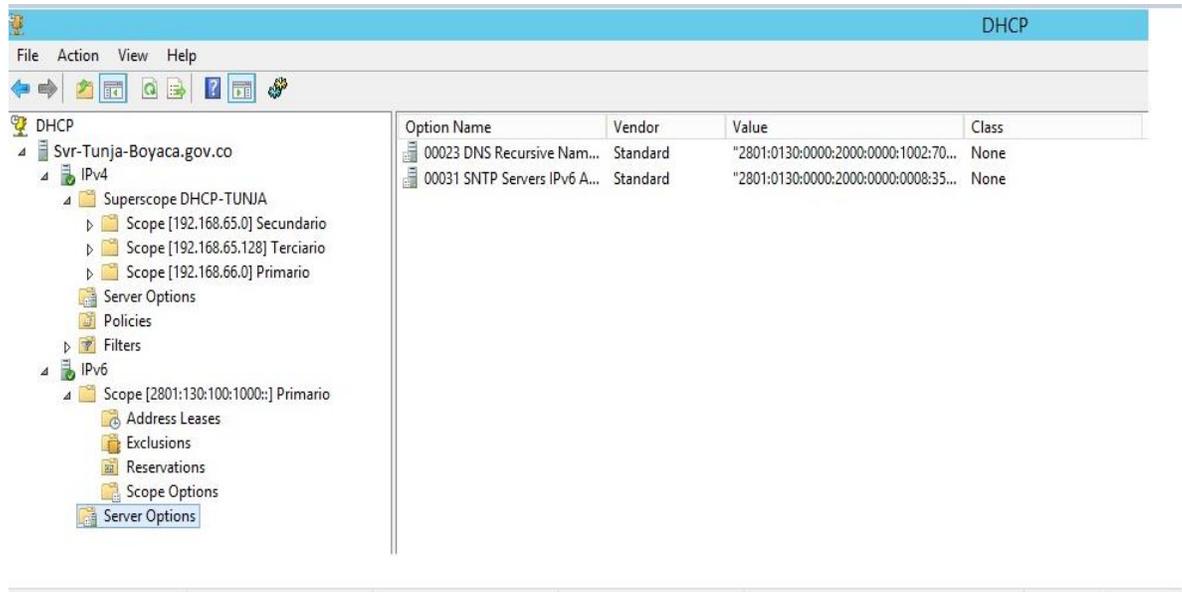
DHCP						
Client IPv6 Address	Name	Lease Expiration	IAID	Type	Unique ID	Description
2801:130:100:1000:459d:c5a...		23/05/2017 8:43:26 p. m.	0	IANA	000300013...	
2801:130:100:1000:a803:3729...		23/05/2017 9:06:38 p. m.	1507329	IANA	00030001f...	
2801:130:100:1000:a897:1d8...		23/05/2017 8:43:22 p. m.	0	IANA	000300013...	
2801:130:100:1000:becd:887...		23/05/2017 4:50:46 p. m.	2128607223	IANA	000416a99...	
2801:130:100:1000:102c:9aaa...	edger-VAIO	23/05/2017 7:10:01 p. m.	300990359	IANA	000100011...	
2801:130:100:1000:189d:ad2...	IMP_SCAN_BL-B	23/05/2017 8:01:01 p. m.	2	IANA	00030001d...	
2801:130:100:1000:63cb:867f...	IMP_SCAN_RYC	23/05/2017 8:27:00 p. m.	2	IANA	000300013...	
2801:130:100:1000:9b96:290...	IMP_SCAN_RYC	23/05/2017 6:55:57 p. m.	2	IANA	000300013...	
2801:130:100:1000:cd1c:570...	JUANPABLO	23/05/2017 8:56:48 p. m.	154676298	IANA	000100011...	
2801:130:100:1000:9861:c542...	NPI36F7E7	23/05/2017 8:41:01 p. m.	2	IANA	00030001d...	
2801:130:100:1000:5b65:7ef8...	NPIFA0091	23/05/2017 5:05:06 p. m.	2	IANA	000300013...	
2801:130:100:1000:dd79:74d...	NPIFA0091	23/05/2017 4:35:07 p. m.	2	IANA	000300013...	

DHCP				
Option Name	Vendor	Value	Class	
00023 DNS Recursive Nam...	Standard	"2801:0130:0000:2000:0000:1003:6003:8536", "	None	
00031 SNTP Servers IPv6 A...	Standard	"2801:0130:0000:2000:0000:0008:0766:27D0", "	None	
00342 Option Tel/Aways	Standard	242="L2Q=1,L2QvLAN=150,VLANTEST=0"	None	

Fuente: Del Autor

Para terminar la migración del protocolo se verifica el resultado en donde se puede verificar el doble apilamiento que corresponde al protocolo IPV4 y el protocolo IPV6, esto permite una transición progresiva uno a uno manteniendo la operación de la red y permitiendo administrar las transiciones.

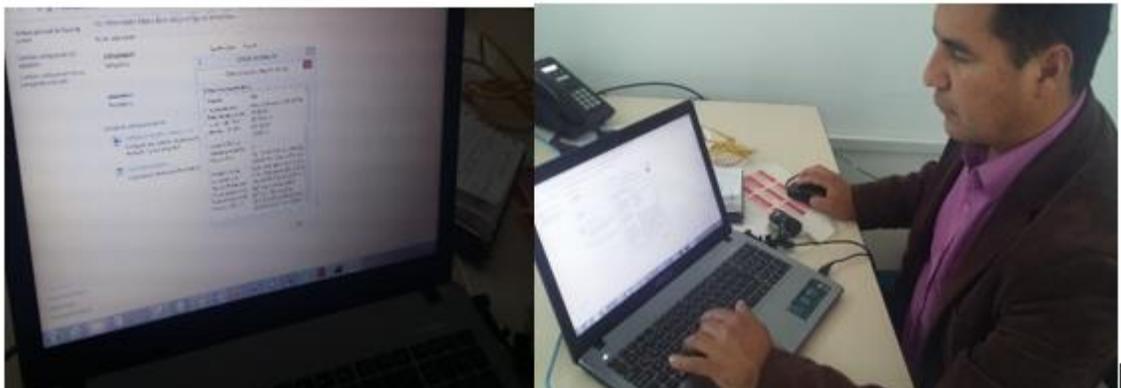
Figura 44. Coexistencia del protocolo IPv4 IPv6 Secretaria Sisben



Fuente: Del Autor

A continuación, se publican las fotos en las realizando la práctica de la migración del protocolo IPV4 A IPV6 En la cual hago ping en distintos equipos. En esta figura se refleja como quedo implementado el protocolo IPV6.

Figura 45. Pruebas de migración IPv4 a IPv6 Secretaria Sisben



Fuente: Del Autor

En esta otra imagen se realiza ping con diferentes equipos donde se muestra la configuración del protocolo IPV6.

Figura 46. Pruebas de migración IPv4 a IPv6 Secretaria Sisben (parte 2)

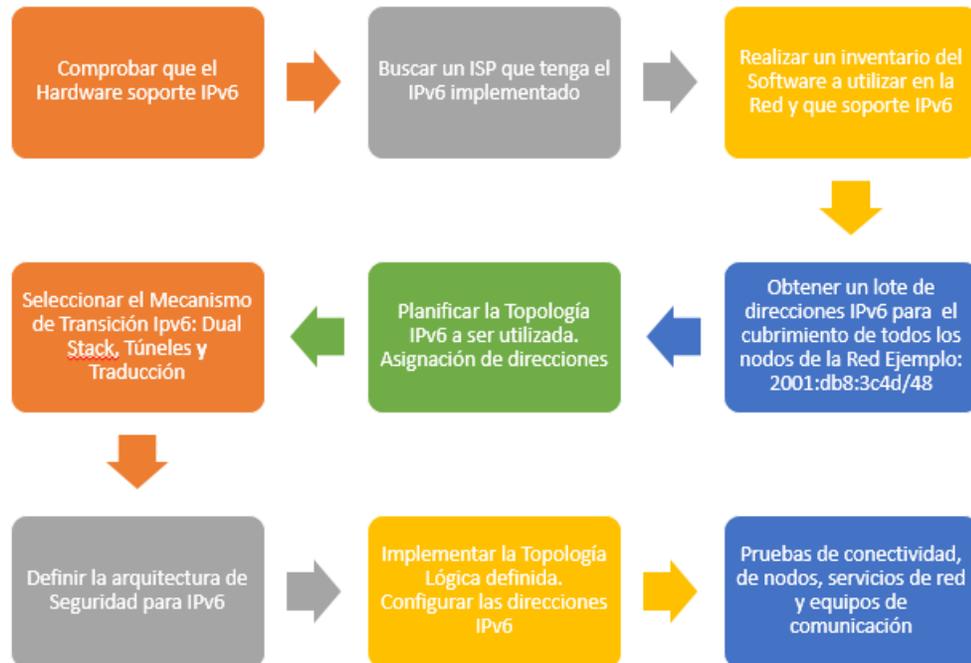


Fuente: **Del Autor**

1.21. HOJA DE RUTA PARA LA IMPLEMENTACION DE IPv6

Como proceso final del proyecto se propone una hoja de ruta con los pasos a tener en cuenta a la hora de implementar IPv6 en cualquier red de datos que cumpla con los requisitos mínimos para su desarrollo. Como evidencia de la implementación de la Hoja de Ruta se coloca en los Anexos “Carta de Referencia: Autorización de Implementación IPv4 IPv6 en la Secretaría de Protección Social y SISBEN de la Alcaldía Mayor de la Ciudad de Tunja”.

Figura 47. Guía de Implementación Ipv6



Fuente: Del Autor

- Comprobar que el Hardware soporte IPV6. Para este primer paso lo primero que se hizo fue revisar los equipos con que cuenta la Secretaria del Sisben, identificar los componentes de las redes y verificar que sean compatibles con el protocolo de Seguridad IPV6. La mayoría de las veces la implementación de IPV6 no modifica la topología de red (cables, enrutadores de red y hosts). Ahora bien, antes de configurar direcciones IPv6 en interfaces de red, es importante preparar para IPv6 el hardware y las aplicaciones.

- ✓ Verifique que el hardware de la red se pueda actualizar a IPv6. Por ejemplo, consulte la documentación de los fabricantes sobre la compatibilidad con IPv6 respecto a los siguientes tipos de hardware:

- ✓ Enrutadores
 - ✓ Servidores de seguridad
 - ✓ Conmutadores
- Disponer de un ISP Que administre IPV6. Comprobar que en nuestro operador de internet tenga implementado el protocolo de seguridad IPV6, como proceso opcional se pueden tener dos operadores uno con el protocolo de seguridad IPV4 y otro con protocolo IPV6.
 - Obtener lote de Direcciones IPV6 para cubrimiento de todos los nodos de la red ejemplo 2001:db8:3c4d.

Se debe planificar la topología de red global y el esquema de direcciones para poder configurar IPV6 en los distintos Nodos de la red. Un prefijo de IPv6 2001:db8:3c4d/48 se ha asignado a un sitio. Se puede entonces establecer la tabla de asignación de prefijos de IPv4 privados a prefijos de IPv6.

Prefijo de subred IPV4 Prefijo de subred ipv6 equivalente

192.168.1.0/24 2001:db8:3c4d:/1:64

192.168.3.0/24 2001:db8:3c4d:/2:64

192.168.3.0/24 2001:db8:3c4d:/3:64

192.168.4.0/24 2001:db8:3c4d:/1:64

- Planificar la Topología IPV6.

Se debe planificar la dirección de servidores, enrutadores y hosts antes de configurar IPv6.

- Seleccionar el mecanismo de transmisión IPV6 dual, stack, túneles y traducción.

✓ Migración de Túneles.

Esta técnica consiste en utilizar algún dispositivo en la red que convierta los paquetes de IPv4 a IPv6 y viceversa. Ese dispositivo tiene que ser capaz de realizar la traducción en los dos sentidos de forma permanente para permitir la comunicación.

✓ Migración de STACK

Este método de migración consiste en tener una red que soporte ambos protocolos IP. Los dispositivos intermediarios y los finales se configuran para admitir tanto IPV4 como IPV6 el protocolo preferido. Es la opción recomendada y requiere que se ejecute IPV4 e IPV6 Simultáneamente.

✓ Migración de Traducción

La Dirección General de Migración y Extranjería brinda las condiciones necesarias para el ciudadano extranjero mientras espera la resolución correspondiente de refugio o asilo, todo esto implica alimentación, atención médica y alojamiento.

CONCLUSIONES

Una vez terminado el proceso de migración del protocolo de seguridad IPv4 a IPv6 en la Secretaria del Sisben de la Alcaldía Mayor de Tunja, se garantiza la conectividad pues este protocolo responde a que múltiples usuarios estén conectado al mismo tiempo sin preocupación de que se queden sin acceso a los recursos y la red.

Al inicio del proyecto se presentaron algunos inconvenientes entre los usuarios como, desconocimiento de este nuevo protocolo, implicaciones de conectividad, resistencia al cambio, temor al cambio de su rutina o proceso de trabajo, los cuales se fueron solucionando una vez realizada la nueva implementación del protocolo IPv6.

Con la nueva implementación del protocolo de seguridad IPv6 en la Secretaria del Sisben de la ciudad de Tunja, se pretende brindar una mayor seguridad de la información y ante todo mejorar la posibilidad de ampliar su conectividad logrando un cambio progresivo en el funcionamiento de toda la red de comunicación, las aplicaciones y los servicios generando mejores resultados a mediano y largo plazo. Es de aclarar que con la versión IPv4 no se contaba con políticas de seguridad específicas para manejo del protocolo.

En la Secretaria del Sisben se mejora la señal de Internet con la migración del Protocolo IPV4 a IPV6 esta secretaria ya no tendrá que preocuparse por el agotamiento de las direcciones IP, pues con esta migración se garantiza que las infraestructuras de internet funcionen de la mejor manera ofreciendo a los funcionarios y usuarios los mejores servicios y gran cobertura de conexión.

Con la migración progresiva o paulatina del Protocolo IPV4 a IPV6 se pretende establecer una convivencia satisfactoria entre dos protocolos sin que perjudique el funcionamiento de los equipos, lo cual brinda una seguridad para todos los dispositivos que se conecten.

Para finalizar, el proyecto final de la Especialización en Seguridad Informática en la migración del protocolo IPV4 a IPV6 se da cumplimiento a los alineamientos dados del ministerio de las TIC los cuales buscan que todas las entidades públicas del estado implanten este Protocolo en sus dependencias para mejorar los servicios a la comunidad en general.

RECOMENDACIONES

Como recomendación, si se implementa la migración del protocolo IPv4 a IPv6 primero hay que solicitar al proveedor de Internet (ISP) que nos informe si ya viene integrado el servicio de direccionamiento IPv6.

Verificar que los equipos de cómputo y equipos de conectividad tengan la infraestructura y el sistema operativo con los requerimientos mínimos necesarios para soportar el protocolo de seguridad IPV6.

Tener en cuenta un plan de contingencia con el análisis de los dispositivos conectados de forma alámbrica y que tengan los requerimientos de IPV6 y evaluar su funcionamiento para verificar su velocidad y seguridad en sus equipos.

Se requiere realizara capacitaciones continuas con el personal que trabaja en la Secretaria del Sisben de la Alcaldia Mayor de Tunja, con el fin de darles a conocer cuáles son las ventajas de la implementación del protocolo IPv6 y de la misma manera se conozcan las ventajas de seguridad con esta nueva implementación.

BIBLIOGRAFÍA

Alcaldiabogota.gov.co. (2017). Consulta de la Norma. [en línea], [Revisado 23 Nov. 2017]. Disponible en Internet:

<http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913>.

Alcancelibre.org. (2017). Introducción a IP versión 4. - Alcance Libre. [en línea], [Revisado 23 Nov. 2017] Disponible en Internet:

<http://www.alcancelibre.org/staticpages/index.php/introdu>.

Cantu, D. (2017). IPv4 vs IPv6 - ¿Cuál es la diferencia? Ipv6.mx [en línea], [Revisado 23 Nov. 2017]. Disponible en Internet:

<http://ipv6.mx/index.php/component/content/article/189-ipv4-vs-ipv6-icual-es-la-diferencia>.

CCM. (2017). Protocolo IPv6. [en línea], [Revisado 23 Nov. 2017]. Disponible en Internet: <http://es.ccm.net/contents/268-protocolo-ipv6>.

Certsuperior.com. (2017). Seguridad en redes | Cert Superior. [en línea], [Accessed 13 Dec. 2017]. Disponible en Internet:

<https://www.certsuperior.com/SeguridadenRedes.aspx>.

Dcc.uchile.cl. (2017). Citar un sitio web - Cite This For Me. [en línea], [Accessed 12 Dec. 2017]. Disponible en Internet: https://www.dcc.uchile.cl/sites/default/files/DCC-Inside/FCFM_40_Se_agotan_direcciones_IP.pdf.

Definista (2017). ¿Qué es Internet? - Su Definición, Concepto y Significado. [En línea], [Revisado 23 Nov. 2017]. ConceptoDefinicion.de. Disponible en Internet:

<http://conceptoDefinicion.de/internet/>.

Es.wikipedia.org. (2017). Seguridad de redes. [en línea], [Revisado 12 Dec. 2017]. .

Disponible en Internet: https://es.wikipedia.org/wiki/Seguridad_de_redes.

Genbeta.com. (2017). Las últimas direcciones IPv4 se han agotado, IPv6 es la solución. [en línea], [Revisado 23 Nov. 2017]. Disponible en Internet: <https://www.genbeta.com/actualidad/las-ultimas-direcciones-ipv4-se-han-agotado-ipv6-es-la-solucion>.

Gómez Prieto, N. and Torres Rojas, Y. (2017). Migración de red IPV4 A IPV6 sobre la red del Ejército Nacional. [en línea], [Revisado 7 Dec. 2017]Hdl.handle.net. Disponible en Internet: <http://hdl.handle.net/10596/1570>

Incibe.es. (2017). MPLEMENTACIÓN DE IPSEC. [en línea], [Revisado 13 Dec. 2017] Disponible en Internet: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_implantacion_ipv6.pdf.

IoT cosas, L. (2017). La historia detrás de la internet de las cosas. elespectador.com. [en línea], [Revisado 12 Dec. 2017]. Disponible en Internet: <https://www.elespectador.com/tecnologia/la-historia-detras-de-la-internet-de-las-cosas-articulo-716678>.

Ipv6.mx. (2017). Fundamentos IPv6. [en línea], [Revisado 23 Nov. 2017]. Disponible en Internet: <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>.

Livre.g6.asso.fr. (2017). Introduccion - Livre IPv6. [en línea], [Revisado 12 Dec. 2017] Disponible en Internet: <http://livre.g6.asso.fr/index.php/Introduccion>.

Mintic.gov.co. (2017). Circular 00002 de 2011 - Ministerio de Tecnologías de la Información y las Comunicaciones. [en línea], [Reviado 25 Oct. 2017]. Disponible en Internet: <http://www.mintic.gov.co/portal/604/w3-article-5932.html>.

Mintic.gov.co. (2017). Citar un sitio web - Cite This For Me. [en línea], [Revisado 23 Nov. 2017] Disponible en Internet: http://www.mintic.gov.co/portal/604/articles-61000_documento.pdf.

Mintic.gov.co. (2017). Citar un sitio web - Cite This For Me. [en línea], [Revisado 10 Oct. 2017]. Disponible en Internet: http://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf.

Mintic.gov.co. (2017). Documentos IPv6 - Ministerio de Tecnologías de la Información y las Comunicaciones. [en línea], [Revisado 23 Nov. 2017]. Disponible en Internet: <http://www.mintic.gov.co/portal/604/w3-article-5903.html>.

Mintic.gov.co. (2017). Entra en vigencia la resolución 2710 del 2017 para la implementation del protocolo IPv6 en Colombia - Ministerio de Technologies de la Information y las Comunicaciones. [en línea], [Revisado 2 Agosto. 2017]. Disponible en Internet: <http://www.mintic.gov.co/portal/604/w3-article-61192.html>.

Network-inventory-advisor.com. (2017). Network Inventory Advisor: Software de gestión de activos de PC. [en línea], [Revisado 28 Nov 2017]. Disponible en Internet: <https://www.network-inventory-advisor.com/es/>.

Portalipv6.lacnic.net. (2017). Portal IPv6 - LACNIC. [en línea], [Revisado 10 Nov. 2017], Disponible en Internet: <http://portalipv6.lacnic.net/mecanismos-de-transicion/>.

Portalipv6.lacnic.net. (2017). Portal IPv6 - LACNIC. [en línea], [Revisado 23 Nov. 2017]. Disponible en Internet: <http://portalipv6.lacnic.net/tunelesencapsulamiento/>.

Portalipv6.lacnic.net. (2017). Portal IPv6 - LACNIC. [en línea], [Revisado 23 Nov. 2017] Disponible en Internet: <http://portalipv6.lacnic.net/traduccion/>.

Psicol.unam.mx. (2017). Métodos de Investigación. [en línea], [Revisado 3 Nov. 2017] . Disponible en Internet: <http://www.psicol.unam.mx/Investigacion2/pdf/METO2F.pdf>.

Repositorio.ucp.edu.co. (2017). Citar un sitio web - Cite This For Me. [en línea], [Revisado 7 Dec. 2017].Disponible en Internet: <http://repositorio.ucp.edu.co:8080/jspui/bitstream/10785/958/1/CDMIST45.pdf>

Repositorio.utp.edu.co. (2017). Citar un sitio web - Cite This For Me. [en línea], [Revisado 13 Dec. 2017]. Disponible en Internet:
<http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2073/004678E82.pdf;sequence=1>.

Repository.ucatolica.edu.co. (2017). Citar un sitio web - Cite This For Me. [en línea], [Revisado 7 Nov. 2017]. Disponible en Internet:
<http://repository.ucatolica.edu.co/bitstream/10983/2803/1/IPV6.pdf>.

Repository.unilibre.edu.co. (2017). Citar un sitio web - Cite This For Me. [en línea], [Revisado 7 Dec. 2017]. Disponible en Internet:
<http://repository.unilibre.edu.co/bitstream/handle/10901/8797/MONOGRAFIA%20MECANISMOS%20DE%20TRANSICIÓN%20DE%20IPV4%20A%20IPV6.pdf?sequence=1>

Rodin.uca.es. (2017). Cite a Website - Cite This For Me. [en línea], [Revisado 23 Nov. 2017]. Disponible en Internet:
http://rodin.uca.es/xmlui/bitstream/handle/10498/16833/temaIII_tcpip.pdf.

Stadium.unad.edu.co. (2017). Citar un sitio web - Cite This for Me. [en línea], [Revisado 7 Dec. 2017]. Disponible en Internet:
<http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/12015/1/14703624.pdf>.

Tecnologías, S., Services, I. and Tecnología, P. (2017). Network Address Translation (NAT) FAQ. [en línea] Cisco. [Revisado 12 Dec. 2017]. Disponible en Internet:
https://www.cisco.com/c/es_mx/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html.

