

UNIVERSIDAD  
**NACIONAL**  
DE COLOMBIA

# **Diseño de una red altamente disponible VxLAN para la transición de protocolo Ipv4 a Ipv6 en el datacenter del Departamento Nacional de Planeación.**

Juan Carlos Navarro Bastidas

Universidad Nacional de Colombia  
Facultad Ingeniería, Departamento Ingeniería de Sistemas e  
Industrial  
Bogotá, Colombia  
2021

# **Diseño de una red altamente disponible VxLAN para la transición de protocolo Ipv4 a Ipv6 en el datacenter del Departamento Nacional de Planeación.**

Juan Carlos Navarro Bastidas

Trabajo de grado presentado como requisito parcial para optar al título de:

**Magíster en Ingeniería Telecomunicaciones**

Director:

MSc. Cesar Manuel Lovera Cabrera

Línea de Investigación:

Redes y Sistemas de Telecomunicaciones

Área:

Ciencia y tecnología

Universidad Nacional de Colombia  
Facultad Ingeniería, Departamento Ingeniería de Sistemas e  
Industrial  
Bogotá, Colombia

2021

*Lema*

*A veces sales de la cama en la mañana y piensas que no lo podrás lograr, pero te ríes por dentro porque recuerdas todas las veces que te has sentido de esa forma.*

*Charles Bukowski*



## **Declaración de obra original**

Yo declaro lo siguiente:

He leído el Acuerdo 035 de 2003 del Consejo Académico de la Universidad Nacional. «Reglamento sobre propiedad intelectual» y la Normatividad Nacional relacionada al respeto de los derechos de autor. Esta disertación representa mi trabajo original, excepto donde he reconocido las ideas, las palabras, o materiales de otros autores.

Cuando se han presentado ideas o palabras de otros autores en esta disertación, he realizado su respectivo reconocimiento aplicando correctamente los esquemas de citas y referencias bibliográficas en el estilo requerido.

He obtenido el permiso del autor o editor para incluir cualquier material con derechos de autor (por ejemplo, tablas, figuras, instrumentos de encuesta o grandes porciones de texto).

Por último, he sometido esta disertación a la herramienta de integridad académica, definida por la universidad.

Juan Carlos Navarro Bastidas

Nombre

09/03/2022

Fecha

## **Agradecimientos**

*"A todas las personas que me apoyaron e hicieron posible que este trabajo se realice con éxito.*

*En especial a mi tutor por compartirme sus conocimientos.*

*A toda mi familia y amigos por acompañarme en este proceso ."*

# Resumen

## **Diseño de una red altamente disponible VxLAN para la transición de protocolo Ipv4 a Ipv6 en el datacenter del Departamento Nacional de Planeación**

Este trabajo final de maestría propone un nuevo de diseño y simulación de red basado en la nueva generación de redes orientadas a software VxLAN, generando una red altamente disponible para la infraestructura del Departamento Nacional de Planeación de Colombia. Por este motivo es necesario hacer previamente un reconocimiento de la red actual del centro de datos a través de la medición de variables, rendimiento y capacidad de los equipos para generar una transición hacia el protocolo de red IPv6. Basado en los datos suministrados, se debe generar un análisis donde se evidencie la compatibilidad del hardware, software y velocidades necesarias para el desarrollo del proyecto.

Por consiguiente, se genera un nuevo diseño de la red actual, involucrando los equipos que conforman la topología, los cuales serán de mayor importancia al momento de generar una simulación que posteriormente podrá ser implementada por la empresa.

Por último, con las pruebas generadas es necesario desencadenar una serie de conclusiones que permita ayudar a la generación de nuevas implementaciones basadas en el documento.

**Palabras clave: (IPv4, IPv6, Doble Pila, DNP, Topología de red, Centro de datos)**

## **Abstract**

**Design of a highly available VxLAN network for the transition from IPv4 to IPv6 protocol in the datacenter of the National Planning Department.**

This degree work proposes a new network design and simulation based on the new generation of VxLAN software-oriented networks, generating a highly available network for the infrastructure of the National Planning Department of Colombia. For this reason, it is necessary to first make a recognition of the current data center network through the measurement of variables, performance, and capacity of the equipment to generate a transition to the IPv6 network protocol. Based on the data supplied, an analysis must be generated where the compatibility of the hardware, software, and speeds necessary for the development of the project is evidenced. Consequently, a new design of the current network is generated, involving the equipment that make up the topology, which will be of greater importance when generating a simulation that can later be implemented by the company. Finally, with the generated tests, it is necessary to unleash a series of conclusions to help generate new implementations based on the document.

**Keywords: (IPv4, IPv6, Dual Stack, DNP, Network Topology, Data Center)**





Este Trabajo Final de maestría fue calificado en mayo de 2022 por el siguiente evaluador:

Jorge Eduardo Ortíz Triviño PhD.  
Profesor Facultad de Ingeniería  
Universidad Nacional de Colombia

## Tabla de contenido

<b>1. Introducción.....</b>	<b>17</b>
<b>2. Marco Teórico.....</b>	<b>18</b>
<b>2.1 Protocolos Ip.....</b>	<b>20</b>
2.1.1 Ipv4.....	20
2.1.2 Ipv6.....	20
2.1.3 Agotamiento de las direcciones Ipv4.....	21
2.1.4 Comparación entre protocolos Ipv4 e Ipv6.....	21
<b>2.2 Mecanismos de transición.....</b>	<b>23</b>
2.2.1 Mecanismos de tipo túnel.....	23
2.2.2 Mecanismos de traducción.....	25
2.2.3 DualStack.....	25
<b>2.3 Redes de área local Virtual.....</b>	<b>26</b>
2.3.1 VLAN en Ipv4.....	26
2.3.2 VxLAN.....	27
2.3.3 Comparación entre VLAN y VxLAN.....	27
<b>3. Marco legal.....</b>	<b>29</b>
3.1 Lineamientos básicos del MinTIC.....	29
3.2 Fase 1 Planeación.....	29
3.3 Fase 2 Implementación.....	30
3.4 Fase 3 Pruebas de funcionalidad.....	30
3.2 Circular 002 de 2011 “Promoción de la adopción de Ipv6 en Colombia”.....	31
3.3 Resolución 180 de 2010 la Unión Internacional de Telecomunicaciones (UIT).....	32
3.4 Resolución 64 de 2012 de la Asamblea Mundial de Normalización.....	32
3.5 Resolución 2710 de 2017.....	33
3.6 ¿Qué se ha hecho en Colombia respecto al protocolo Ipv6?.....	34
<b>4. Requisitos previos.....</b>	<b>35</b>
4.1 Capacitación.....	35
4.2 Programa de Emulación.....	35
<b>5. Indagación de la red actual del Departamento Nacional de Planeación.....</b>	<b>36</b>
5.1 Topología actual en el centro de datos de la empresa.....	38

<b>5.2 Funcionamiento de la red actual en datacenter de la empresa.....</b>	<b>39</b>
<b>5.3 Inventario de equipos de comunicaciones .....</b>	<b>40</b>
<b>5.4 Inventario de equipos de infraestructura .....</b>	<b>42</b>
<b>5.5 Inventario de equipos de seguridad .....</b>	<b>44</b>
<b>5.6 Emulación topología actual .....</b>	<b>45</b>
<b>5.7 Pruebas de comunicación a través de la MPLS .....</b>	<b>56</b>
<b>5.8 Resultado de pruebas realizadas.....</b>	<b>59</b>
<b>6. Nuevo diseño de red .....</b>	<b>62</b>
<b>6.1 Direccionamiento propuesto en Ipv6 .....</b>	<b>63</b>
<b>6.1.1 Direccionamiento DualStack equipos Core.....</b>	<b>64</b>
<b>6.2 Topología de red propuesta en Ipv6.....</b>	<b>66</b>
<b>6.3 Validación experimental y ambiente de prueba.....</b>	<b>66</b>
<b>6.4 Configuración de topología en DualStack por medio de red Ipv6 .....</b>	<b>68</b>
<b>6.5 Implementación de VxLAN .....</b>	<b>76</b>
<b>6.5.1 Direccionamiento de VxLAN.....</b>	<b>76</b>
<b>6.5.2 Implementación en Zona franca.....</b>	<b>77</b>
<b>6.5.3 Implementación en DNP.....</b>	<b>79</b>
<b>6.5.4 Configuración de servidores .....</b>	<b>80</b>
<b>6.6 Pruebas de funcionamiento VxLAN.....</b>	<b>81</b>
<b>6.6.1 Pruebas de DualStack por medio de VxLAN.....</b>	<b>81</b>
<b>6.7 Configuración de servidores a través de DNS.....</b>	<b>82</b>
<b>6.7.1.1 Implementación DNS .....</b>	<b>82</b>
<b>6.7.2 Implementación DNS DNP .....</b>	<b>83</b>
<b>6.8 Resultado de pruebas realizadas .....</b>	<b>83</b>
<b>6.8.1 Pruebas desde sede alterna .....</b>	<b>83</b>
<b>6.8.1.1 Configuración de Router.....</b>	<b>84</b>
<b>6.8.1.2 Configuración de PC.....</b>	<b>85</b>
<b>6.8.1.2 Salida a internet del PC .....</b>	<b>86</b>
<b>6.8.1.3 Prueba de resolución de DNS externo.....</b>	<b>86</b>
<b>6.8.1.4 Prueba de resolución de DNS interno .....</b>	<b>88</b>
<b>7. Conclusiones .....</b>	<b>90</b>

<b>8. Recomendaciones .....</b>	<b>91</b>
<b>9. Bibliografía .....</b>	<b>92</b>

## Lista de tablas

<b>TABLA 1.</b> TABLA COMPARATIVA ENTRE IPV4 E IPV6 .....	22
<b>TABLA 2.</b> MÉTODOS DE TRANSICIÓN HACIA IPV6 .....	24
<b>TABLA 3.</b> TIPOS DE TÚNELES EN IPV6 .....	25
<b>TABLA 4.</b> COMPARACIÓN ENTRE VLAN Y VXLAN .....	28
<b>TABLA 5.</b> DIRECCIONAMIENTO DE DNP EN IPV4 .....	39
<b>TABLA 6.</b> INVENTARIO DE CARACTERÍSTICAS FÍSICAS DE ROUTER Y SWITCH .....	40
<b>TABLA 7.</b> CARACTERÍSTICAS LÓGICAS DE ROUTER Y SWITCH .....	42
<b>TABLA 8.</b> INVENTARIO DE EQUIPO DE INFRAESTRUCTURA .....	43
<b>TABLA 9.</b> CARACTERÍSTICAS LÓGICAS DE SERVIDORES .....	43
<b>TABLA 10.</b> CARACTERÍSTICAS FÍSICAS DE LOS FIREWALL .....	44
<b>TABLA 11.</b> CARACTERÍSTICAS LÓGICAS DE LOS FIREWALL .....	45
<b>TABLA 12.</b> DIRECCIONAMIENTO DUALSTACK EQUIPOS CORE .....	65
<b>TABLA 13.</b> DIRECCIONAMIENTO PARA PROTOCOLO VXLAN .....	77

## Lista de figuras

FIGURA 1. FUNCIONAMIENTO DE DUALSTACK .....	26
FIGURA 2. EMULADOR GRÁFICO DE REDES VERSIÓN 3 .....	36
FIGURA 3. TOPOLOGÍA EN RACK DNP .....	37
FIGURA 4. TOPOLOGÍA LÓGICA DE DNP .....	38
FIGURA 5. CONFIGURACIÓN ISPCORE .....	46
FIGURA 6. CONFIGURACIÓN ROUTER CLARO ZONA FRANCA .....	47
FIGURA 7. CONFIGURACIÓN ROUTER CLARO DNP .....	47
FIGURA 8. CONFIGURACIÓN ROUTER ZONA FRANCA 1 Y 2 .....	48
FIGURA 9. CONFIGURACIÓN ROUTER DNP 1 Y 2 .....	48
FIGURA 10. CONFIGURACIÓN ALTA DISPONIBILIDAD FIREWALL ZONA FRANCA .....	49
FIGURA 11. CONFIGURACIÓN PUERTO WAN FIREWALL ZONA FRANCA .....	49
FIGURA 12. CONFIGURACIÓN PUERTO DE GESTIÓN FIREWALL ZONA FRANCA .....	50
FIGURA 13. CONFIGURACIÓN VLAN Y LACP ZONA FRANCA .....	50
FIGURA 14. CONFIGURACIÓN DE GRUPO DE VLAN FIREWALL ZONA FRANCA .....	50
FIGURA 15. SALIDA A INTERNET DE VLAN FIREWALL ZONA FRANCA .....	51
FIGURA 16. CONFIGURACIÓN ALTA DISPONIBILIDAD FIREWALL DNP .....	51
FIGURA 17. CONFIGURACIÓN PUERTO WAN FIREWALL DNP .....	52
FIGURA 18. CONFIGURACIÓN PUERTO DE GESTIÓN FIREWALL DNP .....	52
FIGURA 19. CONFIGURACIÓN DE VLANS Y LACP DNP .....	52
FIGURA 20. CREACIÓN DE POLÍTICAS FIREWALL DNP .....	53
FIGURA 21. CONFIGURACIÓN DE SWITCH ZONA FRANCA 1 .....	53
FIGURA 22. CONFIGURACIÓN DE SWITCH ZONA FRANCA 2 .....	54
FIGURA 23. CONFIGURACIÓN DE SWITCH DNP 1 .....	54
FIGURA 24. CONFIGURACIÓN DE SWITCH DNP 2 .....	55
FIGURA 25. CONFIGURACIÓN DE SERVIDORES .....	55
FIGURA 26. TABLA DE ENRUTAMIENTO ISPCORE IPV4 .....	56
FIGURA 27. TABLA DE ENRUTAMIENTO ROUTER CLARO ZONA FRANCA IPV4 .....	56
FIGURA 28. TABLA DE ENRUTAMIENTO ROUTER CLARO DNP IPV4 .....	57
FIGURA 29. TABLA DE ENRUTAMIENTO ROUTER ZONA FRANCA 1 IPV4 .....	57
FIGURA 30. TABLA DE ENRUTAMIENTO ROUTER ZONA FRANCA 2 IPV4 .....	58
FIGURA 31. TABLA DE ENRUTAMIENTO ROUTER DNP 1 IPV4 .....	58
FIGURA 32. TABLA DE ENRUTAMIENTO ROUTER DNP 2 IPV4 .....	58
FIGURA 33. TABLA DE ENRUTAMIENTO FIREWALL ZONA FRANCA IPV4 .....	59
FIGURA 34. PRUEBAS DE PING DESDE SEDE ZONA FRANCA IPV4 .....	60
FIGURA 35. TABLA DE ENRUTAMIENTO FIREWALL DNP IPV4 .....	61
FIGURA 36. PRUEBAS DE PING DESDE SEDE DNP IPV4 .....	61
FIGURA 38. TOPOLOGÍA EMULADA EN GNS3 .....	67
FIGURA 39. CONFIGURACIÓN ROUTER ISPCORE IPV6 .....	68
FIGURA 40. CONFIGURACIÓN ROUTER CLARO ZONA FRANCA IPV6 .....	68
FIGURA 41. CONFIGURACIÓN ROUTER CLARO DNP IPV6 .....	69
FIGURA 42. CONFIGURACIÓN ROUTER ZONA FRANCA 1 IPV6 .....	69
FIGURA 43. CONFIGURACIÓN ROUTER CLARO ZONA FRANCA 2 IPV6 .....	69
FIGURA 44. CONFIGURACIÓN ROUTER CLARO DNP 1 IPV6 .....	70
FIGURA 45. CONFIGURACIÓN ROUTER CLARO DNP 2 IPV6 .....	70
FIGURA 46. HABILITACIÓN PROTOCOLO IPV6 EN FIREWALL .....	71
FIGURA 47. CONFIGURACIÓN IPV6 FIREWALL ZONA FRANCA .....	71
FIGURA 48. CONFIGURACIÓN IPV6 FIREWALL DNP .....	71
FIGURA 49. CONFIGURACIÓN DE ROUTER SEDE WORLD SERVICE .....	72
FIGURA 50. TABLA DE ENRUTAMIENTO ISPCORE IPV6 .....	72
FIGURA 51. TABLA DE ENRUTAMIENTO CLARO ZONA FRANCA IPV6 .....	73
FIGURA 52. TABLA DE ENRUTAMIENTO CLARO DNP IPV6 .....	73

FIGURA 53. TABLA DE ENRUTAMIENTO ZONA FRANCA 1 IPV6.....	74
FIGURA 54. TABLA DE ENRUTAMIENTO ZONA FRANCA 2 IPV6.....	74
FIGURA 55. TABLA DE ENRUTAMIENTO DNP 1 IPV6 .....	75
FIGURA 56. TABLA DE ENRUTAMIENTO DNP 2 IPV6 .....	75
FIGURA 57. TABLA DE ENRUTAMIENTO SEDE WORLD SERVICE IPV6 .....	76
FIGURA 58. CONFIGURACIÓN FIREWALL ZONA FRANCA TÚNEL VxLAN .....	77
FIGURA 59. APROVISIONAMIENTO DE LOS PUERTOS DE VxLAN FIREWALL ZONA FRANCA .....	78
FIGURA 60. APROVISIONAMIENTO DEL PUERTO DE SALIDA DE VxLAN FIREWALL ZONA FRANCA .....	78
FIGURA 61. CONFIGURACIÓN DE INTERFACES VxLAN FIREWALL ZONA FRANCA.....	78
FIGURA 62. CONFIGURACIÓN FIREWALL DNP TÚNEL VxLAN .....	79
FIGURA 63. APROVISIONAMIENTO DE LOS PUERTOS DE VxLAN FIREWALL DNP .....	79
FIGURA 64. APROVISIONAMIENTO DEL PUERTO DE SALIDA DE VxLAN FIREWALL DNP .....	79
FIGURA 65. CONFIGURACIÓN DE INTERFACES VxLAN FIREWALL DNP.....	80
FIGURA 66. CONFIGURACIÓN DE SERVIDORES IPV6.....	80
FIGURA 67. TRÁFICO DEL TÚNEL VxLAN DESDE FIREWALL ZONA FRANCA.....	81
FIGURA 68. TRÁFICO DEL TÚNEL VxLAN DESDE FIREWALL DNP .....	81
FIGURA 69. PRUEBAS DE IPV4 A TRAVÉS DEL TÚNEL VxLAN .....	81
FIGURA 70. PRUEBAS DE IPV6 A TRAVÉS DEL TÚNEL VxLAN .....	82
FIGURA 71. CONFIGURACIÓN DE DNS DUALSTACK ZONA FRANCA.....	82
FIGURA 72. CONFIGURACIÓN DE DNS DUALSTACK DNP .....	83
FIGURA 73. CONFIGURACIÓN DE ROUTER WORLD SERVICE EN DUALSTACK.....	84
FIGURA 74. CONFIGURACIÓN DE PC WORLD SERVICE.....	85
FIGURA 75. CONFIGURACIÓN DE DNS EN PC WORLD SERVICE .....	85
FIGURA 76. PRUEBAS DE PING EN DUALSTACK.....	86
FIGURA 77. RESOLUCIÓN DNS EN MÁQUINA WORLD SERVICE .....	86
FIGURA 78. PRUEBA DE INGRESO A GOOGLE.COM .....	87
FIGURA 79. PRUEBA DE INGRESO A YAHOO.COM .....	87
FIGURA 80. PRUEBA DE INGRESO A YOUTUBE.COM.....	87
FIGURA 81. PRUEBA DE RESOLUCIÓN DE DNS INTERNO .....	88
FIGURA 82. PRUEBA HACIA PÁGINA DNP.....	88
FIGURA 83. PRUEBA HACIA PÁGINA SISBEN .....	89
FIGURA 84. PRUEBA HACIA PÁGINA SISCONPES .....	89
FIGURA 85. PRUEBA HACIA SERVER TFTP .....	89



## 1. Introducción

El día de hoy el internet es parte fundamental de los seres humanos con un total de 4.540 millones de personas que están conectadas a la red en todo el mundo, gracias a los avances tecnológicos el día de hoy, en cuestión de milésimas de segundo se puede generar una interacción con una persona estando a miles de kilómetros de distancia, por este motivo se genera la necesidad de nuevas tecnologías, protocolos y demás herramientas que permitan seguir conectados al mundo [Campher ,2020].

Con el inicio del internet que conocemos hoy en día en el año 1983 donde luego de varias versiones experimentales del protocolo IP, se logra desarrollar la cuarta versión de este protocolo; con esto se ha logrado la conexión de todos los proveedores de componentes informáticos, gracias a su óptimo funcionamiento sigue siendo raído hoy en día, teniendo varias características esenciales como una cantidad de 4300 millones de direcciones que en su momento se esperaba nunca ocupar pero por la mala administración a lo largo de los años se fueron agotando. Por este motivo en 2011 la IANA (Autoridad de asignación de números en internet) asigna el último direccionamiento disponible a nivel mundial lo que conlleva a la necesidad de migrar a una nueva tecnología, por la amenaza de agotamiento de direcciones para el acceso a internet [Delong, 2017].

Por este motivo, se genera una sexta versión del protocolo IP que tiene la capacidad de albergar una cantidad de 340 sextillones de direcciones. El vasto espacio de direccionamiento en el protocolo IPv6 es capaz de hacer frente al crecimiento mundial de Internet teniendo en cuenta la creación y aparición de dispositivos adaptables, como PDAs, teléfonos inteligentes, artículos del hogar, movilidad inteligente y una variedad de nuevas tecnologías [Wang, 2011].

La gran cantidad de direcciones IPv6 genera la necesidad de tener una cantidad de subredes mucho más amplia con la cual se distribuyen las redes a nivel interno, dado que el protocolo que tenía predeterminada el protocolo IPv4 es

VLAN (Subredes en redes locales), la cual cuenta con un número total de 4094 de subredes. Por lo tanto, se crea a su vez el protocolo VxLAN (Subredes virtuales extensibles en redes locales) el cual permite una cantidad de 16 millones de subredes [Juniper,2020].

El uso de estos dos protocolos IPv6 junto con VxLAN tiene la capacidad de creación de nuevas topologías para los centros de datos que se catalogan de nueva generación, supliendo la necesidad de tener cada vez más equipos conectados [Jopseph, 2020].

Por este motivo se planteará el diseño y simulación del uso de los protocolos anteriormente mencionados a partir de los centros de datos del Departamento Nacional de Planeación. Por tal motivo los resultados obtenidos podrán ser utilizados para la puesta en marcha y continuar con la necesidad de innovación de las empresas.

## 2. Marco Teórico

Con el fin de apodar el cambio de los protocolos que conllevaron a lo que hoy en día se utiliza para la vinculación a la internet, se describen de modo resumida cada una de las versiones que a lo dispendioso de la narración han existido y que a su vez han optado por las nuevas tecnologías<sup>1</sup>.

Los inicios del internet datan de 1969 con la génesis de la primera red de computadores por medio de la Red de la Agencia de Proyectos de Investigación Avanzada (ARPANET), donde se realizó el lazo de los primeros cuatro nodos teniendo la zona de influencia de expedir comunicación entre sí<sup>2</sup>. Hasta ese segundo cada uno de los fabricantes de piezas de computadores tenían

---

[1] <sup>1</sup> Historia de internet.” <https://www.fib.upc.edu/retro-informatica/historia/internet.html> (accessed May 30, 2020).

[2] <sup>2</sup> “Internet History Timeline: ARPANET to the World Wide Web | Live Science.” <https://www.livescience.com/20727-internet-history.html> (accessed May 30, 2020).

componentes que no eran compatibles con otros fabricantes, lo cual hacía impracticable la comunicación entre ellos <sup>3</sup>.

Uno de los primeros protocolos desarrollados fue el 1822, que fue reemplazado de prisa por el Protocolo de Control de red (NCP). Este rótulo fue implementado en diciembre de 1970 con la necesidad de interconectar computadoras con el microprocesador de mensajes de interfaz (IMP) entre varios sitios a través de una red troncal proporcionada. A finales de 1971, diseñaron protocolo de transmisión de control (TCP) con el fin de reemplazar NCP<sup>1</sup>.

Desarrollado a principios de los 70s, la etiqueta IP es el epíteto de red cardinal usado a través de Internet para encadenar redes domésticas y redes empresariales. El protocolo IP se utiliza a menudo inmediato con la formalidad TCP y entonces puede ser calificativo IP, así como calificativo TCP/IP<sup>4</sup>.

A finales de la década de los 70s, fue desarrollada la versión 1 y 2 del protocolo IP, cuyo fin era realizar la separación de las capas de comunicación del protocolo NCP, el cual no fue utilizado dado que para este momento la comunicación se estaba realizando por medio del protocolo IP, por este motivo no se llegó a implementar<sup>5</sup>.

Posteriormente se desarrolla la versión 3 del protocolo, donde por primera vez TCP está separado de IP, pero el cual no tiene una separación clara y definida, por este motivo este protocolo no se utilizó en las redes de comunicaciones y quedó descartado <sup>6</sup>.

---

[<sup>3</sup>] “Cómo nació Internet: del ARPANET a Internet.” <https://theconversation.com/how-the-internet-was-born-from-the-arpanet-to-the-internet-68072> (accessed May 30, 2020)

<sup>4</sup> “Qué es y cómo funciona el protocolo IP | VIU.” <https://www.universidadviu.com/funciona-protocolo-ip/>

<sup>5</sup> “IETF Standards Written by ISC Contributors - Internet Systems Consortium.” <https://www.isc.org/rfc/>

<sup>6</sup> O. DeLong, “Why does IP have Versions? Why do I care?,” 2017.

## 2.1 Protocolos Ip

Todos los servicios en una red utilizan un sistema de envío de paquetes, el cual se define en dos grandes grupos; los protocolos orientados o no a la conexión, la unidad de información o el archivo se fragmenta en partes y a cada una de ellas se le agrega una cabecera, la cual contiene la dirección del remitente del paquete, la dirección del destino del paquete y el número de secuencia entre otros campos, esto permite la conexión con otras redes ubicadas en diferentes partes del mundo<sup>7</sup>.

### 2.1.1 Ipv4

El protocolo IpV4 fue creado en 1981, en este año se realiza por primera vez una conexión entre equipos, lo que da el primer paso al internet moderno, este protocolo se proyectó con una cantidad de 4300 millones de direcciones, teniendo en cuenta que para ese año no se visualizaba la cantidad de equipos terminales de datos e intermedios de red que se conectan a internet actualmente.

Por este motivo se implementaron varios métodos para alargar su vida útil, como lo fueron, creación de las direcciones NAT (Sistema de conversión de direcciones privadas en públicas y viceversa), la implementación de subredes y el crecimiento de las redes privadas con posibilidad de acceso a la internet de una cantidad mayor de máquinas<sup>8</sup>.

### 2.1.2 Ipv6

En el año 1999 se desarrolló la versión 6 del protocolo de internet; epíteto de comunicaciones que proporciona un sistema de señas y posición para computadoras en redes y enruta a través de Internet. Ipv6 fue creado por la IETF (Internet Engineering Task Force) para tallar frente al desasosiego

---

<sup>7</sup> <https://tools.ietf.org/html/rfc791>

<sup>8</sup> H. Shah, "Comparing TCP-IPV4/TCP-IPV6 Network Performance", Diss. University of Missouri--Columbia, Pp.123-126, 2013.

cumplidamente esperado del agotamiento de las direcciones Ipv4. El direccionamiento Ipv6 está encauzado a reemplazar al Ipv4.

### 2.1.3 Agotamiento de las direcciones Ipv4

En julio de 2011, la sociedad dirigente de direcciones de internet administrado por la IANA anuncia el decaimiento a cota universal de las direcciones IPv4, lo que hace que los administradores de cada región empiecen a despabilarse en búsqueda de alternativas teniendo en cuenta la demanda de tecnología y el incremento de nuevas conexiones<sup>10</sup>. Por partida, es trabajoso su habilitación a las nuevas aplicaciones, más aún cuando a altitud ecuménico se presenta la ampliación granosa de las mismas, las cuales requieren una Ip pública única, estereotipo de ello son: los teléfonos con tecnología Volp, televisión y radio, aplomo, video, mercados virtuales, juegos, videoconferencia, redes inalámbricas, etc.<sup>11</sup>.

### 2.1.4 Comparación entre protocolos Ipv4 e Ipv6

Ipv6 ofrece una condición de mejoras que incluyen una mayor importancia de direccionamiento, aprovisionamiento de calidad de servicio<sup>12</sup>, nueva generación de redes<sup>13</sup>, seguridad integrada a través de IpSec<sup>14</sup> y eficiencia de enrutamiento mejorada<sup>15</sup>. Pero pasar de la versión actual de Ipv4 a la versión futura de Ipv6 no es un proceso sencillo debido a su incompatibilidad lo que consumirá una cantidad significativa de tiempo, ambos protocolos deben coexistir. Para la interoperación fluida de los dos protocolos, hasta ahora se han propuesto varios

---

<sup>10</sup> B. Hinden, "IPv6 Background," 2018.

<sup>11</sup> "Fases de Agotamiento de IPv4." <https://www.lacnic.net/1001/1/lacnic/fases-de-agotamiento-de-ipv4> (accessed May 31, 2020).

<sup>12</sup> E. Chen and P.-J. Lin, "A performance study for IPv4-IPv6 translation in IP multimedia core network subsystem," *Int. J. Commun. Syst.*, p. n/a-n/a, 2009, doi: 10.1002/dac.1071

<sup>13</sup> B. Fgee, W. J. Phillips, W. Robertson, and S. C. Sivakumar, "Implementing QoS capabilities in IPv6 networks and comparison with MPLS and RSVP," in *CCECE 2003 - Canadian Conference on Electrical and Computer Engineering. Toward a Caring and Humane Technology (Cat. No.03CH37436)*, 2003, vol. 2, pp. 851–854, doi: 10.1109/CCECE.2003.1226028.

<sup>14</sup> B. Adebisi *et al.*, "IP-centric high rate narrowband PLC for smart grid applications," *IEEE Commun. Mag.*, vol. 49, no. 12, pp. 46–54, Dec. 2011, doi: 10.1109/MCOM.2011.6094005.

<sup>15</sup> E. Alexander *et al.*, "METODOLOGÍA PARA HACER UNA TRANSICIÓN EN UNA RED IPV4 A IPV6," 2017.

mecanismos de transición bien definidos<sup>16</sup>. Se realiza una comparación entre los protocolos y las diferencias más relevantes.

<i>Comparación entre protocolo Ipv4 e Ipv6</i>	
<i>Ipv4</i>	<i>Ipv6</i>
Desarrollado en 1983	Desarrollado en 1999
Tamaño de la dirección 32 bits	Tamaño de la dirección 128 bits
Registros de recursos de dirección (A) en DNS para asignar nombres de host a direcciones Ipv4.	Registros de recursos de dirección (AAAA) en DNS para asignar nombres de host a direcciones Ipv6.
Registros de recursos de puntero (PTR) en el dominio DNS INADDR.ARPA para asignar direcciones Ipv4 a nombres de host.	Registros de recursos de puntero (PTR) en el dominio DNS Ip6.ARPA para asignar direcciones Ipv6 a nombres de host.
IpSEC es opcional	IpSEC no es opcional
El encabezado no identifica el flujo de paquetes para el manejo de QoS por enrutadores	El encabezado contiene el campo Etiqueta de flujo, que identifica el flujo de paquetes para el manejo de QoS por enrutador.
Un host Ipv4 con un adaptador de red particular normalmente tiene una sola dirección Ipv4 asignada a ese adaptador.	Un host Ipv6, generalmente tiene varias direcciones Ipv6 asignadas a cada adaptador.
Los enrutadores admiten fragmentación de paquetes.	Los enrutadores no admiten la fragmentación de paquetes.
Checksum está incluido en el encabezado	El encabezado no incluye checksum
Configurado manualmente o mediante DHCP.	No requiere configuración manual o DHCP.
Tipo de configuración Configuración de un sistema recién instalado para que pueda comunicarse con otros por medio de la asignación de rutas y direcciones Ip.	Tipos de configuración 1.Configuración automática stateless sin router. 2.Configuración automática stateless con router o servidor. 3.Configuración automática DHCPv6. 4.Configuración manual de la dirección.
La interfaz Ip utiliza la conexión de LAN para acceder a la red física. Existen muchos tipos diferentes; por ejemplo, token ring y Ethernet. También se conoce como la interfaz, enlace o línea física.	Ipv6 puede utilizarse con cualquier adaptador Ethernet y también se soporta a través de Ethernet virtual entre particiones lógicas.

*Tabla 1. Tabla comparativa entre Ipv4 e Ipv6*

<sup>16</sup> G. Eduardo, M. Ramírez, S. Andrés, and Q. Burgos, "IPV6: ESTUDIO SOBRE LAS BARRERAS PARA SU IMPLEMENTACIÓN AUTORES."

## 2.2 Mecanismos de transición

Con respecto a los mecanismos que se desarrollaron para realizar una transición de un protocolo a otro, se contemplaron diferentes sistemas que se pueden clasificar en doble pila, túneles y traducción. Sin embargo, realizar este proceso en una empresa puede ser traumático, teniendo en cuenta los siguientes factores:

- Transición lenta
- Costo económico
- Desconocimiento del protocolo
- Incompatibilidad entre equipos con el protocolo Ipv6

### 2.2.1 Mecanismos de tipo túnel<sup>12</sup>

Los mecanismos de tipo túnel dan la posibilidad de utilizar una infraestructura Ipv4 y transportar el tráfico que está en Ipv6, buscando una transición suave, sin embargo, esto puede presentar inconvenientes como incompatibilidad de los equipos.

---

<sup>12</sup> [ibm.com/docs/es/aix/7.2?topic=6-ipv6-tunneling](http://ibm.com/docs/es/aix/7.2?topic=6-ipv6-tunneling)

Tipo de túnel	Función
Direccionado a direccionado	Los equipos que usan Ipv6 o Ipv4 interconectados por una infraestructura Ipv4 pueden establecer túneles de paquetes Ipv6 entre dichos paquetes. En este caso, el túnel abarca un segmento de la vía de acceso de extremo a extremo que toma el paquete Ipv6.
Sistema principal a direccionado	Los sistemas principales Ipv6 o Ipv4 pueden establecer túneles de paquetes Ipv6 hacia un direccionado Ipv6 o Ipv4 intermediario que se pueda alcanzar a través de una infraestructura de Ipv4. Este tipo de túnel abarca el primer segmento de la vía de acceso de extremo a extremo del paquete.
Sistema principal a sistema principal	Los sistemas principales Ipv6 o Ipv4 que están interconectados por una infraestructura Ipv4 pueden establecer túneles de paquetes Ipv6 entre dichos paquetes. En este caso, el túnel abarca la vía de acceso entera de extremo a extremo que toma el paquete.
Direccionado a sistema principal	Los equipos que utilizan Ipv6/Ipv4 pueden establecer túneles de paquetes Ipv6 hasta el sistema principal Ipv6 o Ipv4 de destino final. Este túnel sólo abarca el último segmento de la vía de acceso de extremo a extremo.

*Tabla 2. Metodos de transición hacia Ipv6*



## 2.2.2 Mecanismos de traducción<sup>16</sup>

Por otro lado, hay infraestructuras que aún no tienen la capacidad de tener equipos compatibles con el protocolo Ipv6 en ninguno de los túneles anteriormente mencionados, se crean los mecanismos de traducción, donde se encuentran los siguientes:

Tipo de túnel	Función
NAT-PT	Es un mecanismo que se define en el RFC 2765 y 2766, que permite que los equipos que son únicamente Ipv6 se puedan comunicar con Ipv4 y viceversa
BIS	BIS (Bump In the stack) es un mecanismo de parecido a NAT-PT pero hay que realizar la implantación desde el código del sistema operativo, lo que lo hace engorroso y poco implementado.
BIA	BIA (Bump in the API) agrega una API de traslación entre la API de Socket y el Stack TCP/IP, permitiendo una mejora al método BIS en cuanto, a la dependencia del driver de red, pero tiene las mismas limitaciones que BIS.
TRT	TRT (Transport Relay Translator) es una conversión de protocolos en la capa de transporte que usa como pieza fundamental un DNS proxy. Éste recibe consultas de los hosts Ipv6 y si el nombre requerido está asociado Ipv4, devuelve una dirección Ipv6
ALG	ALG (Application Layer Gateway) es una traslación realizada en la capa de aplicación. No hay RFCs específicas a seguir, pues su implementación depende del protocolo de capa aplicación al que se dará soporte.

*Tabla 3. Tipos de túneles en Ipv6<sup>16</sup>*

## 2.2.3 DualStack

Por último, como mecanismo de implementación de redes Ipv6, se realizó la creación de una solución que permite la inclusión de las dos generaciones de red al mismo tiempo, el DualStack, permite tener todas las facultades de los dos protocolos Ipv4/Ipv6, sobre los mismos equipos de manera completamente

---

<sup>16</sup> J. Hagino, K. Yamamoto, An IPv6-to-IPv4 Transport Relay Translator, RFC 3142, June 2001

<sup>16</sup> <https://tools.ietf.org/html/rfc4241>

independiente, lo que permite realizar una implementación completa del nuevo protocolo sin tener que dar de baja las configuraciones de su antecesor<sup>16</sup>.

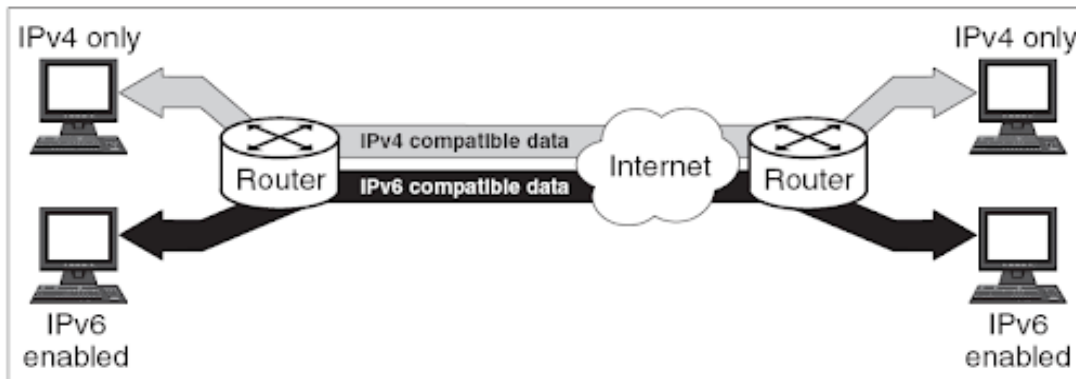


Figura 1. Funcionamiento de DualStack

## 2.3 Redes de área local Virtual

El siguiente punto busca mencionar la manera de realizar la distribución del direccionamiento de direcciones IP, teniendo en cuenta la gran cantidad de dispositivos que se van a concatenar a internet, es necesario realizar agrupaciones de equipos según el funcionamiento que se va a dar, brindando una capa de seguridad y organización dentro de una red de datos.

### 2.3.1 VLAN en Ipv4

Las VLANs tienen la capacidad de realizar una separación lógica del tráfico de la red, permite hasta 4096 subredes, permite utilizar únicamente una interfaz de un router para enviar varias interfaces, permite etiquetar el tráfico entre subredes para lograr una comunicación<sup>18</sup>.

---

<sup>18</sup> <https://nsrc.org/workshops/2013/walc/campus/raw-attachment/wiki/Agenda/VLAN.pdf>

### 2.3.2 VxLAN<sup>19</sup>

VxLAN es una tecnología de virtualización de red que encapsula los paquetes de datos enviados desde los hosts originales en paquetes UDP y encapsula las direcciones Ip y MAC utilizadas en la red física en encabezados externos antes de enviar los paquetes a través de una red Ip. El punto final del túnel virtual (VTEP) luego desencapsula los paquetes y los envía al host de destino, teniendo la capacidad de 16 millones de subredes disponibles.

### 2.3.3 Comparación entre VLAN y VxLAN<sup>21</sup>

Con el fin de buscar la mejor solución al despliegue en un centro de datos, se realiza la comparación entre la manera de implementación de subredes virtuales a continuación:

---

<sup>19</sup> <https://tools.ietf.org/html/rfc7348>

<sup>21</sup> <https://forum.huawei.com/enterprise/en/what-is-vxlan-and-comparison-between-vlan-and-vxlan/thread/580668-861>

ÍTEM	VLAN	VxLAN
Concepto	Red de área local virtual	Red de área local extensible virtual
Método de implementación	Una LAN física se divide lógicamente en varios BD para limitar la red a un rango geográfico pequeño	Las redes virtuales de capa 2 se establecen entre redes con rutas accesibles. Estas redes no están sujetas a restricciones geográficas y pueden ofrecer una escalabilidad a gran escala.
Capacidad admitida	VLAN es la tecnología de aislamiento de red más utilizada. El campo VLAN en paquetes tiene solo 12 bits de longitud, lo que significa que solo se puede usar un máximo de 4096 VLAN en una red. En la nube pública u otros escenarios de computación en la nube que involucran a decenas de miles o incluso más inquilinos, la tecnología VLAN ya no puede cumplir con los requisitos de aislamiento de la red.	VxLAN es una nueva tecnología de aislamiento de red definida en IETF RFC. Tiene un identificador de segmento de 24 bits (VNI) y puede aislar hasta 16 millones (aproximadamente 16 millones) de inquilinos. Esta tecnología permite de manera efectiva el aislamiento de inquilinos masivos en la computación en la nube.
Modo de división de red	Las ID de VLAN se utilizan para dividir los dominios de transmisión. Los hosts dentro de una BD pueden comunicarse en la Capa 2.	Los BD se utilizan para dividir los dominios de transmisión. Las máquinas virtuales dentro de una BD pueden comunicarse en la capa 2
Modo de encapsulación	Se agrega una etiqueta VLAN a los paquetes.	Durante la encapsulación VxLAN, un encabezado VxLAN, encabezado UDP, encabezado IP y encabezado MAC externo se agregan en secuencia a un paquete original.
Modo de comunicación de red	La comunicación entre VLAN se implementa mediante interfaces VLANIF. Como interfaces lógicas de Capa 3, las interfaces VLANIF permiten la comunicación de Capa 3 entre VLAN.	La comunicación entre VLAN o entre VxLAN y no VxLAN se implementa mediante interfaces VBDIF. Las interfaces VBDIF se configuran en puertos de enlace VxLAN Layer 3 y son interfaces lógicas de Layer 3 basadas en BD.
Beneficios	Limita los dominios de transmisión: un dominio de transmisión está limitado en una VLAN, lo que ahorra ancho de banda y mejora las capacidades de procesamiento de la red.	Capacidad independiente de la ubicación: los servicios se pueden implementar de manera flexible en cualquier ubicación, resolviendo problemas de expansión de la red relacionados con la virtualización de servidores.
	Mejora la seguridad de la LAN: los paquetes de diferentes VLAN se transmiten por separado. Los hosts de una VLAN no pueden comunicarse directamente con los hosts de otra VLAN	Implementación de red flexible: las VxLAN se construyen sobre la red tradicional. Son fáciles de implementar y altamente escalables al tiempo que evitan las tormentas de transmisión en una gran red de Capa 2.
		Adaptación del servicio en la nube: una VxLAN puede aislar a diez millones de inquilinos y admitir la implementación a gran escala de servicios en la nube.
		Ventaja técnica: VxLAN utiliza encapsulación MAC-in-UDP. Dicho modo de encapsulación no depende de las direcciones MAC de las VM, lo que reduce la cantidad de entradas de direcciones MAC necesarias en una red de Capa 2 grande.

*Tabla 4. Comparación entre VLAN y VxLAN*

## 3. Marco legal

Con respecto a la normatividad que se maneja en Colombia relacionada con las nuevas tecnologías, en este caso; la transición del protocolo Ipv4 hacia el protocolo Ipv6, se realizó una revisión de los documentos, guías y manuales que orientan a las empresas en la adopción protocolo de nueva generación en el país. Por este motivo y su relevancia, será abordado en este capítulo.

### 3.1 Lineamientos básicos del MinTIC

Dentro de los lineamientos que plantea el MinTIC para el desarrollo de proyectos de esta índole en el país, se plantea un plan de trabajo estándar donde se evalúa un desarrollo por fases de la implementación del protocolo Ipv6. El desarrollo de estas fases se ejecutará de la siguiente manera<sup>7</sup>:

### 3.2 Fase 1 Planeación<sup>8</sup>

La empresa debe realizar una investigación profunda de los elementos que componen la topología, con el fin de realizar un plan diagnóstico del estado actual de la red, se toma como referencia los siguientes ítems para su desarrollo:

- Inventario de activos de información.
- Identificar la topología con la que cuenta la empresa actualmente.
- Servicios transversales como DNS, LDAP, Servidores Web, DHCP, entre otros.
- Validar la compatibilidad de todos los elementos de red con el protocolo Ipv6.

---

<sup>7</sup> “Cartilla Guía de Transición de IPv4 a IPv6” [https://www.mintic.gov.co/portal/715/articles-125210\\_recurso\\_2.pdf](https://www.mintic.gov.co/portal/715/articles-125210_recurso_2.pdf)

<sup>8</sup> [https://www.mintic.gov.co/portal/715/articles-125210\\_recurso\\_2.pdf](https://www.mintic.gov.co/portal/715/articles-125210_recurso_2.pdf)

### 3.3 Fase 2 Implementación<sup>8</sup>

En esta fase las empresas ya deben tener establecido el alcance que se va a dar a la implementación del protocolo Ipv6 de manera DualStack, el cual será explicado en el documento. Por este motivo se plantea como mínimo alcance los siguientes ítems:

- Realizar el despliegue del direccionamiento de Ipv6 en todos los elementos de red que sean compatibles con el protocolo.
- Generar pruebas piloto por medio de VLANs de prueba.
- Trabajar de la mano con los proveedores de internet para que los servicios sean publicados en la red.

### 3.4 Fase 3 Pruebas de funcionalidad<sup>8</sup>

En la última fase se evalúa el alcance que se planteó en la planeación, buscando generar tráfico por medio del protocolo Ipv6 desde internet hacia la empresa y viceversa, esto con el fin de encontrar falencias en el despliegue y poder corregirlas, por este motivo se plantean los siguientes elementos básicos a cumplir:

- Afinamiento de las nociones de hardware y programa que se indicaron en el grado de implementación.
- Realizar un nuevo inventario de servicios, aplicaciones y sistemas de información implementados en el protocolo Ipv6.
- Entregar toda la documentación con pruebas de funcionalidad de la transición del protocolo Ipv4 hacia Ipv6.

### 3.2 Circular 002 de 2011 “Promoción de la adopción de Ipv6 en Colombia”<sup>23</sup>

Ahora bien, para realizar una adopción coherente de la adopción del protocolo Ipv6 en Colombia, se establece en primer lugar la circular 002 del año 2011, donde se establecen los siguientes lineamientos:

- Las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones.
- Es función del Ministerio de Tecnologías de la Información y las Comunicaciones, diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.
- El estado debe garantizar 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.
- Es preciso resaltar, que se agotó el remanente del stock de direcciones de Ipv4 de la Autoridad Internacional de Asignación de Números de Internet y dentro de pocos meses, el del Registro de Internet Regional para Latinoamérica y Caribe LACNIC.
- Es decir, a partir de ahora ya no se podrán adquirir direcciones Ipv4 y la alternativa de transición a Ipv6 es una necesidad inminente y está ocurriendo en todo el mundo(16).
- En el orden mundial gran cantidad de países y organizaciones se están preparando desde comienzos de este siglo para adoptar el protocolo de Internet Ipv6. Esto ha generado acciones concretas definiendo políticas gubernamentales para una ordenada transición.

---

<sup>23</sup> [https://normograma.mintic.gov.co/mintic/docs/circular\\_mintic\\_0002\\_2011.htm](https://normograma.mintic.gov.co/mintic/docs/circular_mintic_0002_2011.htm)

- Se hace necesario recomendar a la Industria del país y al sector TIC que utilice, comercialice o fabrique cualquier sistema, aplicación, software, hardware, equipo activo o de red, equipo terminal de usuario y, en general, todo tipo de tecnología soportada bajo plataforma IP, los provea y/o fabrique sobre Ipv6, con total compatibilidad y soporte Ipv4, demostrable mediante los RFCs concretos del IETF y demás normas que determinan esta compatibilidad.

### 3.3 Resolución 180 de 2010 la Unión Internacional de Telecomunicaciones (UIT)

Esta resolución reconoce que la adopción temprana del Ipv6 es la mejor forma de evitar escasez de direcciones y las consecuencias del agotamiento de las direcciones Ipv4 pueda implicar para el país, altos costos, además de resaltar el importante rol que los gobiernos desempeñan como catalizadores de la transición hacia Ipv6; por lo tanto hace un llamado al fomento y despliegue de dicho protocolo en las administraciones públicas, donde el Ministerio de Tecnologías de la Información y las Comunicaciones ha adelantado desde el año 2010 diversos estudios y actividades de sensibilización, promoción, divulgación y concertación con los diferentes actores del sector TIC <sup>22</sup>.

### 3.4 Resolución 64 de 2012 de la Asamblea Mundial de Normalización<sup>24</sup>

En la asamblea mundial de normalización, a la cual pertenece la UIT y por este motivo influye en la normatividad para Colombia, se establecen los siguientes lineamientos que motivan la transición hacia el protocolo Ipv6 en Colombia:

- Estudiar la forma de obtener, de conformidad con la Agenda de Túnez para la Sociedad de la Información, una mayor colaboración y coordinación recíproca entre la UIT y organizaciones pertinentes que participan en el desarrollo de las redes IP y de la Internet futura.

---

<sup>22</sup> [https://www.itu.int/dms\\_pub/itu-s/opb/conf/S-CONF-ACTF-2010-TOC-HTML-S.htm](https://www.itu.int/dms_pub/itu-s/opb/conf/S-CONF-ACTF-2010-TOC-HTML-S.htm)

<sup>24</sup> <https://www.itu.int/en/council/Documents/basic-texts/RES-180-S.pdf>



- Intensificar el intercambio con todas las partes interesadas de experiencias e información sobre Ipv6, con objeto de crear oportunidades de colaboración y de velar porque la circulación de información contribuya a esta labor.
- Colaborar estrechamente con los socios internacionales reconocidos pertinentes, incluida la comunidad de Internet (RIR), el Grupo Especial sobre Ingeniería de Internet, para fomentar el desarrollo de Ipv6 a través de la divulgación y la capacitación.
- Apoyar a aquellos Estados miembros que, de conformidad con las actuales políticas de atribución, necesitan asistencia para la gestión y atribución de recursos Ipv6, de conformidad con las resoluciones pertinentes.
- Seguir adelante con los estudios sobre la atribución o distribución de direcciones IP, tanto en lo referente a las direcciones Ipv4 como a las direcciones Ipv6, en cooperación con otras partes interesadas pertinentes en función de sus respectivas competencias.

### 3.5 Resolución 2710 de 2017<sup>25</sup>

La presente resolución tiene por objeto formular medidas para la adopción del protocolo Ipv6 en Colombia por parte de los obligados a establecer medidas para los Proveedores de Redes y Servicios de Telecomunicaciones para que cursen tráfico y ofrezcan conectividad y servicios en Ipv6 a las entidades objeto de esta resolución.

Se fundamenta la implementación de esta resolución por medio de los siguientes artículos:

1. Establecer una base de lineamientos para los proveedores de internet, que desplieguen el servicio de Ipv6 para las entidades implicadas.
2. Realizar una verificación del cumplimiento de las entidades prestadoras del servicio de internet, que cumplan con aplicaciones web, sistemas de

---

<sup>25</sup> [https://normograma.mintic.gov.co/mintic/docs/resolucion\\_mintic\\_2710\\_2017.htm](https://normograma.mintic.gov.co/mintic/docs/resolucion_mintic_2710_2017.htm)

almacenamiento, seguridad, sistemas de computación y demás elementos que cumplan con el despliegue de Ipv6 por medio de DualStack.

3. Establecer un plazo máximo de despliegue de la infraestructura Ipv6, por medio de la publicación de servicios en la internet.
4. La transición debe realizarse de manera controlada, teniendo en cuenta que la red actual se encuentra implementada en Ipv4, esto por medio de protocolos de DualStack compartiendo los equipos en sus versiones 4 y 6 del protocolo de internet.
5. Realizar una compra abierta por medio de Colombia Compra Eficiente, permitiendo la participación de múltiples entidades.
6. La ejecución de sanciones a las entidades prestadoras del servicio de internet, en la ejecución para las empresas del estado.
7. La vigencia de esta resolución teniendo en cuenta las modificaciones de fecha que puede tener, en este caso la pandemia de Sars-Covid 19.

### 3.6 ¿Qué se ha hecho en Colombia respecto al protocolo Ipv6?

El despliegue del protocolo Ipv6 en Colombia, se ha dado de manera paulatina, realizando primero la implementación de DualStack en la red Renata (es la red nacional de investigación y educación de Colombia que conecta, articula e integra a los actores del Sistema Nacional de Ciencia Tecnología e Innovación (SNCTI) entre sí y con el mundo, a través del suministro de servicios, herramientas e infraestructura tecnológica para contribuir al mejoramiento del nivel de productividad, efectividad y competitividad de la producción científica y académica del país), quienes desde 2008 empezaron a trabajar con este protocolo hasta que en 2009, se realizó la completa migración hacia el nuevo protocolo. En paralelo las empresas prestadoras de servicios de telecomunicaciones realizaron la implementación de la doble pila en su infraestructura, buscando cubrir la necesidad de la adopción de la nueva red<sup>4</sup>.

---

<sup>4</sup> <https://www.renata.edu.co/tag/ipv6-colombia>

Para realizar un seguimiento a nivel internacional del proceso de adopción del protocolo Ipv6 en Colombia respecto al mundo, para el 2019 la adopción total era de un 5%, para el 2020 de un 9% y la proyección del 2021 es de un 14% del total de las empresas, quedando muy por detrás de países de la región como México con un 40% de implementación o Brasil con un 38%. Teniendo en cuenta que la cantidad de ingenieros, infraestructura y economía no está preparada para acogerse a la implementación<sup>5</sup>.

## 4. Requisitos previos

Para lograr la ejecución de este proyecto es necesario contar con una capacitación previa que se podrá recomendar en su realización para la implementación de la topología, así como la escogencia del programa de emulación que permitirá el desarrollo de la red.

### 4.1 Capacitación

Para poder lograr el alcance de la simulación es necesario tener una capacitación básica en dos temas principales, el primero es la configuración básica de equipos de redes, que en este caso por el tipo de equipos que se maneja se tiene bajo la certificación CCNA Routing And Switching obtenida con el proveedor Cisco. Por otro lado, es necesario un conocimiento previo en Ipv6, que actualmente es únicamente brindado por Ipv6 Fórum para Latinoamérica, donde por lineamientos del MinTIC es necesario obtener una certificación de mínimo 24 horas.

### 4.2 Programa de Emulación

Previo a la realización de la topología tanto el diseño actual como la topología propuesta es necesario generar una leve descripción del programa de emulación que se va a utilizar, para nuestro caso GNS3(Graphic Network

---

<sup>5</sup> <https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption>

Simulation Version 3). Por su utilización en redes de datos es uno de los más usados, por este motivo se mencionan algunas de sus características relevantes:

- Programa compatible con fabricantes como: Cisco, Fortinet, Windows, Linux entre muchos otros.
- Posibilidad de tener varias máquinas virtuales a través de software de virtualización como virtual box o VMWare.
- Es capaz de emular las capacidades reales de los equipos de redes, dando una posibilidad de encontrar inconvenientes, protocolos y demás herramientas que no suelen estar en ningún simulador de red.
- Tiene la capacidad de mezclar redes emuladas en el software y realizar conexiones con equipos reales.



*Figura 2. Emulador grafico de redes versión 3*

Por este motivo se realizó la escogencia de este software para la topología de red en el Departamento Nacional de Planeación.

## 5. Indagación de la red actual del Departamento Nacional de Planeación

Con el fin de buscar un nuevo planteamiento de la red del Departamento Nacional de Planeación, es necesario realizar una breve descripción de la red, que se puede determinar de la siguiente manera:

1. Estructura de red Top of Rack, lo que permite implementar los equipos intermedios de red en el mismo bastidor.
2. Topología espejo de los centros de procesamiento de información, que permite tener un plan de continuidad, sujeta a una disponibilidad del 99.95% brindando una alta capacidad de funcionamiento.

3. La red está conectada por medio de una MPLS entre las sedes por medio de equipos de seguridad.
4. Las estaciones cliente están ubicadas en la sede del Departamento Nacional de planeación, la cual está distribuida en 20 pisos con más de 1000 usuarios.
5. Los centros de datos cuentan con una red eléctrica y una planta para soportar el funcionamiento por más de 2 horas sin red comercial.
6. El ingreso a los equipos está controlado por medio de una planilla de ingreso y ejecución de cambios que debe ser autorizada previamente por los líderes de los equipos de ingeniería.

Se genera un esquema topológico básico que muestra de manera general la distribución actual de la red de la siguiente manera:

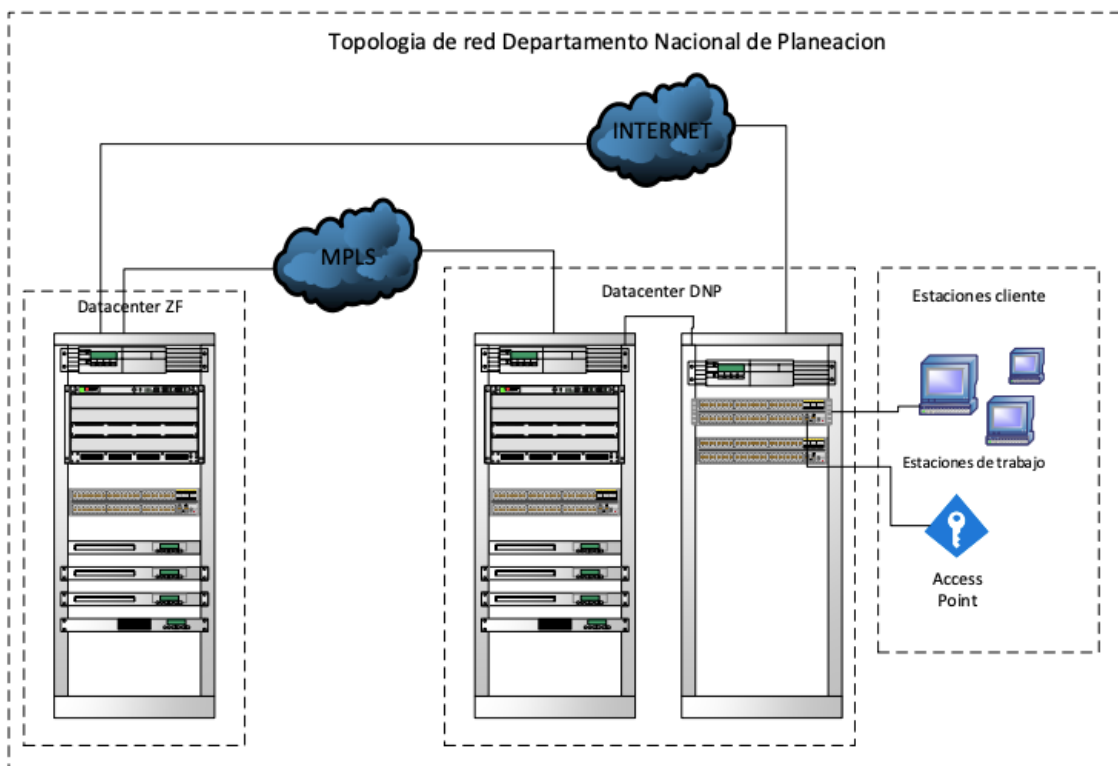


Figura 3. Topología en rack DNP

## 5.1 Topología actual en el centro de datos de la empresa

La topología actual del centro de datos es una red en espejo, es decir que toda las operaciones, cambios o implementaciones que se realicen en el centro de datos o centro de procesamiento de datos principal ubicado en la Zona Franca, va a ser replicada automáticamente en el centro de datos alterno ubicado en la Oficina DNP.

Esto se realiza con el fin de tener un plan de continuidad del negocio, lo que permite continuar con las labores en el caso de que se evidencie una falla, catástrofe o demás anomalías en el servicio.

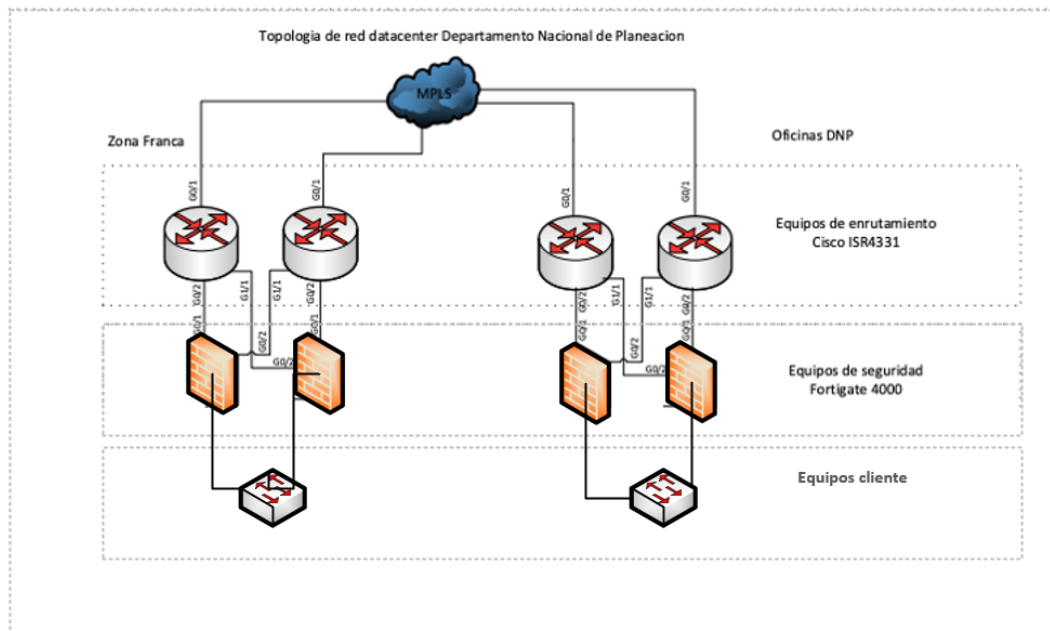


Figura 4. Topología lógica de DNP

Por este motivo es necesario realizar una validación del direccionamiento que se tiene actualmente en la topología, con el fin de tener un punto de partida que permitirá realizar el planteamiento de los nuevos segmentos que se van a establecer en Ipv6, razón por la cual se relacionan a continuación:

DIRECCIONAMIENTO ACUTUAL DE LA RED EN IPv4					
Zona franca					
VLAN	Servicio	Nombre de red	Dirección Ipv4	Primer Host	Ultimo Host
31	Datos	Windows server 1	172.16.20.0/24	172.16.20.1	172.16.20.254
32	Datos	Windows server 2	172.16.21.0/24	172.16.21.1	172.16.21.254
33	Datos	Windows server 3	172.16.22.0/24	172.16.22.1	172.16.22.254
34	Datos	Windows server 4	172.16.23.0/24	172.16.23.1	172.16.23.254
DNP					
35	Datos	Windows server 4	172.16.24.0/24	172.16.24.1	172.16.24.254
36	Datos	Windows server 5	172.16.25.0/24	172.16.25.1	172.16.25.254
37	Datos	Windows server 6	172.16.26.0/24	172.16.26.1	172.16.26.254
37	Datos	Windows server 7	172.16.27.0/24	172.16.27.1	172.16.27.254
Equipos Core					
10	Datos	Conexiones MPLS	193.254.20.0/28	193.254.20.1	193.254.20.14
99	Fonade	Comunicación SW	172.16.0.0/25	172.16.0.1	172.16.0.126
400	Fonade	Gestión FW	172.16.1.0/25	172.16.1.1	172.16.1.126

*Tabla 5. Direccionamiento de DNP en IPv4*

## 5.2 Funcionamiento de la red actual en datacenter de la empresa

Para comenzar con el funcionamiento de la red del Departamento Nacional de Planeación, es necesario contemplar los enlaces a través de internet privado, por medio de una red MPLS (conmutación de etiquetas multiprotocolo) formando así una red espejo entre el centro de datos ubicado en la oficina principal y el centro de datos que se establece en zona franca.

Seguido a esto se ubican los equipos de enrutamiento lógico Cisco ISR4331 que permiten generar la conexión entre los centros de datos hacia la red MPLS y que estos puedan establecer una conexión en dos vías, por medio del protocolo BGP (protocolo de puerta de enlace) generando el anuncio del AS (Sistema Autónomo). Por tratarse de una empresa estatal, este código de AS es reservado para la empresa de manera estática y permite anunciarse en cualquier parte del mundo. Se contemplan dos equipos por cada zona hacia la MPLS para buscar la mayor disponibilidad posible y tener un servicio redundante de los equipos.

Por otro lado, la conexión hacia la red interna se establece en primera medida hacia los Firewalls (Corta Fuegos) que tienen la función de permitir o denegar la entrada de tráfico hacia las redes de la empresa, buscando generar una serie de reglas previamente contempladas con el área de la infraestructura tecnológica. A continuación, se ubican los conmutadores de la red, que permiten generar por medio de direcciones IP internas, la interconexión desde y hacia fuera de la red, siendo estos los equipos que controlan las subredes VLAN y por los cuales los equipos pueden transmitir información entre ellos.

Por último, se encuentra la granja de servidores Windows que tienen los aplicativos, páginas Web y demás desarrollos de software, lo que se vuelve el principal elemento de la topología, dado que aquí se ubica la información de las bases de datos el cual es la información confidencial y hay que protegerla por todos los medios posibles.

### 5.3 Inventario de equipos de comunicaciones

Con el fin de validar las características de cada uno de los componentes, se realiza una descripción básica de los equipos que componen la topología de red de la empresa, por este motivo se genera una tabla con las cualidades físicas de los equipos de la siguiente manera:

ÍTEM	ROUTER	SWITCH
<b>Marca</b>	Cisco	Cisco
<b>Modelo</b>	ISR4331-SEC/K9	Nexus 7000
<b>Puertos WAN/LAN</b>	3 x 10/100/1000 Mbit/s	24 x 10/100/1000 Mbit/s
<b>Puertos RJ-45</b>	2	24
<b>Puertos SFP</b>	2	12
<b>Módulo SM-X</b>	1	1
<b>Módulos de Interfaz de Red</b>	2	2
<b>Ranura ISC a bordo</b>	1	N/A
<b>Desempeño</b>	Memoria Flash: 4 GB (predeterminado) / 16 GB (máximo)	Memoria Flash: 2 GB (predeterminado) / 8 GB (máximo)
	Memoria Interna: 4 GB (predeterminado) / 16 GB (máximo)	Memoria Flash: 2 GB (predeterminado) / 8 GB (máximo)
<b>Cantidad de equipos</b>	4	4

*Tabla 6. Inventario de características físicas de Router y Switch*



Por otro lado, es necesario realizar una descripción detallada de cada uno de los componentes de red a nivel lógico, lo que permitirá posteriormente la validación de la compatibilidad de los componentes, por este motivo se establece de la siguiente manera:

ÍTEM	ROUTER	SWITCH
Protocolos soportados	Ipv4, Ipv6, rutas estáticas, Protocolo de información de enrutamiento Versiones 1 y 2 (RIP y RIPv2), Open Shortest Path First (OSPF), mejorado Protocolo de enrutamiento de puerta de enlace interior (EIGRP), puerta de enlace frontera Protocolo (BGP), reflector de enrutador BGP, sistema intermedio a sistema intermedio (IS-IS), grupo de Internet de multidifusión Protocolo de gestión versión 3 (IGMPv3), independiente del protocolo Modo disperso de multidifusión (PIM SM), multidifusión PIM de origen específico (SSM), Protocolo de reserva de recursos (RSVP), Protocolo de descubrimiento de Cisco, Analizador de puertos conmutados remotos encapsulados (ERSPAN), Acuerdos de nivel de servicio IP de Cisco IOS (IPSLA), Call Home, Cisco IOS Embedded Event Manager (EEM), intercambio de claves de Internet (IKE), listas de control de acceso (ACL), conexiones virtuales Ethernet (EVC), Protocolo de configuración dinámica de host (DHCP), Frame Relay (FR), DNS, Protocolo de separación de ID de localizador (LISP), Superposición Transporte virtualización (OTV), protocolo de enrutador Hot Standby (HSRP), RADIUS, autenticación, autorización y contabilidad (AAA), visibilidad y control de aplicaciones (AVC), vector de distancia Protocolo de enrutamiento de multidifusión (DVMRP), multidifusión de Ipv4 a Ipv6, MPLS, VPN de capa 2 y capa 3, Ipv6, protocolo de túnel de capa 2 Versión 3 (L2TPv3), detección de reenvío bidireccional (BFD), IEEE 802.1ag y IEEE 802.3ah	Capacidad de conmutación local máxima 600 Gbps Capacidad máxima de conmutación entre ranuras 440 Gbps Compatibilidad de software Cisco NX-OS Software Release 6.1 (2) o posterior Opciones Puerta del módulo frontal con cerradura Rendimiento 1,44 mil millones de paquetes por segundo (bps) (unidifusión Ipv4) en combinación con el módulo supervisor y la estructura incorporada Fiabilidad y disponibilidad Inserción y extracción en línea (OIR) de todos los componentes redundantes: módulos de supervisor, fuentes de alimentación y bandejas de ventiladores Los MIB admiten las versiones 3, 2c y 1 del Protocolo simple de administración de redes (SNMP) (consulte las notas de la versión del software Cisco NX-OS para obtener detalles sobre el soporte específico de MIB) Administración de red Cisco Data Center Network Manager (DCNM) 6.1. (2) o posterior
Encapsulamiento	Encapsulación de enrutamiento genérico (GRE), Ethernet, VLAN 802.1q, Protocolo punto a punto (PPP), protocolo punto a punto multienlace (MLPPP), Frame Relay, Frame Relay multienlace (MLFR) (FR.15 y FR.16), control de enlace de datos de alto nivel (HDLC), serie (RS-232, RS449, X.21, V.35 y EIA-530) y PPP sobre Ethernet (PPPoE)	N/A
Gestión de tráfico	QoS, Cola equitativa ponderada basada en clases (CBWFQ), ponderada Detección temprana aleatoria (WRED), QoS jerárquica, basada en políticas Enrutamiento (PBR), enrutamiento de rendimiento (PfR) y basado en red Reconocimiento de aplicaciones (NBAR)	N/A

Algoritmos criptográficos	Cifrado: DES, 3DES, AES-128 o AES-256 (en CBC y GCM modos); Autenticación: RSA (748/1024/2048 bit), ECDSA (256/384 bits); Integridad: MD5, SHA, SHA-256, SHA-384, SHA-512	N/A
Soporte para VxLAN	N/A	<p>Colocación flexible de cargas de trabajo en la estructura del centro de datos.</p> <p>Proporciona una forma de extender los segmentos de Capa 2 sobre la infraestructura de red de Capa 3 compartida subyacente para que las cargas de trabajo de los inquilinos se puedan colocar en pods físicos en un solo centro de datos. O incluso en varios centros de datos geográficamente diversos. Mayor escalabilidad para permitir más segmentos de Capa 2.</p> <p>VxLAN utiliza un ID de segmento de 24 bits, el identificador de red VxLAN (VNID). Esto permite que coexistan un máximo de 16 millones de segmentos VxLAN en el mismo dominio administrativo. En comparación, las VLAN tradicionales utilizan un ID de segmento de 12 bits que puede admitir un máximo de 4096 VLAN.</p> <p>Utilización optimizada de las rutas de red disponibles en la infraestructura subyacente. Los paquetes VxLAN se transfieren a través de la red subyacente según sus encabezados de Capa 3. Utilizan protocolos de agregación de enlaces y enrutamiento de múltiples rutas de igual costo (ECMP) para usar todas las rutas disponibles. Por el contrario, una red de Capa 2 podría bloquear rutas de reenvío válidas para evitar bucles.</p>

*Tabla 7. Características lógicas de Router y Switch*

## 5.4 Inventario de equipos de infraestructura

Para generar una descripción detallada de los equipos de infraestructura, se desglosan las características de hardware de la siguiente manera:

ÍTEM	SERVIDORES
Marca	Dell
Modelo	Poweredge r350
Puertos WAN/LAN	2 x 1GbE LOM
Puertos RJ-45	2
Puertos SFP	2
Módulo SM-X	N/A
Módulos de Interfaz de Red	2
Ranura ISC a bordo	N/A
Desempeño	Memoria RAM: 128 GB Almacenamiento: 64 TB - 128 TB

*Tabla 8. Inventario de equipo de infraestructura*

Para continuar, es necesario hacer una descripción del alcance de los equipos de manera lógica, a pesar de que en muchos casos esto dependerá del sistema operativo que sea instalado, para este caso se tienen implementados con Windows Server 2016, por este motivo se destacan las características más importantes para el proyecto, las cuales se destacan de la siguiente manera:

ÍTEM	SERVIDORES
Ipv6 Preferido	Microsoft Windows Server 2016 utiliza la pila TCP / IP de próxima generación, una pila de protocolos TCP / IP que integra tanto Ipv4 como Ipv6. Por ejemplo, si una consulta de DNS devuelve direcciones Ipv6 e Ipv4, la pila primero intentará comunicarse a través de Ipv6. La preferencia de Ipv6 sobre Ipv4 ofrece a las aplicaciones habilitadas para Ipv6 una mejor conectividad de red.
Configuración de Ipv6	<p>1. Un host Ipv6 envía un mensaje de multidifusión y recibe uno o más mensajes de enrutador. Estos últimos contienen prefijos de subred que utiliza el host Ipv6 para especificar direcciones Ipv6 adicionales y agregar rutas a la tabla de enrutamiento Ipv6. También se incluyen otros parámetros de configuración, por ejemplo, la puerta de enlace estándar.</p> <p>2. DHCPv6 proporciona prefijos de subred y otros parámetros de configuración para el host Ipv6. Por ejemplo, DHCPv6 se usa a menudo en hosts Ipv6 en Windows para configurar las direcciones Ipv6 de los servidores DNS, lo que no es posible con la detección de enrutadores. Windows Server 2016 tiene un servidor DHCP habilitado para Ipv6.</p>
Adaptación de DNS para Ipv6	En la configuración avanzada de Ipv6, la pestaña DNS le permite realizar ajustes para la resolución del nombre. No es necesario realizar cambios aquí para agregar Windows Server 2016 a un dominio de manera general. Recién instalado, las siguientes opciones están habilitadas de forma predeterminada: Agregar sufijos DNS primarios y específicos de la conexión Agregar sufijos principales del sufijo DNS principal Registre las direcciones de esta conexión en DNS
Prueba y optimización de la resolución de nombres	Si Ipv4 e Ipv6 están disponibles en una red, Windows Server 2016 prioriza el tráfico sobre Ipv6. Si no funciona correctamente, Windows Server 2016 lo detecta y cambia automáticamente a Ipv4 en segundo plano. Para probar la resolución de nombres en Windows Server 2016.

*Tabla 9. Características lógicas de servidores*

## 5.5 Inventario de equipos de seguridad

En este caso se encuentran los equipos de seguridad; Firewall de referencia Fortinet 4000, que permiten gestionar todas las reglas de entrada y de salida de la red, por este motivo se genera una descripción de los componentes físicos del mismo de la siguiente manera:

ÍTEM	FIREWALL
Marca	Fortinet
Modelo	FortiGate® Serie 400E
Puertos WAN/LAN	16 GE RJ45
Puertos RJ-45	2 GE RJ45 MGMT / HA
Puertos SFP	16 GE SFP
Módulo SM-X	N/A
Módulos de Interfaz de Red	34
Ranura ISC a bordo	N/A
Desempeño	2 unidades SSD de 240 GB
Cantidad de equipos	4

*Tabla 10. Características físicas de los Firewall*

Es necesario realizar una validación de seguridad a los equipos, en su comportamiento lógico hacia Ipv6, para poder generar la confirmación de la compatibilidad del proyecto y la necesidad de este, por este motivo se mencionan los más relevantes en la siguiente tabla:

ÍTEM	FIREWALL
Protocolos soportados	"Actualización automática de la base de datos de virus de Red FortiResponse Escanea HTTP, FTP, SMTP, POP3, IMAP, y túneles VPN cifrados Modos y características del cortafuegos NAT, PAT, transparente (puente) Modo de enrutamiento (RIP v1, v2) Etiquetado de VLAN (802.1q) Lista de control de acceso (IP de origen, IP de destino, Puerto TCP y puerto UDP) Autenticación basada en grupos de usuarios H 323 NAT transversal Soporte WINS VPN "
Encapsulamiento	Base de datos interna Soporte LDAP Base de datos RADIUS (externa) Soporte de Xauth sobre RADIUS para IPSec VPN Enlace de dirección IP / MAC
Gestión de tráfico	"Modelado de tráfico basado en políticas ancho de banda garantizado ancho de banda máximo asignación prioritaria "
Algoritmos criptográficos	PPTP, L2TP e IPSec Túneles dedicados Cifrado (DES, 3DES, AES) Autenticación SHA-1 / MD5 Admite el cliente VPN remoto de Fortinet Sin embargo, el cliente PPTP, L2TP, VPN pasa Compatibilidad con Hub y Spoke VPN Autenticación de certificado IKE (X.509) IPSec NAT transversal Detección de pares muertos Interoperabilidad con los principales proveedores de VPN
Soporte para VxLAN	VxLAN a través de encapsulación

*Tabla 11. Características lógicas de los Firewall*

## 5.6 Emulación topología actual

Para empezar, es necesario contemplar el protocolo de enrutamiento dinámico dada la cantidad de direcciones que deben ser conocidas por la MPLS, por este motivo se utilizó OSPF (Open Shortest Path First) en la topología actual, teniendo en cuenta que es uno de los más utilizados en las redes IP, dado que cuenta con las siguientes ventajas para su implementación:

- OSPF permite tener una convergencia de redes y escalabilidad de manera rápida.
- Es un protocolo de estándar abierto, lo que permite ser instalado en diferentes dispositivos de múltiples fabricantes.
- Cada enrutador tiene la capacidad de tener una tabla de enrutamiento completa de las redes lejanas.
- Soporta el uso de host, redes y subredes de manera específica para completar su tabla de rutas.

- OSPF utiliza la multidifusión a través de sus rutas únicamente cuando hay actualizaciones en la red.
- Permite tener una jerarquía en la red para distinguir los equipos.

## Configuración de equipos de MPLS

Una de las configuraciones que deben ir en la base del protocolo OSPF es que al menos las máquinas principales requieren al menos una conexión con el área 0, por este motivo los equipos del ISP en la simulación se implementan de esta manera.

## Configuración enrutador IspCore

Se realiza la configuración del enrutador IspCore, que está en la parte más alta de la jerarquía en la topología, y cada una de sus interfaces para la conexión hacia las redes de la empresa, como se evidencia en la siguiente imagen.

```
interface Ethernet0/0
 ip address 193.254.20.1 255.255.255.240
 half-duplex
!
interface Ethernet1/0
 ip address 193.254.21.1 255.255.255.240
 half-duplex
!
router ospf 1
 log-adjacency-changes
 network 193.254.20.0 0.0.0.15 area 0
 network 193.254.21.0 0.0.0.15 area 0
!
```

*Figura 5. Configuración IspCore*

## Configuración enrutador RoClaroZF

Para este equipo la configuración de sus interfaces y protocolo OSPF, debe compartir tanto el área 0 como el área 1 teniendo en cuenta que va a ser la conexión directa hacia la red empresarial en Zona Franca, por este motivo se realizan las siguientes configuraciones:

```

interface Ethernet0/0
ip address 193.254.20.2 255.255.255.240
half-duplex
!
interface Ethernet1/0
ip address 193.254.18.1 255.255.255.240
half-duplex
!
interface Ethernet2/0
ip address 193.254.19.1 255.255.255.240
half-duplex
!
router ospf 1
log-adjacency-changes
network 193.254.18.0 0.0.0.15 area 1
network 193.254.19.0 0.0.0.15 area 1
network 193.254.20.0 0.0.0.15 area 0

```

Figura 6. Configuración router claro Zona Franca

## Configuración enrutador RoClaroDNP

Como se muestra en la topología, este equipo es un espejo de la configuración del RoClaroZF, por este motivo se implementa en el área 0 y área 1 de OSPF de la siguiente manera:

```

interface Ethernet0/0
ip address 193.254.22.1 255.255.255.240
half-duplex
!
interface Ethernet1/0
ip address 193.254.21.2 255.255.255.240
half-duplex
!
interface Ethernet2/0
ip address 193.254.23.1 255.255.255.240
half-duplex
!
router ospf 1
log-adjacency-changes
network 193.254.21.0 0.0.0.15 area 0
network 193.254.22.0 0.0.0.15 area 1
network 193.254.23.0 0.0.0.15 area 1

```

Figura 7. Configuración router claro DNP

## Configuración enrutador RoZonaFranca1 y 2

Para lograr la alta disponibilidad en los equipos del proveedor es necesario generar la implementación del protocolo VRRP (Virtual Router Redundancy Protocol), que permite a nivel de enrutamiento la capacidad de ser un equipo principal y uno backup a través de un switch sin configuración, en caso de que alguno de los dos falle. Asimismo, se realiza la conexión en el área 1 la cual está conectada hacia la red empresarial interna, generando las siguientes configuraciones:

```

interface GigabitEthernet1
ip address 193.254.18.2 255.255.255.240
negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet2
ip address 172.16.0.1 255.255.255.128
negotiation auto
vrrp 5 ip 172.16.0.5
vrrp 5 priority 90
no mop enabled
no mop sysid
!
interface GigabitEthernet3
no ip address
shutdown
negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet4
no ip address
shutdown
negotiation auto
no mop enabled
no mop sysid
!
router ospf 1
network 172.16.0.0 0.0.0.127 area 1
network 193.254.18.0 0.0.0.15 area 1

```

```

interface GigabitEthernet1
ip address 193.254.19.2 255.255.255.240
negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet2
ip address 172.16.0.3 255.255.255.128
negotiation auto
vrrp 5 ip 172.16.0.5
vrrp 5 priority 80
no mop enabled
no mop sysid
!
interface GigabitEthernet3
no ip address
shutdown
negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet4
no ip address
shutdown
negotiation auto
no mop enabled
no mop sysid
!
router ospf 1
network 172.16.0.0 0.0.0.127 area 1
network 193.254.19.0 0.0.0.15 area 1

```

Figura 8. Configuración router Zona Franca 1 y 2

## Configuración enrutador RoDNP1 y 2

Como se mencionó anteriormente, la red implementada en la oficina DNP es un espejo de la que va hacia Zona Franca por este motivo se implementaron las siguientes configuraciones:

```

interface GigabitEthernet1
ip address 193.254.22.2 255.255.255.240
negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet2
ip address 172.16.2.1 255.255.255.128
negotiation auto
vrrp 5 ip 172.16.2.5
vrrp 5 priority 90
no mop enabled
no mop sysid
!
interface GigabitEthernet3
no ip address
shutdown
negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet4
no ip address
shutdown
negotiation auto
no mop enabled
no mop sysid
!
router ospf 1
network 172.16.2.0 0.0.0.127 area 1
network 193.254.22.0 0.0.0.15 area 1

```

```

interface GigabitEthernet1
ip address 193.254.23.2 255.255.255.240
negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet2
ip address 172.16.2.3 255.255.255.128
negotiation auto
vrrp 5 ip 172.16.2.5
vrrp 5 priority 80
no mop enabled
no mop sysid
!
interface GigabitEthernet3
no ip address
shutdown
negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet4
no ip address
shutdown
negotiation auto
no mop enabled
no mop sysid
!
router ospf 1
network 172.16.2.0 0.0.0.127 area 1
network 193.254.23.0 0.0.0.15 area 1

```

Figura 9. Configuración router DNP 1 y 2



## Configuración equipos de premisas

Para poder contemplar una topología altamente disponible se deben contar con mínimo dos equipos en cada sede, los cuales van a tener la capacidad de recibir, direccionar y generar tráfico en espejo.

## Configuración de Firewall en alta disponibilidad Zona Franca

En este caso se va a realizar la configuración de los equipos de seguridad por medio de un establecimiento de alta disponibilidad, lo que habilita la posibilidad de tener 2 equipos físicos, pero uno lógico, con una redundancia esperada.

## Configuración de HA entre Firewalls

Se realiza el establecimiento de alta disponibilidad entre los Fortinet por medio de los puertos 9 y 10, dando la prioridad al maestro, quedando el segundo como backup en caso de alguna falla.

Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throug
		FortiGate VM64-KVM	1 3 5 7 9 11 13 15 17				
		FortiGate VM64-KVM	2 4 6 8 10 12 14 16 18				
	128	FortiGate-VM64-KVM	FGVMEVQUOE-TWIFD	Master	00:00:08:42	16	35.00 k
		FortiGate VM64-KVM	1 3 5 7 9 11 13 15 17				
		FortiGate VM64-KVM	2 4 6 8 10 12 14 16 18				
	127	FortiGate-VM64-KVM	FGVMEVSVF9ILZZE9	Slave	00:00:08:40	8	35.00 k

Figura 10. Configuración alta disponibilidad firewall Zona Franca

## Configuración puertos Firewall

En la topología actual, los equipos cuentan con un puerto para la salida hacia la WAN y otro puerto de administración como se evidencia en la imagen:

### Puerto de WAN

		172.16.0.2/255.255.255.128	PING HTTPS SSH SNMP +4
--	--	----------------------------	------------------------------------

Figura 11. Configuración puerto WAN firewall Zona Franca

## Puerto de gestión

port1	Physical Interface	172.16.1.2/255.255.255.128	PING HTTPS SSH HTTP FMG-Access
-------	--------------------	----------------------------	--

Figura 12. Configuración puerto de gestión firewall Zona Franca

## VLANs y agregación de puertos

Puerto de agregación hacia los Switches por medio de los puertos 8 y 9 así como la creación de las VLANs hacia los servidores.

LACP1	802.3ad Aggregate	port8 port7	10.10.10.1/255.255.255.0
VLAN20	VLAN		172.16.20.1/255.255.255.0
VLAN21	VLAN		172.16.21.1/255.255.255.0
VLAN22	VLAN		172.16.22.1/255.255.255.0
VLAN23	VLAN		172.16.23.1/255.255.255.0
VLAN121 (VLAN121)	VLAN		172.16.121.1/255.255.255.0
VLAN122 (VLAN122)	VLAN		172.16.122.1/255.255.255.0
VLAN 123 (VLAN 123)	VLAN		172.16.123.1/255.255.255.0
VLAN120 (VLAN120)	VLAN		172.16.120.1/255.255.255.0

Figura 13. Configuración VLAN y LACP Zona Franca

## Creación de grupos de VLANs

Name:

Block intra-zone traffic:

Interface members:

- ⊗ LACP1 ✕
- ⊗ VLAN 123 (VLAN 123) ✕
- ⊗ VLAN20 ✕
- ⊗ VLAN21 ✕
- ⊗ VLAN22 ✕
- ⊗ VLAN23 ✕
- ⊗ VLAN120 (VLAN120) ✕
- ⊗ VLAN121 (VLAN121) ✕
- ⊗ VLAN122 (VLAN122) ✕

+

Comments:

Figura 14. Configuración de grupo de VLAN firewall Zona Franca

## Creación de políticas hacia internet

Edit Policy

Name: VLANS-INTERNET

Incoming Interface: VLANS

Outgoing Interface: WAN (port2)

Source: all

Destination: all

Schedule: always

Service: ALL

Action: ACCEPT

Figura 15. Salida a internet de VLAN firewall Zona Franca

## Configuración de Firewall en alta disponibilidad DNP

La implementación en el brazo de DNP, se realiza como una copia de seguridad a la configuración realizada en el área de la zona franca.

## Configuración de HA entre Firewalls

Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
		FortiGate VM64-KVM					
	128	FortiGate-VM64-KVM	FGVMEV-YIQ0PWG31	Master	00:00:19:30	9	34.00 kbps
		FortiGate VM64-KVM					
	127	FortiGate-VM64-KVM	FGVMEVJKRVZBGS4B	Slave	00:00:19:26	7	35.00 kbps

Figura 16. Configuración alta disponibilidad firewall DNP

## Configuración puertos Firewall

Se realiza la configuración con el fin de establecer comunicación con el Firewall de Zona franca.

## Puerto de WAN

WAN (port2)	Physical Interface		172.16.2.2/255.255.255.128	PING HTTPS SSH SNMP +4
-------------	--------------------	--	----------------------------	------------------------------------

Figura 17. Configuración puerto WAN firewall DNP

## Puerto de gestión

port1	Physical Interface		172.16.1.104/255.255.255.128	PING HTTPS HTTP
-------	--------------------	--	------------------------------	-----------------------

Figura 18. Configuración puerto de gestión firewall DNP

## VLANs y agregación de puertos

Agregación de los puertos a través de LACP hacia los Switches, la creación de las VLANs de los servidores.

LACP1 (LACP1)	802.3ad Aggregate	port7 port8	11.11.11.1/255.255.255.0
VLAN24	VLAN		172.16.24.1/255.255.255.0
VLAN25	VLAN		172.16.25.1/255.255.255.0
VLAN26	VLAN		172.16.26.1/255.255.255.0
VLAN27	VLAN		172.16.27.1/255.255.255.0
VLAN124	VLAN		172.16.124.1/255.255.255.0
VLAN125	VLAN		172.16.125.1/255.255.255.0
VLAN126	VLAN		172.16.126.1/255.255.255.0
VLAN127	VLAN		172.16.127.1/255.255.255.0

Figura 19. Configuración de VLANs y LACP DNP

## Creación de políticas hacia internet

Edit Policy	
Name <span>!</span>	VLANS-INTERNET
Incoming Interface	<input type="checkbox"/> VLANS
Outgoing Interface	<input checked="" type="checkbox"/> WAN (port2)
Source	<input checked="" type="checkbox"/> all <span>+</span>
Destination	<input checked="" type="checkbox"/> all <span>+</span>
Schedule	<input checked="" type="checkbox"/> always
Service	<input checked="" type="checkbox"/> ALL <span>+</span>
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY

Figura 20. Creación de políticas firewall DNP

## Configuración de Switch Zona franca 1

```
interface GigabitEthernet1/0
switchport access vlan 20
switchport mode access
media-type rj45
negotiation auto
!
interface GigabitEthernet1/1
switchport access vlan 21
switchport mode access
media-type rj45
negotiation auto
!
interface GigabitEthernet1/2
switchport access vlan 22
switchport mode access
media-type rj45
negotiation auto
!
interface GigabitEthernet1/3
switchport access vlan 23
switchport mode access
media-type rj45
negotiation auto
!
interface Port-channel1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Port-channel2
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
media-type rj45
negotiation auto
channel-group 1 mode active
!
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
media-type rj45
negotiation auto
channel-group 1 mode active
!
interface GigabitEthernet3/2
switchport trunk encapsulation dot1q
switchport mode trunk
media-type rj45
negotiation auto
channel-group 2 mode active
!
interface GigabitEthernet3/3
switchport trunk encapsulation dot1q
switchport mode trunk
media-type rj45
negotiation auto
channel-group 2 mode active
!
```

Figura 21. Configuración de switch Zona Franca 1

## Configuración de Switch Zona franca 2

```
interface GigabitEthernet3/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
 channel-group 2 mode active
!
interface GigabitEthernet3/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
 channel-group 2 mode active
!
interface GigabitEthernet1/0
 switchport access vlan 120
 switchport mode access
 media-type rj45
 negotiation auto
!
interface GigabitEthernet1/1
 switchport access vlan 121
 switchport mode access
 media-type rj45
 negotiation auto
!
interface GigabitEthernet1/2
 switchport access vlan 122
 switchport mode access
 media-type rj45
 negotiation auto
!
interface GigabitEthernet1/3
 switchport access vlan 123
 switchport mode access
 media-type rj45
 negotiation auto
!
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
 channel-group 1 mode active
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
 channel-group 1 mode active
```

Figura 22. Configuración de switch Zona Franca 2

## Configuración de Switch DNP 1

```
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
 channel-group 1 mode active
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
 channel-group 1 mode active
!
interface GigabitEthernet1/0
 switchport access vlan 24
 switchport mode access
 media-type rj45
 negotiation auto
!
interface GigabitEthernet1/1
 switchport access vlan 25
 switchport mode access
 media-type rj45
 negotiation auto
!
interface GigabitEthernet1/2
 switchport access vlan 26
 switchport mode access
 media-type rj45
 negotiation auto
!
interface GigabitEthernet1/3
 switchport access vlan 27
 switchport mode access
 media-type rj45
 negotiation auto
!
interface GigabitEthernet3/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
 channel-group 2 mode active
!
interface GigabitEthernet3/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
 channel-group 2 mode active
```

Figura 23. Configuración de switch DNP 1

## Configuración de Switch Zona DNP 2

```
interface GigabitEthernet3/2
switchport trunk encapsulation dot1q
switchport mode trunk
media-type rj45
negotiation auto
channel-group 2 mode active
!
interface GigabitEthernet3/3
switchport trunk encapsulation dot1q
switchport mode trunk
media-type rj45
negotiation auto
channel-group 2 mode active
interface Port-channel1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Port-channel2
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
media-type rj45
negotiation auto
channel-group 1 mode active
!
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
media-type rj45
negotiation auto
channel-group 1 mode active

interface GigabitEthernet1/0
switchport access vlan 124
switchport mode access
media-type rj45
negotiation auto
!
interface GigabitEthernet1/1
switchport access vlan 125
switchport mode access
media-type rj45
negotiation auto
!
interface GigabitEthernet1/2
switchport access vlan 126
switchport mode access
media-type rj45
negotiation auto
!
interface GigabitEthernet1/3
switchport access vlan 127
switchport mode access
media-type rj45
negotiation auto
```

Figura 24. Configuración de switch DNP 2

## Configuración de servidores

Se realiza la configuración de los equipos de red en cada uno de los lados de la MPLS, con el número de host terminado en .10 como se muestra en la imagen

```
root@GranjaServer1:~# ifconfig eth0 172.16.20.10 netmask 255.255.255.0
root@GranjaServer1:~# route add default gw 172.16.20.1
root@GranjaServer1:~# ifconfig eth1 172.16.120.10 netmask 255.255.255.0
root@GranjaServer1:~# route add default gw 172.16.120.1
root@GranjaServer1:~# route -v
Kernel IP routing table
Destination      Gateway         Genmask        Flags Metric Ref    Use Iface
default          172.16.120.1   0.0.0.0        UG    0      0      0 eth1
default          172.16.20.1    0.0.0.0        UG    0      0      0 eth0
172.16.20.0     *              255.255.255.0  U    0      0      0 eth0
172.16.120.0    *              255.255.255.0  U    0      0      0 eth1
```

Figura 25. Configuración de servidores

## 5.7 Pruebas de comunicación a través de la MPLS

Para evidenciar el protocolo OSPF implementado a través de la MPLS es posible validarlo a través de las tablas de enrutamiento de los equipos.

### ISPCORE

```
IspCore#sho ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    193.254.40.0/28 is subnetted, 1 subnets
C       193.254.40.0 is directly connected, Ethernet2/0
    193.254.20.0/28 is subnetted, 1 subnets
C       193.254.20.0 is directly connected, Ethernet0/0
    193.254.21.0/28 is subnetted, 1 subnets
C       193.254.21.0 is directly connected, Ethernet1/0
    193.254.18.0/28 is subnetted, 1 subnets
O IA    193.254.18.0 [110/20] via 193.254.20.2, 00:00:13, Ethernet0/0
O       192.168.100.0/24 [110/11] via 193.254.40.2, 00:00:13, Ethernet2/0
    193.254.19.0/28 is subnetted, 1 subnets
O IA    193.254.19.0 [110/20] via 193.254.20.2, 00:00:14, Ethernet0/0
```

Figura 26. Tabla de enrutamiento ISPCORE IPv4

### Router Claro Zona Franca

```
RoClaroZF#sho ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    193.254.40.0/28 is subnetted, 1 subnets
O       193.254.40.0 [110/20] via 193.254.20.1, 00:00:44, Ethernet0/0
    193.254.20.0/28 is subnetted, 1 subnets
C       193.254.20.0 is directly connected, Ethernet0/0
    193.254.21.0/28 is subnetted, 1 subnets
O       193.254.21.0 [110/20] via 193.254.20.1, 00:00:44, Ethernet0/0
    193.254.22.0/28 is subnetted, 1 subnets
O IA    193.254.22.0 [110/30] via 193.254.20.1, 00:00:44, Ethernet0/0
    193.254.23.0/28 is subnetted, 1 subnets
O IA    193.254.23.0 [110/30] via 193.254.20.1, 00:00:45, Ethernet0/0
    193.254.18.0/28 is subnetted, 1 subnets
C       193.254.18.0 is directly connected, Ethernet1/0
O       192.168.100.0/24 [110/21] via 193.254.20.1, 00:00:45, Ethernet0/0
    193.254.19.0/28 is subnetted, 1 subnets
C       193.254.19.0 is directly connected, Ethernet2/0
```

Figura 27 Tabla de enrutamiento router claro Zona Franca IPv4



## Router Claro DNP

```
193.254.40.0/28 is subnetted, 1 subnets
O   193.254.40.0 [110/20] via 193.254.21.1, 00:05:18, Ethernet1/0
193.254.20.0/28 is subnetted, 1 subnets
O   193.254.20.0 [110/20] via 193.254.21.1, 00:05:18, Ethernet1/0
193.254.21.0/28 is subnetted, 1 subnets
C   193.254.21.0 is directly connected, Ethernet1/0
193.254.22.0/28 is subnetted, 1 subnets
C   193.254.22.0 is directly connected, Ethernet0/0
193.254.23.0/28 is subnetted, 1 subnets
C   193.254.23.0 is directly connected, Ethernet2/0
193.254.18.0/28 is subnetted, 1 subnets
O IA 193.254.18.0 [110/30] via 193.254.21.1, 00:00:39, Ethernet1/0
O   192.168.100.0/24 [110/21] via 193.254.21.1, 00:05:18, Ethernet1/0
193.254.19.0/28 is subnetted, 1 subnets
O IA 193.254.19.0 [110/30] via 193.254.21.1, 00:00:39, Ethernet1/0
RoClaroDNP#
```

Figura 28. Tabla de enrutamiento router claro DNP IPv4

## Router Zona Franca 1

```
RoClaroDNP#sho ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

193.254.40.0/28 is subnetted, 1 subnets
O   193.254.40.0 [110/20] via 193.254.21.1, 00:01:38, Ethernet1/0
193.254.20.0/28 is subnetted, 1 subnets
O   193.254.20.0 [110/20] via 193.254.21.1, 00:01:38, Ethernet1/0
193.254.21.0/28 is subnetted, 1 subnets
C   193.254.21.0 is directly connected, Ethernet1/0
193.254.22.0/28 is subnetted, 1 subnets
C   193.254.22.0 is directly connected, Ethernet0/0
193.254.23.0/28 is subnetted, 1 subnets
C   193.254.23.0 is directly connected, Ethernet2/0
193.254.18.0/28 is subnetted, 1 subnets
O IA 193.254.18.0 [110/30] via 193.254.21.1, 00:01:39, Ethernet1/0
O   192.168.100.0/24 [110/21] via 193.254.21.1, 00:01:39, Ethernet1/0
193.254.19.0/28 is subnetted, 1 subnets
O IA 193.254.19.0 [110/30] via 193.254.21.1, 00:01:39, Ethernet1/0
```

Figura 29. Tabla de enrutamiento router Zona Franca 1 IPv4

## Router Zona Franca2

```
O IA 192.168.100.0/24 [110/22] via 193.254.19.1, 00:00:08, GigabitEthernet1
193.254.18.0/28 is subnetted, 1 subnets
O   193.254.18.0 [110/11] via 193.254.19.1, 00:00:08, GigabitEthernet1
193.254.19.0/24 is variably subnetted, 2 subnets, 2 masks
C   193.254.19.0/28 is directly connected, GigabitEthernet1
L   193.254.19.2/32 is directly connected, GigabitEthernet1
193.254.20.0/28 is subnetted, 1 subnets
O IA 193.254.20.0 [110/11] via 193.254.19.1, 00:00:08, GigabitEthernet1
193.254.21.0/28 is subnetted, 1 subnets
O IA 193.254.21.0 [110/21] via 193.254.19.1, 00:00:08, GigabitEthernet1
193.254.22.0/28 is subnetted, 1 subnets
O IA 193.254.22.0 [110/31] via 193.254.19.1, 00:00:08, GigabitEthernet1
193.254.23.0/28 is subnetted, 1 subnets
O IA 193.254.23.0 [110/31] via 193.254.19.1, 00:00:08, GigabitEthernet1
193.254.40.0/28 is subnetted, 1 subnets
O IA 193.254.40.0 [110/21] via 193.254.19.1, 00:00:08, GigabitEthernet1
```

Figura 30. Tabla de enrutamiento router Zona Franca 2 IPv4

## Router DNP1

```
Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C   172.16.2.0/25 is directly connected, GigabitEthernet2
L   172.16.2.1/32 is directly connected, GigabitEthernet2
O IA 192.168.100.0/24 [110/22] via 193.254.22.1, 00:02:01, GigabitEthernet1
193.254.18.0/28 is subnetted, 1 subnets
O IA 193.254.18.0 [110/31] via 193.254.22.1, 00:02:01, GigabitEthernet1
193.254.19.0/28 is subnetted, 1 subnets
O IA 193.254.19.0 [110/31] via 193.254.22.1, 00:02:01, GigabitEthernet1
193.254.20.0/28 is subnetted, 1 subnets
O IA 193.254.20.0 [110/21] via 193.254.22.1, 00:02:01, GigabitEthernet1
193.254.21.0/28 is subnetted, 1 subnets
O IA 193.254.21.0 [110/11] via 193.254.22.1, 00:02:01, GigabitEthernet1
193.254.22.0/24 is variably subnetted, 2 subnets, 2 masks
C   193.254.22.0/28 is directly connected, GigabitEthernet1
L   193.254.22.2/32 is directly connected, GigabitEthernet1
193.254.23.0/28 is subnetted, 1 subnets
O   193.254.23.0 [110/11] via 193.254.22.1, 00:00:32, GigabitEthernet1
193.254.40.0/28 is subnetted, 1 subnets
O IA 193.254.40.0 [110/21] via 193.254.22.1, 00:02:01, GigabitEthernet1
```

Figura 31. Tabla de enrutamiento router DNP 1 IPv4

## Router DNP2

```
Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C   172.16.2.0/25 is directly connected, GigabitEthernet2
L   172.16.2.3/32 is directly connected, GigabitEthernet2
O IA 192.168.100.0/24 [110/22] via 193.254.23.1, 00:00:07, GigabitEthernet1
193.254.18.0/28 is subnetted, 1 subnets
O IA 193.254.18.0 [110/31] via 193.254.23.1, 00:00:07, GigabitEthernet1
193.254.19.0/28 is subnetted, 1 subnets
O IA 193.254.19.0 [110/31] via 193.254.23.1, 00:00:07, GigabitEthernet1
193.254.20.0/28 is subnetted, 1 subnets
O IA 193.254.20.0 [110/21] via 193.254.23.1, 00:00:07, GigabitEthernet1
193.254.21.0/28 is subnetted, 1 subnets
O IA 193.254.21.0 [110/11] via 193.254.23.1, 00:00:07, GigabitEthernet1
193.254.22.0/28 is subnetted, 1 subnets
O   193.254.22.0 [110/2] via 172.16.2.1, 00:00:06, GigabitEthernet2
193.254.23.0/24 is variably subnetted, 2 subnets, 2 masks
C   193.254.23.0/28 is directly connected, GigabitEthernet1
L   193.254.23.2/32 is directly connected, GigabitEthernet1
193.254.40.0/28 is subnetted, 1 subnets
O IA 193.254.40.0 [110/21] via 193.254.23.1, 00:00:07, GigabitEthernet1
```

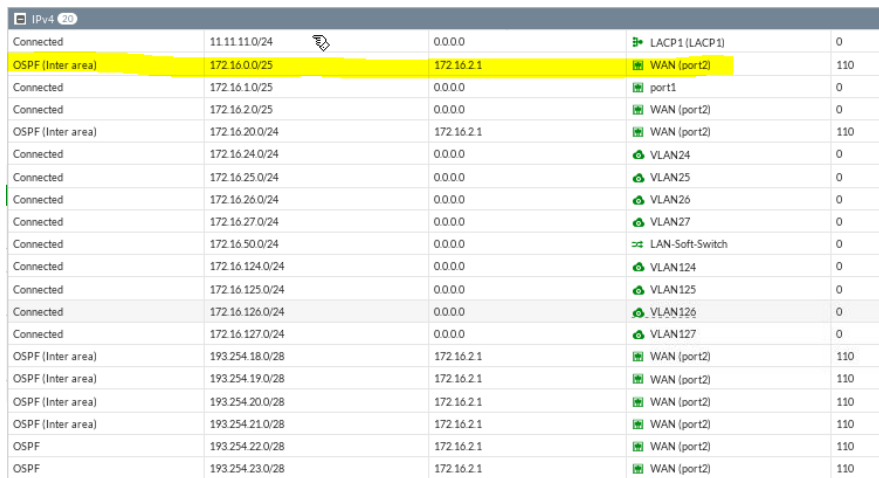
Figura 32. Tabla de enrutamiento router DNP 2 IPv4

## 5.8 Resultado de pruebas realizadas

Teniendo en cuenta la topología base del Departamento Nacional de Planeación, se realizan varias pruebas de comunicación, lo que logra emular el funcionamiento actual por medio del desarrollo de la emulación.

### Firewall ubicado en Zona Franca

Se realiza la validación a través del protocolo OSPF, donde se evidencia conexión hacia la puerta de enlace de la red.

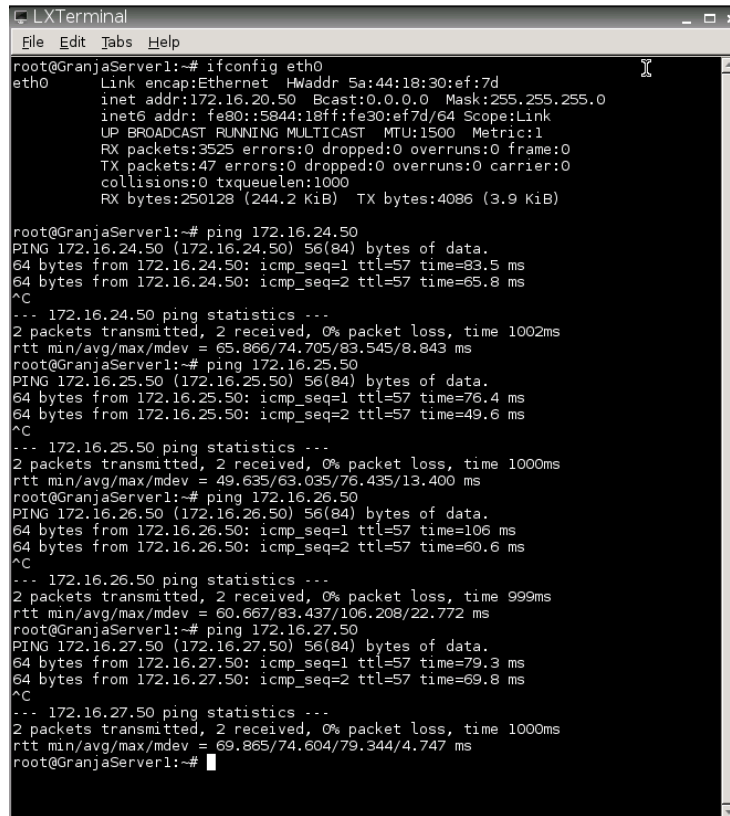


IP v4	11.11.11.0/24	0.0.0.0	LACP1 (LACP1)	0
OSPF (Inter area)	172.16.0.0/25	172.16.2.1	WAN (port2)	110
Connected	172.16.1.0/25	0.0.0.0	port1	0
Connected	172.16.2.0/25	0.0.0.0	WAN (port2)	0
OSPF (Inter area)	172.16.20.0/24	172.16.2.1	WAN (port2)	110
Connected	172.16.24.0/24	0.0.0.0	VLAN24	0
Connected	172.16.25.0/24	0.0.0.0	VLAN25	0
Connected	172.16.26.0/24	0.0.0.0	VLAN26	0
Connected	172.16.27.0/24	0.0.0.0	VLAN27	0
Connected	172.16.50.0/24	0.0.0.0	LAN-Soft-Switch	0
Connected	172.16.124.0/24	0.0.0.0	VLAN124	0
Connected	172.16.125.0/24	0.0.0.0	VLAN125	0
Connected	172.16.126.0/24	0.0.0.0	VLAN126	0
Connected	172.16.127.0/24	0.0.0.0	VLAN127	0
OSPF (Inter area)	193.254.18.0/28	172.16.2.1	WAN (port2)	110
OSPF (Inter area)	193.254.19.0/28	172.16.2.1	WAN (port2)	110
OSPF (Inter area)	193.254.20.0/28	172.16.2.1	WAN (port2)	110
OSPF (Inter area)	193.254.21.0/28	172.16.2.1	WAN (port2)	110
OSPF	193.254.22.0/28	172.16.2.1	WAN (port2)	110
OSPF	193.254.23.0/28	172.16.2.1	WAN (port2)	110

Figura 33. Tabla de enrutamiento firewall Zona Franca IPv4

## Equipo ubicado en Zona Franca

Se realizan las pruebas desde un equipo ubicado en Zona Franca con dirección IP 172.16.20.50 el cual puede alcanzar los equipos de las redes ubicadas en las VLANs 24, 25, 26 y 27 de manera correcta.



```
root@GranjaServer1:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 5a:44:18:30:ef:7d
          inet addr:172.16.20.50  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: fe80::5844:18ff:fe30:ef7d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3525 errors:0 dropped:0 overruns:0 frame:0
          TX packets:47 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:250128 (244.2 KiB)  TX bytes:4086 (3.9 KiB)

root@GranjaServer1:~# ping 172.16.24.50
PING 172.16.24.50 (172.16.24.50) 56(84) bytes of data.
64 bytes from 172.16.24.50: icmp_seq=1 ttl=57 time=83.5 ms
64 bytes from 172.16.24.50: icmp_seq=2 ttl=57 time=65.8 ms
^C
--- 172.16.24.50 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 65.866/74.705/83.545/8.843 ms
root@GranjaServer1:~# ping 172.16.25.50
PING 172.16.25.50 (172.16.25.50) 56(84) bytes of data.
64 bytes from 172.16.25.50: icmp_seq=1 ttl=57 time=76.4 ms
64 bytes from 172.16.25.50: icmp_seq=2 ttl=57 time=49.6 ms
^C
--- 172.16.25.50 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 49.635/63.035/76.435/13.400 ms
root@GranjaServer1:~# ping 172.16.26.50
PING 172.16.26.50 (172.16.26.50) 56(84) bytes of data.
64 bytes from 172.16.26.50: icmp_seq=1 ttl=57 time=106 ms
64 bytes from 172.16.26.50: icmp_seq=2 ttl=57 time=60.6 ms
^C
--- 172.16.26.50 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 60.667/83.437/106.208/22.772 ms
root@GranjaServer1:~# ping 172.16.27.50
PING 172.16.27.50 (172.16.27.50) 56(84) bytes of data.
64 bytes from 172.16.27.50: icmp_seq=1 ttl=57 time=79.3 ms
64 bytes from 172.16.27.50: icmp_seq=2 ttl=57 time=69.8 ms
^C
--- 172.16.27.50 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 69.865/74.604/79.344/4.747 ms
root@GranjaServer1:~#
```

Figura 34. Pruebas de Ping desde sede Zona Franca Ipv4

## Firewall ubicado en DNP

IPv4	IP	IP	Interface	Cost
Connected	11.11.110/24	0.0.0	LACP1 (LACP1)	0
OSPF (Inter area)	172.16.0/25	172.16.2.1	WAN (port2)	110
Connected	172.16.10/25	0.0.0	port1	0
Connected	172.16.20/25	0.0.0	WAN (port2)	0
OSPF (Inter area)	172.16.20.0/24	172.16.2.1	WAN (port2)	110
Connected	172.16.24.0/24	0.0.0	VLAN24	0
Connected	172.16.25.0/24	0.0.0	VLAN25	0
Connected	172.16.26.0/24	0.0.0	VLAN26	0
Connected	172.16.27.0/24	0.0.0	VLAN27	0
Connected	172.16.50.0/24	0.0.0	LAN-Soft-Switch	0
Connected	172.16.124.0/24	0.0.0	VLAN124	0
Connected	172.16.125.0/24	0.0.0	VLAN125	0
Connected	172.16.126.0/24	0.0.0	VLAN126	0
Connected	172.16.127.0/24	0.0.0	VLAN127	0
OSPF (Inter area)	193.254.18.0/28	172.16.2.1	WAN (port2)	110
OSPF (Inter area)	193.254.19.0/28	172.16.2.1	WAN (port2)	110
OSPF (Inter area)	193.254.20.0/28	172.16.2.1	WAN (port2)	110
OSPF (Inter area)	193.254.21.0/28	172.16.2.1	WAN (port2)	110
OSPF	193.254.22.0/28	172.16.2.1	WAN (port2)	110
OSPF	193.254.23.0/28	172.16.2.1	WAN (port2)	110

Figura 35. Tabla de enrutamiento firewall DNP IPv4

## Equipo ubicado en DNP

```

LXTerminal
File Edit Tabs Help
root@GranjaServer8:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr ea:c5:64:6a:81:90
          inet addr:172.16.27.50  Bcast:0.0.0.0  Mask:255.255.0
          inet6 addr: fe80::e8c5:64ff:fe6a:8190/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:128 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8986 (8.7 KiB)  TX bytes:1426 (1.3 KiB)

root@GranjaServer8:~# ping 172.16.120.50
PING 172.16.120.50 (172.16.120.50) 56(84) bytes of data.
64 bytes from 172.16.120.50: icmp_seq=1 ttl=57 time=65.2 ms
64 bytes from 172.16.120.50: icmp_seq=2 ttl=57 time=47.5 ms
^C
--- 172.16.120.50 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 47.531/56.403/65.275/8.872 ms
root@GranjaServer8:~# ping 172.16.121.50
PING 172.16.121.50 (172.16.121.50) 56(84) bytes of data.
64 bytes from 172.16.121.50: icmp_seq=1 ttl=57 time=72.8 ms
64 bytes from 172.16.121.50: icmp_seq=2 ttl=57 time=51.5 ms
^C
--- 172.16.121.50 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 51.505/62.187/72.869/10.682 ms
root@GranjaServer8:~# ping 172.16.122.50
PING 172.16.122.50 (172.16.122.50) 56(84) bytes of data.
64 bytes from 172.16.122.50: icmp_seq=1 ttl=57 time=67.8 ms
64 bytes from 172.16.122.50: icmp_seq=2 ttl=57 time=58.6 ms
^C
--- 172.16.122.50 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 58.624/63.260/67.896/4.636 ms
root@GranjaServer8:~# ping 172.16.123.50
PING 172.16.123.50 (172.16.123.50) 56(84) bytes of data.
64 bytes from 172.16.123.50: icmp_seq=1 ttl=57 time=71.7 ms
64 bytes from 172.16.123.50: icmp_seq=2 ttl=57 time=45.5 ms
^C
--- 172.16.123.50 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 45.536/58.661/71.786/13.125 ms
root@GranjaServer8:~#

```

Figura 36. Pruebas de Ping desde sede DNP IPv4

Los resultados obtenidos permiten llegar a los siguientes eventos para tener en cuenta en el momento de generar la nueva topología, los protocolos a utilizar y demás componentes que se tienen en la red, destacando los siguientes hallazgos:

- Los equipos actuales están en la capacidad de implementar el protocolo Ipv6 de la mano de VxLAN.
- Es posible utilizar el protocolo OSPF teniendo en cuenta que la versión 3 del mismo es capaz de resolver tanto redes Ipv4 como Ipv6.
- El establecimiento de redes backup en cada centro de datos de la red permite generar una topología nueva de manera redundante.
- Se evidencia la creación de reglas independientes para el protocolo Ipv4 como para Ipv6, dado que versiones que no son compatibles entre si a pesar de que puedan compartir la misma infraestructura física.

## 6. Nuevo diseño de red

En este trabajo se propone una nueva topología lógica de red para los equipos en los centros de datos ubicados en la zona franca y en las oficinas de la entidad, tomando en cuenta la necesidad de la compañía de estar a la vanguardia de las nuevas tecnologías, en este caso cabe mencionar la transición necesaria y especificada por el MinTIC hacia el protocolo Ipv6 en primera fase como una etapa de planeación.

Ahora bien, el crecimiento exponencial de servicios expuestos que han tenido en el desarrollo de cada uno de los aplicativos que solicita el estado, es necesario pensar en una cantidad más grande de subredes por este motivo se propone la implementación de las VxLAN.

Los dispositivos de ingreso a la MPLS en este caso los enrutadores están en la posibilidad de ser actualizados constantemente lo que ayuda a presentar un ahorro de dinero en la compañía, para no ser invertido en la adquisición de

nuevos equipos. Por otro lado, la entidad cuenta con un direccionamiento propio a través de Lacnic (Registro de Direcciones de Internet de América Latina y Caribe), tanto en protocolo Ipv4 e Ipv6.

Por otro lado, se encuentran los equipos de seguridad, que cuentan con una licencia de 10 años, lo que permite tener soporte a fabricante por este tiempo lo que ayuda a realizar la implementación propuesta cumpliendo con los lineamientos establecidos por el gobierno.

Por último, se realiza un inventario de los servidores donde se alojará la información de aplicativos y bases de datos confidenciales almacenadas como múltiples máquinas virtuales dentro de servidores Windows Server 2016.

## 6.1 Direccionamiento propuesto en Ipv6

El direccionamiento que se propone para realizar la implementación del proyecto se realizó con base a los nombres y direcciones mencionadas en el capítulo 4, para realizar este tipo de transiciones lo ideal es seguir con la nomenclatura, para que sea más fácil su administración en los dos protocolos.

Teniendo en cuenta lo mencionado al principio del capítulo, la entidad cuenta con la capacidad de tener un direccionamiento propio brindado por Lacnic quienes al analizar previamente la cantidad de equipos de la entidad otorgan una subred /56, con lo cual es posible realizar una fragmentación del segmento. Como norma impuesta a nivel mundial se debe establecer una subred /64 para los equipos de uso final.

Por tratarse de redes Ipv6 propias estas pueden ser anunciadas a través del protocolo BGP en cualquier conexión hacia internet, permitiendo una distribución más eficiente.

## 6.1.1 Direccionamiento DualStack equipos Core

Nombre del equipo	Interfaz	Direccionamiento Ipv4	Direccionamiento Ipv6	Descripción
ISP Core	Eth0/0	193.254.20.1	2021::1	Conexión hacia RoClaroZF
	Eth1/0	193.254.21.1	2020::1	Conexión hacia RoClaroDNP
	Eth2/0	193.254.40.1	FD31:9046:5493:50::20	Conexión hacia sede WorldService
RoClaroZF	Eth0/0	193.254.20.2	2020::2	Conexión hacia ISP Core
	Eth1/0	193.254.18.1	2018::1	Conexión hacia router Zona franca 1
	Eth2/0	193.254.19.1	2019::1	Conexión hacia router Zona franca 2
Router Claro DNP	Eth0/0	193.254.22.1	2022::1	Conexión hacia router DNP1
	Eth1/0	193.254.21.2	2021::2	Conexión hacia ISP Core
	Eth2/0	193.254.23.1	2023::1	Conexión hacia router DNP2
Router Zona Franca 1	Gi1	193.254.18.2	2018::2	Conexión hacia RoClaroZF
	Gi2	172.16.0.1	2002:16::1	Conexión hacia Firewall Zona franca
	VRRP 5	172.16.0.5	2002:16::5	Conexión Router Zona franca 2
Router Zona Franca 2	Gi1	193.254.19.2	2019::2	Conexión hacia RoClaroZF
	Gi2	172.16.0.3	2002:16::3	Conexión hacia Firewall Zona franca
	VRRP 5	172.16.0.5	2002:16::5	Conexión Router Zona franca 1
Router DNP 1	Gi1	193.254.22.2	2022::2	Conexión hacia Router Claro DNP
	Gi2	172.16.2.1	2002:16:2::1	Conexión hacia Firewall DNP
	VRRP 5	172.16.2.5	2002:16:2::5	Conexión hacia router DNP2



Nombre del equipo	Interfaz	Direccionamiento Ipv4	Direccionamiento Ipv6	Descripción
Router DNP 2	Gi1	193.254.23.2	2023::2	Conexión hacia Router Claro DNP
	Gi2	172.16.2.3	2002:16:2::3	Conexión hacia Firewall DNP
	VRRP 5	172.16.2.5	2002:16:2::5	Conexión hacia router DNP1
Firewall Zona Franca	Port 1	172.16.0.2	2002:16::2	Conexión hacia Los router Zona Franca
	Port7	N/A	N/A	Puerto VLANs y LanSoftSwitch VxLAN
	Port 8	N/A	N/A	Puerto VLANs y LanSoftSwitch VxLAN
	Port9	N/A	N/A	Alta disponibilidad Firewall
	Port 10	N/A	N/A	Alta disponibilidad Firewall
Firewall Zona Franca	Port 1	172.16.2.2	2002:16:2::2	Conexión hacia Los router Zona Franca
	Port7	N/A	N/A	Puerto VLANs y LanSoftSwitch VxLAN
	Port 8	N/A	N/A	Puerto VLANs y LanSoftSwitch VxLAN
	Port9	N/A	N/A	Alta disponibilidad Firewall
	Port 10	N/A	N/A	Alta disponibilidad Firewall
Router World Service	F0/0	192.168.100.1	FD31:9046:5493:3::20	Conexión hacia PC WorldService
	F1/0	193.254.40.2	FD31:9046:5493:50::30	Conexión hacia ISP Core
	F2/0	192.168.122.161	FD31:5493:50::30	Salida hacia internet

*Tabla 12. Direccionamiento DualStack equipos Core*

## 6.2 Topología de red propuesta en Ipv6

Para lograr la configuración de una red altamente disponible, es necesario generar una serie de enlaces redundantes entre los equipos de la empresa, buscando tener la menor posibilidad de fallos por este motivo cada uno de los componentes está conectado hacia sus rutas de salida con un mínimo de 2 puertos Gigabit Ethernet, lo que hace factible el ingreso en caso de falla por distintos medios.

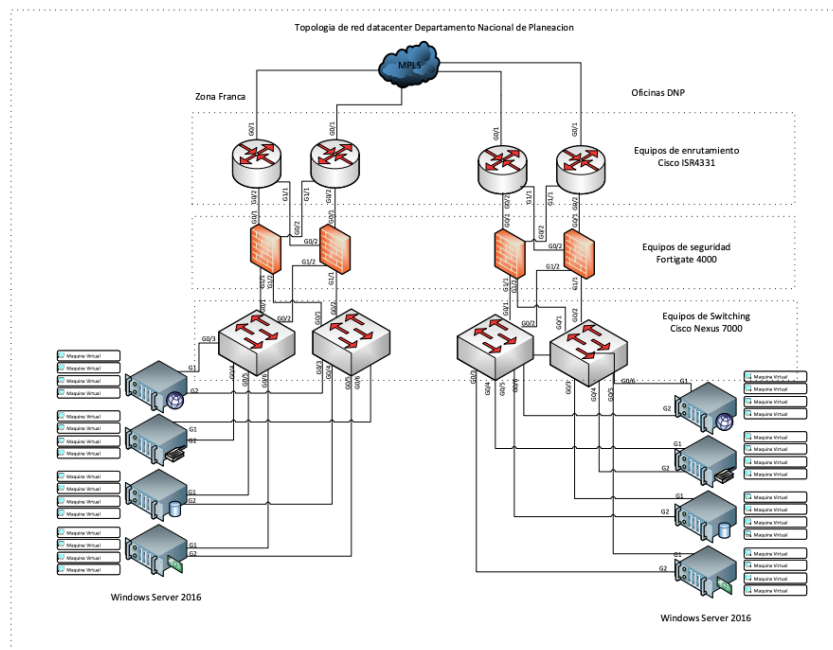


Figura. Topología propuesta en Ipv6

## 6.3 Validación experimental y ambiente de prueba

En este capítulo se realizará el planteamiento inicial con los equipos, configuraciones y protocolos con los cuales cuenta actualmente la empresa para tener un punto de partida, con la adición de una sede alterna y un DNS para cada brazo de la MPLS.

Seguido a esto se realizará la emulación del protocolo Ipv6 y la segmentación a través de VxLAN; para lograr esto es necesario generar un esquema altamente

disponible basado en los equipos con los que se cuenta en la red, por este motivo se realizara la propuesta de mejora a topología.

Teniendo en cuenta que los equipos tienen las mismas características se genera la topología de la siguiente manera:

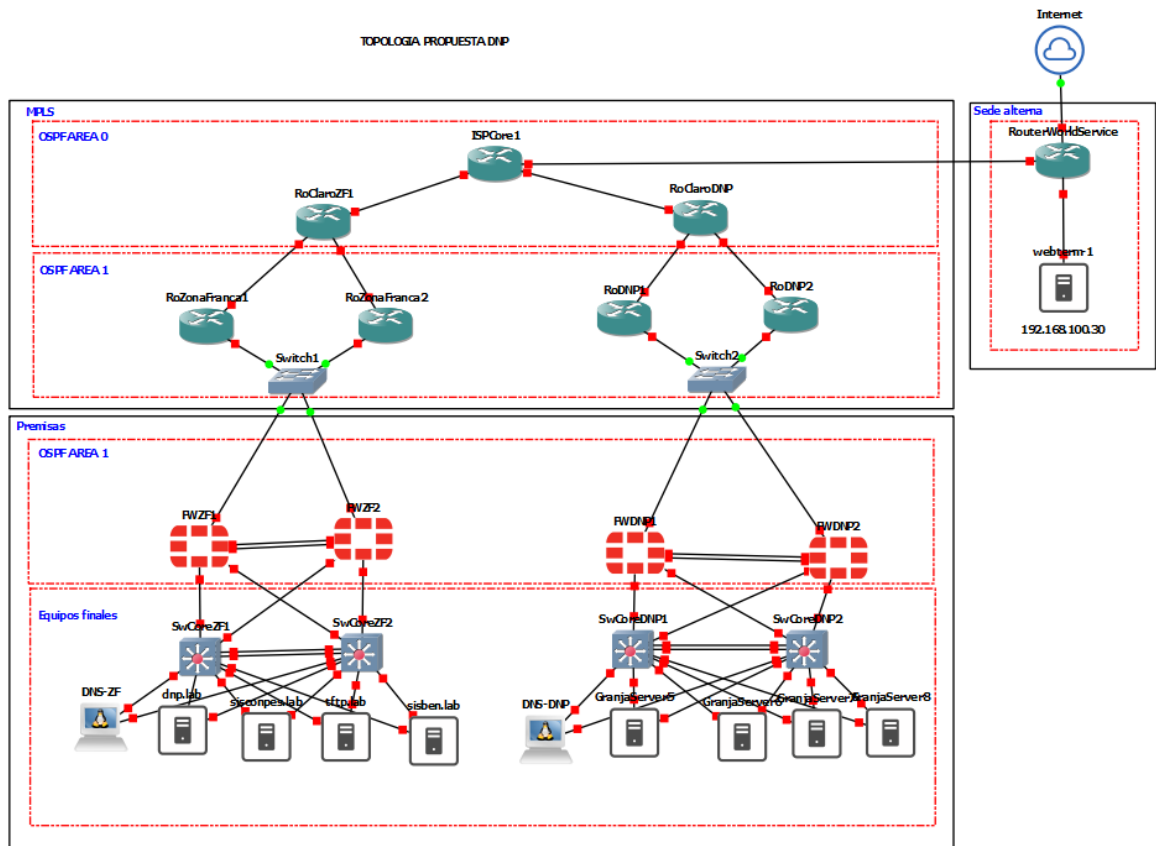


Figura 37. Topología Emulada en GNS3

## 6.4 Configuración de topología en DualStack por medio de red Ipv6

### ISP CORE IMPLEMENTACIÓN IPv6

```
IspCore(config)#ipv6 unicast-routing
IspCore(config)#int e0/0
IspCore(config-if)#ipv6 add 2021::1/64
IspCore(config-if)#int e1/0
IspCore(config-if)#ipv6 add 2020::1/64
IspCore(config-if)#exi
IspCore(config)#ipv6 router ospf 1
IspCore(config-rtr)#int e0/0
IspCore(config-if)#ipv6 ospf 1 area 0
IspCore(config-if)#int e1/0
IspCore(config-if)#ipv6 ospf 1 area 0
```

Figura 38. Configuración router ISPCORE Ipv6

### Router claro zona franca

```
RoClaroZF(config)#ipv6 unicast-routing
RoClaroZF(config)#int e1/0
RoClaroZF(config-if)#ipv6 add 2020::2/64
RoClaroZF(config-if)#no ipv6 add 2020::2/64
RoClaroZF(config-if)#int e0/0
RoClaroZF(config-if)#ipv6 add 2020::2/64
RoClaroZF(config-if)#int e1/0
RoClaroZF(config-if)#ipv6 add 2018::1/64
RoClaroZF(config-if)#int e2/0
RoClaroZF(config-if)#ipv6 add 2019::1/64
RoClaroZF(config-if)#exi
RoClaroZF(config)#ipv6 router ospf 1
RoClaroZF(config-rtr)#int e0/0
RoClaroZF(config-if)#ipv6 ospf 1 area 0
RoClaroZF(config-if)#
*Mar 1 00:30:45.211: %OSPFv3-5-ADJCHG: Process 1, Nbr 193.254.21.1 on Ethernet0/0 from LOADING to FULL, Loading Done
RoClaroZF(config-if)#int e1/0
RoClaroZF(config-if)#ipv6 ospf 1 area 1
RoClaroZF(config-if)#int e2/0
RoClaroZF(config-if)#ipv6 ospf 1 area 1
```

Figura 39. Configuración router claro Zona Franca Ipv6

## Router claro DNP

```
RoClaroDNP#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RoClaroDNP(config)#ipv6 unicast-routing
RoClaroDNP(config)#int e0/0
RoClaroDNP(config-if)#ipv6 add 2022::1/64
RoClaroDNP(config-if)#int e1/0
RoClaroDNP(config-if)#ipv6 add 2021::2/64
RoClaroDNP(config-if)#int e2/0
RoClaroDNP(config-if)#ipv6 add 2023::1/64
RoClaroDNP(config-if)#exi
RoClaroDNP(config)#ipv6 router ospf 1
RoClaroDNP(config-rtr)#exi
RoClaroDNP(config)#int e0/0
RoClaroDNP(config-if)#ipv6 ospf 1 area 1
RoClaroDNP(config-if)#int e1/0
RoClaroDNP(config-if)#ipv6 ospf 1 area 0
RoClaroDNP(config-if)#int e1/0
*Mar 1 00:39:25.083: %OSPFv3-5-ADJCHG: Process 1, Nbr 193.254.21.1 on Ethernet1/0 from LOADING to FULL, Loading Done
RoClaroDNP(config-if)#int e2/0
RoClaroDNP(config-if)#ipv6 ospf 1 area 1
```

Figura 40. Configuración router claro DNP Ipv6

## Router zona franca 1

```
Router(config)#ipv6 unicast-routing
Router(config)#int g1
Router(config-if)#ipv6 add 2018::2/64
Router(config-if)#int g2
Router(config-if)#ipv6 add 2002:16:0::1/64
Router(config-if)#exi
Router(config)#ipv6 router ospf 1
Router(config-rtr)#int g1
Router(config-if)#ipv6 ospf 1 area 1
Router(config-if)#int g2
Router(config-if)#ipv6 ospf 1 area 1
Router(config-if)#exi
```

Figura 41 Configuración router Zona Franca 1 Ipv6

## Zona franca 2

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ipv6 unic
Router(config)#ipv6 unicast-routing
Router(config)#int gi1
Router(config-if)#ipv6 add 2019::2/64
Router(config-if)#int gi2
Router(config-if)#ipv6 add 2002:16::3/64
Router(config-if)#exi
Router(config)#ipv6 router ospf 1
Router(config-rtr)#exi
Router(config)#
*Dec 9 00:20:24.512: %OSPFv3-6-DFT_OPT: Protocol timers for fast convergence are Enabled.
Router(config)#int gi1
Router(config-if)#ipv6 ospf 1 area 1
Router(config-if)#int gi1
*Dec 9 00:20:41.534: %OSPFv3-5-ADJCHG: Process 1, Nbr 193.254.20.2 on GigabitEthernet1 from LOADING to FULL, Loading Done
Router(config-if)#int gi2
Router(config-if)#ipv6 ospf 1 area 1
Router(config-if)#
*Dec 9 00:20:56.385: %OSPFv3-5-ADJCHG: Process 1, Nbr 193.254.18.2 on GigabitEthernet2 from LOADING to FULL, Loading Done
```

Figura 42. Configuración router claro Zona Franca 2 Ipv6

## DNP 1

```
Router(config)#ipv6 unicast-r
Router(config)#ipv6 unicast-routing
Router(config)#int gi1
Router(config-if)#ipv6 address 2022::2/64
Router(config-if)#int gi2
Router(config-if)#ipv6 address 2002:16:2::3/64
Router(config-if)#exit
Router(config)#ipv6 router ospf 1
Router(config-rtr)#router-id 8.8.8.8
Router(config-rtr)#int gi1
Router(config-if)#ipv6 ospf 1 area 1
Router(config-if)#int gi2
Router(config-if)#ipv6 ospf 1 area 1
Router(config-if)#exit
Router(config)#exit
```

*Figura 43. Configuración router claro DNP 1 Ipv6*

## DNP 2

```
Router(config)#ipv6 unicast-routing
Router(config)#int gi1
Router(config-if)#ipv6 address 2023::2/64
Router(config-if)#int gi2
Router(config-if)#ipv6 address 2002:16:2::4/64
Router(config-if)#exit
Router(config)#ipv6 router ospf 1
Router(config-rtr)#router-id 9.9.9.9
Router(config-rtr)#int gi1
Router(config-if)#ipv6 ospf 1 area 1
Router(config-if)#int gi2
Router(config-if)#ipv6 ospf 1 area 1
Router(config-if)#exit
Router(config)#exit
Router#wr
```

*Figura 44. Configuración router claro DNP 2 Ipv6*

# Firewall

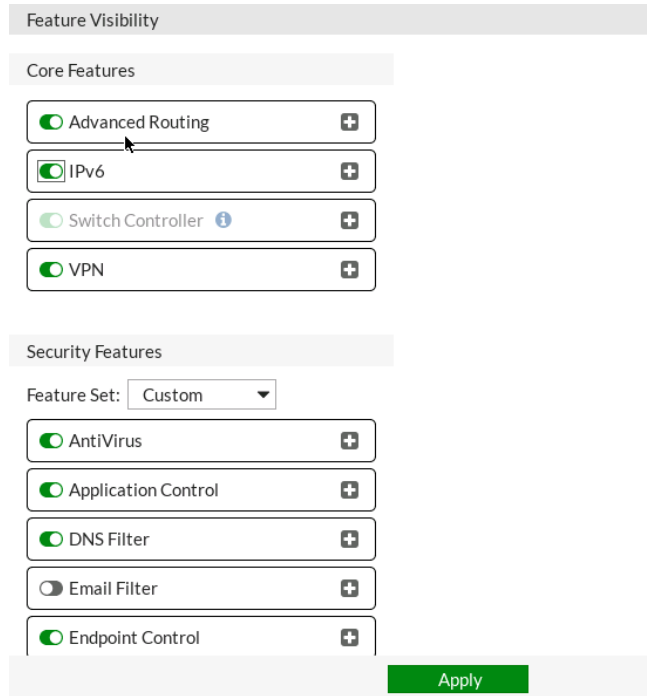


Figura 45. Habilitación protocolo Ipv6 en firewall

# Zona franca

```
config system interface
  edit "port1"
    set vdom "root"
    set ip 172.16.0.2 255.255.255.0
    set allowaccess ping https ssh snmp http fgfm radius-acct fabric ftm
    set type physical
    set alias "WAN"
    set lldp-reception enable
    set snmp-index 1
    config ipv6
      set ip6-address 2002:16::1/64
      set ip6-allowaccess ping
    end
end
```

```
end
config router ospf6
  set router-id 10.10.10.10
  config area
    edit 0.0.0.1
      next
    end
  config ospf6-interface
    edit "1"
      set area-id 0.0.0.1
      set interface "port1"
    next
end
```

Figura 46. Configuración Ipv6 firewall zona franca

# DNP

```
config system interface
  edit "port1"
    set vdom "root"
    set ip 172.16.2.2 255.255.255.0
    set allowaccess ping https ssh http fgfm
    set type physical
    set snmp-index 1
    config ipv6
      set ip6-address 2002:16:2::2/64
      set ip6-allowaccess ping
    end
  next
```

```
config router ospf6
  set router-id 20.20.20.20
  config area
    edit 0.0.0.1
      next
    edit 1.1.1.1
      next
    end
  config ospf6-interface
    edit "1"
      set area-id 0.0.0.1
      set interface "port1"
    next
end
```

Figura 47. Configuración Ipv6 firewall DNP

## Sede alterna World Service

```
interface FastEthernet0/0
ip address 192.168.100.1 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
ipv6 address FD31:9046:5493:3::20/64
ipv6 ospf 1 area 0
!
interface FastEthernet1/0
ip address 193.254.40.2 255.255.255.240
duplex auto
speed auto
ipv6 address FD31:9046:5493:50::30/64
ipv6 ospf 1 area 0
!
interface FastEthernet2/0
ip address dhcp
ip nat outside
ip virtual-reassembly
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
network 192.168.100.0 0.0.0.255 area 0
network 193.254.40.0 0.0.0.255 area 0
!
no ip http server
no ip http secure-server
!
ip nat inside source static 192.168.100.30 192.168.122.140
!
no cdp log mismatch duplex
ipv6 router ospf 1
router-id 32.32.32.32
log-adjacency-changes
```

Figura 48. Configuración de router sede World Service

### 6.4.1 Pruebas de funcionamiento IPv6

Las pruebas de funcionamiento del protocolo IPv6 en la red se pueden evidenciar a través de los equipos por medio de las tablas de enrutamiento

## ISPCORE

```
OI 2002:16:2::/64 [110/21]
   via FE80::CE01:25FF:FECE:10, Ethernet1/0
OI 2018::/64 [110/20]
   via FE80::CE03:2BFF:FE5A:0, Ethernet0/0
OI 2019::/64 [110/20]
   via FE80::CE03:2BFF:FE5A:0, Ethernet0/0
C 2020::/64 [0/0]
   via ::, Ethernet1/0
L 2020::1/128 [0/0]
   via ::, Ethernet1/0
C 2021::/64 [0/0]
   via ::, Ethernet0/0
L 2021::1/128 [0/0]
   via ::, Ethernet0/0
OI 2022::/64 [110/20]
   via FE80::CE01:25FF:FECE:10, Ethernet1/0
OI 2023::/64 [110/20]
   via FE80::CE01:25FF:FECE:10, Ethernet1/0
O FD31:9046:5493:3::/64 [110/11]
   via FE80::CE04:CFF:FE76:10, Ethernet2/0
C FD31:9046:5493:50::/64 [0/0]
   via ::, Ethernet2/0
L FD31:9046:5493:50::20/128 [0/0]
   via ::, Ethernet2/0
L FE80::/10 [0/0]
   via ::, Null0
L FF00::/8 [0/0]
   via ::, Null0
```

Figura 49. Tabla de enrutamiento ISPCORE IPv6



## Router Claro Zona Franca

```
O 2002:16::/64 [110/11]
  via FE80::E88:19FF:FEAB:0, Ethernet1/0
  via FE80::E85:53FF:FE8B:0, Ethernet2/0
OI 2002:16:2::/64 [110/31]
  via FE80::CE02:2AFF:FE62:0, Ethernet0/0
C 2018::/64 [0/0]
  via ::, Ethernet1/0
L 2018::1/128 [0/0]
  via ::, Ethernet1/0
C 2019::/64 [0/0]
  via ::, Ethernet2/0
L 2019::1/128 [0/0]
  via ::, Ethernet2/0
C 2020::/64 [0/0]
  via ::, Ethernet0/0
L 2020::2/128 [0/0]
  via ::, Ethernet0/0
O 2021::/64 [110/10]
  via ::, Ethernet0/0
OI 2022::/64 [110/30]
```

Figura 50. Tabla de enrutamiento claro Zona Franca Ipv6

## Router Claro DNP

```
OI 2002:16::/64 [110/31]
  via FE80::CE02:2AFF:FE62:10, Ethernet1/0
O 2002:16:2::/64 [110/11]
  via FE80::E9F:F6FF:FED6:0, Ethernet0/0
  via FE80::E6A:96FF:FEB2:0, Ethernet2/0
OI 2018::/64 [110/30]
  via FE80::CE02:2AFF:FE62:10, Ethernet1/0
OI 2019::/64 [110/30]
  via FE80::CE02:2AFF:FE62:10, Ethernet1/0
O 2020::/64 [110/10]
  via ::, Ethernet1/0
C 2021::/64 [0/0]
  via ::, Ethernet1/0
L 2021::2/128 [0/0]
  via ::, Ethernet1/0
C 2022::/64 [0/0]
  via ::, Ethernet0/0
L 2022::1/128 [0/0]
  via ::, Ethernet0/0
C 2023::/64 [0/0]
  via ::, Ethernet2/0
L 2023::1/128 [0/0]
  via ::, Ethernet2/0
```

Figura 51. Tabla de enrutamiento claro DNP Ipv6

## Router Zona franca 1

```
C 2002:16::/64 [0/0]
  via GigabitEthernet2, directly connected
L 2002:16::1/128 [0/0]
  via GigabitEthernet2, receive
L 2002:16::5/128 [0/0]
  via GigabitEthernet2, receive
OI 2002:16:2::/64 [110/32]
  via FE80::CE03:2BFF:FE5A:10, GigabitEthernet1
C 2018::/64 [0/0]
  via GigabitEthernet1, directly connected
L 2018::2/128 [0/0]
  via GigabitEthernet1, receive
O 2019::/64 [110/2]
  via FE80::EB5:53FF:FE8B:1, GigabitEthernet2
OI 2020::/64 [110/11]
  via FE80::CE03:2BFF:FE5A:10, GigabitEthernet1
OI 2021::/64 [110/11]
  via FE80::CE03:2BFF:FE5A:10, GigabitEthernet1
OI 2022::/64 [110/31]
  via FE80::CE03:2BFF:FE5A:10, GigabitEthernet1
OI 2023::/64 [110/31]
  via FE80::CE03:2BFF:FE5A:10, GigabitEthernet1
```

Figura 52. Tabla de enrutamiento Zona Franca 1 Ipv6

## Router Zona Franca 2

```
a - Application
C 2002:16::/64 [0/0]
  via GigabitEthernet2, directly connected
L 2002:16::3/128 [0/0]
  via GigabitEthernet2, receive
OI 2002:16:2::/64 [110/32]
  via FE80::CE03:2BFF:FE5A:20, GigabitEthernet1
O 2018::/64 [110/2]
  via FE80::E88:19FF:FEAB:1, GigabitEthernet2
C 2019::/64 [0/0]
  via GigabitEthernet1, directly connected
L 2019::2/128 [0/0]
  via GigabitEthernet1, receive
OI 2020::/64 [110/11]
  via FE80::CE03:2BFF:FE5A:20, GigabitEthernet1
OI 2021::/64 [110/11]
  via FE80::CE03:2BFF:FE5A:20, GigabitEthernet1
OI 2022::/64 [110/31]
  via FE80::CE03:2BFF:FE5A:20, GigabitEthernet1
OI 2023::/64 [110/31]
  via FE80::CE03:2BFF:FE5A:20, GigabitEthernet1
```

Figura 53. Tabla de enrutamiento Zona Franca 2 Ipv6

## Router DNP 1

```
      a - Application
OI 2002:16::/64 [110/32]
   via FE80::CE01:25FF:FECE:0, GigabitEthernet1
C 2002:16:2::/64 [0/0]
   via GigabitEthernet2, directly connected
L 2002:16:2::3/128 [0/0]
   via GigabitEthernet2, receive
L 2002:16:2::5/128 [0/0]
   via GigabitEthernet2, receive
OI 2018::/64 [110/31]
   via FE80::CE01:25FF:FECE:0, GigabitEthernet1
OI 2019::/64 [110/31]
   via FE80::CE01:25FF:FECE:0, GigabitEthernet1
OI 2020::/64 [110/11]
   via FE80::CE01:25FF:FECE:0, GigabitEthernet1
OI 2021::/64 [110/11]
   via FE80::CE01:25FF:FECE:0, GigabitEthernet1
C 2022::/64 [0/0]
   via GigabitEthernet1, directly connected
L 2022::2/128 [0/0]
   via GigabitEthernet1, receive
O 2023::/64 [110/2]
   via FE80::E6A:96FF:FEB2:1, GigabitEthernet2
```

Figura 54. Tabla de enrutamiento DNP 1 Ipv6

## Router DNP 2

```
      a - Application
OI 2002:16::/64 [110/32]
   via FE80::CE01:25FF:FECE:20, GigabitEthernet1
C 2002:16:2::/64 [0/0]
   via GigabitEthernet2, directly connected
L 2002:16:2::4/128 [0/0]
   via GigabitEthernet2, receive
OI 2018::/64 [110/31]
   via FE80::CE01:25FF:FECE:20, GigabitEthernet1
OI 2019::/64 [110/31]
   via FE80::CE01:25FF:FECE:20, GigabitEthernet1
OI 2020::/64 [110/11]
   via FE80::CE01:25FF:FECE:20, GigabitEthernet1
OI 2021::/64 [110/11]
   via FE80::CE01:25FF:FECE:20, GigabitEthernet1
O 2022::/64 [110/2]
   via FE80::E9F:F6FF:FED6:1, GigabitEthernet2
C 2023::/64 [0/0]
   via GigabitEthernet1, directly connected
L 2023::2/128 [0/0]
   via GigabitEthernet1, receive
```

Figura 55. Tabla de enrutamiento DNP 2 Ipv6

## Router Sede World Service

```

O I 2002:16::/64 [110/22]
    via FE80::CE02:2AFF:FE62:20, FastEthernet1/0
O I 2002:16:2::/64 [110/22]
    via FE80::CE02:2AFF:FE62:20, FastEthernet1/0
O I 2018::/64 [110/21]
    via FE80::CE02:2AFF:FE62:20, FastEthernet1/0
O I 2019::/64 [110/21]
    via FE80::CE02:2AFF:FE62:20, FastEthernet1/0
O 2020::/64 [110/11]
    via FE80::CE02:2AFF:FE62:20, FastEthernet1/0
O 2021::/64 [110/11]
    via FE80::CE02:2AFF:FE62:20, FastEthernet1/0
O I 2022::/64 [110/21]
    via FE80::CE02:2AFF:FE62:20, FastEthernet1/0
O I 2023::/64 [110/21]
    via FE80::CE02:2AFF:FE62:20, FastEthernet1/0
C FD31:9046:5493:3::/64 [0/0]
    via ::, FastEthernet0/0
L FD31:9046:5493:3:20/128 [0/0]
    via ::, FastEthernet0/0
C FD31:9046:5493:50::/64 [0/0]
    via ::, FastEthernet1/0
L FD31:9046:5493:50:30/128 [0/0]
    via ::, FastEthernet1/0

```

Figura 56. Tabla de enrutamiento Sede World Service Ipv6

## 6.5 Implementación de VxLAN

Este proyecto tiene como fin el uso de la nueva generación de subredes VxLAN, lo que permite el transporte de la capa de datos inmersa en la capa de red, es decir la encapsulación de las MAC en el protocolo UDP, en este caso se va a realizar a través de los equipos de seguridad Fortinet. A través de la encapsulación de Ipsec esto genera una mayor confiabilidad dado que la información transportada cuenta con el algoritmo criptográfico MD5 escogido por su estructura de 128 bits.

### 6.5.1 Direccionamiento de VxLAN

Se realiza un cambio en el direccionamiento con el fin de usar los mismos segmentos de red en ambos lados con el uso de 2 Gateway diferentes en cada lado de la MPLS de la siguiente manera:

PLAN DE DIRECCIONAMIENTO DUALSTACK VxLAN							
VLAN	Servicio	Nombre de red	Uso	Gateway Ipv4 ZF	Gateway Ipv4 DNP	Gateway Ipv6 ZF	Gateway Ipv6 DNP
20	Datos	Windows server 1	Principal	172.16.20.1/24	172.16.20.2/24	fd31:9046:5493:0201::1/64	fd31:9046:5493:0201::2/64
21	Datos	Windows server 2	Principal	172.16.21.1/24	172.16.21.2/24	fd31:9046:5493:0202::1/64	fd31:9046:5493:0202::2/64
22	Datos	Windows server 3	Principal	172.16.22.1/24	172.16.22.2/24	fd31:9046:5493:0203::1/64	fd31:9046:5493:0203::2/64
23	Datos	Windows server 4	Principal	172.16.23.1/24	172.16.23.2/24	fd31:9046:5493:0204::1/64	fd31:9046:5493:0204::2/64
120	Datos	Windows server 1	Backup	172.16.120.1/24	172.16.120.2/24	fd31:9046:5493:0211::1/64	fd31:9046:5493:0211::2/64
121	Datos	Windows server 2	Backup	172.16.121.1/24	172.16.121.2/24	fd31:9046:5493:0212::1/64	fd31:9046:5493:0212::2/64
122	Datos	Windows server 3	Backup	172.16.122.1/24	172.16.122.2/24	fd31:9046:5493:0213::1/64	fd31:9046:5493:0213::2/64
123	Datos	Windows server 4	Backup	172.16.123.1/24	172.16.123.2/24	fd31:9046:5493:0214::1/64	fd31:9046:5493:0214::2/64

*Tabla 13. Direccionamiento para protocolo VxLAN*

Para las pruebas se utilizará la IP terminada en 50 para el lado Zona Franca, la IP terminada en 60 para el lado DNP y se establecen los DNS en la VLAN 20 y 120 de datos con la dirección IP terminada en 10.

## 6.5.2 Implementación en Zona franca

Se realiza la creación de una VPN sitio a sitio por medio del protocolo VxLAN-on-ipsec, dando como Gateway local la Ipv4 de salida hacia internet del firewall, adicional a esto se genera como dirección remota la Ipv4 del firewall de DNP.

También, se realiza el encapsulamiento a través de las direcciones Ipv6 de origen y destino entre los Firewalls. Asimismo, la implementación de un método de cifrado y una clave como se evidencia en la imagen.

```

FortiGate-VM64-KVM (phase1-interface) # show
config vpn ipsec phase1-interface
  edit "VxLAN-on-IPsec"
    set interface "port1"
    set local-gw 172.16.0.2
    set peertype any
    set net-device disable
    set proposal des-md5
    set dpd on-idle
    set encapsulation vxlan
    set encapsulation-address ipv6
    set encap-local-gw6 2002:16::1
    set encap-remote-gw6 2002:16:2::2
    set remote-gw 172.16.2.2
    set psksecret E1C QDXrDfDgsyijHKsascErsL4nUHTFh+qK2d9oXieiRRRn+jPQ0wDDadhIcKXQqA/Si9I3YwnhJBqw1tYXOXYynb9lWwrZ8u0M6s0
    OVJelRfjORGS09YwK+oXoDwKkmd/ZTBruTiuziPTZ1BT5Hkeyyb35xxcdeoRRP/xQY+M99ru+LGCZUHS2NJun+m64QpF+FVStxMA==
  next
end

```

*Figura 57. Configuración firewall Zona Franca túnel VxLAN*

Se realiza el aprovisionamiento de los puertos que van hacia los Switch por medio del protocolo VxLAN.

```
FortiGate-VM64-KVM (switch-interface) # show
config system switch-interface
  edit "LAN-Soft-Switch"
    set vdom "root"
    set member "port7" "port8" "VXLAN-on-IPsec"
  next
end
```

Figura 58. Aprovisionamiento de los puertos de VxLAN firewall Zona Franca

Se genera el establecimiento del túnel y la adición del puerto hacia la salida del Firewall.

```
config system interface
  edit "VXLAN-on-IPsec"
    set vdom "root"
    set type tunnel
    set snmp-index 21
    set interface "port1"
  next
end
```

Figura 59. Aprovisionamiento del puerto de salida de VxLAN firewall Zona Franca

## Configuración de las interfaces del firewall

Software Switch						
	LAN-Soft-Switch	Software Switch	port7 port8 VXLAN-on-IPsec	172.16.50.1/255.255.255.0	::/0	PING
→	VLAN20	VLAN		172.16.20.1/255.255.255.0	fd31-9046-5493-201-1/64	PING
→	VLAN21	VLAN		172.16.21.1/255.255.255.0	fd31-9046-5493-202-1/64	PING
→	VLAN22	VLAN		172.16.22.1/255.255.255.0	fd31-9046-5493-203-1/64	PING
→	VLAN23	VLAN		172.16.23.1/255.255.255.0	fd31-9046-5493-204-1/64	PING
→	VLAN120	VLAN		172.16.120.1/255.255.255.0	fd31-9046-5493-211-1/64	PING
→	VLAN121	VLAN		172.16.121.1/255.255.255.0	fd31-9046-5493-212-1/64	PING
→	VLAN122	VLAN		172.16.122.1/255.255.255.0	fd31-9046-5493-213-1/64	PING
→	VLAN123	VLAN		172.16.123.1/255.255.255.0	fd31-9046-5493-214-1/64	PING

Figura 60. Configuración de interfaces VxLAN firewall Zona Franca

## 6.5.3 Implementación en DNP

### Establecimiento del túnel

```
config vpn ipsec phase1-interface
  edit "VXLAN-on-IPsec"
    set interface "port1"
    set local-gw 172.16.0.2
    set peertype any
    set net-device disable
    set proposal des-md5
    set dpd on-idle
    set encapsulation vxlan
    set encapsulation-address ipv6
    set encap-local-gw6 2002:16::1
    set encap-remote-gw6 2002:16:2::2
    set remote-gw 172.16.2.2
    set psksecret ENC VsT3hbhckvdK6jLgZAoUTGKHgA672fnXS/s8bkYqi0DxGaE+OA1Zryg7tpE3bhtq4LqxfXKHQ0u77Eq4KA80EhF+8nEpVVDV65
    next
  end
```

Figura 61. Configuración firewall DNP túnel VxLAN

### Aprovisionamiento de puertos VxLAN

```
FortiGate-VM64-KVM (switch-interface) # show
config system switch-interface
  edit "LAN-Soft-Switch"
    set vdom "root"
    set member "port7" "port8" "VXLAN-on-IPsec"
  next
end
```

Figura 62. Aprovisionamiento de los puertos de VxLAN firewall DNP

### Establecimiento del túnel por puerto de salida

```
config system interface
  edit "VXLAN-on-IPsec"
    set vdom "root"
    set type tunnel
    set snmp-index 21
    set interface "port1"
  next
end
```

Figura 63. Aprovisionamiento del puerto de salida de VxLAN firewall DNP

## Configuración de las interfaces del firewall

	LAN-Soft-Switch	Software Switch	VXLAN-on-IPsec	172.16.50.2/255.255.255.0	=/0	PING
	VLAN20	VLAN	part7 part8	172.16.20.2/255.255.255.0	fd31-9046:5493:201::2/64	PING
	VLAN21	VLAN		172.16.21.2/255.255.255.0	fd31-9046:5493:202::2/64	PING
	VLAN22	VLAN		172.16.22.2/255.255.255.0	fd31-9046:5493:203::2/64	PING
	VLAN23	VLAN		172.16.23.2/255.255.255.0	fd31-9046:5493:204::2/64	PING
	VLAN120	VLAN		172.16.120.2/255.255.255.0	fd31-9046:5493:211::2/64	PING
	VLAN121	VLAN		172.16.121.2/255.255.255.0	fd31-9046:5493:212::2/64	PING
	VLAN122	VLAN		172.16.122.2/255.255.255.0	fd31-9046:5493:213::2/64	PING
	VLAN123	VLAN		172.16.123.2/255.255.255.0	fd31-9046:5493:214::2/64	PING

Figura 64. Configuración de interfaces VxLAN firewall DNP

### 6.5.4 Configuración de servidores

Como se mencionó en el numeral 5.4 se realiza la configuración de los servidores en Ipv6, para el lado Zona franca terminado en la IP 50 y en el lado DNP terminado en la IP 60 de la siguiente manera:

```
#
# This is a sample network config uncomment lines to configure the network
#

#Static config for eth0
auto eth0
iface eth0 inet static
    address 172.16.20.50
    netmask 255.255.255.0
    gateway 172.16.20.1

iface eth0 inet6 static
    address fd31:9046:5493:0201::50
    netmask 64
    gateway fd31:9046:5493:0201::1
#
up echo nameserver 192.168.0.1 > /etc/resolv.conf

# DHCP config for eth0
# auto eth0
# iface eth0 inet dhcp
#Static config for eth1
auto eth1
iface eth1 inet static
    address 172.16.120.50
    netmask 255.255.255.0
    gateway 172.16.120.1

iface eth1 inet6 static
    address fd31:9046:5493:0211::50
    netmask 64
    gateway fd31:9046:5493:0211::1
#
up echo nameserver 192.168.1.1 > /etc/resolv.conf

# DHCP config for eth1
# auto eth1
# iface eth1 inet dhcp

#
# This is a sample network config uncomment lines to configure the network
#

#Static config for eth0
auto eth0
iface eth0 inet static
    address 172.16.20.60
    netmask 255.255.255.0
    gateway 172.16.20.2

iface eth0 inet6 static
    address fd31:9046:5493:0201::60
    netmask 64
    gateway fd31:9046:5493:0201::2
#
up echo nameserver 192.168.0.1 > /etc/resolv.conf

# DHCP config for eth0
# auto eth0
# iface eth0 inet dhcp
#Static config for eth1
auto eth1
iface eth1 inet static
    address 172.16.120.60
    netmask 255.255.255.0
    gateway 172.16.120.2

iface eth1 inet6 static
    address fd31:9046:5493:0211::60
    netmask 64
    gateway fd31:9046:5493:0211::2
#
up echo nameserver 192.168.1.1 > /etc/resolv.conf

# DHCP config for eth1
# auto eth1
# iface eth1 inet dhcp
```

Figura 65. Configuración de servidores IPv6



## 6.6 Pruebas de funcionamiento VxLAN

En el desarrollo de las pruebas de VxLAN se evidencia que las redes son capaces de compartir el mismo segmento, a través de dos Gateway por un canal VPN-Ipsec, brindando una red extensa a través de la red MPLS.

### Verificación desde el Firewall Zona Franca

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
VXLAN-on-IPsec	172.16.2.2		1.65 MB	683.65 kB	VXLAN-on-IPsec	VXLAN-on-IPsec

Figura 66. Tráfico del túnel VxLAN desde firewall Zona Franca

### Verificación desde el Firewall DNP

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
VXLAN-on-IPsec	172.16.0.2		1.87 MB	578.30 kB	VXLAN-on-IPsec	VXLAN-on-IPsec

Figura 67. Tráfico del túnel VxLAN desde firewall DNP

### 6.6.1 Pruebas de DualStack por medio de VxLAN

#### Ipv4

```
root@GranjaServer5:~# ping 172.16.20.60
PING 172.16.20.60 (172.16.20.60) 56(84) bytes of data.
64 bytes from 172.16.20.60: icmp_seq=1 ttl=64 time=0.012 ms
^C
--- 172.16.20.60 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.012/0.012/0.012/0.000 ms
root@GranjaServer5:~# ping 172.16.21.60
PING 172.16.21.60 (172.16.21.60) 56(84) bytes of data.
64 bytes from 172.16.21.60: icmp_seq=1 ttl=63 time=41.9 ms
^C
--- 172.16.21.60 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 41.963/41.963/41.963/0.000 ms
root@GranjaServer5:~# ping 172.16.22.60
PING 172.16.22.60 (172.16.22.60) 56(84) bytes of data.
64 bytes from 172.16.22.60: icmp_seq=1 ttl=63 time=41.6 ms
^C
--- 172.16.22.60 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 41.621/41.621/41.621/0.000 ms
root@GranjaServer5:~# ping 172.16.23.60
PING 172.16.23.60 (172.16.23.60) 56(84) bytes of data.
64 bytes from 172.16.23.60: icmp_seq=1 ttl=63 time=48.8 ms
^C
--- 172.16.23.60 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 48.736/48.736/48.736/0.000 ms

root@GranjaServer5:~# ping 172.16.120.60
PING 172.16.120.60 (172.16.120.60) 56(84) bytes of data.
64 bytes from 172.16.120.60: icmp_seq=1 ttl=64 time=0.013 ms
^C
--- 172.16.120.60 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.013/0.013/0.013/0.000 ms
root@GranjaServer5:~# ping 172.16.121.60
PING 172.16.121.60 (172.16.121.60) 56(84) bytes of data.
64 bytes from 172.16.121.60: icmp_seq=1 ttl=63 time=16.6 ms
^C
--- 172.16.121.60 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 16.697/16.697/16.697/0.000 ms
root@GranjaServer5:~# ping 172.16.122.60
PING 172.16.122.60 (172.16.122.60) 56(84) bytes of data.
64 bytes from 172.16.122.60: icmp_seq=1 ttl=63 time=26.7 ms
^C
--- 172.16.122.60 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 26.724/26.724/26.724/0.000 ms
root@GranjaServer5:~# ping 172.16.123.60
PING 172.16.123.60 (172.16.123.60) 56(84) bytes of data.
64 bytes from 172.16.123.60: icmp_seq=1 ttl=63 time=12.7 ms
^C
--- 172.16.123.60 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 12.736/12.736/12.736/0.000 ms
```

Figura 68. Pruebas de Ipv4 a través del túnel VxLAN

## Ipv6

```
root@GranjaServer1:~# ping6 fd31:9046:5493:201::50
PING fd31:9046:5493:201::50(fd31:9046:5493:201::50) 56 data bytes
64 bytes from fd31:9046:5493:201::50: icmp_seq=1 ttl=64 time=0.017 ms
^C
--- fd31:9046:5493:201::50 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.017/0.017/0.017/0.000 ms
root@GranjaServer1:~# ping6 fd31:9046:5493:202::50
PING fd31:9046:5493:202::50(fd31:9046:5493:202::50) 56 data bytes
64 bytes from fd31:9046:5493:202::50: icmp_seq=1 ttl=63 time=12.5 ms
^C
--- fd31:9046:5493:202::50 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 12.503/12.503/12.503/0.000 ms
root@GranjaServer1:~# ping6 fd31:9046:5493:203::50
PING fd31:9046:5493:203::50(fd31:9046:5493:203::50) 56 data bytes
64 bytes from fd31:9046:5493:203::50: icmp_seq=1 ttl=63 time=24.7 ms
^C
--- fd31:9046:5493:203::50 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 24.740/24.740/24.740/0.000 ms
root@GranjaServer1:~# ping6 fd31:9046:5493:204::50
PING fd31:9046:5493:204::50(fd31:9046:5493:204::50) 56 data bytes
64 bytes from fd31:9046:5493:204::50: icmp_seq=1 ttl=63 time=15.5 ms
^C
--- fd31:9046:5493:204::50 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 15.503/15.503/15.503/0.000 ms
root@GranjaServer1:~# ping6 fd31:9046:5493:211::50
PING fd31:9046:5493:211::50(fd31:9046:5493:211::50) 56 data bytes
64 bytes from fd31:9046:5493:211::50: icmp_seq=1 ttl=64 time=0.016 ms
^C
--- fd31:9046:5493:211::50 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.016/0.016/0.016/0.000 ms
root@GranjaServer1:~# ping6 fd31:9046:5493:212::50
PING fd31:9046:5493:212::50(fd31:9046:5493:212::50) 56 data bytes
64 bytes from fd31:9046:5493:212::50: icmp_seq=1 ttl=63 time=11.3 ms
^C
--- fd31:9046:5493:212::50 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 11.333/11.333/11.333/0.000 ms
root@GranjaServer1:~# ping6 fd31:9046:5493:213::50
PING fd31:9046:5493:213::50(fd31:9046:5493:213::50) 56 data bytes
64 bytes from fd31:9046:5493:213::50: icmp_seq=1 ttl=63 time=14.3 ms
^C
--- fd31:9046:5493:213::50 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 14.330/14.330/14.330/0.000 ms
root@GranjaServer1:~# ping6 fd31:9046:5493:214::50
PING fd31:9046:5493:214::50(fd31:9046:5493:214::50) 56 data bytes
64 bytes from fd31:9046:5493:214::50: icmp_seq=1 ttl=63 time=22.0 ms
^C
--- fd31:9046:5493:214::50 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 22.015/22.015/22.015/0.000 ms
```

Figura 69. Pruebas de Ipv6 a través del túnel VxLAN

## 6.7 Configuración de servidores a través de DNS

Para continuar con las pruebas del proyecto, se implementará el uso de un DNS en cada una de las sedes, tanto en Zona franca como en DNP, lo que permitirá al usuario final poder ingresar a cualquiera de los dos servidores sin tener necesidad de especificar una dirección IP.

### 6.7.1.1 Implementación DNS

Se realiza la implementación de un DNS por zona, lo que ayuda a tener un backup en toda la configuración de la topología, por este motivo se implementa el principal en Zona franca como se muestra en la imagen.

```
GNU nano 4.8 /etc/hosts
127.0.1.1 DNS-ZF
127.0.0.1 localhost
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.16.0.2 gestionfirewallzf.lab gestionfirewallzf
172.16.20.50 dnp.lab dnp
172.16.21.50 sisconpes.lab sisconpes
172.16.22.50 tftp.lab tftp
172.16.23.50 sisben.lab sisben
172.16.120.50 dnp.lab dnp
172.16.121.50 sisconpes.lab sisconpes
172.16.122.50 tftp.lab tftp
172.16.123.50 sisben.lab sisben
fd31:9046:5493:0201::50 dnp.lab dnp
fd31:9046:5493:0202::50 sisconpes.lab sisconpes
fd31:9046:5493:0203::50 tftp.lab tftp
fd31:9046:5493:0204::50 sisben.lab sisben
fd31:9046:5493:0211::50 dnp.lab dnp
fd31:9046:5493:0212::50 sisconpes.lab sisconpes
fd31:9046:5493:0213::50 tftp.lab tftp
fd31:9046:5493:0214::50 sisben.lab sisben
```

Figura 70. Configuración de DNS DualStack Zona Franca

## 6.7.2 Implementación DNS DNP

Se genera la implementación de un DNS de backup en la zona DNP, buscando un respaldo de todos los componentes de networking que se pueden ver afectados en caso de una falla.

```
GNU nano 4.8 /etc/hosts
127.0.1.1    DNS-DNP
127.0.0.1    localhost
::1         localhost ip6-localhost ip6-loopback
fe00::0     ip6-localnet
ff00::0     ip6-mcastprefix
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
172.16.2.3  gestionfirewalldnp.lab gestionfirewalldnp
172.16.20.60 dnpbk.lab dnpbk
172.16.21.60 sisconpesbk.lab sisconpesbk
172.16.22.60 tftpbk.lab tftpbk
172.16.23.60 sisbenbk.lab sisbenbk
172.16.120.60 dnpbk.lab dnpbk
172.16.121.60 sisconpesbk.lab sisconpesbk
172.16.122.60 tftpbk.lab tftpbk
172.16.123.60 sisbenbk.lab sisbenbk
fd31:9046:5493:0201::60 dnpbk.lab dnpbk
fd31:9046:5493:0202::60 sisconpesbk.lab sisconpesbk
fd31:9046:5493:0203::60 tftpbk.lab tftpbk
fd31:9046:5493:0204::60 sisbenbk.lab sisbenbk
fd31:9046:5493:0211::60 dnpbk.lab dnpbk
fd31:9046:5493:0212::60 sisconpesbk.lab sisconpesbk
fd31:9046:5493:0213::60 tftpbk.lab tftpbk
fd31:9046:5493:0214::60 sisbenbk.lab sisbenbk
```

Figura 71. Configuración de DNS DualStack DNP

## 6.8 Resultado de pruebas realizadas

En la infraestructura topológica propuesta en una nueva generación de redes de datos implementado a través de DualStack VxLAN, fue necesario generar la implementación de una nueva sede remota que no tenga relación directa hacia la red, buscando generar las pruebas necesarias del funcionamiento óptimo de la red.

### 6.8.1 Pruebas desde sede alterna

Para la realización de pruebas en DualStack es necesario realizar la validación desde un host externo a la infraestructura DualStack VxLAN, por este motivo se implementa un equipo que cuenta con salida a internet.



## 6.8.1.2 Configuración de PC

Se realiza la implementación de una dirección IP estática DualStack para la comunicación hacia la red.

```
#
# This is a sample network config uncomment lines to configure the network
#

#Static config for eth0
auto eth0
iface eth0 inet static
    address 192.168.100.30
    netmask 255.255.255.0
    gateway 172.16.100.1

iface eth0 inet6 static
    address fd31:9046:5493:3::30
    netmask 64
    gateway fd31:9046:5493:3::20
#
# up echo nameserver 192.168.0.1 > /etc/resolv.conf

# DHCP config for eth0
# auto eth0
# iface eth0 inet dhcp
```

Figura 73. Configuración de Pc World Service

Se realiza la configuración en la máquina de sede alterna para que empiece a resolver por el DNS principal, así como por el DNS que provee el ISP hacia internet de la siguiente manera:

```
GNU nano 2.2.6 File: /etc/resolv.conf
nameserver 172.16.20.10
nameserver 8.8.8.8
nameserver fd31:9046:5493:0201::10
```

Figura 74. Configuración de DNS en PC World Service

### 6.8.1.2 Salida a internet del PC

Se realizan pruebas de comunicación hacia Google donde se evidencia respuesta tanto en Ipv4 como en Ipv6 como se evidencia en la siguiente imagen:

```
root@webterm-1:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=126 time=15.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=126 time=16.8 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 15.395/16.101/16.807/0.706 ms
root@webterm-1:~# ping google.com
PING google.com (172.217.172.14) 56(84) bytes of data.
64 bytes from bog02s09-in-f14.1e100.net (172.217.172.14): icmp_seq=1 ttl=126 time=20.7 ms
64 bytes from bog02s09-in-f14.1e100.net (172.217.172.14): icmp_seq=2 ttl=126 time=13.0 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 13.075/16.900/20.726/3.827 ms
root@webterm-1:~# ping6 google.com
PING google.com(2800:3f0:4005:408::200e) 56 data bytes
```

Figura 75. Pruebas de Ping en DualStack

### 6.8.1.3 Prueba de resolución de DNS externo

Como se logra evidenciar el equipo es capaz de tener la resolución de direcciones públicas en DualStack.

DNS								
<input type="button" value="Refresh"/> <input type="checkbox"/> Autorefresh every 3 seconds								
Hostname	Family	TRR	Addresses	Expires (Seconds)				
yahoo.com	ipv4	false	98.137.11.164	88				
			74.6.143.25					
			74.6.143.26					
			74.6.231.20					
			74.6.231.21					
			98.137.11.163					
			2001:4998:44:3507::8000					
			2001:4998:124:1507::f000					
youtube.com	ipv4	false	172.217.28.110	117				
			2800:3f0:4005:406::200e					
			google.com		ipv4	false	172.217.28.110	83
							2800:3f0:4005:408::200e	

Figura 76. Resolución DNS en maquina World Service

## Prueba hacia Google.com



Figura 77. Prueba de ingreso a Google.com

## Prueba hacia Yahoo.com

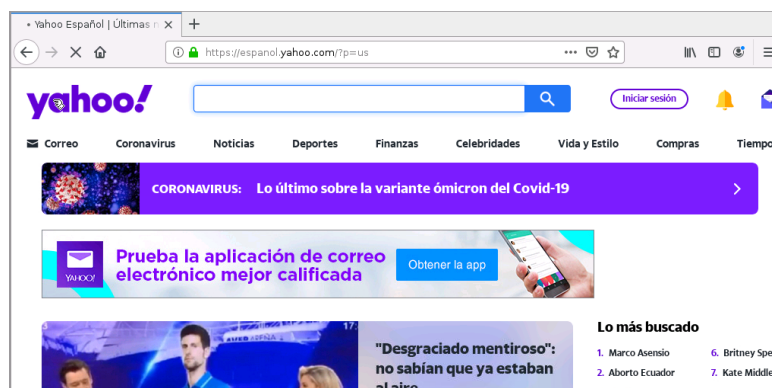


Figura 78. Prueba de ingreso a Yahoo.com

## Prueba hacia Youtube.com

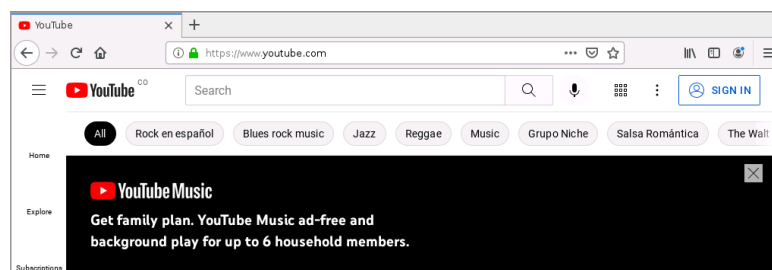
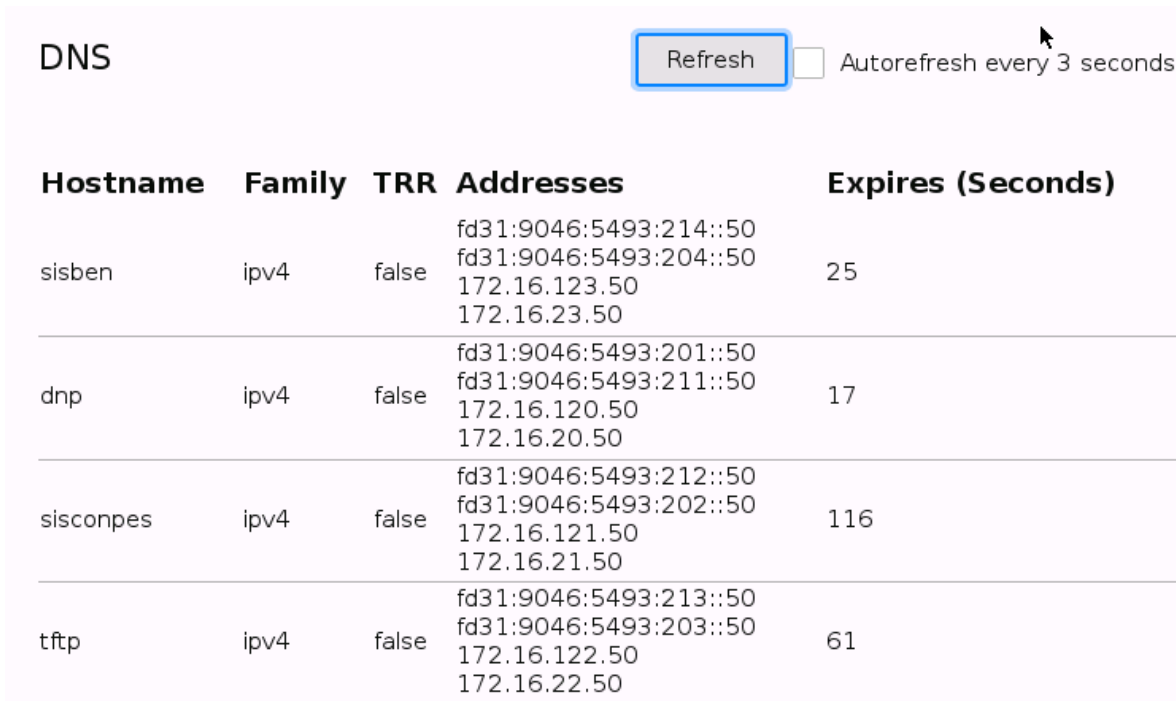


Figura 79. Prueba de ingreso a Youtube.com

### 6.8.1.4 Prueba de resolución de DNS interno

Se evidencia que el equipo al intentar ingresar a cualquiera de las direcciones ubicadas en el DNS interno puede resolverlo como se evidencia en la imagen:



The screenshot shows a DNS configuration window with a 'Refresh' button and an 'Autorefresh every 3 seconds' checkbox. Below is a table of DNS records:

Hostname	Family	TRR	Addresses	Expires (Seconds)
sisben	ipv4	false	fd31:9046:5493:214::50 fd31:9046:5493:204::50 172.16.123.50 172.16.23.50	25
dnp	ipv4	false	fd31:9046:5493:201::50 fd31:9046:5493:211::50 172.16.120.50 172.16.20.50	17
sisconpes	ipv4	false	fd31:9046:5493:212::50 fd31:9046:5493:202::50 172.16.121.50 172.16.21.50	116
tftp	ipv4	false	fd31:9046:5493:213::50 fd31:9046:5493:203::50 172.16.122.50 172.16.22.50	61

Figura 80. Prueba de resolución de DNS interno

### Prueba hacia dnp.lab



Figura 81. Prueba hacia pagina DNP



## Prueba hacia sisben.lab

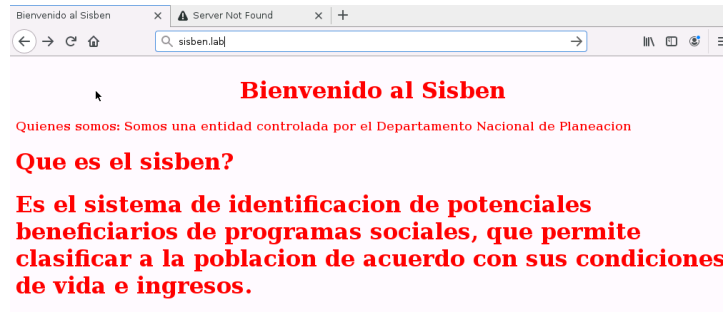


Figura 82.Prueba hacia pagina Sisben

## Prueba hacia sisconpes.lab

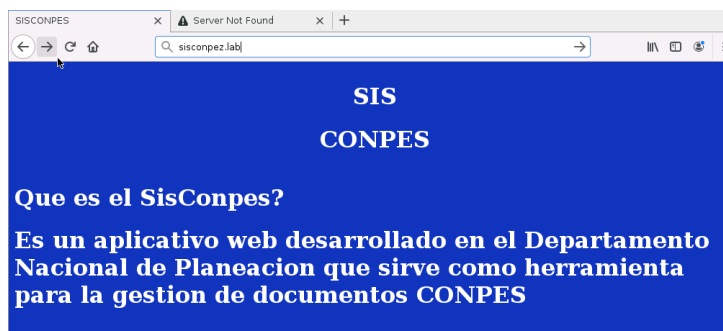


Figura 83.Prueba hacia pagina Sisconpes

## Prueba hacia tftp.lab



Figura 84.Prueba hacia server TFTP

## 7. Conclusiones

- El protocolo Ipv4 tiende a desaparecer por la cantidad de direcciones disponibles con las que cuenta, es necesario comenzar con la migración hacia el protocolo IPv6 dado que cuenta con un número lo suficientemente grande para tener la capacidad de expansión que buscan las empresas sin comprar nuevos equipos.
- Buscando seguir los lineamientos instruidos por el MinTIC, a las empresas públicas colombianas, es necesario crear un punto de partida que permita hacer la transición del protocolo IPv4 hacia IPv6, a través de una serie de pasos que permiten validar, qué tan preparada está la empresa para el cumplimiento de este nuevo protocolo.
- En la simulación realizada a través de GNS3, dónde se realizó la emulación de la topología inicial de la empresa, se encontraron hallazgos cómo:
  1. Necesidad de reutilizar las direcciones Ipv4 teniendo en cuenta el agotamiento que se presenta a nivel mundial.
  2. La gran cantidad de subredes que son necesarias para tener un control jerárquico de la infraestructura de la red de datos.
- Para lograr tener un protocolo altamente redundante es de gran ayuda la inclusión de nuevos protocolos como VxLAN, dado que posibilita una gestión más amigable con los administradores. Logrando tener una sola subred en la infraestructura eliminando la necesidad de dividir las.
- Gracias a los protocolos de nueva generación en este caso VxLAN, con la inclusión del IPv6 es posible tener una mayor cantidad de servicios disponibles, sin tener la necesidad de contemplar un agotamiento próximo de los recursos.

- El proceso de transición de IPv4 hacia IPv6 se puede lograr sin afectar los servicios que ya se tienen implementados teniendo en cuenta que, a pesar de compartir la infraestructura física, al momento de configurar cada uno de los equipos se puede confirmar que actúan de manera independiente y no interrumpen los servicios entre sí.

## 8. Recomendaciones

Es necesaria la creación de un lineamiento de administración DualStack teniendo en cuenta que cada protocolo es independiente lo que genera una doble administración, hasta el momento en el cual no existan más direcciones IPv4 en la red.

En este momento el Departamento Nacional de Planeación tiene a su disposición el recurso de tener un direccionamiento propio lo que permite configurar direcciones públicas de IPv6 dando un mayor alcance sin la necesidad del uso de otro tipo de métodos de transición.

A pesar de que IPv6 ya cuenta con el protocolo IPsec por defecto, es necesario aumentar los controles de seguridad dado que al tener una dirección IP pública en cada equipo se abren las posibilidades de ataques informáticos.

## 9. Bibliografía

Historia de internet.” <https://www.fib.upc.edu/retro-informatica/historia/internet.html> (accessed May 30, 2020).

“Internet History Timeline: ARPANET to the World Wide Web | Live Science.” <https://www.livescience.com/20727-internet-history.html> (accessed May 30, 2020).

“Cómo nació Internet: del ARPANET a Internet.” <https://theconversation.com/how-the-internet-was-born-from-the-arpamet-to-the-internet-68072> (accessed May 30, 2020).

“Qué es y cómo funciona el protocolo ip | VIU.” <https://www.universidadviu.com/funciona-protocolo-ip/> (accessed May 27, 2020).

“IETF Standards Written by ISC Contributors - Internet Systems Consortium.” <https://www.isc.org/rfcs/> (accessed May 30, 2020).

O. Delong, “Why does IP have Versions? Why do I care?,” 2017.

Saklani, And S. C. Dimri, "Technical Comparison Between Ipv4 & Ipv6 And Migration From Ipv4 To Ipv6", International Journal Of Science And Research (IJSR), 7 July 2013.

H. Shah, “Comparing TCP-IPV4/TCP-IPV6 Network Performance”, Diss. University Of Missouri--Columbia, Pp.123-126, 2013.

O. Delong, “Why does IP have Versions? Why do I care?,” 2017.

Z. Wang and M. Yan, “The research and application of internet protocol version 6 (IPv6),” in Proceedings - 4th International Conference on Intelligent

Computation Technology and Automation, ICICTA 2011, 2011, vol. 1, pp. 275–278, doi: 10.1109/ICICTA.2011.79.

D. Ferney, R. Pulido, J. G. Pantoja, J. Alirio, and B. Diaz, “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.”

Planning Report 05-2, IPv6 Economic Impact Assessment. Prepared by: RTI International for National Institute of Standards & Technology October 2005

A. Shiranzaei and R. Z. Khan, "Internet protocol versions — A review," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2015, pp. 397-401.

B. Hinden, “IPv6 Background,” 2018.

“Fases de Agotamiento de IPv4.” <https://www.lacnic.net/1001/1/lacnic/fases-de-agotamiento-de-ipv4> (accessed May 31, 2020).

K. Chakraborty, N. Dutta, and S. R. Biradar, “Simulation of IPv4-to-IPv6 Dual Stack Transition Mechanism (DSTM) between IPv4 hosts in integrated IPv6/IPv4 network,” in Codec - 2009 - 4th International Conference on Computers and Devices for Communication, 2009.

“Guía transición IPV6” [https://www.mintic.gov.co/portal/604/articles-5903\\_archivo\\_pdf\\_IPv6\\_para\\_Todos.pdf](https://www.mintic.gov.co/portal/604/articles-5903_archivo_pdf_IPv6_para_Todos.pdf) (accessed May 27, 2020).

K. L. Bansal and C. Singh, “Dual Stack Implementation of Mobile IPv6 Software Architecture,” *Int. J. Comput. Appl.*, 2011, doi: 10.5120/3062-4182.

“Evaluating Performance of IPv6 Migration Techniques.”

J. L. Shah and J. Parvez, "An examination of next generation IP migration techniques: Constraints and evaluation," in 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Jul. 2014, pp. 776–781, doi: 10.1109/ICCICCT.2014.6993064.

Y. Wu and X. Zhou, "Research on the IPv6 performance analysis based on dual-protocol stack and tunnel transition," in 2011 6th International Conference on Computer Science & Education (ICCSE), Aug. 2011, pp. 1091–1093, doi: 10.1109/ICCSE.2011.6028824.

J. Govil and J. Govil, "On the investigation of transactional and interoperability issues between IPv4 and IPv6," in 2007 IEEE International Conference on Electro/Information Technology, May 2007, pp. 604–609, doi: 10.1109/EIT.2007.4374518.

K. EL KHADIRI, O. LABOUIDYA, N. ELKAMOUN, and R. HILAL, "Performance Evaluation of IPv4/IPv6 Transition Mechanisms for Real-Time Applications using OPNET Modeler," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 4, 2018, doi: 10.14569/IJACSA.2018.090454.

G. Eduardo, M. Ramírez, S. Andrés, and Q. Burgos, "IPV6: ESTUDIO SOBRE LAS BARRERAS PARA SU IMPLEMENTACIÓN AUTORES."

E. Alexander et al., "METODOLOGÍA PARA HACER UNA TRANSICIÓN EN UNA RED IPV4 A IPV6," 2017.

B. Adebisi et al., "IP-centric high rate narrowband PLC for smart grid applications," *IEEE Commun. Mag.*, vol. 49, no. 12, pp. 46–54, Dec. 2011, doi: 10.1109/MCOM.2011.6094005.

X. Zhou, H. Uijterwaal, R. E. Kooij, and P. Van Mieghem, "Estimation of perceived quality of service for applications on IPv6 networks," in *Proceedings of the ACM*

international workshop on Performance monitoring, measurement, and evaluation of heterogeneous wireless and wired networks - PM2HW2N '06, 2006, p. 74, doi: 10.1145/1163653.1163667.

E.-B. Fgee, W. J. Phillips, W. Robertson, and S. C. Sivakumar, "Implementing QoS capabilities in IPv6 networks and comparison with MPLS and RSVP," in CCECE 2003 - Canadian Conference on Electrical and Computer Engineering. Toward a Caring and Humane Technology (Cat. No.03CH37436), 2003, vol. 2, pp. 851–854, doi: 10.1109/CCECE.2003.1226028.

W.-E. Chen and P.-J. Lin, "A performance study for IPv4-IPv6 translation in IP multimedia core network subsystem," Int. J. Commun. Syst., p. n/a-n/a, 2009, doi: 10.1002/dac.1071.

M. Marchese, QoS Over Heterogeneous Networks. Chichester, UK: John Wiley & Sons, Ltd, 2007

E. por and M. Badillo, "PORTAFOLIO SERVICIOS DE TIC OFICINA DE TECNOLOGIAS Y SISTEMAS DE INFORMACIÓN Departamento Nacional de Planeación," 2018. Accessed: May 31, 2020. [Online]. Available: [www.dnp.gov.co](http://www.dnp.gov.co).

"Comprender las VXLAN - TechLibrary - Juniper Networks." [https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/sdn-vxlan.html](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/sdn-vxlan.html) (accessed Jun. 18, 2020).

D. Joseph, Understanding IPv6: Your Essential Guide to IPv6 on Windows Networks. " O'Reilly Media, Inc.", ch.1,pp.3-4, 2012.

D. G. Chandra, M. Kathing and D. P. Kumar, "A Comparative Study on IPv4 and IPv6," 2013 International Conference on Communication Systems and Network Technologies, Gwalior, 2013, pp. 286-289, doi: 10.1109/CSNT.2013.67.

