UNIVERSIDAD
NACIONAL
DE LOJA

Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

"Despliegue del Protocolo de Internet versión 6 (IPv6) para los dispositivos Core y Switchs de distribución en la red de datos de la Universidad Nacional de Loja"

Tesis previa a la Obtención del título de Ingeniero en Sistemas

Autor:

- Walter Agusto – Camacho Saritama

Director:

- Ing. Luis Roberto - Jácome Galarza, Mg. Sc.

LOJA-ECUADOR

2017

Certificación del Director

Ing. Luis Roberto Jácome Galarza, Mg. Sc.

DOCENTE DE LA CARRERA DE INGENIERÍA EN SISTEMAS DE LA UNIVERSIDAD NACIONAL DE LOJA, DIRECTOR DE TESIS

CERTIFICA:

Que el egresado **Walter Agusto Camacho Saritama**, realizó el trabajo de investigación titulado **"Despliegue del Protocolo de Internet versión 6 (IPv6) para los dispositivos Core y Switchs de distribución en la red de datos de la Universidad Nacional de Loja"** bajo mi dirección y asesoramiento, mismo que fue revisado, enmendado y corregido minuciosamente. En virtud que la Tesis reúne, a satisfacción, las cualidades de fondo y forma exigidas para un trabajo de este nivel, autorizo su presentación, sustentación y defensa ante el tribunal respectivo.

Loja, 02 de Junio del 2017

Ing. Luis Roberto Jácome Galarza, Mg. Sc.

DIRECTOR DE TESIS

Autoría

WALTER AGUSTO CAMACHO SARITAMA declaro ser autor del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de la tesis en el Repositorio Institucional – Biblioteca Virtual.

Firma: 

Cédula: 0705383487

Fecha: 07 de julio del 2017

CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO

Yo **WALTER AGUSTO CAMACHO SARITAMA**, declaro ser autor de la tesis titulada: **"DESPLIEGUE DEL PROTOCOLO DE INTERNET VERSIÓN 6 (IPV6) PARA LOS DISPOSITIVOS CORE Y SWITCHS DE DISTRIBUCIÓN EN LA RED DE DATOS DE LA UNIVERSIDAD NACIONAL DE LOJA"**, como requisito para optar al grado de: **INGENIERO EN SISTEMAS**; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional:

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de las tesis que realice el tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los siete días del mes de julio del dos mil diecisiete.

Firma: 

Autor: Walter Agusto Camacho Saritama

Cédula: 0705383487

Dirección: Loja (Teodoro Wolf y Pascal)

Correo Electrónico: wacamachos@unl.edu.ec

Teléfono: **Celular:** 0992201139

DATOS COMPLEMENTARIOS

Director de Tesis: Ing. Luis Roberto Jácome Galarza, Mg. Sc.

Tribunal de Grado: Ing. Mario Enrique Cueva Hurtado, Mg. Sc.

Ing. Gastón René Chamba Romero, Mg. Sc.

Ing. Roberto Carlos Pineda López, Mg. Sc.

Agradecimiento

Quiero empezar expresando mis sinceros agradecimientos a la Universidad Nacional de Loja, Área de la Energía, las Industrias y los Recursos Naturales no Renovables, Carrera de Ingeniería en Sistemas, quienes me abrieron sus puertas; a los docentes por su apoyo y portadores de mi formación académica quienes mediante su conocimiento lo supieron impartir de mejor manera durante estos cinco años de vida universitaria.

De manera especial agradezco al Ing. Luis Roberto Jácome Galarza, director del presente trabajo de titulación, la ayuda con su conocimiento profesional fue el pilar fundamental para cumplir con la meta propuesta, reciba mi agradecimiento por el tiempo dedicado.

Finalmente expreso mi agradecimiento a todo el personal del departamento de Unidad de Telecomunicaciones e Información (UTI), por recibirme, guiarme y permitirme todas las facilidades para la realización de este trabajo de titulación.

Dedicatoria

Dedicado el presente trabajo primeramente a Dios, portador de mis fortalezas, debilidades, alegrías, tristezas pero sobre todo sabiéndome guiar y dar su mano en momentos de duro camino, recibiendo su apoyo siempre para seguir adelante sin importar los obstáculos.

A mis padres: Walter y Herminia por su apoyo incondicional instruyéndome siempre en cada etapa de mi vida. A mis hermanos: Silvia, Mayra, Lorena, Carlos y Alicia por su infinito apoyo incentivándome siempre, aconsejándome en los duros desafíos, a su amor recibido y brindado por toda mi familia para culminar con la meta trazada.

A todas las personas, amigos, compañeros que en el transcurso de mi formación profesional tuve la oportunidad de conocer y compartir momentos agradables en mi vida, gracias a ustedes por hacer este trayecto sencillo y poderlos tener siempre presente.

ÍNDICE DE CONTENIDOS

Certificación del Director ..... **II**

Autoría ..... **III**

CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR ..... **IV**

Agradecimiento ..... **V**

Dedicatoria ..... **VI**

Índice de contenidos ..... **VII**

Índice de Figuras ..... **XIII**

Índice de Tablas ..... **XXI**

1. Título **1**

2. Resumen **2**

2.1. Summary 3

3. Introducción **4**

4. Revisión Literaria **6**

4.1. Protocolo de Internet versión 6 (IPv6) 6

4.1.1. Introducción 6

4.1.2. Características de IPv6 6

4.1.3. Formato de la cabecera IPv6 7

4.1.4. IPv4 frente a IPv6 9

4.1.5. Direccionamiento IPv6 10

4.1.5.1. Espacio de direcciones en IPv6 10

4.1.5.2. Sintaxis de las direcciones en IPv6 10

4.1.6. Prefijos IPv6 13

4.1.6.1. Prefijos no ruteables en IPv6 13

4.1.7. Tipos de direcciones IPv6 14

4.1.7.1. Direccionamiento Unicast IPv6 14

4.1.7.2. Direccionamiento Anycast IPv6 16

4.1.7.3. Direccionamiento Multicast IPv6 16
4.1.8. Direcciones Compatibles [10] 17
4.1.9. Identificadores de Interfaz de IPv6 17
4.1.10. Equivalencias de Direcciones de IPv4 e IPv6 18
4.1.11. Principales Protocolos en IPv6 19
4.1.11.1. Protocolo ICMPv6 19
4.1.11.2. Neighbor Discovery – El “ARP” de IPv6 21
4.1.11.3. Protocolo DHCPv6 24
4.1.11.4. Protocolo RIPng 27
4.1.11.5. Protocolo OSPFv6 29
4.2. Mecanismos de Coexistencia y Transición de IPv4 a IPv6 32
4.2.1. Mecanismo Doble Pila 32
4.2.2. Mecanismo de Tunelización [10] [40] 33
4.2.3. Tipos de Túneles 34
4.2.3.1. Túneles Configurados 34
4.2.3.2. Túnel Automático 6to4 35
4.2.3.3. Túnel reenvío 6over4 36
4.2.3.4. Servidor TEREDO 37
4.2.3.5. ISATAP [9] 37
4.2.4. Mecanismo de Traducción o SIIT (Stateless IP/ICMP Translation Algorithm) [27]. 38
4.2.4.1. Traducción de IPv4 a IPv6 [44] 39
4.2.4.2. Traducción de IPv6 a IPv4 39
5. Materiales y Métodos 41
5.1. Métodos de Investigación 41
5.2. Técnicas de Investigación 41
5.3. Metodología 42
6. Resultados 43
6.1. OBJETIVO 1: Analizar la situación actual de los dispositivos Core y Switchs de distribución en la red de datos de la Universidad Nacional de Loja. 43

6.1.1. Infraestructura de la red de datos de la Universidad Nacional de Loja... 44

6.1.2. Dispositivos de red: Cuarto de Telecomunicaciones..... 45

6.1.3. Tecnología de la Universidad Nacional de Loja 45

6.1.3.1. Servidores Web Públicos..... 46

6.1.3.2. Servidores Web Privados 47

6.1.4. Servicios que presta la Universidad Nacional de Loja..... 48

6.1.5. Topología intranet de la Universidad Nacional de Loja 49

6.1.6. Descripción de los dispositivos de red: Core y Switch de Distribución ... 50

6.1.7. Distribución de dispositivos de red: Facultades de la Universidad Nacional de Loja 53

6.1.8. Soporte de IPv6 en los dispositivos de red 54

6.2. OBJETIVO 2: Determinar el mecanismo de transición a utilizar entre IPv4 a IPv6 55

6.2.1. Mecanismos de Transición a IPv6 55

6.2.1.1. Mecanismo de Transición Dual Stack (Doble Pila) 56

6.2.1.2. Mecanismo de Transición Túneles 57

6.2.1.3. Mecanismo de Transición Traducción de Direcciones 57

6.2.2. Resumen de los Mecanismos de Transición..... 59

6.2.3. Comparación de los Mecanismos de Transición..... 60

6.2.3.1. Parámetros a evaluar de los mecanismos de Transición 61

6.2.4. Análisis comparativo de los Mecanismos de Transición mediante sus parámetros 63

6.2.5. Caso de estudio aplicando el Mecanismo Doble Pila para IPv6..... 69

6.3. OBJETIVO 3: Diseñar el esquema de Direccionamiento utilizando IPv6 para la red privada de la Universidad Nacional de Loja 71

6.3.1. Direccionamiento IPv4 de la Universidad Nacional de Loja 71

6.3.2. Asignación de la dirección IPv6 a la Universidad Nacional de Loja..... 76

6.3.2.1. Requisitos en la Asignación de una dirección IPv6..... 76

6.3.3. Plan de direccionamiento de IPv6 en la Universidad Nacional de Loja .. 78

6.3.4. Direccionamiento IPv6 en el dispositivo Core y Switchs de Distribución para la Universidad Nacional de Loja 78

6.3.5. Topología de Red del Backbone de la Universidad Nacional de Loja en IPv6 85

6.4. OBJETIVO 4: Establecer un escenario de pruebas de acuerdo al Mecanismo de Transición seleccionado 87

6.4.1. ESCENARIO DE PRUEBAS 1: Equipos Mikrotik y Equipo CISCO 87

6.4.1.1. Requerimientos para el Escenario de Pruebas 1 87

6.4.1.2. Instalación de la Herramienta Winbox 87

6.4.1.3. SWITCH CORE: Configuración Protocolo de Internet versión 4 (IPv4) 89

6.4.1.4. SWITCH DISTRIBUCIÓN L3: Configuración Protocolo de Internet versión 4 (IPv4) 96

6.4.1.5. SWITCH ACCESO L2: Configuración Protocolo de Internet versión 4 (IPv4) 101

6.4.1.6. SWITCH CORE: Configuración Protocolo de Internet versión 6 (IPv6) 105

6.4.1.7. SWITCH DISTRIBUCIÓN: Configuración Protocolo de Internet versión 6 (IPv6) 107

6.4.1.8. SWITCH ACCESO: Configuración Protocolo de Internet versión 6 (IPv6) 112

6.4.1.9. WIRESHARK: Captura de paquetes IPv4 e IPv6 113

6.4.2. ESCENARIO DE PRUEBAS 2: Simulador de Redes GNS3 121

6.4.2.1. Configuración Switch CORE 123

6.4.2.2. Configuración de Switch L3 Facultad Administración - Departamento UTI 124

6.4.2.3. Configuración Switch L2 Facultad Administración - Departamento UTI 125

6.4.2.4. PC1: Usuario Final - Administración 126

6.4.2.5. Pruebas de conectividad 126

6.4.2.6. Configuración de Switch L3 Facultad Energía - Departamento Biblioteca 127

6.4.2.7. Configuración Switch L2 Facultad Energía - Departamento Biblioteca 128

6.4.2.8. PC1: Usuario Final – Energía 128

6.4.2.9. Pruebas de conectividad 129

6.5. OBJETIVO 5: Realizar las configuraciones necesarias para la implementación del Protocolo de Internet versión 6 (IPv6) en la Universidad Nacional de Loja..... 129

6.5.1. Plan de Implementación: Protocolo de Internet versión 6 (IPv6)..... 130

6.5.2. Configuración Switch Core (Facultad Administración-UTI / Facultad Energía-Biblioteca) 132

6.5.3. Configuración Switch Distribución o L3 (Facultad Administración – Departamento UTI) 134

6.5.4. Configuración Switch Acceso o L2 (Facultad Administración – Departamento UTI) 137

6.5.5. USUARIO FINAL (Facultad Administración - Departamento UTI): Asignación de dirección IPv6 138

6.5.6. Pruebas de Conectividad..... 139

6.5.6.1. Switch CORE..... 139

6.5.6.2. Switch Distribución o L3 (Facultad Administración) 141

6.5.6.3. Switch Acceso o L2 (Facultad Administración) 141

6.5.6.4. Usuario Final o PC en IPv6 (Administración) 143

6.5.7. Configuración Switch Distribución o L3 (Facultad Energía – Departamento Biblioteca)..... 144

6.5.8. Configuración Switch Acceso o L2 (Facultad Energía – Departamento Biblioteca)..... 146

6.5.9. USUARIO FINAL (Facultad Energía - Departamento Biblioteca): Asignación de dirección IPv6 147

6.5.10. Pruebas de Conectividad 147

6.5.10.1. Switch CORE..... 147

6.5.10.2. Switch Distribución o L3 (Energía)..... 149

6.5.10.3. Switch Acceso o L2 (Energía)..... 149

6.5.10.4. Usuario Final o PC en IPv6 (Energía)..... 151

6.5.11. Pruebas de Conectividad entre Facultades..... 152

6.5.12. Configuración Equipos Mikrotik 154

6.5.12.1. Configuración enlace Switch CORE hacia: Jardín Botánico y Obelisco 154

6.5.12.2. Configuración Mikrotik – Jardín Botánico 155
6.5.12.3. Configuración Mikrotik – Obelisco 159
7. Discusión 161
7.1. Evaluación del objeto de investigación 161
7.2. Valoración Técnico – Económica – Ambiental 164
8. Conclusiones 166
9. Recomendaciones 168
10. BIBLIOGRAFÍA 170
11. ANEXOS 175
Anexo I: Manual Técnico de configuración Equipos Switch Core y Switch de Distribución de la Universidad Nacional de Loja 175
Anexo II: Certificado de Implementación otorgado por la Unidad de Telecomunicaciones e Información (UTI) 188
Anexo III: Entrevista realizada al Subdirector de Redes y Equipos Informáticos 190
Anexo IV: Especificaciones y soporte de IPv6 en Equipos CISCO 194
Anexo V: Acta de Reunión No. 034-UTI-2016 exposición Avance del Proyecto de Titulación 199

ÍNDICE DE FIGURAS

Figura 1: Formato cabeceras IPv6 frente a IPv4 [7]. 8

Figura 2: Tipos de direcciones [20]. 14

Figura 3: Tipo de dirección Global IPv6 [21]. 15

Figura 4: Tipo de dirección de Enlace Local IPv6 [21]..... 15

Figura 5: Tipo de dirección de Sitio Local IPv6 [10]. 15

Figura 6: Tipo de dirección Anycast IPv6 [3]. 16

Figura 7: Tipo de dirección Multicast IPv6 [23]..... 16

Figura 8: Direcciones Multicast IPv6 reservadas [23]..... 17

Figura 9: Generación de una dirección IPv6: Método EUI-64 [7]..... 18

Figura 10: Formato mensaje ICMPv6 [28]..... 20

Figura 11: Mensaje de Error e Información de ICMPv6 [25]..... 21

Figura 12: Esquema DHCPv6 [27]. 25

Figura 13: Mensaje RIPng [27]. 28

Figura 14: Datagrama OSPFv3 [27]..... 31

Figura 15: Esquema general del funcionamiento Doble Pila [39]. 33

Figura 16: Arquitectura de encapsulación de IPv6 sobre IPv4 [10]. 34

Figura 17: Túnel Automático 6to4 [41]. 36

Figura 18: Arquitectura 6over4 [9]..... 37

Figura 19: SIIT para redes pequeñas IPv6 [27]..... 38

Figura 20: Traducción de IPv4 a IPv6 [44]. 39

Figura 21: Traducción de IPv6 a IPv4 [44]. 40

Figura 22: Backbone Red de Datos - Universidad Nacional de Loja. 44

Figura 23. Principales Equipos de Red. 49

Figura 24: Cisco CATALYST 6506-E [45]. 50

Figura 25: Cisco CATALYST 3750X-24T-S [46]..... 51

Figura 26: Cisco CATALYST 3750X-48PF-S [47]. 51

Figura 27: Mikrotik CCR1036-12G-4S [48]..... 51

Figura 28: Mikrotik CRS125-24G-1S [48]..... 52

Figura 29: Cisco CATALYST 2960-48TT-S [49]..... 52

Figura 30. Mecanismo basado en Doble-Pila [Autor]. 56

Figura 31. Dos redes IPv6 se comunican utilizando una red IPv4 [Autor]. 57

Figura 32: Traducción de IPv4 a IPv6 [Autor]..... 58

Figura 33: Traducción de IPv6 a IPv4 [Autor]..... 58

Figura 34: Valoración de parámetros de los Mecanismos de Transición..... 67

Figura 35: Porcentajes de los Mecanismos de Transición. 68

Figura 36: Backbone Universidad Nacional de Loja en IPv6. 86

Figura 37: Descargar Winbox para Mikrotik. 87

Figura 38: Ejecutable Winbox. 88

Figura 39: Interfaz Gráfica de Winbox..... 88

Figura 40: Equipo CCR1016 – 12G. 89

Figura 41: Ingreso para activar IPv6. 89

Figura 42: Activar paquete IPv6..... 90

Figura 43: Reiniciar equipo Mikrotik..... 90

Figura 44: Verificar paquete IPv6 instalado..... 91

Figura 45: Interfaces equipo CCR1016 – 12G – Switch Core. 91

Figura 46: Crear VLAN – Switch Core. 92

Figura 47: Agregar Dirección IPv4 – Switch Core. 92

Figura 48: Crear Pool de direcciones IPv4 – Switch Core..... 93

Figura 49: Crear DHCP Server en IPv4 – Switch Core. 93

Figura 50: Networks agregadas en IPv4 – Switch Core. 93

Figura 51: OSPF Interfaces en IPv4 – Switch Core..... 94

Figura 52: OSPF Instances en IPv4 – Switch Core..... 94

Figura 53: OSPF - Networks en IPv4 – Switch Core. 94
Figura 54: OSPF - Áreas en IPv4 – Switch Core..... 95
Figura 55: OSPF - Neighbors en IPv4 – Switch Core..... 95
Figura 56: OSPF - Routes en IPv4 – Switch Core..... 95
Figura 57: OSPF – Lista de Rutas aprendidas en IPv4 – Switch Core. 96
Figura 58: Equipo CRS125 – 24G – 1S. 96
Figura 59: Interfaces equipo Switch Distribución..... 96
Figura 60: Crear VLAN en IPv4 - Switch Distribución..... 97
Figura 61: Dirección IPv4 para VLAN - Switch Distribución..... 97
Figura 62: Crear Pool de direcciones IPv4 - Switch Distribución..... 97
Figura 63: Crear DHCP Server en IPv4 - Switch Distribución. 98
Figura 64: Networks agregadas en IPv4 - Switch Distribución. 98
Figura 65: OSPF Interfaces en IPv4 - Switch Distribución. 98
Figura 66: OSPF Instances en IPv4 - Switch Distribución..... 99
Figura 67: OSPF - Networks en IPv4 - Switch Distribución. 99
Figura 68: OSPF - Áreas en IPv4 - Switch Distribución..... 99
Figura 69: OSPF - Neighbors en IPv4 - Switch Distribución..... 99
Figura 70: OSPF - Routes en IPv4 - Switch Distribución..... 100
Figura 71: OSPF – Lista de Rutas aprendidas en IPv4 - Switch Distribución. 100
Figura 72: Comando “ip routing print” – Switch Distribución..... 100
Figura 73: Comprobación de conexión Switch Distribución al Switch Core. 101
Figura 74: Comprobación de conexión hacia VLAN. 101
Figura 75: Switch Acceso Catalyst 2960X-Series. 101
Figura 76: Crear VLAN – Switch Acceso..... 102
Figura 77. Asignar VLAN a interfaz – Switch Acceso..... 102
Figura 78: Habilitar modo trunk – Switch Acceso. 103
Figura 79: IPv4 para VLAN nativa – Switch Acceso..... 103

Figura 80: Comprobando conexión hacia Switch Distribución y Switch Core. 103
Figura 81: Dirección IPv4 en usuario final. 104
Figura 82: Conectividad hacia los Swtichs Acceso-Distribución-Core. 104
Figura 83: Dirección IPv6 – Switch Core. 105
Figura 84: Configuración OSPFv3 – Switch Core. 105
Figura 85: OSPFv3 Instances IPv6 – Switch Core. 106
Figura 86: OSPFv3 - Áreas en IPv6 – Switch Core. 106
Figura 87: OSPFv3 Neighbors IPv6 – Switch Core. 107
Figura 88: OSPFv3 Routes en IPv6 – Switch Core. 107
Figura 89: OSPFv3 Route List en IPv6 – Switch Core. 107
Figura 90: Direcciones IPv6 – Switch Distribución. 108
Figura 91: Crear Pool de direcciones IPv6 - Switch Distribución. 109
Figura 92: DHCPv6 Server en IPv6 - Switch Distribución. 109
Figura 93: OSPFv3 Interfaces IPv6– Switch Distribución. 110
Figura 94: OSPFv3 Instances IPv6 – Switch Distribución. 110
Figura 95: OSPFv3 - Áreas en IPv6 – Switch Distribución. 111
Figura 96: OSPFv3 Neighbors IPv6 – Switch Distribución. 111
Figura 97: OSPFv3 Routes en IPv6 – Switch Distribución. 111
Figura 98: OSPFv3 Route List en IPv6 – Switch Distribución. 112
Figura 99: Dirección IPv4 e IPv6 usuario final. 112
Figura 100: Ping -6 VLAN-Cámaras. 113
Figura 101: Ping -6 Switch Distribución. 113
Figura 102: Ping -6 Switch Core. 113
Figura 103: Direcciones Broadcast en IPv4. 114
Figura 104: Paquete DHCPv6 para IPv6. 115
Figura 105: Paquete ICMPv4 para IPv4. 116
Figura 106: Tipo de mensaje ICMPv6 - RA. 117

Figura 107: Tipo de mensaje ICMPv6 – NS. 117

Figura 108: Tipo de mensaje ICMPv6 - NA. 118

Figura 109: Paquete ICMPv6 para IPv6 prueba de ping -6. 118

Figura 110: Protocolo OSPFv2 para IPv4. 119

Figura 111: Protocolo OSPFv3 para IPv6. 119

Figura 112: Comparativa Cabeceras IPv4 – IPv6. 120

Figura 113: Comparativa Cabecera OSPFv2 – OSPFv3. 121

Figura 114: Topología de Red para el despliegue de IPv6 – GNS3. 123

Figura 115: Asignación de Dirección IPv6 Administración. 126

Figura 116: Conectividad desde PC1-Administración hacia Switch CORE. 126

Figura 117: Asignación de Dirección IPv6 Energía. 128

Figura 118: Conectividad desde PC1-Energía hacia Switch CORE. 129

Figura 119: Topología implementación IPv6. 130

Figura 120: Esquema Facultad Administración - Facultad Energía en IPv6. 131

Figura 121: Acceso Switch Core. 132

Figura 122: Inicio Sesión Switch Core. 133

Figura 123: Rutas Aprendidas OSPFv3 Switch CORE. 134

Figura 124: Acceso Switch Distribución o L3 - Administración. 134

Figura 125: Inicio Sesión Switch L3 - Administración. 135

Figura 126: Rutas Aprendidas OSPFv3 Switch L3 Administración. 136

Figura 127: Acceder Switch de Acceso o L2. 137

Figura 128: Inicio Sesión Switch L2. 137

Figura 129: Asignación de dirección IPv6 a usuario final – Facultad Administración. 139

Figura 130: Conectividad Core – L3 (Administración). 139

Figura 131: Conectividad Core - Switch L3 (Administración-Interface VLAN 2). 140

Figura 132: Conectividad Switch Core - Switch L2 (Administración-Interface VLAN 2). 140

Figura 133: Conectividad Switch Core - Switch L3 (Administración-Interface VLAN 3). 140

Figura 134: Conectividad Switch Core – Usuario Final (Administración). 140

Figura 135: Conectividad Switch L3 (Administración) - Switch CORE. 141

Figura 136: Conectividad Switch L3 (Administración) - Switch L2 (Administración-Interface VLAN 2). 141

Figura 137: Conectividad Switch Distribución – Usuario Final. 141

Figura 138: Conectividad Switch L2 (Administración) – SwitchCORE (Interface GiX/X). 141

Figura 139: Conectividad Switch L2 (Administración) – Switch L3 (Administración-Interface GiX/X/X). 142

Figura 140: Conectividad Switch L2 (Administración) – Switch L3 (Administración-Interface VLAN 2). 142

Figura 141: Conectividad Switch L2 (Administración) – Switch L3 (Administración-Interface VLAN 3). 142

Figura 142: Conectividad Switch L2 (Administración) – Usuario Final (Administración). 142

Figura 143: Conectividad PC (Administración) – Switch CORE (Interface GiX/X). 143

Figura 144: Conectividad PC (Administración) – Switch L3 (Administración-Interface GiX/X/X). 143

Figura 145: Conectividad PC (Administración) – Switch L3 (Administración-Interface VLAN 2) 143

Figura 146: Conectividad PC (Administración) – Switch L3 (Administración-Interface VLAN 3). 144

Figura 147: Conectividad PC (Administración) – Switch L2 (Administración-Interface VLAN 2). 144

Figura 148: Rutas Aprendidas OSPFv3 Switch L3 Energía. 146

Figura 149: Asignación de dirección IPv6 a usuario final – Facultad Energía. 147

Figura 150: Conectividad Core – L3 (Energía). 147

Figura 151: Conectividad Core - Switch L3 (Energía-Interface VLAN 2). 148

Figura 152: Conectividad Switch Core - Switch L2 (Energía-Interface VLAN 2). 148

Figura 153: Conectividad Switch Core - Switch L3 (Energía-Interface VLAN 30). 148

Figura 154: Conectividad Switch Core – Usuario Final (Energía). 148

Figura 155: Conectividad Switch Distribución - Switch CORE. 149

Figura 156: Conectividad Switch L3 (Energía) - Switch L2 (Energía-Interface VLAN 2). 149

Figura 157: Conectividad Switch L3 (Energía) – Usuario Final (Energía). 149

Figura 158: Conectividad Switch L2 (Energía) – Switch CORE. 149

Figura 159: Conectividad Switch L2 (Energía) – Switch L3 (Energía). 150

Figura 160: Conectividad Switch L2 (Energía) – Switch L3 (Energía-Interface VLAN 2). 150

Figura 161: Conectividad Switch L2 (Energía) – Switch L3 (Energía-Interface VLAN 30). 150

Figura 162: Conectividad Switch L2 (Energía) – Usuario Final (Energía). 150

Figura 163: Conectividad PC (Energía) – Switch CORE. 151

Figura 164: Conectividad PC (Energía) – Switch L3 (Energía-Interface Gi1/1/4). 151

Figura 165: Conectividad PC (Energía) – Switch L3 (Energía-Interface VLAN 2). 151

Figura 166: Conectividad PC (Energía) – Switch L3 (Energía-Interface VLAN 30). 152

Figura 167: Conectividad PC (Energía) – Switch L2 (Energía-Interface VLAN 2). 152

Figura 168: Conectividad Facultad Administración – Facultad Energía. 153

Figura 169: Conectividad Facultad Energía – Facultad Administración. 153

Figura 170: Esquema Switch CORE hacia Jardín Botánico y Obelisco. 155

Figura 171: Configurar dirección IPv6. 156

Figura 172: Pool DHCPv6. 156

Figura 173: Configuración DHCPv6 server. 157

Figura 174: OSPFv3: Interfaces. 157

Figura 175: OSPFv3: Instances. 157

Figura 176: OSPFv3: Areas. 158

Figura 177: OSPFv3: Neighbors. 158

Figura 178: Rutas aprendidas por OSPFv3. 158

Figura 179: Asignación IPv6 a Usuario Final. 159

Figura 180: Rutas aprendidas con OSPFv3. 160

ÍNDICE DE TABLAS

TABLA I: Principales diferencias entre IPv4 e IPv6 [9]. 9

TABLA II: IPv4 vs Pv6 [12]. 10

TABLA III: Direcciones IPv6 reservadas [14]. 12

TABLA IV: Prefijos que no deben ser ruteados. 13

TABLA V: Equivalencia entre IPv4 e IPv6 [25]. 18

TABLA VI: Tipos de mensajes DHCPv6 [31]. 24

TABLA VII: Servidores Web Públicos. 46

TABLA VIII: Servidores Web Privados. 47

TABLA IX: Protocolos habilitados en IPv4 e IPv6. 48

TABLA X: Características de Equipos de red. 52

TABLA XI: Distribución de las Facultades Académico Administrativas (FAA). 53

TABLA XII: Soporte de IPv6 en los Equipos de red. 54

TABLA XIII: Resumen Mecanismos de Transición. 59

TABLA XIV: Criterios de Evaluación. 63

TABLA XV: Evaluación de Parámetros. 64

TABLA XVI: Valoración individual de Parámetros establecidos para los Mecanismos de Transición. 67

TABLA XVII: Casos de éxito – Implementación Doble Pila. 69

TABLA XVIII: Direccionamiento IPv4 de la Universidad Nacional de Loja. 72

TABLA XIX: Direccionamiento IPv6 para la Universidad Nacional de Loja. 79

TABLA XX: Materiales adicionales. 88

TABLA XXI: Comparación de Simuladores de Redes. 121

TABLA XXII: Recursos Humanos. 164

TABLA XXIII: Recursos Materiales. 164

TABLA XXIV: Recursos Técnicos/Tecnológicos. 165

TABLA XXV: Imprevistos. 165

TABLA XXVI: Resumen de Presupuesto utilizado. 165

1. TÍTULO

“Despliegue del Protocolo de Internet versión 6 (IPv6) para los dispositivos Core y Switchs de distribución en la red de datos de la Universidad Nacional de Loja”

2. RESUMEN

El presente trabajo de titulación tiene como objetivo configurar el Protocolo de Internet versión 6 (IPv6) para los dispositivos Core y Switchs de distribución en la red de datos de la Universidad Nacional de Loja. El fin del proyecto se debe a la inminente escasez y agotamiento de direcciones en el Protocolo de Internet versión 4 (IPv4), para ello el mecanismo de transición Doble Pila se debe adaptar a las configuraciones que se requieran y que en la Universidad Nacional de Loja necesiten para brindar un servicio de calidad a toda la comunidad universitaria.

Con el fin de mantener la misma infraestructura, aplicaciones y servicios se plantea una alternativa de solución a los administradores de red tanto para las instituciones públicas como privadas, mientras se avanza en la consolidación de IPv6.

El desarrollo de las configuraciones de IPv6 en el Switch Core y los Switchs de distribución se realizó mediante la metodología análisis, diseño e implementación que se ajusta al mecanismo de transición seleccionado Doble Pila, tomando en cuenta los parámetros que se plantearon y el estudio por la IETF (Internet Engineering Task Force) que se menciona para su utilización.

Para evaluar los resultados del estudio realizado se tomó como objeto de implementación desglosado la Facultad de Administración Central específicamente el Departamento de Telecomunicaciones e Información (UTI) y la Facultad de Energía el Departamento de Biblioteca, pudiendo obtener los resultados esperados y la total asignación de los parámetros en los equipos finales con el nuevo y mejorado protocolo de internet versión 6 (IPv6), mientras que para todo el despliegue se tomó todo lo que el tema de trabajo de titulación menciona, es decir, todo el backbone de la Universidad Nacional de Loja.

2.1. Summary

The present work of titling is to configure the Internet Protocol version 6 (IPv6) for devices Core and Switchs of distribution in the data network of the National University of Loja. The end of the project is due to the imminent scarcity and exhaustion of addresses in the Internet Protocol version 4 (IPv4), for this the Double Stack transition mechanism must be adapted to the configurations that are required and that at the National University of Loja Need to provide a quality service to the entire university community.

In order to maintain the same infrastructure, applications and services, an alternative solution is proposed to network administrators for both public and private institutions, while progress is being made in consolidating IPv6.

The development of IPv6 configurations on the Switch Core and the Switchs of distribution was carried out by means of the methodology analysis, design and implementation that conforms to the transition mechanism Double Stack selected taking into account the parameters that were raised and the study by the Internet Engineering Task Force (IETF) for their use.

To evaluate the results of the study was taken as the implementation object broken down the “Facultad de Administración Central”, specifically the “Departamento de Telecomunicaciones e Información (UTI)” and the “Facultad de Energía, Departamento de Biblioteca”, being able to obtain the expected results and the total allocation of the parameters in the teams end with the new and improved Internet Protocol version 6 (IPv6), while for the entire deployment took everything that the topic of tituclacion mentions, that is to say, all the backbone of the University, as well as nationally.of Loja.

3. INTRODUCCIÓN

El incremento del número de usuarios y dispositivos conectados a internet ha ocasionado un rápido agotamiento de las direcciones que hoy en día se utilizan, direcciones IPv4, razón por la cual el dar a conocer el nuevo Protocolo de Internet versión 6 (IPv6) ha generado un gran interés y expectativa a nivel mundial.

El Protocolo de Internet (IP) fue desarrollado en la década de los 70, un gran éxito que hizo posible la Internet de hoy en día. Actualmente Internet funciona con la versión 4 que son direcciones conformadas por 32 bits separadas en 4 octetos sin embargo el crecimiento del internet ha producido que estas direcciones lleguen a su límite, por otro lado el tráfico circundante hoy en día exige garantías de autenticidad, seguridad, confiabilidad y movilidad elementos que IPv4 no poseen en su estructura sino que podría implementarse mediante la inclusión de parches.

La arquitectura de Internet se basa en el principio extremo a extremo, el cual mantiene que dos nodos cualesquiera de Internet deben poder comunicarse sin impedimento alguno. Esta restricción frena el crecimiento de Internet así como la creación de nuevos servicios y aplicaciones. Por tales motivos principales, la IETF diseñó un sustituto para IPv4 denominado IPv6.

Internet aún está usando IPv4, pero en el futuro, es previsible que Internet sea sólo IPv6, hasta el momento, IPv4 e IPv6 deben coexistir; esto se consigue usando mecanismos de transición, que permiten la comunicación entre el mundo IPv4 y el IPv6.

El objetivo del presente trabajo es configurar el Protocolo de Internet versión 6 (IPv6) para los dispositivos Core y Switchs de distribución en la red de datos de la Universidad Nacional de Loja. Para su cumplimiento se utilizó el Mecanismo de Transición Doble Pila realizando de esta manera la coexistencia de ambos protocolos IPv4 e IPv6. Este objetivo general se descompone en varios objetivos específicos como son:

- Analizar la situación actual de los dispositivos Core y Switchs de distribución en la red de datos de la Universidad Nacional de Loja.
- Determinar el mecanismo de transición a utilizar entre IPv4 a IPv6.
- Diseñar el esquema de direccionamiento utilizando IPv6 para la red privada de la Universidad Nacional de Loja.
- Establecer un escenario de pruebas de acuerdo al mecanismo de transición seleccionado.

- Realizar las configuraciones necesarias para la implementación del Protocolo de Internet versión 6 en los dispositivos Core y Switchs de distribución de la Universidad Nacional de Loja.

El presente trabajo de titulación se estructura en 9 secciones:

- Sección 1: **TEMA**
- Sección 2: **RESUMEN**
- Sección 3: **INTRODUCCIÓN**
- Sección 4: **REVISIÓN LITERARIA**, describiendo de lleno el protocolo de internet versión 6, una introducción que nos permita empaparnos de información relevante como su nuevo formato de cabecera, así mismo la estructura de una dirección IPv6, los principales protocolos de enrutamiento manejados por IPv6 y por supuesto los mecanismos que hacen posible la transición y coexistencia de los protocolos de internet, versión 4 y versión 6.
- Sección 5: **MATERIALES y MÉTODOS** detallando los métodos y técnicas de investigación utilizadas en todo el proyecto.
- Sección 6: **RESULTADOS**, donde se estudia la situación actual de la Universidad Nacional de Loja, su estructura, el mecanismo de transición a utilizar para la coexistencia de IPv4 e IPv6. También se indica el direccionamiento en IPv6 para la institución antes mencionada, los escenarios de pruebas planteados tanto en equipos físicos como en la utilización de un simulador de redes y por último, la puesta en marcha de IPv6 mediante las configuraciones finales en los equipos reales de la Universidad Nacional de Loja – Departamento de Telecomunicaciones e Información (UTI), Switch Core, Switch Distribución y Switch de Acceso, logrando así el primer paso para la transición a IPv6.
- Sección 7: **DISCUSIÓN,** se evalúan los resultados obtenidos según los objetivos planteados, los inconvenientes presentados y la forma de resolverlos.
- Sección 8: **CONCLUSIONES** del trabajo de titulación realizado.
- Sección 9: **RECOMENDACIONES** del trabajo de titulación realizado.

4. REVISIÓN LITERARIA

4.1. Protocolo de Internet versión 6 (IPv6)

4.1.1. Introducción

El protocolo IP versión 4 según [1] y [2] es el protocolo de direccionamiento más usado en la actualidad, siendo desarrollado en 1973 junto con el protocolo TCP, como parte del proyecto que fue patrocinado por la Agencia de Programas Avanzados de Investigación (ARPA) del departamento de Defensa de los Estados Unidos (DoD).

Las principales características del protocolo IPv4 serán tratadas en paralelo a las características de IPv6, con el único objetivo de comprender de mejor manera los cambios incluidos en el nuevo protocolo de Internet.

Actualmente la versión IPv4 tiene limitaciones debido a que no ha tenido cambios substanciales desde RFC 791 en 1981. A pesar de ser un protocolo robusto, y fácil de implementar, con el pasar de los años ha ido mostrando grandes problemas, enfocándonos directamente en el número de IPs que puede suministrar, al usar 32 bits da un número de combinaciones de 2^{32} lo que resulta 4294967296 direcciones, a simple vista un número grande, pero debido al crecimiento exitoso de Internet este número ha quedado pequeño [3].

La necesidad de crear un nuevo protocolo surge por la falta de direcciones antes mencionada y en el IETF-Internet Engineering Task Force (Fuerza de Tareas de Ingeniería de Internet) se crea IPv6 que en un primer momento se denominó IPng-Internet Protocol Next Generation (Protocolo de Internet de la siguiente Generación) [4]. Dentro de las principales ventajas que brinda IPv6, se encuentra el amplio espectro de direcciones que admite, cerca de $6.67x10^{27}$. Si se utiliza una comparativa, 340 billones de billones de billones de direcciones IPs, se puede decir también 340 sextillones de direcciones por cada milímetro cuadrado de la superficie de la Tierra [5].

4.1.2. Características de IPv6

Según [6] el Protocolo de comunicaciones IPv6 Internet Protocol Version 6, fue desarrollado por Steve Deering y Craig Mudge en el año 1994, posteriormente fue adoptado por la IETF (Internet Engineering Task Force). El nuevo protocolo tiene el propósito de reemplazar progresivamente el protocolo IPv4 actualmente en uso por la

comunidad de Internet, en razón al limitado número de direccionamientos en IP que no hace posible su crecimiento en las redes y servicios; las características generales del nuevo protocolo son:

- Definido por la RFC (Request For Comments) 2460 de 1998.
- Tamaño del paquete 128 bits.
- Encabezado de base simplificado y de extensión.
- Identificación de flujo de datos, mejor calidad de servicio (QoS).
- Direccionamiento en Anycast, Multicast y Unicast.
- Incorpora mecanismos de IPSec (IP Security) al protocolo, cuya seguridad está a nivel del núcleo del mismo; por lo tanto la carga de paquetes se cifra con IPSec.
- Fragmentación de origen y destino de ensamble de paquetes.
- Conectividad extremo a extremo.
- Autoconfiguración, aspecto útil que implementa IPv6 en su capacidad para configurarse automáticamente sin utilizar un protocolo de configuración dinámica como DHCP [2].
- IPv6 ofrece mejoramiento de las capacidades de autenticación y privacidad de los datos que transmite porque los paquetes que proceden de un origen son los indicados en la cabecera de autenticación, mientras que en IPv4, los paquetes pueden venir de orígenes distintos a los indicados en la cabecera.
- Interacción con nodos vecinos a través del protocolo ICMP (Internet Control Messsage Protocol for IPv6).
- Mecanismos de seguridad avanzada sobre los datos transmitidos.
- Espacio de direccionamiento elevado de aproximadamente 340 Sextillones, 340 trillones de direcciones por pulgada cuadrada, 670 mil billones de direcciones por metro cuadrado.

4.1.3. Formato de la cabecera IPv6

Tiene una cabecera de longitud fija de 40 octetos, distribuidos en 8 campos. IPv6 incrementa las capacidades para los requerimientos actuales en direccionamiento y enrutamiento. IPv6 ha simplificado el formato de la cabecera, algunos campos de la cabecera IPv4 se han eliminado, cambiado de posición, modificado, mantenido y se han establecido otros nuevos [2].

Los campos de la cabecera IPv6 frente a los de IPv4, se presentan en la Figura 1.

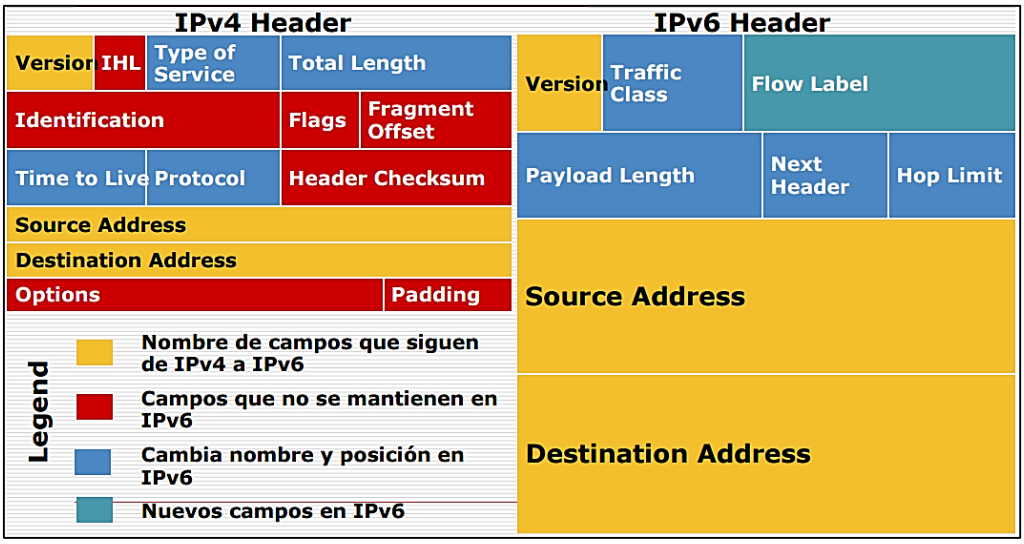


Figura 1: Formato cabeceras IPv6 frente a IPv4 [7].

La nueva versión de IP (IPv6) se compone de 8 campos detallados a continuación [2] [8]:

Versión (Version)-campo 4 bits. Versión del protocolo IP en este caso representa la versión 6.

Clase de Tráfico (Class of Traffic)-campo 8 bits. Asigna prioridad a cada paquete, es decir distingue entre paquetes con requisitos diferentes de entrega en tiempo real, aun si es de la misma fuente.

Etiqueta de Flujo (Flow Label)-campo 20 bits. Permite la diferenciación de flujos de tráfico. Esto tiene importancia a la hora de manejar calidad de servicio (QoS).

Longitud de carga útil (Payload Length)-campo 16bits. Especifica la longitud de los datos IPv6 en bytes y no incluye la cabecera IPv6.

Siguiente cabecera (Next Header)-campo 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6.

Límite de saltos (Hop Limit)-campo 8bits. Decrementado en 1 por cada nodo que reenvía el paquete. Se descarta el paquete si el límite de saltos es decrementado hasta cero.

Dirección Origen (Source Address)-campo 128bits. Contiene la dirección IP del host origen.

Dirección Destino (Destination Address)-campo 128bits. Corresponde a la dirección IP del destino.

4.1.4. IPv4 frente a IPv6

IPv6 conserva varias de las funciones que ofrece IPv4, sin embargo existen funciones que en IPv4 no son utilizadas o simplemente no se las utiliza, es por este motivo es que en IPv6 estas funcionalidades son eliminadas, dando paso a si a que en el nuevo protocolo se pueda implementar nuevas funciones que permiten mejorar la transmisión de los datos en la red [9] [10].

La TABLA I presenta las diferencias más significativas y las mejoras que ofrece IPv6 frente a IPv4.

TABLA I: PRINCIPALES DIFERENCIAS ENTRE IPV4 E IPV6 [9].

IPv4	IPv6
Las direcciones de origen y destino tienen una longitud de 32 bits (4 bytes), con lo que se tiene cerca de 4 mil millones de direcciones para ser asignadas.	Las direcciones de origen y destino tienen una longitud de 128 bits (16 bytes), con lo que se tiene cerca de $3.4x10^{38}$ direcciones para ser asignadas.
La implementación del protocolo de seguridad IPSec es opcional.	La implementación y soporte para IPSec es obligatorio.
No implementa identificación para el control de flujo de paquetes, la Calidad de Servicio o QoS es manejada por los routers y no por la cabecera de IPv4	La identificación de control de flujo de paquetes para la calidad de servicio o QoS está presente en la cabecera de IPv6 usando el campo “Flow Label”.
La fragmentación de paquetes involucra tanto al host como a los routers, es por ello que este proceso produce retardos en el rendimiento del router.	El proceso de fragmentación en IPv6 solamente involucra al host ya que el paquete es procesado solo en el nodo final de destino.
No tiene ningún requisito para el tamaño de un paquete de capa de enlace y debe ser capaz de re ensamblar un paquete de 576 bytes.	La capa de enlace debe soportar un paquete de 1280 bytes de tamaño y debe ser capaz de re ensamblar un paquete de 1500 bytes.
La cabecera incluye campos que no son utilizados y presentan mayor procesamiento en los routers.	Se elimina los campos innecesarios, que presenta IPv4, con lo que se reduce el procesamiento que realizan los routers.
El protocolo ARP envía tramas broadcast para realizar peticiones ARP de modo que se pueda resolver una dirección IPv4 en una dirección de capa física.	Las tramas para solicitar peticiones ARP son reemplazadas con mensajes multicast “Neighbor Discovery”, el cual a más de resolver la dirección IPv4 a capa física provee información adicional de los hosts y routers vecinos.

IGMP (Internet Group Management Protocol) es usado para manejar grupos de subredes locales.	IGMP es reemplazado por MLD (Multicast Listener Discovery) que es un set de mensajes que son intercambiados por los ruteadores para descubrir direcciones multicast.
Las direcciones de broadcast son utilizadas para enviar tráfico a todos los nodos en una subred.	No existen direcciones IPv6 de broadcast, en su lugar los enlaces en todos los nodos en donde direcciones multicast son usadas.
Las direcciones deben ser configuradas manualmente o mediante DHCP.	Las direcciones IPv6 no requieren configuración manual o DHCP.

4.1.5. Direccionamiento IPv6

4.1.5.1. Espacio de direcciones en IPv6

"La característica más obvia que distingue a IPv6 es el uso de direcciones mucho más largas, el tamaño de una dirección en IPv6 es de 128 bits, es decir, cuatro veces más larga que una dirección IPv4. Con IPv6 es muy difícil concebir que el espacio de direcciones se agote" [11].

TABLA II: IPV4 VS PV6 [12].

	Protocolo de Internet versión 4 (IPv4)	**Protocolo de Internet versión 6 (IPv6)**
Lanzada en	1981	1999
Tamaño de las direcciones	Número de 32 bits.	Número de 128 bits.
Formato de las direcciones	Notación decimal con puntos 199.43.0.202	Notación hexadecimal: 2001:500:4::/48
Cantidad de direcciones	$2^{32} = 4$ mil millones de direcciones	$2^{128} = 16$ trillones de direcciones.

"El uso de 128 bits permite tener múltiples niveles de jerarquía y flexibilidad en el diseño jerárquico de direccionamiento y ruteo, lo que no se tiene en el actual internet basado en IPv4" [11].

4.1.5.2. Sintaxis de las direcciones en IPv6

Se ha definido una nueva notación para describir las direcciones IPv6. Esta comprende una longitud de 128 bits divididos en bloques de 16 bits donde cada bloque es

representado por 4 dígitos hexadecimales separados por el signo "**:**", a diferencia de IPv4 en donde los grupos de 8 bits eran representados por dígitos decimales y separados por el signo "**.**".

Debido a que muchas direcciones tienen demasiados ceros en su sintaxis. Se han definido 3 optimizaciones:

- No es preciso escribir los ceros a la izquierda de cada campo, ejemplo:

FEDC**:**BA98**:**7654**:0**321**:0**EDC**:**BA98**:00**54**:**3210

FEDC**:**BA98**:**7654**:**321**:**EDC**:**BA98**:**54**:**3210

- Los "ceros" consecutivos son opcionales y se los puede representar en la dirección como:

FEDC**:**0DB8**:**85A3**:0000:**1319**:**8A2E**:**0370**:**3210

FEDC**:**0DB8**:**85A3**:0:**1319**:**8A2E**:**0370**:**3210

- Si uno o más grupos consecutivos son nulos, también pueden comprimirse con el signo "**::**". Si la dirección tiene más de una serie de grupos nulos consecutivos la compresión solo se permite en uno de ellos. Así, las siguientes son representaciones posibles de una misma dirección:

FEDC**:**0DB8**:0000:0000:0000:0000:**1428**:**3210

FEDC**:**0DB8**:0000:0000:0000::**1428**:**3210

FEDC**:**0DB8**:0:0:0:0:**1428**:**3210

FEDC**:**0DB8**:0::0:**1428**:**3210

FEDC**:**0DB8**::**1428**:**3210

Todas las expresiones anteriores son válidas y significan lo mismo, sin embargo se debe tener en cuenta que si se presentan dos grupos nulos no consecutivos como por ejemplo:

FEDC::25DE::3210

La dirección no es válida ya que no se puede definir cuantos grupos nulos existen en cada lado según [9] y [10].

Así mismo con el fin de simplificar la escritura y memorización de direcciones, se pueden aplicar las siguientes reglas a las direcciones IPv6 [13]:

- No se hace distinción entre mayúsculas y minúsculas. "ABC9" es equivalente a "abc9".
- Tal como en el caso de IPv4, para señalar las secciones de la dirección que identifican a la red y al dispositivo, se utiliza el formato CIDR (Encaminamiento Inter-Dominios sin Clases) en la forma ***<dirección / longitud de prefijo>***. Por ejemplo, una dirección en la forma **2001:DB8:c18:1::1/64** señala que los primeros 64 bits identifican a la red **(2001:DB8:c18:1)** y los restantes 64 bits identifican al dispositivo de dicha red (**::1**).
- Tradicionalmente el uso del símbolo "**:**" en las dirección IPv4 señala un puerto en un determinado nodo, por ejemplo 192.168.1.1:80 señala al puerto 80 (www) del nodo 192.168.1.1. Esto representa un problema de incompatibilidad al utilizar direcciones IPv6, por lo que se ha establecido que para señalar un puerto en una determinada dirección IPv6, esta debe estar encerrada por paréntesis cuadrados en la forma **[*dirección-IPv6*]:*puerto***

Las direcciones mencionadas son asignadas a una interface o a un grupo de interface, algunas direcciones se reservaron para usos futuros. La Tabla III muestra el direccionamiento IPv6 en la actualidad.

TABLA III: DIRECCIONES IPV6 RESERVADAS [14].

Dirección IPv6	Longitud del Prefijo (Bits)	Descripción	Notas
::	128 bits	Sin especificar.	Como 0.0.0.0 en IPv4.
::1	128 bits	Dirección de bucle local (loopback).	Como las 127.0.0.1 en IPv4.
::00:xx:xx:xx:xx	96 bits	Direcciones IPv6 compatibles con IPv4.	Los 32 bits más bajos contienen una dirección IPv4. También se denominan direcciones “empotradas”.
::ff:xx:xx:xx:xx	96 bits	Direcciones IPv6 mapeadas a IPv4.	Los 32 bits más bajos contienen una dirección IPv4. Se usan para representar direcciones IPv4 mediante direcciones IPv6
fe80::	10 bits	Direcciones link-local.	El prefijo de *enlace local (link local)* especifica que la dirección sólo es válida en el enlace físico local.

fec0::	10 bits	Dirección site-local	Equivale al direccionamiento privado IPv4
ff::	8 bits	Multicast	
001 (base 2)	3 bits	Direcciones unicast globales.	Todas las direcciones IPv6 globales se asignan a partir de este espacio. Los primeros tres bits siempre son “001”.

4.1.6. Prefijos IPv6

El prefijo se emplea en las direcciones con formato ***<dirección> / <longitud del prefijo>*** donde la longitud del prefijo en IPv4 equivalía a la longitud de la máscara de la subred para separarla de la porción del host [9].

Como menciona [15] el prefijo de dirección se emplea para indicar los bits que tienen valores fijos o que son los bits del identificador de red. Los prefijos de las rutas y los identificadores de subred en IPv6 se expresan de la misma forma que en la notación *Enrutamiento entre dominios sin Clase* (CIDR, Classless Inter-Domain Routing) de IPv4. Un prefijo IPv6 se escribe con la notación ***<dirección* IPv6> / *<longitud de prefijo>***.

Por ejemplo, 3FFE:B00::/48 siendo un prefijo de ruta y 3FFE:B00:C18:1::/64 siendo un prefijo de subred.

En las direcciones IPv6 se usa la longitud del prefijo para poder especificar jerarquías en las direcciones, debido a esto es que no existe mucha importancia como la máscara de subred en las direcciones IPv4.

4.1.6.1. Prefijos no ruteables en IPv6

Existen en IPv6 prefijos que no son ruteables, estos son conocidos como “Improper routes” mostrados en la tabla a continuación, de acuerdo a la IANA [16].

TABLA IV: PREFIJOS QUE NO DEBEN SER RUTEADOS.

Notación IPv6 Tipo de dirección	Notación IPv6 Tipo de dirección
::/128	No especificada
::/96	Reservada por la IETF [17]
::1/128	Loopback
::ffff:0:0/96	Mapeadas-IPv4

0100::/8	Discard-only prefix [18]
2001:0002::/48	BMWG
2001:10::/28	ORCHID
2001:DB8::/32	Para documentación
FE80::/10	Unicast de enlace local
FEC0::/10	Reservada por IETF
3FFE::/16	6Bone [19]

4.1.7. Tipos de direcciones IPv6

En la siguiente figura se muestra 3 tipos de direcciones que se detallan de la siguiente manera:

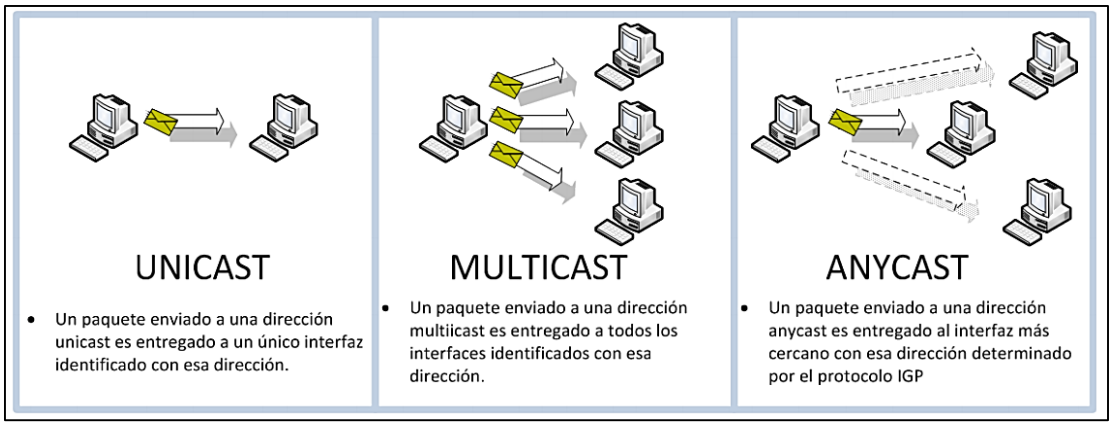


Figura 2: Tipos de direcciones [20].

4.1.7.1. Direccionamiento Unicast IPv6

Las direcciones Unicast o de Unidifusión identifican una interfaz única en el ámbito de direcciones. Los paquetes que son dirigidos a una dirección unicast son entregadas en una interfaz única.

Para dar cabida a los sistemas de balanceo de carga la norma RFC 2373 permite a múltiples interfaces utilizar la misma dirección siempre y cuando aparezcan como una sola interfaz para la implementación de IPv6 en el host [2].

Dentro de IPv6, las direcciones Unicast se las puede diferenciar por el tipo de uso que hacemos de ellas, así:

- **Direccionamiento Global de Unidifusión IPv6**

Son las direcciones que proceden del prefijo (2000::/16) asignado por la IANA para el grupo de direcciones públicas globales. Estas direcciones serán visibles en internet [21].

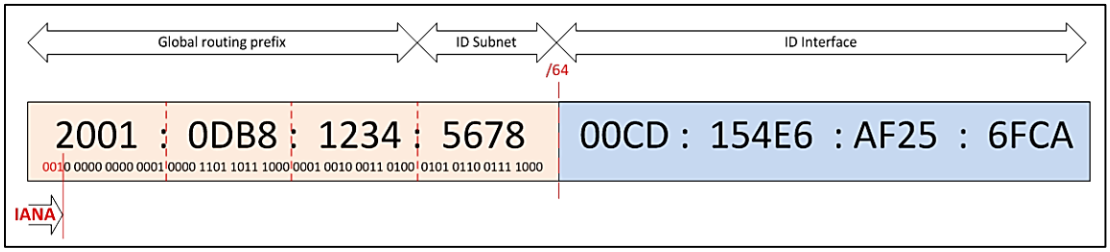


Figura 3: Tipo de dirección Global IPv6 [21].

- **Direccionamiento Unicast Locales de Enlace (Link-Local)**

Estas direcciones se configuran automáticamente y se usan para descubrir vecinos (en el mismo enlace), descubrimiento de rutas y por distintos protocolos de enrutamiento. El prefijo asignado para este tipo de direcciones es FE80::/10 más el identificador de interface. Su alcance solo llega al segmento local de red [20].

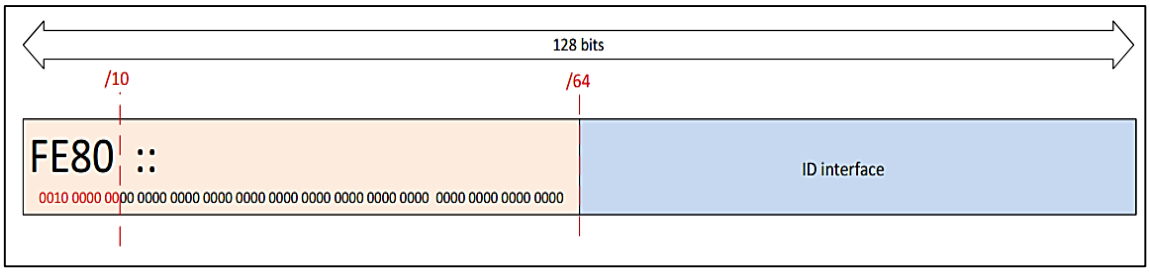


Figura 4: Tipo de dirección de Enlace Local IPv6 [21].

- **Direccionamiento Unicast Locales de Sitio (Site Local)**

Las direcciones site-local equivalen a las direcciones privadas que se definen en IPv4 como: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. Las direcciones site-local no son accesibles desde sitios ubicados fuera del enlace local, disminuyendo el tráfico que se genera en los routers. Estas direcciones son utilizadas dentro de las intranets en host que no tienen una conexión directa del internet a través de IPv6 [2].

10 bits	38 bits	16 bits	64 bits
1111111010	0	Id de Sub red	Identificador de interfaz

Figura 5: Tipo de dirección de Sitio Local IPv6 [10].

4.1.7.2. Direccionamiento Anycast IPv6

"Una dirección anycast identifica múltiples interfaces. Con la topología apropiada de ruteo, los paquetes direccionados a una dirección anycast son entregados a una sola interfaz, la interfaz más cercana que es identificada por la dirección. La interfaz más cercana es definida en términos de distancia de ruteo. Las direcciones anycast son usadas para comunicaciones "uno a alguno de muchos", con entrega a una sola interfaz" [11].

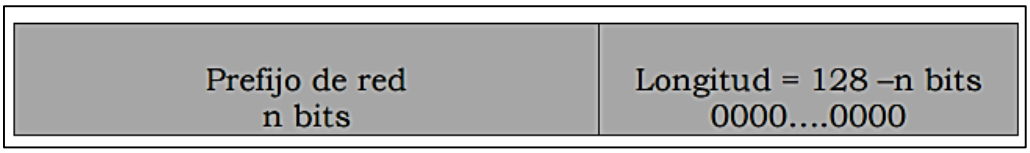


Figura 6: Tipo de dirección Anycast IPv6 [3].

4.1.7.3. Direccionamiento Multicast IPv6

Las direcciones Multicast de IPv6 se utilizan para identificar a los grupos de interfaces. Los paquetes son enviados desde un único host a múltiples receptores según lo definido por la dirección Multicast. Un router no se limita a un solo grupo Multicast y pueden pertenecer a varios grupos Multicast. Una dirección Multicast se identifica por la presencia de ocho bits en 1 al inicio de la dirección IPv6 [22].

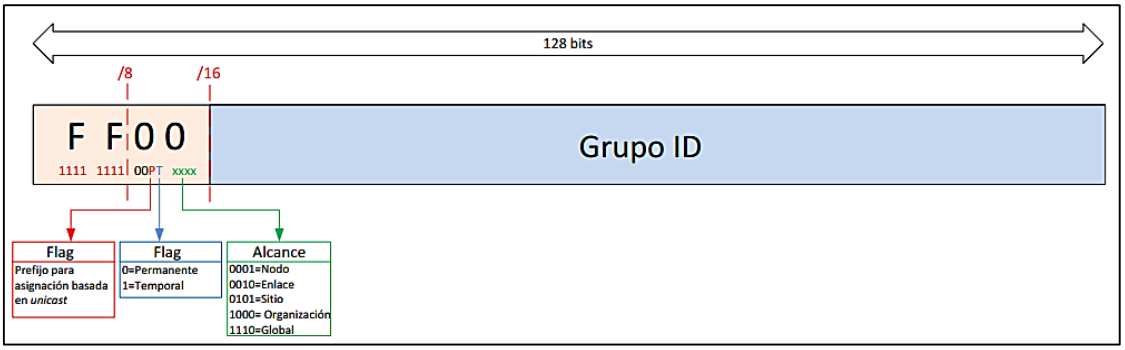


Figura 7: Tipo de dirección Multicast IPv6 [23].

Los flags nos indica el prefijo, el tiempo de vida y el alcance de la dirección. Hay algunas direcciones IPv6 multicast reservadas como son:

Dirección IPv6	Descripción
FF02::1	Indica todos los nodos de un enlace local
FF02::2	Indica todos los encaminadores de un enlace.
FF02::9	Indica a todos los encaminadores RIP de un enlace.
FF02::1:FFxx:xxxx	Indica a la dirección *multicast* de un nodo para la solicitud de autoconfiguración de host y descubrimiento de vecinos. El xx:xxxx son los 24 bits más a la derecha de la dirección *unicast* o *anycast* del nodo.
FF05::101	Indica todos los servidores NTP.

Figura 8: Direcciones Multicast IPv6 reservadas [23].

4.1.8. Direcciones Compatibles [10]

Las direcciones compatibles se diseñaron con la finalidad de permitir la migración y coexistencia entre protocolos IPv4 e IPv6, las principales direcciones son: direcciones IPv4 compatibles, direcciones 6over4, direcciones 6to4 y direcciones ISATAP (Intra-Site Automatic Tunnel Addressing Protocol).

Las direcciones IPv4 compatibles son usadas por nodos que se encuentran configurados con direcciones IPv6 e IPv4 que se comunican con redes IPv6 sobre una infraestructura IPv6 pública.

Las direcciones 6over4 al igual que las direcciones 6to4 son usadas para representar la interfaz del host en el mecanismo de transición tipo túnel (tunneling), y las direcciones ISATAP son usadas para representar a un nodo para el mecanismo de asignación de direcciones entre nodos con doble pila.

4.1.9. Identificadores de Interfaz de IPv6

Hemos visto en los tipos de direcciones que el indicador de un nodo concreto en las redes IPv6 es el “Identificador de Interfaz”. Este número, que normalmente será de 64 bits, puede ser configurado manualmente, dándole un valor concreto como se hacía en IPv4, pero para facilitar la autoconfiguración de direcciones IPv6, se ha definido un método para generar este identificador de tal manera que sea único en cada red, el método se ha denominado EUI-64.

Todas las tarjetas de red del mercado disponen de un único identificador de acceso al medio o MAC de 48 bits o 6 octetos. Los 3 primeros octetos de una MAC son asignados por la IEEE a cada fabricante para evitar posibles duplicidades de direcciones MAC y el resto de bits el fabricante asigna una única dirección a cada uno de las interfaces que fabrica [20].

Para generar una dirección EUI-64 para la autoconfiguración de la parte de Identificador de Interface de una dirección IPv6, según se especifica en el RFC 4291 [24], se realiza los siguientes pasos:

1. Se divide la dirección MAC por la mitad, generando dos partes de 3 octetos cada una.
2. Se le añade en medio dos octetos consecutivos fijos que son, **FF:FE**.
3. Al primer octeto, se le cambia de valor del segundo bit de menor peso.
4. Se unen todos los octetos, generando una dirección de 64 bits.

En la siguiente figura se indica:

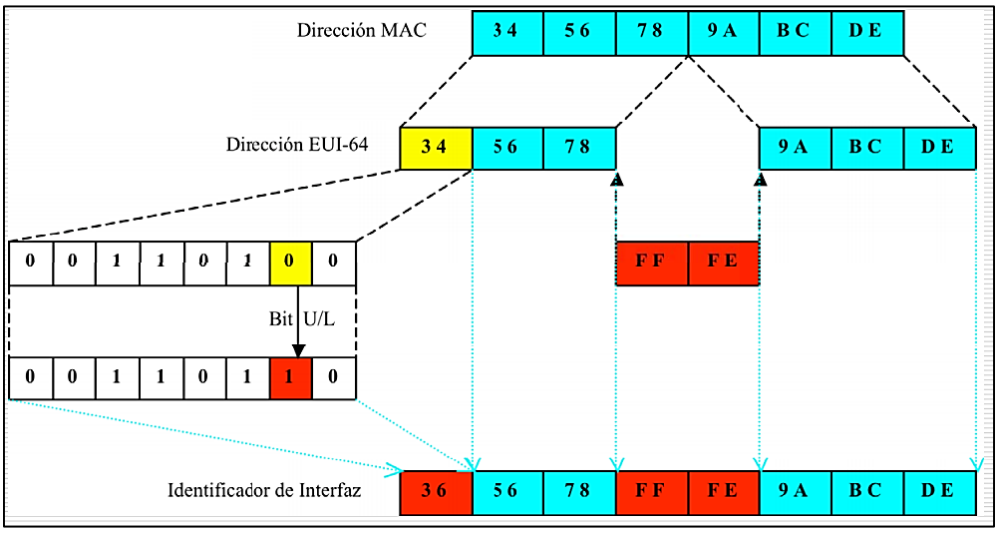


Figura 9: Generación de una dirección IPv6: Método EUI-64 [7].

4.1.10. Equivalencias de Direcciones de IPv4 e IPv6

Existe una equivalencia entre direcciones IPv4 e IPv6, en la Tabla IV se muestra su equivalente:

TABLA V: EQUIVALENCIA ENTRE IPV4 E IPV6 [25].

CONCEPTO	IPv4	IPv6
Clases de Red	Sí	No
Direcciones Multicast	224.0.0.0/4	FF00::/8
Direcciones Broadcast	Sí	No

Dirección sin especificar	0.0.0.0	::
Dirección loopback	127.0.0.1	::1
Direcciones Públicas	Sí	Direcciones unicast globales
Direcciones Privadas	10.0.0.0/8 172.16.0.0/12 192.168.0.0	Direcciones únicas locales FD00::/8

4.1.11. Principales Protocolos en IPv6

Los protocolos de enrutamiento bridan diferentes herramientas para proyectar y mantener las tablas de encaminamiento en los distintos routers de una red, así también define el mejor camino para llegar a un equipo remoto. Dentro de un router pueden coexistir protocolos de encaminamiento autónomos, levantando y actualizando rutas en las tablas de encaminamiento para distintos protocolos configurados [26].

IPv6 básicamente adopta los mismos protocolos que los existentes en las redes IPv4: ICMPv6, RIP, OSPF, BGP, etc. Pero además se está trabajando en nuevos protocolos como son IDRP (ISO Inter-Domain Routing Protocol) e IS-IS (Intermediate System to Intermediate System) [27]. A continuación se describe los principales protocolos y las nuevas características de funcionamiento:

4.1.11.1. Protocolo ICMPv6

“ICMP- Internet Control Message Protocol – (Protocolo de Mensajes de Control de Internet) ha sido actualizado para su uso bajo IPv6 y se le ha asignado el valor de 58 en el campo de “siguiente cabecera” para saber que es un ICMPv6. Este protocolo es parte integral de IPv6 y debe ser totalmente incorporado a cualquier implementación de nodo IPv6” [28].

Como mencionan [28] [29] “ICMPv6 es empleado por IPv6 para reportar errores que se encuentran durante el procesado de los paquetes, así como para la realización de otras funciones relativas a la capa de Internet, como son las de diagnósticos ping”.

Para garantizar el buen funcionamiento de los procesos de IPv6, se incluyen funciones como [22]:

- Procesamiento de paquetes de informe de errores.
- Diagnóstico.

- Descubrimiento de vecinos.
- Informes de membrecía Multicast.

El formato genérico de los mensajes ICMPv6 es el siguiente:

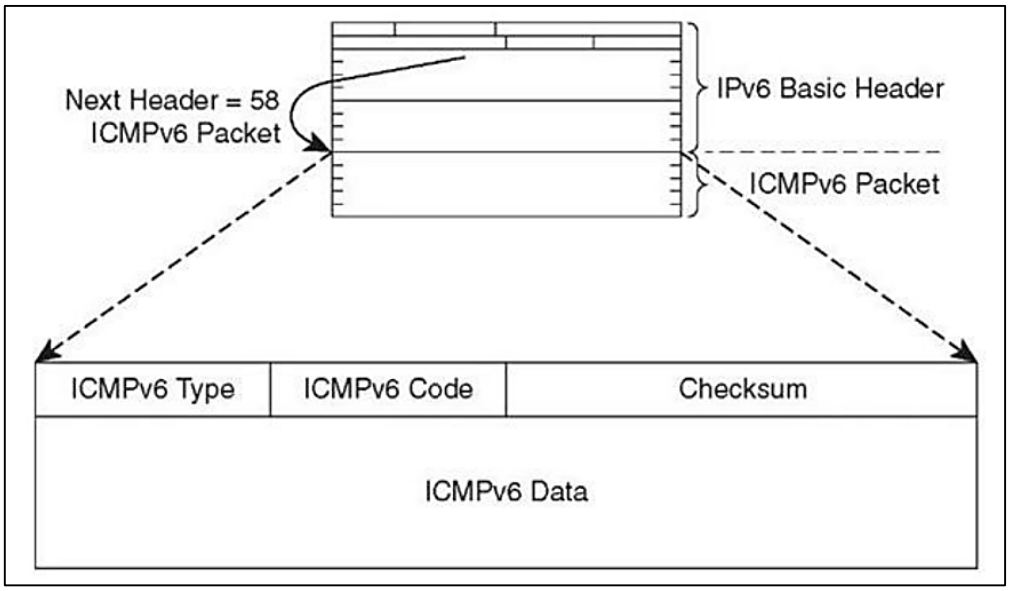


Figura 10: Formato mensaje ICMPv6 [28].

La estructura del mensaje antes mencionado se detalla a continuación [30]:

- El campo “tipo” indica el tipo de mensaje, y su valor determina el formato del resto de la cabecera.
- El campo “código” depende del tipo de mensaje, y se emplea para crear un nivel adicional de jerarquía para la clasificación del mensaje.
- El campo “checksum” o código de redundancia nos permite detectar errores en el mensaje ICMPv6.
- Y el “cuerpo del mensaje” contiene datos del mensaje ICMPv6.

ICMPv6 es simplificado para suprimir las funciones que ICMPv4 ya no usa, y combina las funciones de tres diferentes protocolos en IPv4 que son: ICMPv4, Protocolo de membrecía de grupos de Internet (IGMP, Internet Group Membership Protocol) y Address Resolution Protocol (ARP) [22].

En [29] nos menciona que los mensajes ICMPv6 se agrupan en dos tipos o clases: mensaje de error y mensajes informativos. Los mensajes de error tienen cero en el bit de mayor peso del campo “tipo”, por lo que sus valores se sitúan entre 0 y 127. Los valores de los mensajes informativos oscilan entre 128 y 255.

Los mensajes definidos por la especificación básica son los siguientes:

Mensajes de error ICMPv6		
Tipo	Descripción y Códigos	
1	*Código*	*Descripción*
	0	Sin ruta hacia el destino
	1	Comunicación prohibida administrativa
	2	Sin asignar
	3	Dirección no alcanzable
	4	Puerto no alcanzable
2	**Paquete demasiado grande**	
3	**Tiempo Excedido**	
	Código	*Descripción*
	0	Límite de saltos excedido
	1	Tiempo de desfragmentación excedido
4	**Problema de parámetros**	
	Código	*Descripción*
	0	Campo erróneo
	1	Tipo de "cabecera siguiente" desconocida"
	2	Opción de IPv6 desconocida
Mensajes informativos ICMPv6		
Tipo	*Descripción*	
128	Solicitud de ECO (Echo Request)	
129	Respuesta de ECO (Echo Replay)	

Figura 11: Mensaje de Error e Información de ICMPv6 [25].

Se está trabajando en nuevos tipos de mensajes, siendo el más interesante de ellos el definido en un borrador de IETF (draft-ietf-ipngwg-icmp-name-lookups- 05.txt), que permitirá solicitar a un nodo información completa como su “nombre de dominio completamente cualificado” (Fully-Qualified-Domain-Name). Por razones de seguridad, las cabeceras ICMPv6 pueden ser autenticadas y encriptadas, usando la cabecera correspondiente. El uso de este mecanismo permite, además, la prevención de ataques ICMP, como el conocido “Negación de Servicio” (DoS o Denial of Service Attack) [25].

4.1.11.2. Neighbor Discovery – El “ARP” de IPv6

En IPv6, el protocolo equivalente, en cierto modo, a ARP en IPv4, es el que denominamos “descubrimiento de vecinos”. Sin embargo, incorpora también la funcionalidad de otros protocolos IPv4, como “ICMP Router Discovery” y “ICMP Redirect”.

Este protocolo consiste, en el mecanismo por el cual un nodo que se incorpora a una red, descubre la presencia de otros, en su mismo enlace, para determinar sus

direcciones en la capa de enlace, para localizar los routers, y para mantener la información de conectividad ("reachability") acerca de las rutas a los "vecinos" activos. El protocolo ND (abreviatura común de "Neighbor Discovery"), también se emplea para mantener limpios los "caches" donde se almacena la información relativa al contexto de la red a la que está conectado un nodo (host o router), y por tanto para detectar cualquier cambio en la misma. Cuando no hay conexión desde un router, o no encuentra una ruta, el host buscará alternativas funcionales. ND emplea los mensajes de ICMPv6, incluso a través de mecanismos de multicast en la capa de enlace, para algunos de sus servicios. El protocolo ND es bastante completo y sofisticado, ya que es la base para permitir el mecanismo de autoconfiguración en IPv6 [27] [29].

Define, entre otros, mecanismos para: descubrir routers, prefijos y parámetros, autoconfiguración de direcciones, resolución de direcciones, determinación del siguiente salto, detección de nodos no alcanzables, detección de direcciones duplicadas o cambios, redirección, balanceo de carga entrante, direcciones anycast, y anunciación de proxies. ND define cinco tipos de paquetes ICMPv6 [29]:

- ✓ **Solicitud de Router (Router Solicitation)** – generado por una interfaz cuando es activada, para pedir a los routers que se "anuncien" inmediatamente. Tipo en paquete ICMPv6 = 133.
- ✓ **Anunciación de Router (Router Advertisement)** – generado por los routers periódicamente (entre cada 4 y 1800 segundos) o como consecuencia de una "solicitud de router", a través de multicast, para informar de su presencia así como de otros parámetros de enlace y de Internet, como prefijos (uno o varios), tiempos de vida, configuración de direcciones, límite de salto sugerido, etc. Es fundamental para permitir la renumeración. Tipo en paquete ICMPv6 = 134.
- ✓ **Solicitud de Vecino (Neighbor Solicitation)** – generado por los nodos para determinar la dirección en la capa de enlace de sus vecinos, o para verificar que el nodo vecino sigue activo (es alcanzable), así como para detectar las direcciones duplicadas. Tipo en paquete ICMPv6 = 135.
- ✓ **Anunciación de Vecino (Neighbor Advertisement)** – generado por los nodos como respuesta a la "solicitud de vecino", o bien para indicar cambios de direcciones en la capa de enlace. Tipo en paquete ICMPv6 = 136.
- ✓ **Redirección (Redirect)** – generado por los routers para informar a los host de un salto mejor para llegar a un determinado destino. Equivalente, en parte a "ICMP redirect". Tipo en paquete ICMPv6 = 137.

El protocolo ND, frente a los mecanismos existentes en IPv4, reporta numerosas ventajas [29]:

- ✓ El descubrimiento de routers es parte de la base del protocolo, no es preciso recurrir a los protocolos de encaminado.
- ✓ La anunciación de router incluye las direcciones de la capa de enlace, no es necesario ningún intercambio adicional de paquetes para su resolución.
- ✓ La anunciación de router incluye los prefijos para el enlace, por lo que no hay necesidad de un mecanismo adicional para configurar la máscara de red.
- ✓ La anunciación de router permite la autoconfiguración de direcciones.
- ✓ Los routers pueden anunciar a los host del mismo enlace el MTU (tamaño máximo de la unidad de transmisión).
- ✓ Se extienden los multicast de resolución de direcciones entre 232 direcciones, reduciendo de forma importante las interrupciones relativas a la resolución de direcciones en nodos distintos al objetivo, y evitando las interrupciones en nodos sin IPv6.
- ✓ Las redirecciones contienen la dirección de la capa de enlace del nuevo salto, lo que evita la necesidad de una resolución de dirección adicional.
- ✓ Se pueden asignar múltiples prefijos al mismo enlace y por defecto los host aprenden todos los prefijos por la anunciación de router. Sin embargo, los routers pueden ser configurados para omitir parte o todos los prefijos en la anunciación, de forma que los host consideren que los destinos están fuera del enlace; de esta forma, enviarán el tráfico a los routers, quien a su vez lo redireccionará según corresponda.
- ✓ A diferencia de IPv4, en IPv6 el receptor de una redirección asume que el siguiente salto está en el mismo enlace. Se prevé una gran utilidad en el sentido de no ser deseable o posible que los nodos conozcan todos los prefijos de los destinos en el mismo enlace (enlaces sin multidifusión y media compartida).
- ✓ La detección de vecinos no alcanzables es parte de la base de mejoras para la robustez en la entrega de paquetes frente a fallos en routers, particiones de enlaces, nodos que cambian sus direcciones, nodos móviles, etc.
- ✓ A diferencia de ARP, en ND se puede detectar fallos de la mitad del enlace, es decir, con conectividad en un sólo sentido, evitando el tráfico hacia ellos.
- ✓ A diferencia de IPv4, no son precisos campos de preferencia (para definir la “estabilidad” de los routers). La detección de vecinos no alcanzables sustituirá los caminos desde routers con fallos a otros activos.

- ✓ El uso de direcciones de enlace local para identificar routers, permite a los hosts que mantengan su asociación con los mismos, en el caso de que se realice una renumeración para usar nuevos prefijos globales.
- ✓ El límite de saltos es siempre igual a 255, lo que evita que haya envíos accidentales o intencionados desde nodos fuera del enlace, dado que los routers decrementan automáticamente este campo en cada salto.
- ✓ Al realizar la resolución de direcciones en la capa ICMP, se independiza el protocolo del medio, permitiendo mecanismos de autenticación y seguridad normalizados.

4.1.11.3. Protocolo DHCPv6

DHCP para IPv6 es un protocolo **UDP** cliente/servidor, diseñado para reducir el coste de gestión de nodos IPv6 en entornos donde los administradores precisan un control sobre la asignación de los recursos de la red, facilitados por el mecanismo de configuración "stateless" [31]. Como ya hemos indicado, ambos mecanismos se pueden usar de forma concurrente para reducir el coste de propiedad y administración de la red. Su objetivo, se centraliza en la gestión de los recursos de la red, tales como direcciones IP, información de encaminado, información de instalación de Sistemas Operativos, información de servicios de directorios, sobre uno o varios servidores DHCP, en lugar de distribuir dicha información en ficheros de configuración locales en cada nodo. DHCPv6 soporta los siguientes tipos de mensajes:

TABLA VI: TIPOS DE MENSAJES DHCPV6 [31].

Tipo de Mensaje	Descripción
SOLICITUD	Usado por los clientes para localizar los servidores de DHCP.
ANUNCIO	Usado por los servidores como una contestación SOLICITAR.
DEMANDA	Usado por los clientes para recibir información de los servidores.
CONFIRMACION	Usado por los clientes para verificar que su dirección y parámetros de configuración todavía son válidos.
RENOVAR	Usado por los clientes para renovar sus parámetros de configuración con su servidor DHCP original cuando está a punto de expirar.
REBIND	Usado por los clientes para extender la vida de su dirección y renueva sus parámetros de configuración con cualquier servidor de DHCP cuando está a punto de expirar.

RESPONDER	Usado por servidores DHCP para responder a los mensajes DEMANDA, CONFIRMACION, RENOVAR, REBIND, RELEASE, y DECLINE MESSAGES.
LANZAR	Usado por los clientes para lanzar su dirección IP.
DECLINE	Usado por los clientes para indicar que una o más direcciones asignadas a ellos ya está en uso.
RECONFIG-INIT	Usado por los servidores de DHCP para informar a los clientes que el servidor tiene información de configuración nueva o actualizada. Los clientes deben realizar una demanda para obtener la información actualizada.
INFORM	Enviado por los clientes para pedir los parámetros de la configuración sin la asignación de cualquier dirección IP al cliente.
RELAY-FORW	Usado por los relay de DHCP para adelantar los mensajes del cliente a los servidores. El relay encapsula el mensaje del cliente en una opción en el mensaje relay -forward.
RELAY-REPL	Usado por los servidores DHCP para enviar los mensajes a los clientes a través de un relay. El mensaje del cliente se encapsula como una opción en el mensaje relay-reply. El relay desencapsula el mensaje y lo envía al cliente

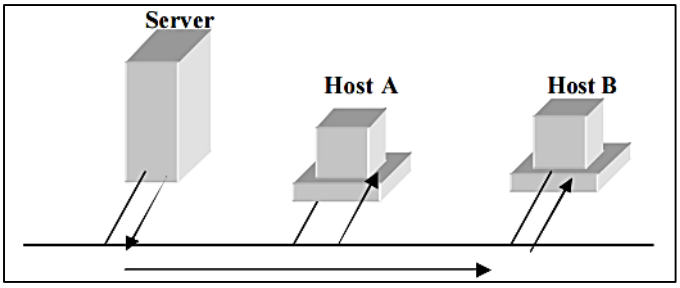


Figura 12: Esquema DHCPv6 [27].

Los hosts obtienen información de la dirección de interfaz y/o configuración desde un servidor. Para ello, el servidor dispone de una base de datos que contiene información de las direcciones que han sido asignadas a determinados hosts. Este proceso es la implementación del protocolo Dynamic Host Configuration Protocol para IPv6-DHCPv6 Además, DHCP ha sido diseñado para ser fácilmente extensible con nuevos parámetros de configuración, a través de “extensiones” que incorporan esta nueva información. Al respecto es fundamental el documento dhc-v6exts-12.txt.

Los objetivos de DHCPv6 son [32]:

- ✓ DHCP es un mecanismo, no una política. La política es establecida por el administrador de la red y DHCP le permite propagar los parámetros adecuados, según dicha política.
- ✓ DHCP es compatible, lógicamente, con el mecanismo de autoconfiguración "stateless".
- ✓ DHCP no requiere configuración manual de parámetros de red en clientes DHCP, excepto en casos donde dicha configuración se requiere debido a medidas de seguridad.
- ✓ DHCP no requiere un servidor en cada enlace, dado que debe funcionar a través de relés DHCP.
- ✓ DHCP coexiste con nodos configurados estáticamente, así como con implementaciones existentes en la red.
- ✓ Los clientes DHCP pueden operar en enlaces donde no hay routers IPv6.
- ✓ Los clientes DHCP proporcionan la habilidad de renumerar la red.
- ✓ Un cliente DHCP puede hacer múltiples y diferentes peticiones de parámetros de configuración, de uno o varios servidores DHCP simultáneamente. DHCP proporciona suficiente información para permitir a los servidores DHCP el seguimiento del estado de configuración de los clientes.
- ✓ DHCP incorpora los mecanismos apropiados de control de tiempo y retransmisiones para operar eficazmente en entornos con una alta latencia y/o reducido ancho de banda.

Los cambios fundamentales entre DHCPv4 y DHCPv6, están basados en el soporte inherente del formato de direccionamiento y autoconfiguración IPv6; son las siguientes [32]:

- ✓ La dirección de enlace local permite a un nodo tener una dirección tan pronto como arranca, lo que significa que todos los clientes tienen una dirección IP fuente para localizar un servidor o relé en su mismo enlace.
- ✓ Los indicadores de compatibilidad BOOTP y broadcast han desaparecido.
- ✓ El multicast y los ámbitos de direccionamiento permiten el diseño de paquetes de descubrimiento, que definen por si mismos su rango por la dirección multicast, para la función requerida.
- ✓ La autoconfiguración stateful ha de coexistir e integrarse con la stateless, soportando la detección de direcciones duplicadas y los dos tiempos de vida de IPv6, para facilitar la renumeración automática de direcciones y su gestión.
- ✓ Se soportan múltiples direcciones por cada interfaz.

Algunas opciones DHCPv4 ya no son precisas, debido a que los parámetros de configuración se obtienen a través de ND o del protocolo de localización de servicios. De esta forma, se soportan las siguientes funciones nuevas [33]:

- ✓ Configuración de actualizaciones dinámicas de DNS.
- ✓ Desaprobación de direcciones, para renumeración dinámica.
- ✓ Relés preconfigurados con direcciones de servidores, o mediante multicast.
- ✓ Autenticación.
- ✓ Los clientes pueden pedir múltiples direcciones IP.
- ✓ Las direcciones pueden ser reclamadas mediante el mensaje de "iniciar-reconfiguración".
- ✓ Integración entre autoconfiguración de direcciones "stateless" y "stateful".
- ✓ Permitir relés para localizar servidores fuera del enlace.

4.1.11.4. Protocolo RIPng

La especificación del Protocolo de Información de Rutas (RIP – "Routing Information Protocol") para IPv6, recoge los cambios mínimos e indispensables al RFC1058 y RFC1723 para su adecuado funcionamiento [34]. RIPng es un protocolo pensado para pequeñas redes, y por tanto se incluye en el grupo de protocolos de pasarela interior (IGP – "Interior Gateway Protocol"), y emplea un algoritmo denominado "Vector-Distancia". Se basa en el intercambio de información entre routers, de forma que puedan calcular las rutas más adecuadas, de forma automática. RIPng sólo puede ser implementado en routers, donde requerirá como información fundamental, la métrica o número de saltos (entre 1 y 15), que un paquete ha de emplear, para llegar a determinado destino. Cada salto supone un cambio de red, por lo general atravesando un nuevo router [35].

Los campos del mensaje RIPng son los siguientes:

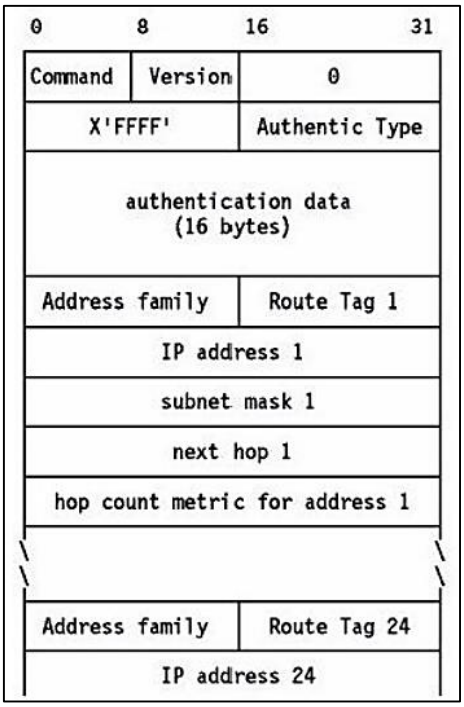


Figura 13: Mensaje RIPng [27].

Descripción de los campos del mensaje RIPng:

Comando: Es 1 para una petición RIP o 2 para una respuesta.

Versión: Es 2. Le dice al "router" RIP-1 que ignore los campos reservados, los que deben ser cero (si el valor es 1, los "routers" deben desechar los mensaje con valores distintos de cero en estos campos, ya que los originó un "router" que dice ser RIP, pero que envía mensajes que no cumplen el protocolo).

Dirección IP: Es la dirección IP de para esta entrada de encaminamiento: un host o una subred (caso en el que el número de host es cero).

Métrica de conteo de salto: Es el número de saltos hasta el destino. La cuenta de saltos para una interfaz conectada directamente es de 1, y cada "router" intermedio la incrementa en 1 hasta un máximo de 15, con 16 indicando que no existe ruta hasta el destino.

Familia de direcciones: Puede ser X'FFFF' sólo en la primera entrada, indicando que se trata de una entrada de autentificación.

Tipo de autentificación: Define como se han de usar los restantes 16 bytes. Los únicos tipos definidos son 0, indicando ninguna autentificación, y 2 indicando que el campo contiene datos de password.

Datos de autentificación El password es de 16 bytes, texto ASCII plano, alineado a la izquierda y rellenado con caracteres nulos ASCII (X'00').

Etiqueta de ruta: Es un campo dirigido a la comunicación de información acerca del origen de la información de encaminamiento. Está diseñado para la interoperabilidad entre RIP y otros protocolos de encaminamiento. Las implementaciones de RIP-2 deben conservarlo, aunque RIP-2 no especifica cómo se debe usar.

Mascara de subred: La máscara de subred asociada con la subred a la que se refiere esta entrada.

Siguiente salto: Una recomendación acerca del siguiente salto que el "router" debería usar para enviar datagramas a la subred o al host dado en la entrada.

Además de la métrica, cada red tendrá un prefijo de dirección destino y la longitud del propio prefijo, donde los parámetros han de ser configurados por el administrador de la red. El router incorporará, en la tabla de encaminado, una entrada para cada destino accesible (alcanzable) por el sistema y cada entrada tendrá como mínimo, los siguientes parámetros:

- El prefijo IPv6 del destino.
- La métrica (número de saltos entre este router y el destino).
- La dirección IPv6 del siguiente router, así como la ruta para llegar a él.
- Un indicador relativo al cambio de ruta.
- Varios contadores asociados con la ruta.

También se podrán crear rutas internas (saltos entre interfaces del propio router), o rutas estáticas (definidas manualmente).

RIPng es un protocolo basado en **UDP**. Cada router tiene un proceso que envía y recibe datagramas en el puerto 521 (puerto RIPng), el inconveniente de RIPng, al igual que en IPv4, siguen siendo, además de su orientación a pequeñas redes (diámetro de 15 saltos como máximo), en que su métrica es fija, es decir, no puede variar en función de circunstancias de tiempo real (retardos, fiabilidad, carga, etc.) [34].

4.1.11.5. Protocolo OSPFv6

El protocolo de encaminado “Abrir Primero el Camino más Corto” (OSPF – “Open Shortest Path First”), es también un protocolo IGP (para redes autónomas), basado en una tecnología de “estado de enlaces” (“link-state”).

Se trata de un protocolo de encaminado dinámico, que detecta rápidamente cambios de la topología (como un fallo en un router o interfaz) y calcula la siguiente ruta disponible (sin bucles), después de un corto período de convergencia con muy poco tráfico de routing [35] .

Cada router mantiene una base de datos que describe la topología del sistema autónomo (de la red), y es lo que denominamos base de datos de “estado de enlaces”. Todos los routers del sistema tienen una base de datos idéntica, indicando el estado de cada interfaz, y de cada “vecino alcanzable” [36].

Los routers distribuyen sus “estados locales” a través del sistema autónomo (la red) por medio de desbordamientos (“flooding”). Todos los routers utilizan el mismo algoritmo, en paralelo, y construyen un árbol de las rutas más cortas, como si fueran la raíz del sistema. Este árbol de “rutas más cortas” proporciona la ruta a cada destino del sistema autónomo.

Si hubiera varias rutas de igual coste a un determinado destino, el tráfico es distribuido equilibradamente entre todas. El coste de una ruta se describe por una métrica simple, sin dimensión. Se pueden crear áreas o agrupaciones de redes, cuya topología no es retransmitida al resto del sistema, evitando tráfico de routing innecesario [27].

OSPF permite el uso de máscaras diferentes para la misma red (“variable length subnetting”), lo que permite el encaminado a las mejores rutas (las más largas o más específicas). Todos los intercambios de protocolo OSPF son autenticados, y por tanto sólo pueden participar los routers verificados (“trusted”). OSPFv6 mantiene los mecanismos fundamentales de la versión para IPv4, pero se han tenido que modificar ciertos parámetros de la semántica del protocolo, así como el incremento del tamaño de la dirección. OSPFv6 se ejecuta basado en cada enlace, en lugar de en cada subred.

Además, ha sido necesario eliminar la autenticación del protocolo OSPFv6, dado que IPv6 incorpora estas características (AH y ESP). A pesar de la mayor longitud de las direcciones, se ha logrado que los paquetes OSPFv6 sean tan compactos como los correspondientes para IPv4, eliminando incluso algunas limitaciones y flexibilizando la manipulación de opciones [27].

Datagrama OSPF

Existen cinco tipos de paquetes diferentes que usa OSPF. Todos los paquetes de OSPF empiezan con una cabecera estándar de 16 byte, en la siguiente figura se muestra el datagrama OSPF para IPv6:

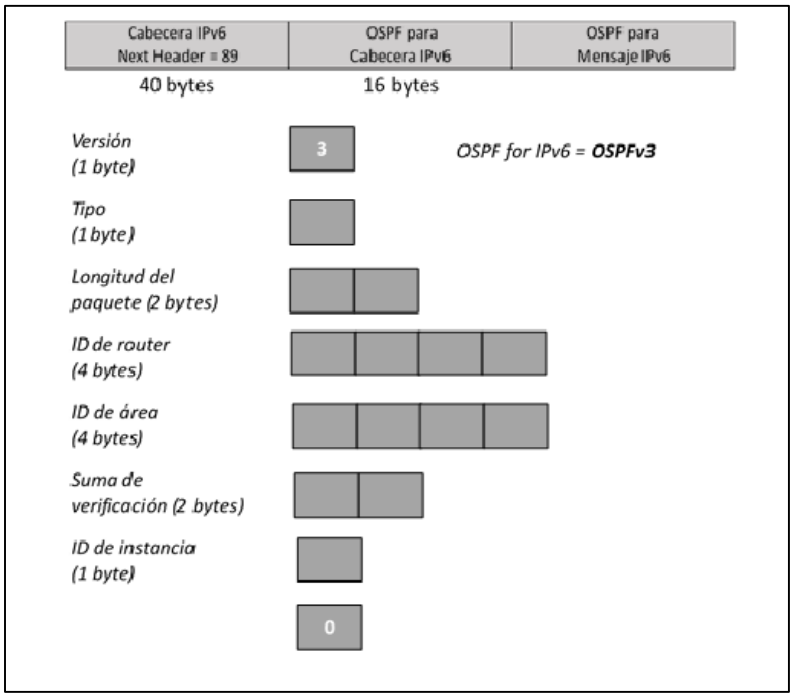


Figura 14: Datagrama OSPFv3 [27].

A continuación se explica cada campo de la cabecera OSPF [27]:

Version (1 byte): OSPF para IPv6 usa la versión número 3

Tipo (1 byte): Este campo representa el tipo de mensajes OSPF.

Longitud del paquete (2 bytes): Representa la longitud del paquete del protocolo OSPF en bytes, incluso la cabecera OSPF.

ID de router (4 bytes): Es la identificación del router que origina este paquete. Cada router debe tener una única ID. La ID de router debe ser única.

ID de área (4 bytes): Es la ID del área de la interfaz dónde se originó el OSPF. Identifica el área a que el paquete pertenece. Todos los paquetes de OSPF son asociados con una sola área.

Suma de verificación (2 bytes): OSPF usa el cálculo de la suma de verificación normal para las aplicaciones de IPv6.

ID de instancia (1 byte): Identifica la instancia OSPF a la que cada paquete pertenece. El ID de instancia es un número del 8-bits asignado a cada interfaz de ruteo. El valor predefinido es 0. El ID de instancia permite a múltiples instancias del protocolo OSPF correr en una sola conexión.

4.2. Mecanismos de Coexistencia y Transición de IPv4 a IPv6

IPv6 e IPv4 coexistirán durante muchos años debido a ello una amplia gama de técnicas se han definido que permiten la coexistencia proporcionando así una fácil transición. Hay tres categorías principales que a continuación se indica:

1. Técnica Doble Pila o Dual-Stack, permite a IPv4 y a IPv6 coexistir en los mismos dispositivos y redes.
2. Técnica de Tunneling, permite el transporte de tráfico de IPv6 a través de la infraestructura de IPv4 existente.
3. Técnica de Traducción, permite comunicar solamente nodos IPv6 con nodos IPv4.

Estas técnicas pueden y probablemente se usarán combinándolas entre sí. La migración a IPv6 puede hacerse paso a paso, empezando con un solo host o subnet. Se puede igualmente emigrar una red corporativa, o partes de la misma, mientras el ISP todavía trabaja sólo con IPv4. O el ISP puede actualizar a IPv6 mientras la red corporativa todavía ejecuta IPv4.

El presente capítulo describe las principales técnicas disponibles y factibles de implementar hoy en día, conforme IPv6 siga creciendo en nuestras redes, se definirán nuevas herramientas y mecanismos para que la transición sea fácil de realizar [37].

4.2.1. Mecanismo Doble Pila[1]

Los nodos se vuelven capaces de enviar o recibir paquetes de ambas versiones protocolares. Este tipo de nodo es a menudo llamado un nodo IPv6/IPv4. En la comunicación con un nodo IPv6, este se comporta como un nodo IPv6 único, y en la comunicación con un nodo IPv4, este se comporta como un nodo IPv4 único [38].

La siguiente gráfica muestra el esquema Doble Pila:

[1] https://tools.ietf.org/html/rfc4213

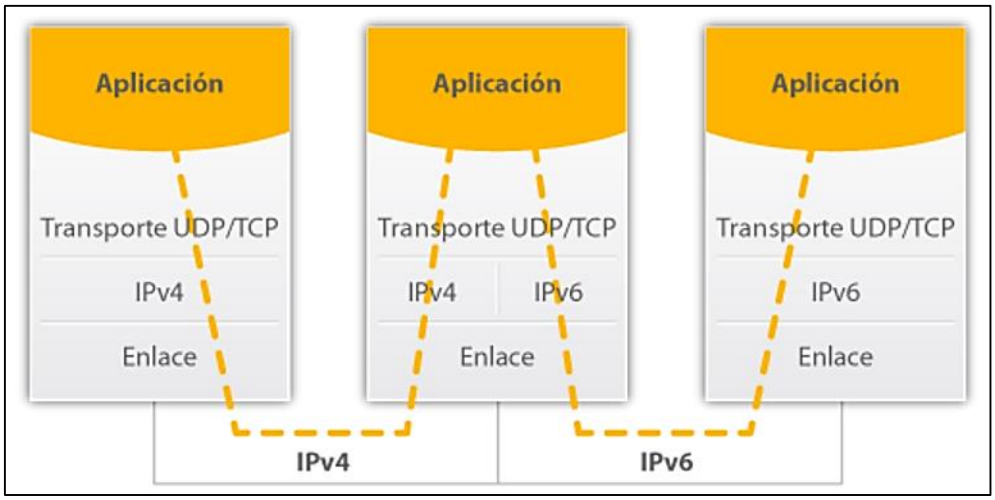


Figura 15: Esquema general del funcionamiento Doble Pila [39].

Las aplicaciones tienen un interruptor de configuración probablemente para habilitar o desactivar una de las pilas. Así que este tipo de nodo puede tener tres modos de funcionamiento [38]:

- Cuando la pila de IPv4 se habilita y la pila de IPv6 es desactivada, el nodo se comporta como un nodo IPv4 único.
- Cuando la pila de IPv6 se habilita y la pila de IPv4 es desactivada, se comporta como un nodo IPv6 único.
- Cuando se habilitan las pilas tanto en IPv4 y de IPv6, el nodo puede usar ambos protocolos.

Un nodo IPv6/IPv4 tiene una dirección por lo menos para cada versión protocolar.

Una red de doble pila es una infraestructura capaz de encaminar tanto paquetes IPv4 como IPv6, sin embargo hay que tener en cuenta aspectos tales como [7]:

- Configuración de los servidores DNS.
- Configuración de los protocolos de enrutamiento
- Configuración de los Firewalls
- Cambios en la administración de las redes.

4.2.2. Mecanismo de Tunelización [10] [40]

Es una técnica que permite conectar redes IPv6 sobre redes IPv4. Estos túneles trabajan encapsulando los paquetes IPv6 en la cabecera de IPv4 de modo que los paquetes son enviados sobre esta infraestructura. En la cabecera de IPv4 se asigna el valor de 42 en el campo de protocolo, con ello se indica que el paquete IPv6 enviado ha

sido encapsulado y los campos origen y destino se encuentran configurados con direcciones IPv4 en los puntos finales del túnel.

Los extremos finales del túnel son siempre los encargados de realizar la operación de encapsulado del paquete IPv6 en IPv4, estos pueden ser configurados manualmente ya sea como parte de la interfaz del túnel o derivando automáticamente de la interfaz que está enviando los paquetes.

Para los casos en que la ruta de acceso de IPv4 no se encuentra almacenada en cada túnel, el paquete IPv4 va a ser fragmentado por un router intermedio, en ese caso IPv6 debe ser configurado con la bandera de no fragmentar en la cabecera IPv4.

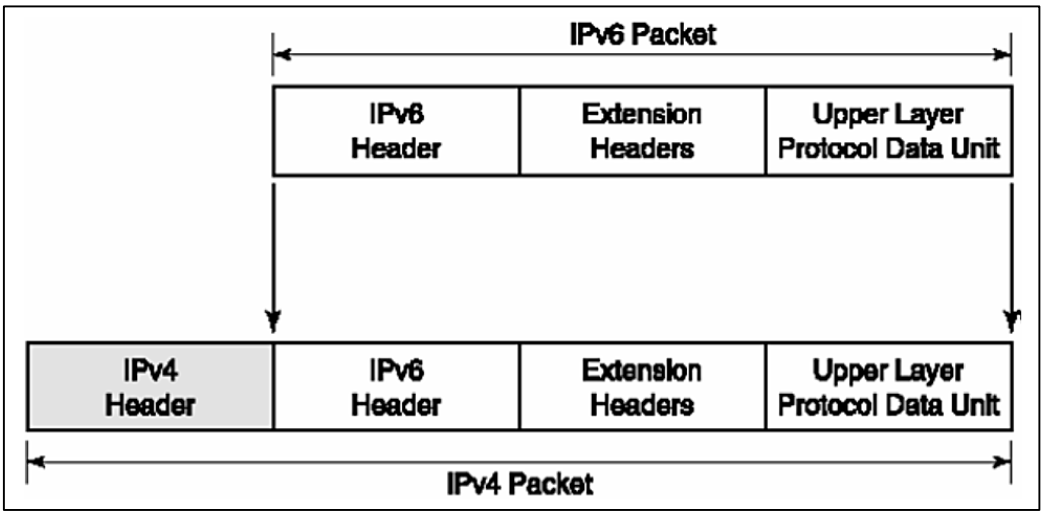


Figura 16: Arquitectura de encapsulación de IPv6 sobre IPv4 [10].

Cabe destacar que en el mecanismo de Túneles se pueden optar de las siguientes configuraciones, dependiendo del escenario donde se requiera implementar:

- Router a Router.
- Host a Router y Router a Host.
- Host a Host.

4.2.3. Tipos de Túneles

No obstante también existen algunos tipos de túneles que se describen a continuación:

4.2.3.1. Túneles Configurados

Están definidos como túneles IPv6-sobre-IPv4, siendo así túneles punto a punto y deben ser configurados manualmente en los dos extremos. Para la configuración de este esquema deben intervenir los administradores de ambos extremos, para de esa manera

controlar las rutas y reducir posibles problemas por denegación de servicio. Este tipo de túnel se usa en las configuraciones router-a-router y host-a-router, y las configuraciones de la interfaz del túnel deben ser especificadas manualmente a lo largo del túnel con rutas estáticas.

Uno de los requisitos para implementar esta configuración es la necesidad de que los routers presenten doble pila de protocolo y que las direcciones IPv4 asignadas sean alcanzables. Se lo recomienda para el uso de pequeñas redes y NAT no tiene que estar presente [9].

4.2.3.2. Túnel Automático 6to4

El mecanismo 6to4 se describe en la RFC 3056[2]. Esta técnica tiene tres elementos principales: los clientes 6to4, los routers 6to4 y los relays 6to4. Los clientes son las computadoras conectadas a una red que utiliza este tipo de túnel para obtener conectividad IPv6. Un router 6to4 es aquel que en la red del cliente oficia como extremo del túnel y, por lo tanto, debe tener una dirección IPv4 válida. A partir de allí, utilizando el prefijo 2002::/16 más los 32 bits de la dirección IPv4, se forma un prefijo IPv6 /48 para ser utilizado en la red. El otro extremo del túnel lo proveen los relays 6to4, que son routers con conectividad nativa IPv4 e IPv6. Muchas redes ofrecen el servicio de relay 6to4 colaborativamente en Internet, utilizando para la conectividad IPv4 la dirección anycast 192.88.99.1. En la Internet IPv6, estos relays se anuncian como routers para el prefijo 2002::/16.

El router encuentra el relay más cercano enviando el paquete a la dirección IPv4 anycast, el relay desencapsula el paquete y lo envía a su destino en la Internet IPv6. El destino enruta la respuesta al relay más próximo, que es el router para 2002::/16. Este encapsula nuevamente el paquete y lo envía al router cuya dirección IPv4 forma parte de la dirección IPv6 de destino. También se puede utilizar direcciones unicast y configurar los routers manualmente para especificar relays 6to4. Para un proveedor de servicios o de contenido que opera en doble pila podría ser ventajoso contar con un relay 6to4, no anunciado públicamente, exclusivamente para responder a consultas provenientes de clientes 6to4 y así garantizar el encapsulamiento del paquete en su origen [41]. La técnica descrita se ilustra en la Figura 17.

[2] https://www.ietf.org/rfc/rfc3056.txt

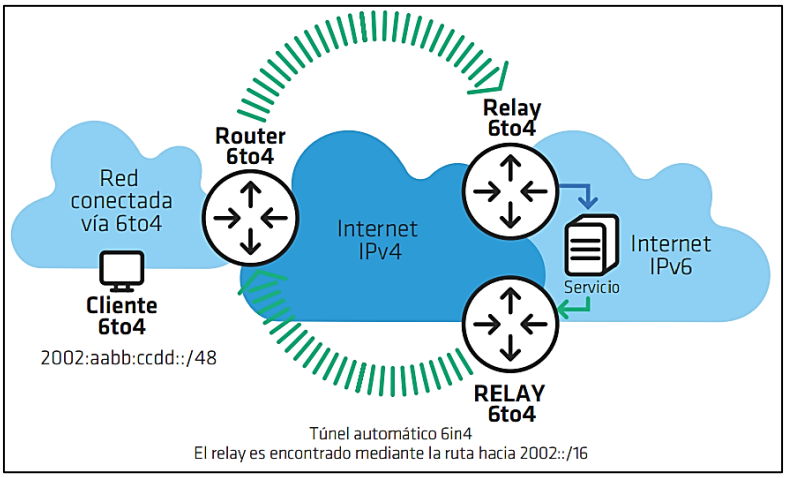


Figura 17: Túnel Automático 6to4 [41].

6to4 es afectado por diferentes problemas. Una vez que se obtiene una dirección IPv4 válida, la computadora pasa a actuar como cliente y router 6to4, por lo tanto, es aconsejable bloquear el uso del "protocolo 41", evitando así que los usuarios utilicen túneles automáticos. También es aconsejable deshabilitar esta funcionalidad en los sistemas operativos de las computadoras y más cuando se trata de entornos empresariales [41].

4.2.3.3. Túnel reenvío 6over4

6over4, también se denomina túnel de multidifusión de IPv4, técnica de túnel que se describe en el documento RFC 2529[3] "Transmisión de IPv6 sobre dominios IPv4 sin túneles explícitos".

Los túneles 6over4, interconectan entre host IPv6 aislados en un sitio por medio de una encapsulación IPv6-sobre-IPv4. Usa direcciones IPv4 como identificador de interfaces y crea un enlace virtual usando un grupo multidifusión. Para que 6over4 funcione correctamente, la infraestructura IPv4 debe estar habilitada para multidifusión IPv4 [9].

Según [29] si alguno de estos hosts IPv6 desea establecer comunicación con algún host ubicado en otro dominio IPv6, será necesario que exista de por medio un enrutador Doble Pila.

[3] https://www.ietf.org/rfc/rfc2529.txt

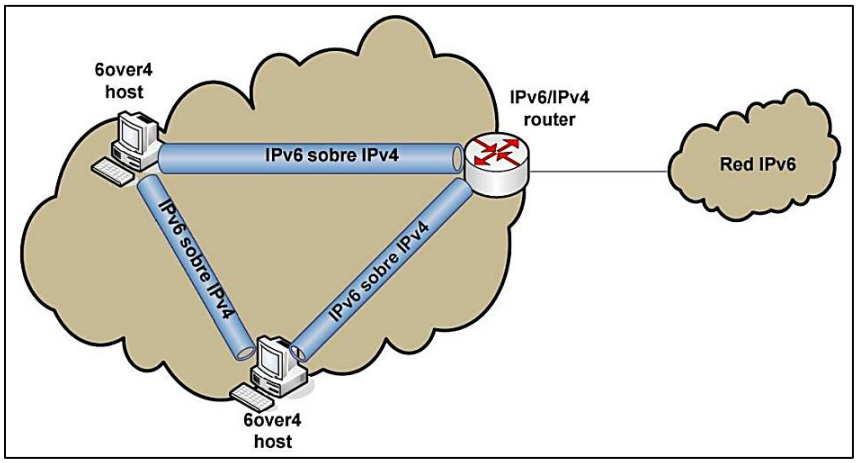


Figura 18: Arquitectura 6over4 [9].

4.2.3.4. Servidor TEREDO

Teredo es un mecanismo bastante similar a 6to4. Este mecanismo se describe en la RFC 4380[4]. El prefijo utilizado para los clientes es 2001:0000::/32. Con Teredo se conecta un único cliente, no toda una red. Para el encapsulamiento se utiliza UDP para que los túneles funcionen también en redes con NAT.

Además de relays similares a los que se utilizan con 6to4, también existen servidores que ayudan a descubrir el tipo de NAT utilizado por la red del usuario y al iniciar la comunicación. Los problemas para las redes corporativas son similares a los que se describieron para 6to4. Por ello se recomienda bloquear activamente el uso de esta técnica, lo que se puede lograr deshabilitándola en los sistemas operativos o bien bloqueando en la red el tráfico de salida al puerto UDP 3544 [41] [42].

4.2.3.5. ISATAP [9]

Una alternativa a los túneles 6over4 son los túneles ISATAP (Intra-Site Automatic Tunnel Addressing Protocol). Utiliza la infraestructura IPv4 como enlace virtual, pero no hace uso de multidifusión.

ISATAP, al igual que 6over4, crea un identificador de interfaz basado en la dirección IPv4. Las direcciones ISATAP pueden ser configuradas manual o automáticamente, pero la dirección IPv4 de la interfaz debe estar embebida en los últimos 32 bits de la nueva dirección IPv6.

[4] https://www.ietf.org/rfc/rfc4380.txt

Hay que tener en cuenta que para que funcionen las solicitudes de router, el host debe haber aprendido de alguna manera las direcciones IPv4 en los posibles routers ISATAP y enviará entonces las solicitudes de manera unicast. ISATAP se ha implementado en algunas plataformas como Windows XP y en las IOS de los equipos Cisco.

4.2.4. Mecanismo de Traducción o SIIT (Stateless IP/ICMP Translation Algorithm) [27].

El método de SIIT (Stateless IP/ICMP Translation Algorithm) se encarga de traducir las cabeceras entre IPv4 e IPv6 (incluyendo las cabeceras ICMP), permitiendo la comunicación entre hosts exclusivamente IPv6 y hosts exclusivamente IPv4. El nodo IPv6 de alguna forma obtendrá una dirección IPv4 temporal y un medio de enrutamiento para los paquetes. La dirección IPv4 temporal será utilizada como una dirección IPv6 llamada *IPv4-traducida*. Después los paquetes pasarán por un traductor SIIT encargado de traducir las cabeceras de los paquetes IPv4 e IPv6, así como las direcciones en las cabeceras. Las direcciones utilizadas en este método pueden ser IPv4, IPv4-traducidas o IPv4-mapeadas. Este método no especifica de qué manera se obtendrá la dirección IPv4 temporal (se sugiere DHCP con algunas extensiones), ni cómo será registrada en el DNS. Tampoco especifica el tipo de enrutamiento de los paquetes.

El método de SIIT puede ser utilizado cuando se desea establecer comunicar redes IPv6 pequeñas o hosts IPv6 y hosts IPv4, como se muestra en la siguiente figura:

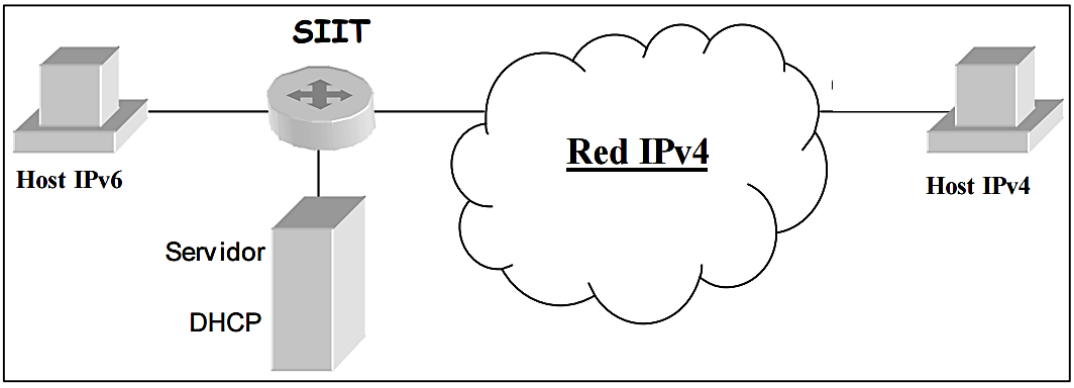


Figura 19: SIIT para redes pequeñas IPv6 [27].

Este método no es recomendable después de la transición, ya que solo existirán algunas redes IPv4 pequeñas y los traductores se encontrarían en los límites de estas, lo que significa un largo recorrido de los paquetes provenientes de los hosts IPv6 para obtener una dirección IPv4 temporal, la cual les permitiría llevar a cabo la comunicación [43].

Las direcciones utilizadas por este método son las siguientes:

- IPv4-mapeada.- Una dirección de la forma 0::FFFF:a.b.c.d que identifica a un nodo que no soporta IPv6.
- IPv4-traducida.- Una dirección de la forma 0::FFFF:0:a.b.c.d que identifica a un nodo que soporta IPv6.

4.2.4.1. Traducción de IPv4 a IPv6 [44]

Cuando el traductor recibe un datagrama IPv4 que contiene una dirección destino que esta fuera de la red IPv4, traduce el encabezado de ese datagrama por uno IPv6 destino.

Esta traducción consiste en que el encabezado IPv4 del paquete es removido y reemplazado por uno IPv6. La Figura 20 muestra el proceso.

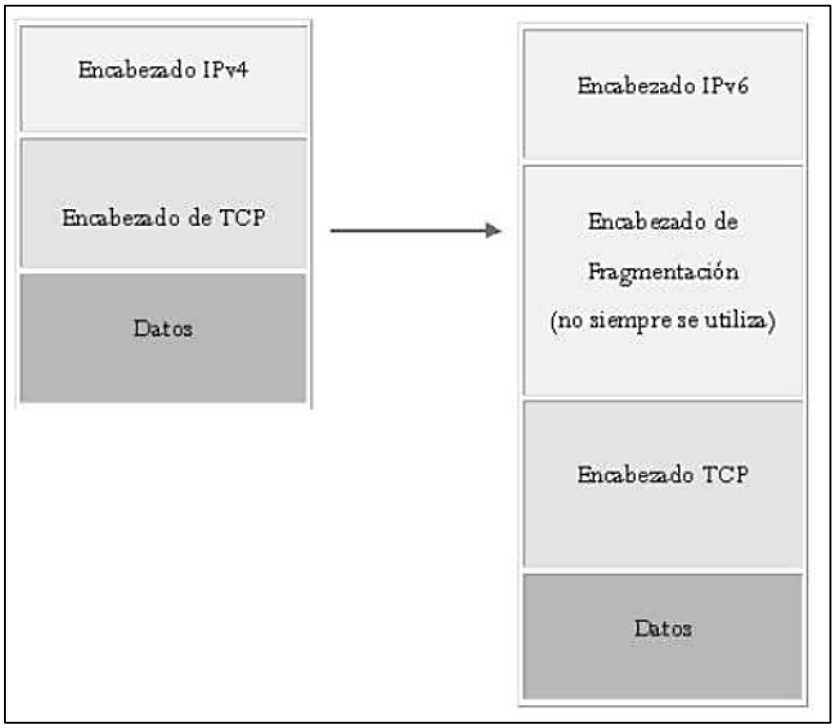


Figura 20: Traducción de IPv4 a IPv6 [44].

4.2.4.2. Traducción de IPv6 a IPv4

En la traducción de IPv6 a IPv4, cuando el traductor recibe un datagrama IPv6 destinado a una dirección IPv4 mapeada, éste traduce el encabezado IPv6 a un encabezado IPv4. Nuevamente, el encabezado original es removido y sustituido, en este caso por un encabezado IPv4. La siguiente figura muestra su proceso:

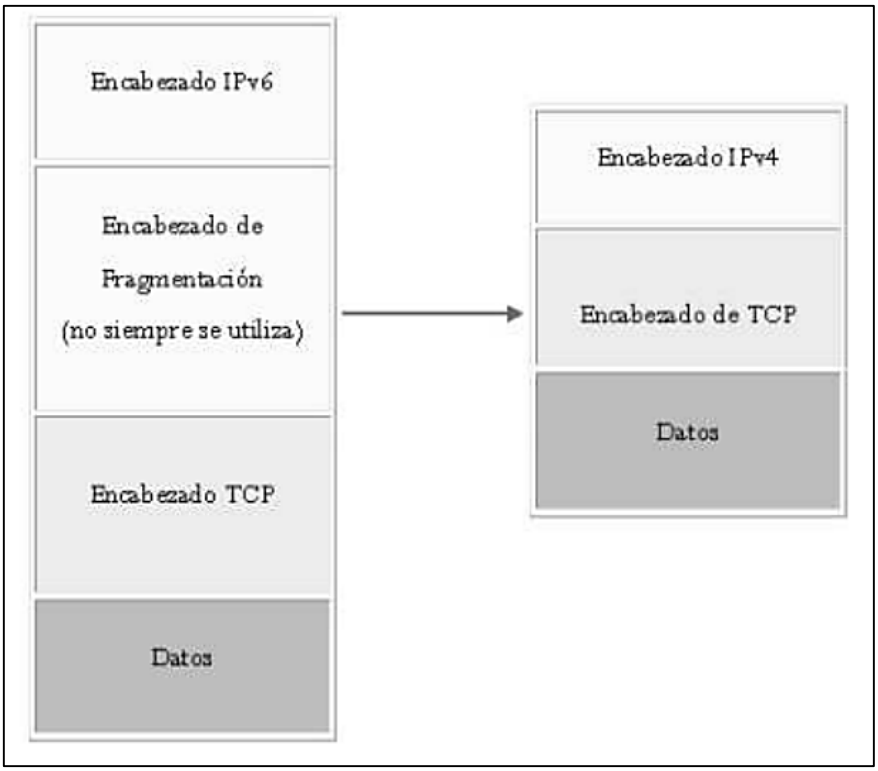


Figura 21: Traducción de IPv6 a IPv4 [44].

Un enlace IPv6 debe tener un MTU de 1280 bytes o más, mientras que IPv4 debe tener un MTU de 68 bytes. Entre IPv4 e IPv6 existen diferencias que afectan la traducción, tales como la fragmentación y el MTU de los enlaces. No es posible realizar un Path MTU Discovery de host a host cuando existe un traductor IPv6-IPv4, debido a que el host IPv6 puede recibir mensajes ICMP de error, indicándole que los paquetes son muy grandes originados por un enrutador IPv4 que reporte un MTU menor de 1280 bytes.

Los host IPv6 responden a estos mensajes de error de ICMP reduciendo el MTU del enlace a 1280 bytes, e incluyen una cabecera de fragmentación IPv6 a cada paquete, indicando que este puede ser fragmentado. Esto permite que se realice el proceso de Path MTU Discovery a través del traductor mientras el MTU del enlace sea de 1280 bytes o menor. Cuando el MTU sea menor de 1280 bytes, el nodo enviará paquetes de 1280 bytes que serán fragmentados por enrutadores IPv4 a lo largo del enlace, antes de ser traducidos a IPv4 [27].

5. MATERIALES Y MÉTODOS

Dentro de esta sección, se da a conocer los métodos, técnicas y metodologías necesarios para la construcción de esta investigación, permitiendo recolectar información relevante para realizar un proceso investigativo eficiente y exitoso, y de esta forma cumplir con éxito los objetivos planteados al comienzo del trabajo de titulación.

5.1. Métodos de Investigación

Aquí se describe los métodos tanto teóricos como prácticos que se utiliza en el trabajo de titulación, ayudando a obtener información teórica y deducir la misma:

- **Científico**: este método permite buscar información en libros, revistas, artículos científicos, lo que da lugar a detectar los problemas fundamentales para lograr esta investigación, porque a través de estos se transmite las posibles soluciones del caso.
- **Deductivo**: se analizó el problema desde lo general que son la escasez inminente de las direcciones IPv4 hasta llegar a lo particular, que es la elección del mecanismo de transición idóneo para la implementación y despliegue de IPv6.
- **Experimental**: este método consiste en provocar voluntariamente una situación que se requiere estudiar, es decir, realizar ambientes de simulación, para ejecutar las pruebas necesarias, con el fin de que tanto IPv4 como IPv6 coexistan dentro de la infraestructura de la Universidad Nacional de Loja.

5.2. Técnicas de Investigación

Dentro del presente trabajo de titulación, se requiere de selección adecuada de técnicas y herramientas que auxilien al investigador, en la realización de su estudio, por ello se detalla cada una de las técnicas utilizadas, para acceder a información real y necesaria:

- **Entrevista:** a través de ellas se realizan diálogos con el administrador de la red del Departamento de Telecomunicaciones e Información (UTI), con la finalidad de obtener la información de la problemática actual de la institución.
- **Observación Directa:** por medio de esta se puede conocer de forma real, las instalaciones e infraestructura, es decir, el backbone interno de la Universidad Nacional de Loja, su distribución de equipos en todo el campus universitario y

lineamientos que se sigue establecidos por la Unidad de Telecomunicaciones e Información (UTI).

- **Tutorías:** con las tutorías se pudo corregir errores y solucionar inconvenientes que aparecieron en el avance del proyecto, esta técnica se basa en el apoyo por parte del docente tutor o del personal de la Unidad de Telecomunicaciones e Información (UTI), que están prestos al apoyo colaborativo para alcanzar el objetivo general del trabajo de titulación.

5.3. Metodología

En todo el proceso investigativo es necesario seguir una secuencia de fases que conforman una metodología, con el fin de ejecutar ordenadamente los procesos, razón por la cual se detalla las fases realizadas dentro del presente trabajo de titulación.

- **Análisis:** en esta fase se estudió la situación actual, mediante entrevistas realizadas al Subdirector de la Unidad de Telecomunicaciones e Información (UTI); también se pudo analizar la estructura interna de la Universidad Nacional de Loja y poder determinar, cuál es el mecanismo de transición para la coexistencia de ambos protocolos que requiere la institución.
- **Diseño:** se realizó el diseño para el despliegue del protocolo de internet versión 6, en base al análisis elaborado sobre la situación actual; seleccionando la mejor alternativa de los mecanismos existentes para el despliegue y poder armar un ambiente de pruebas adecuado para las configuraciones necesarias.
- **Implementación:** en esta fase se realizó la implementación del protocolo de internet versión 6, diseñado en base al estudio total del trabajo de titulación; utilizando los equipos reales para las configuraciones y dando una solución óptima para la escasez de direcciones IPv4 que hoy en día se viene dando.

6. RESULTADOS

Todo lo que se expone en este apartado refleja las actividades llevadas a cabo para el cumplimiento de objetivos del tema de trabajo de titulación.

En el primero punto se realiza el estudio de la situación actual presentando en gráficos la distribución de equipos de red en el campus universitario, en el segundo punto se realiza una comparativa de los mecanismos de transición existentes para la coexistencia de ambos protocolos de internet tanto para IPv4 como IPv6, en el tercer punto a base de la dirección IPv6 otorgada por el proveedor de internet a la Universidad Nacional de Loja se realiza el esquema de direccionamiento y su mejor distribución de direcciones IP para la versión 6 del protocolo de internet presentando en tablas el esquema lógico distribuido dentro de la UNL, en el cuarto punto se plantea el escenario de pruebas acorde a los equipos de red que posee la UNL y configurándolos conforme se requiera dentro de la institución y por último se realiza las configuraciones necesarias en los equipos reales para verificar la funcionalidad en donde ambos protocolos deban coexistir tanto la versión 4 como la versión 6 de IP.

6.1. OBJETIVO 1: Analizar la situación actual de los dispositivos Core y Switchs de distribución en la red de datos de la Universidad Nacional de Loja.

Cada entidad educativa necesita ir a la par conforme avanza la tecnología, por ende la Universidad Nacional de Loja (UNL), en los últimos años, busca la mejora cuando se refiere a infraestructura física y tecnológica, todo ello contribuye a ser persistentes en brindar a la colectividad universitaria sus mejores servicios de calidad y eficiencia y de estar siempre a la vanguardia con respecto a la era tecnológica que se viene dando hoy en día.

La institución, se encuentra estructurada por varios departamentos que hacen el buen funcionamiento de la misma, entre ellos está la Unidad de Telecomunicaciones e Información (UTI) siendo este departamento el cerebro para el funcionamiento de la red, compuesto en secciones: Redes y Equipos Informáticos, desde donde se llevan a cabo métodos y técnicas para mantener la infraestructura de la red de datos 100% activa y

funcional para la transmisión de datos, voz y video, dando directrices para mejorar la conectividad entre los diferentes dispositivos de networking y equipos finales; teniendo en cuenta su objetivo principal, la seguridad de la red de datos.

6.1.1. Infraestructura de la red de datos de la Universidad Nacional de Loja

El flujo de información que transita dentro del campus en la Universidad Nacional de Loja es primordial y de vital importancia por ello la red de datos se encuentra distribuida lógicamente utilizando un modelo jerárquico de 3 capas: núcleo, distribución y acceso, sus distribuciones del backbone de la UNL se observa en la Figura 22.

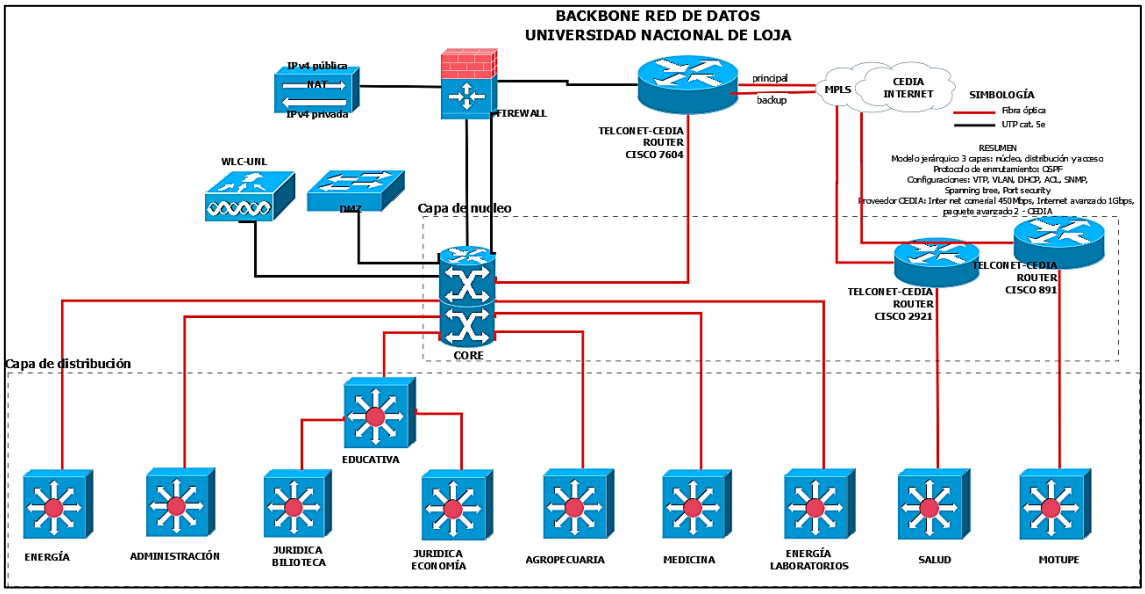


Figura 22: Backbone Red de Datos - Universidad Nacional de Loja.

La figura mostrada corresponde al backbone de la red de datos de la UNL, indica las principales conexiones empezando desde su proveedor de servicios de internet (ISP) como es TELCONET S.A que garantiza la conexión con la red de redes para el uso de internet pasando por el Firewall ASA, indicándonos también en su distribución la zona DMZ y teniendo en cuenta que desde el Switch Core y el gran número de Switchs de Distribución con los que cuenta la institución será el sector de estudio para el desarrollo de los objetivos y dando una solución al trabajo de titulación planteado denominado “Despliegue del Protocolo de Internet versión 6 (IPv6) para los dispositivos Core y Switchs de distribución en la red de datos de la Universidad Nacional de Loja”, todos los equipos mencionados se encuentran interconectados llevando información a cada departamento utilizando como medio de transmisión fibra óptica, cable UTP cat. 5e, radio enlace, etc.

Actualmente la Universidad Nacional de Loja cuenta con un ancho de banda de 450 Mbps de internet comercial y 1 Gbps de red avanzada.

La red de datos se compone de la interconexión de los bloques de Administración Central (bloque 1 y bloque 2) con las Áreas Académico Administrativas (AAA) y que actualmente mediante disposición académica y reformación de Estatutos para la Universidad Nacional de Loja con fecha de 24 de Enero del 2017 y aprobación de las mismas, todas las "Áreas" cómo se las conocía anteriormente pasaran a llamarse ahora "Facultades", estableciendo de ahora en adelante en el trabajo de titulación como Facultades Académico Administrativas (FAA).

En los bloques de Administración Central la red de datos se compone de un "backbone" que utiliza como medio de transmisión fibra óptica multimodo comunicando así las FAA: Educativa, Jurídica, Agropecuaria y Energía, los dispositivos de networking activos para la comunicaciones, se orientan al uso del estándar Fast Ethernet (normas 100Base TX y 100BaseFX) y Gigabit Ethernet (1000Mbps). Cabe destacar, que todas las comunicaciones dentro de la institución, permiten de esta manera la prestación de diferentes servicios de red en la Universidad Nacional de Loja como son: Internet, Sistema de Gestión Académico, Acceso inalámbrico, Correo Electrónico, Correo Institucional y Videoconferencia, etc.

6.1.2. Dispositivos de red: Cuarto de Telecomunicaciones

El cuarto de telecomunicaciones consta de varios equipos que hacen fácil la interconexión dentro de la institución (router, switch, AP, etc) y mediante esta estructura la comunicación a los equipos de los usuarios finales (laptop, pc, impresora, teléfono, etc).

Se debe mencionar la gestión que realizan los servidores pudiendo hacer posible brindar servicio de internet (DNS, DHCP, FTP, E-MAIL, etc) llegando a cumplir con eficiencia los servicios requeridos por los usuarios.

6.1.3. Tecnología de la Universidad Nacional de Loja

Para brindar un mejor servicio, nuestra entidad de educación superior UNL, consta de un Data Center ubicada en la Unidad de Telecomunicaciones e Información y es donde están alojados los servidores web tanto públicos como privados, estos servidores funcionales se encuentran en la zona desmilitarizada (DMZ); virtualizados en un servidor BLADE.

En la actualidad el BLADE tiene en 70% de disponibilidad de su capacidad total; tienen copado 6 cuchillas, de las cuales 4 cuchillas son de sexta generación y las 2 cuchillas de séptima generación, en los que se distribuye los servidores públicos y privados de la institución universitaria.

6.1.3.1. Servidores Web Públicos

En la siguiente tabla se detallan los servidores Web Públicos con los que la Universidad Nacional de Loja cuenta. También se hace mención que las configuraciones del nuevo protocolo IPv6 no se realizarán en los servidores mencionados, mas bien se realiza un estudio para tener en cuenta como esta distribuida la UNL, bajo que Sistemas Operativos (S.O.) trabajan con el fin de verificar si existe soporte para IPv6 en todos sus servicios y aplicaciones o si requieren que sus S.O. sean actualizados para que se pueda ejecutar el despliegue de IPv6.

TABLA VII: SERVIDORES WEB PÚBLICOS.

Nº	Servidor	Software	Servicios / Aplicaciones	Soporte IPv6
1	Eva	GNULinux Centos 5.8	xxx.unl.edu.ec	✓
2	Virtual, Cursos	GNULinux Centos 5.8	xxx.unl.edu.ec	✓
3	Graduados	GNULinux Centos 7.0	xxx.unl.edu.ec	✓
4	Evaluación Docente	GNULinux Centos 7.0	xxx.unl.edu.ec	✓
5	Capacitación	GNULinux Debian 8.2	xxx.unl.edu.ec	✓
6	DSpace	GNULinux Debian 8.2	xxx.unl.edu.ec	✓
7	Facturación Tesorería	Windows Server 2012 Standard	xxx.unl.edu.ec	✓
8	SGA	GNULinux Debian 6.0	xxx.unl.edu.ec	✓
9	Servidor UNL	GNULinux Debian 7.7	xxx.unl.edu.ec	✓
10	Servidor OPEN-VPN	GNULinux Centos 7.0	xxx.unl.edu.ec	✓

11	Servidor Formación	GNULinux Debian 8.2	xxx.unl.edu.ec	✓

6.1.3.2. Servidores Web Privados

El estudio realizado para los servidores Web Privados se detallan en la siguiente tabla:

TABLA VIII: SERVIDORES WEB PRIVADOS.

Nº	Descripción Servidor	Sistema (versión)	Servicios / Aplicaciones	Soporte IPv6
1	Biblioteca	GNULinux Debian 8.4	xxx.unl.edu.ec	✓
2	LDAP	GNULinux Centos 7.0	xxx.unl.edu.ec	✓
3	NOC	GNULinux Centos 7.0	noc.unl.edu.ec	✓
4	Systemas Legacy	Windows Server 2008 32 Bits	xxx.unl.edu.ec	✓
5	Git	GNULinux Debian 8.2	xxx.unl.edu.ec	✓
6	Soporte – GLPI	GNULinux Debian 8.2	xxx.unl.edu.ec	✓
7	Desarrollo	GNULinux Debian 8.2	xxx.unl.edu.ec	✓
8	OCS – Inventory	GNULinux Centos 7.0	xxx.unl.edu.ec	✓
9	Security	GNULinux Centos 7.0	xxx.unl.edu.ec	✓
10	Evaluaciones	GNULinux Debian 8.2	xxx.unl.edu.ec	✓
11	NTP	GNULinux Centos 7.0	xxx.unl.edu.ec	✓
12	Name Server 01	GNULinux Centos 7.1	xxx.unl.edu.ec	✓
13	Repositorio	GNULinux Centos 7.0	xxx.unl.edu.ec	✓

14	Quipux	GNULinux Centos 7.0	xxx.unl.edu.ec	✓
15	Respaldo	GNULinux Debian 8.4	xxx.unl.edu.ec	✓

Luego de haber realizado el análisis de la situación actual de los servidores y aplicaciones web tanto públicos como privados, se detallan algunos puntos como:

- Las últimas versiones de distribución Linux instaladas y utilizadas por la Unidad de Telecomunicaciones e Información en sus equipos ya incorporan soporte para IPv6 en su Kernel.
- Las versiones para las distribuciones de Windows instaladas para Facturación Tesorería y Systemas Legacy, tiene incorporado soporte para IPv6 en su Kernel.
- Los sistemas operativos utilizados por los usuarios para la utilización de los servicios que presta la UNL, en todas sus últimas versiones tanto de distribución Linux como Windows tiene soporte para IPv6, a excepción del S.O. Windows XP donde no tiene habilitado dicho soporte pero a su vez no presenta ningún impedimento para poder utilizar el protocolo de internet IPv6 ya que solo se requiere ser habilitado bajo una secuencia de pasos sencillos a ejecutar.

6.1.4. Servicios que presta la Universidad Nacional de Loja

Antes de verificar el esquema topológico que la institución maneja, se debe analizar los protocolos o servicios con los que la UNL trabaja en toda su red, así mismo se detalla mediante una tabla y se verifica cuales se habilitaran para el despliegue de IPv6.

TABLA IX: SERVICIOS HABILITADOS EN IPV4 E IPV6.

Nº	Capa	Protocolo	IPv4	IPv6
1	Red	DHCP	Habilitado	Habilitado
2	Red	OSPF	Habilitado	Habilitado
3	Aplicación	DNS	Habilitado	Deshabilitado
4	Aplicación	NTP	Habilitado	Deshabilitado
5	Aplicación	HTTP	Habilitado	Deshabilitado
6	Aplicación	HTTPS	Habilitado	Deshabilitado
7	Aplicación	SSH	Habilitado	Deshabilitado

Una vez analizados los protocolos y enfocándonos en nuestras configuraciones las cuales se las realiza en la capa 3 del modelo OSI (Capa de Red) podemos indicar que los equipos utilizados en dicha capa, se habilita el Protocolo DHCPv6 (Dynamic Host Configuration Protocol version 6 - Protocolo de configuración dinámica de host versión 6) y el Protocolo OSPFv3 (Open Shortest Path First - Primer Camino Más Corto) los cuales trabajan en la Capa de Red y donde radica el despliegue de IPv6 del Trabajo de Titulación, equipos de Capa 3.

6.1.5. Topología intranet de la Universidad Nacional de Loja

Los equipos utilizados en la infraestructura de red en la UNL juegan un papel importante, en el siguiente diagrama de topología de red (Ver Figura 23), se muestra el esquema utilizado que es estrella donde interconectan el dispositivo CORE desprendiendo de él los Switchs de Distribución para cada facultad de la institución mediante fibra óptica, se debe acotar que la facultad de Salud Humana y Motupe con fecha de diciembre del 2015 estaban conectadas por radio enlace debido a la distancia a la que se encuentran ubicadas pero actualmente y gracias a las gestiones realizadas por la Unidad de Telecomunicaciones e Información (UTI) hay conexión mediante fibra óptica, siguiendo su conexión mediante cable UTP categoría 5e por los Switchs de Acceso que hace fácil la comunicación dentro del campus universitario a los usuarios finales.

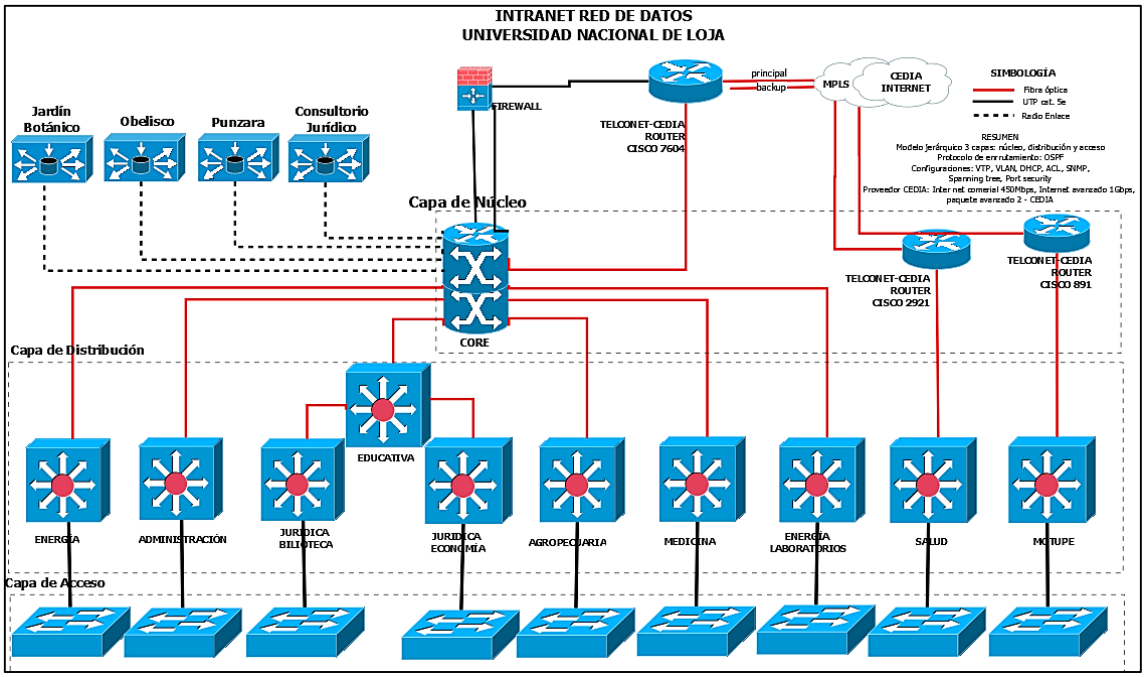


Figura 23. Principales Equipos de Red.

Los equipos activos que nos competen analizar y que son notables en el diagrama de red son los siguientes:

- **Capa de Núcleo:** Switch CORE WS-C6506-E
- **Capa de Distribución o L3**: Switch WS-C3750X-24T-S, WS-C3750X-48PF-S, MKR CCR1036-12G-4S, MKR CCR1016-12G, MKR CRS125-24G-1S.
- **Capa de Acceso o L2**: Switch WS-C2960-48TT-S

El análisis de la Capa de Acceso se la realizó con el fin de constatar las configuraciones y los parámetros que al usuario final se le deben asignar como: dirección IPv6, puerta de enlace o Gateway, dirección IPv6 de DNS, nombre de dominio, etc; ya que en el equipo CORE y los equipos de distribución es donde se realiza la mayoría de las configuraciones del despliegue del Protocolo de Internet versión 6.

Asi mismo se hace mención a los equipos que funcionan en los sectores de Jardín Botánico, Obelisco, Punzara y Consultorio Jurídico; lugares en los cuales se manejan equipos de la tecnología Mikrotik y conectados mediante radio enlace desde su equipo principal Switch CORE llegando a sus usuarios finales mediante Access Point y conecciones con puntos de red fijos.

6.1.6. Descripción de los dispositivos de red: Core y Switch de Distribución

Switch (Core) WS-C6506-E: Dispone de una dirección IPv4 privada, éste enrutador facilita la comunicación de todas las Facultades Académico Administrativas (FAA) con las que cuenta la Universidad Nacional de Loja, el núcleo del backbone, un equipo dedicado al enrutamiento de los paquetes dentro de la intranet de la institución mediante el protocolo de enrutamiento OSPF (Open Shortest Path First) hacia los equipos de la siguiente capa distribución y por seguridad aplicando la técnica de VLAN.

Figura 24: Cisco CATALYST 6506-E [45].

Switch (Distribución-L3) WS-C3750X-24T-S: Consta de una dirección IPv4 privada, equipo funcionando en la capa 3 del modelo OSI, en el direccionamiento interno realizado por la institución en este equipo también se ve reflejado y por seguridad con VLAN con su respectivo nombre y ID-VLAN (Identificador de VLAN) donde cada una le corresponde un pool de direcciones IPv4 creado utilizando asignación dinámica de direcciones mediante DHCP.

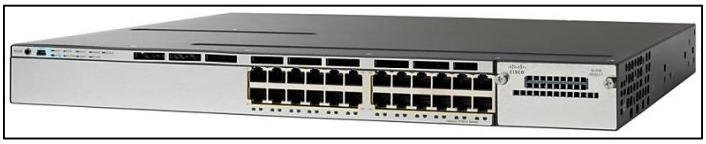


Figura 25: Cisco CATALYST 3750X-24T-S [46]

Switch (Distribución-L3) WS-C3750X-48PF-S: Cumple la misma función descrita con el equipo anterior, la única diferencia es que consta de 48 puertos y dedicado para la Facultad de la Energía específicamente sus Laboratorios, este equipo también trabaja en la capa 3 del modelo OSI con direccionamiento privado utilizando los mismos protocolos de enrutamiento descritos con anterioridad.

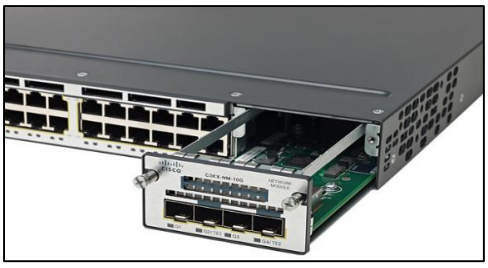


Figura 26: Cisco CATALYST 3750X-48PF-S [47].

Switch (Distribución-L3) MKR CCR1036-12G-4S: su función la cumple tanto en la Capa L2 como en la Capa L3 del Modelo OSI, consta de 12 Interfaces Ethernet, panel de pantalla táctil, manejando los mismos protocolo de enrutamiento como son DHCP, VLAN, OSPF. El equipo MKR CCR1016-12G como pertenece a la misma familia de fabricación posee las mismas características del equipo antes descrito.

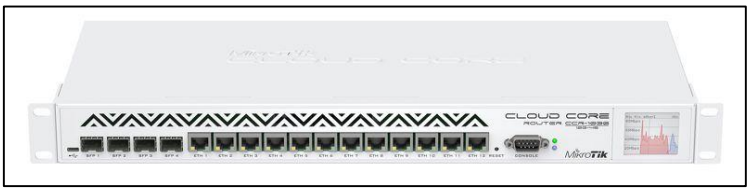


Figura 27: Mikrotik CCR1036-12G-4S [48].

Switch (Distribución-L3) MKR CRS125-24G-1S: se describe con las mismas funciones de equipo anterior, su diferencia se encuentra en el total de puertos con los que trabaja ya que son 24 Interfaces Ethernet manejando los mismos protocolos de enrutamiento y capa L2 y L3 del Modelo OSI.

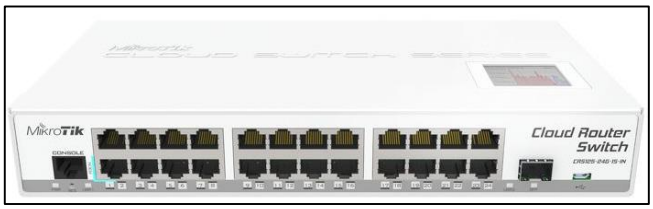


Figura 28: Mikrotik CRS125-24G-1S [48].

Switch (Acceso-L2) WS-C2960-48TT-S: Tiene una dirección IPv4 privada para realizar la administración, este dispositivo funciona en la capa 2 del modelo OSI y opera con direcciones MAC para el envío de tramas en la red. Cada servicio prestado por la institución como (DNS, DHCP, E-MAIL, PROXY, SGA, VOIP, etc) se debe al manejo interno de los equipos por parte del Departamento de Telecomunicaciones e Información facilitando la comunicación de las Facultades Académico Administrativas pudiendo así llegar los paquetes enviados por medio de la red a sus usuarios finales y personal administrativo.

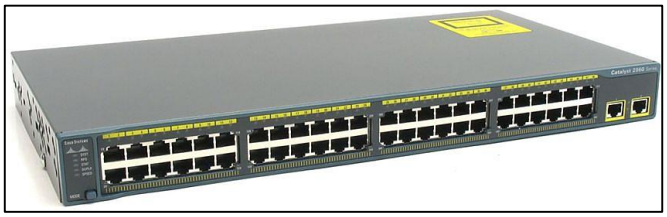


Figura 29: Cisco CATALYST 2960-48TT-S [49].

Los equipos descritos son columna vertebral dentro de la infraestructura de red de datos de la UNL, presentando en la siguiente tabla características específicas de los dispositivos de red existentes en el cuarto de telecomunicaciones.

TABLA X: CARACTERÍSTICAS DE EQUIPOS DE RED.

Nº	Dispositivo	Marca/Modelo	Puertos
1	Switch (Core)	CISCO WS-C6506-E	16

2	Switch (Distribución-L3)	CISCO WS-C3750X-24T-S	24
3	Switch (Distribución-L3)	CISCO WS-C3750X-48PF-S	48
4	Switch (Distribución-L3-L2)	MIKROTIK CCR1036-12G-4S	12
5	Switch (Distribución-L3-L2)	MIKROTIK CRS125-24G-1S	24
6	Switch (Acceso-L2)	CISCO WS-C2960-48TT-S	48

6.1.7. Distribución de dispositivos de red: Facultades de la Universidad Nacional de Loja

La Universidad Nacional de Loja se distribuye específicamente en 9 facultades utilizando equipos de red que se describió anteriormente para la interconexión, adicional a ello se agregan los sitios remotos que pertenecen a la UNL distribución que se da por cada facultad con los equipos que operan actualmente.

TABLA XI: DISTRIBUCIÓN DE LAS FACULTADES ACADÉMICO ADMINISTRATIVAS (FAA).

Nº	Facultad	Código	Dispositivo	Marca/Modelo
1	**Administración Central**	ADMS1MA0204SD01_1.0	Switch (Distribución-L3)	CISCO WS-C3750X-24T-S
2	**Educativa**	EDUS1MB0101SD01_1.0	Switch (Distribución-L3)	CISCO WS-C3750X-24T-S
3	**Jurídica_1 (Biblioteca)**	JURS2MC0801SD01_1.0	Switch (Distribución-L3)	CISCO WS-C3750X-24T-S
4	**Jurídica_2 (Economía)**	JURS2MD0602SD01_1.0	Switch (Distribución-L3)	CISCO WS-C3750X-24T-S
5	**Agropecuaria**	SW-L3-AROPECUARIA_1.0	Switch (Distribución-L3)	CISCO WS-C3750X-24T-S
6	**Modalidad de Estudios a Distancia (MED)**	SW-L3-MED_1.0	Switch (Distribución-L3)	CISCO WS-C3750X-24T-S
7	**Energía**	SW-L3-ENERGIA_1.0	Switch (Distribución-L3)	CISCO WS-C3750X-24T-S
8	**Laboratorio Energía**	SW-L3-LAB-ENERGIA_B12_1.0	Switch (Distribución-L3)	CISCO WS-C3750X-48PF-S

9	**Salud**	SW-L3-Salud_1.0	Switch (Distribución-L3)	CISCO WS-C3750X-24T-S
10	**Jardín Botánico**	MKT-JAR-BOT_1.0	Switch (Distribución-L3-L2)	CCR1036-12G-4S
11	**Obelisco**	MKT-OBELISCO_1.0	Switch (Distribución-L3-L2)	CCR1016-12G
12	**Punzara**	MKT-PUNZARA_1.0	Switch (Distribución-L3-L2)	CCR1016-12G
13	**Consultorio Jurídico**	MKT-CON-JUR_1.0	Switch (Distribución-L3-L2)	MIKROTIK CRS125-24G-1S

6.1.8. Soporte de IPv6 en los dispositivos de red

Los dispositivos de red analizados en la tabla anterior (Ver TABLA XI) son los mismos para este apartado, incluyendo un punto importante, el análisis del soporte del Protocolo de Internet versión 6 (IPv6) utilizando solo como objeto de investigación los equipos que se mencionan en el Proyecto de Titulación planteado que son el equipo Switch Core y los equipos Switch de Distribución, tomando en cuenta que ahora los dispositivos están operando en perfectas condiciones bajo el Protocolo de Internet versión 4 (IPv4).

Apoyando y reafirmando el soporte del nuevo protocolo versión 6 se pudo investigar en la página oficial de los Equipos Cisco mediante sus características y modelos la diferente gama y variedad de equipos de red que la línea CISCO ofrece. Todas las especificaciones de los equipos se exponen en el Anexo IV, indicando sus catálogos y su debido soporte con el nuevo protocolo IPv6. Se agrega una nota al pie de la página donde se puede acceder a las especificaciones de los equipos de red.

TABLA XII: SOPORTE DE IPV6 EN LOS EQUIPOS DE RED.

Nº	Dispositivo	Marca/Modelo	Soporta IPv6	
			Sí	No
1	Switch Core	WS-C6506-E[5]	✓	

[5] http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/product_data_sheet09186a0080159856.html

2	Switch (Distribución-L3)	WS-C3750X-24T-S[6]	✓	
3	Switch (Distribución-L3)	WS-C3750X-48PF-S	✓	
4	Switch (Distribución-L3-L2)	CCR1036-12G-4S	✓	
5	Switch (Acceso-L2)	WS-C2960-48TT-S[7]	✓	

6.2. OBJETIVO 2: Determinar el mecanismo de transición a utilizar entre IPv4 a IPv6

Con la creación de la nueva versión del protocolo de internet (IPv6), por la necesaria utilización y el agotamiento de las direcciones IP, se dio la creación de diferentes mecanismos para la transición y coexistencia de IPv4 a IPv6 utilizando dichos mecanismos conforme se encuentre estructurado el esquema de red y dependiendo al 100% de la estructura que manejen las instituciones o negocios en los que se quiera implementar IPv6 ya sea una transición de la versión 4 a la versión 6 o algo más drástico IPv6 en todo el segmento de red utilizando así un solo protocolo, la versión 6 de IP.

Todo lo concerniente a IPv6 se detalla en la Sección 4.1 de la Revisión Literaria utilizada, características, ventajas, desventajas, como está estructurada una dirección IPv6 y en cumplimiento con el Objetivo 2 se analizará explícitamente los mecanismos para la transición y coexistencia de ambos protocolos establecidos por al IETF.

6.2.1. Mecanismos de Transición a IPv6

Como lo menciona [37] no es previsible que IPv6 se despliegue de manera rápida, esto significa que, aunque IPv4 e IPv6 no son compatibles, deberán coexistir por un periodo de tiempo indeterminado. Dicho de otra manera los mecanismos de transición proporcionan comunicación entre ambos protocolos (IPv4 e IPv6) y viceversa, en el presente trabajo de titulación se tomó información de la IETF (Internet Engineering Task

[6] http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3750-series-switches/product_data_sheet0900aecd80371991.pdf
[7] http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-series-switches/prod_qas0900aecd80322c37.html

Force), que se centra en 3 categorías: Dual Stack (Doble Pila), Túneles y Traducción de Direcciones.

6.2.1.1. Mecanismo de Transición Dual Stack (Doble Pila)

Como su nombre lo indica Doble-Pila, significa literalmente mantener las dos pilas de protocolos donde trabajen paralela y secuencialmente en los dispositivos o equipos de red tanto IPv4 e IPv6.

El mecanismo de transición doble pila hace uso de las pilas, tanto en los host o usuarios finales como en los routers, switchs o hablando de forma general equipos de red en los que se configure el mecanismo de transición estudiado; es decir, que un host o equipos de red puede tener configurado los dos protocolos (IPv4 e IPv6) y cuando hace uso de la dirección IPv4 accede a su respectiva pila, de la misma manera cuando se usa la dirección IPv6; en lo correspondiente a los enrutadores, cada protocolo crea y administra su propia tabla de enrutamiento para poder conectarse con otro host o a internet [38].

Esta resulta ser la técnica más sencilla de implementar por lo que no requiere duplicar redes ni interfaces de red para que los sistemas accedan a la versión 4 o a la versión 6 del protocolo de internet. Sólo es necesario que los sistemas operativos de los ordenadores y equipos de red sean capaces de utilizar ambas pilas de protocolos en paralelo, distinguiendo el paquete en el momento de la recepción por medio de la cabecera de nivel de red y más concretamente a través del campo de versión de protocolo IP. En la Figura 30 se muestra la arquitectura de Doble-Pila y como funciona ambos Protocolos de Internet.

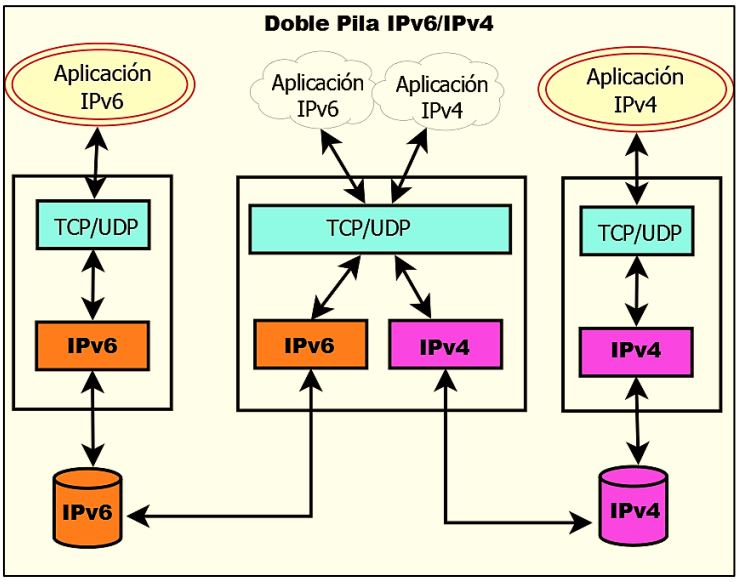


Figura 30. Mecanismo basado en Doble-Pila [Autor].

6.2.1.2. Mecanismo de Transición Túneles

El mecanismo de túneles o tunelización es una técnica que nos permite conectar redes IPv6 sobre redes IPv4, es un mecanismo en el que un paquete es encapsulado, dentro de otro tipo de paquete; es decir, podemos encapsular paquetes IPv6 dentro de paquetes IPv4. Es la forma más sencilla de configurar una conexión IPv6 a través de una red IPv4, aunque no es fácil de administrar [39].

Los extremos finales del túnel son siempre los encargados de realizar la operación de encapsulado de paquete/es IPv6 en IPv4, estos pueden ser configurados manualmente ya sea como parte de la interfaz de túnel o derivando automáticamente de la interfaz que está enviando los paquetes.

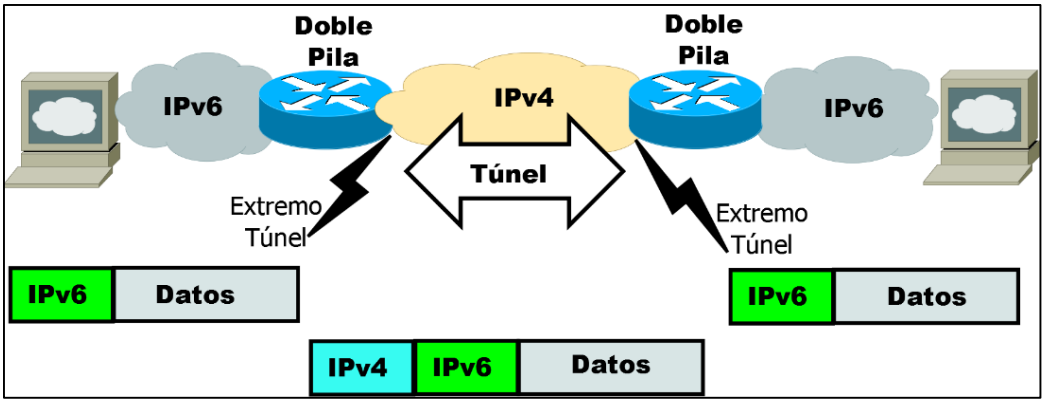


Figura 31. Dos redes IPv6 se comunican utilizando una red IPv4 [Autor].

6.2.1.3. Mecanismo de Transición Traducción de Direcciones

Este mecanismo de transición permite a un nodo que solo cuenta con la pila IPv6 habilitado dentro de una red IPv6 comunicarse con otro nodo que solo tiene la pila IPv4 habilitado dentro de una red IPv4 [27].

La cabecera IP ha de ser convertida y puede ser requerido un pool de direcciones IPv4 para proporcionar un alias al host IPv6 durante la comunicación. Sin embargo, ésta técnica requiere tener también habilitados mecanismos de traducción entre IPv4 e IPv6 en las orillas de ambas redes (enrutadores) [43]. La conversión será más compleja si la aplicación procesa las direcciones IP. La principal desventaja es que todo el peso de este mecanismo de transición recae en los equipos de red.

La traducción puede darse de dos maneras:

- **Traducción de IPV4 a IPv6**

Una descripción de esta traducción consiste en que el encabezado IPv4 del paquete es removido y reemplazado por un encabezado IPv6. En la Figura 32 muestra como es el proceso que realiza esta traducción.

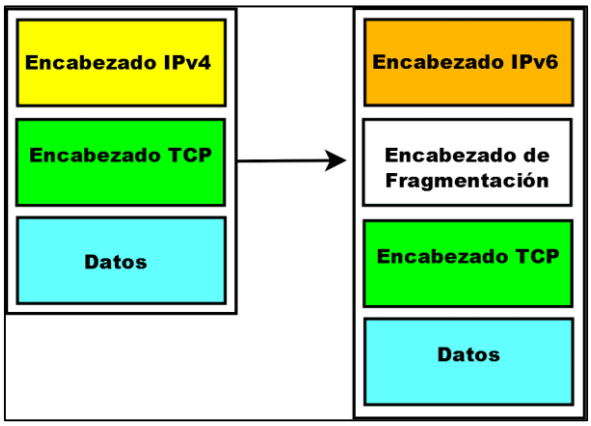


Figura 32: *Traducción de IPv4 a IPv6 [Autor].*

- **Traducción de IPv6 a IPv4**

Esta traducción IPv6 a IPv4, se da cuando el traductor recibe un datagrama IPv6 destinado a una dirección IPv4 mapeada, este traduce el encabezado IPv6 a un encabezado IPv4. Posteriormente el encabezado original es removido y sustituido por un encabezado IPv4, como se muestra en la Figura 33.

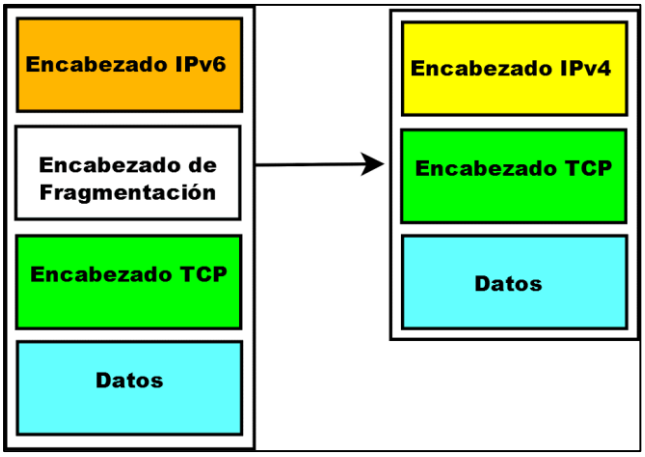


Figura 33: Traducción de IPv6 a IPv4 [Autor].

Cabe destacar que los expertos en desplegar redes de datos IPv6 no recomiendan este mecanismo de transición. Sin embargo se lo tomará en cuenta ya que se encuentra mencionado por LACNIC, organización encargada del buen funcionamiento de las redes

y gestión del nuevo protocolo IPv6, tanto para su análisis como para la selección del mecanismo de transición adecuado con los parámetros que se mencionarán más adelante.

6.2.2. Resumen de los Mecanismos de Transición

Una vez detallado cada uno de los mecanismos propuestos para la transición de IPv4 a IPv6, se presenta un cuadro resumen señalando conectividad, ventajas y desventajas de dichos mecanismos que dentro de la infraestructura de un ISP, son los más utilizados y que de una u otra manera conllevaran a la migración total de direcciones IPv6.

Se debe mencionar que la transición no siempre es la solución pero en estos momentos es la más efectiva y al desplegar estos mecanismos a gran escala puede implicar problemas que podrían limitar enormemente el rendimiento de IPv6 en comparación con una solución nativa.

TABLA XIII: RESUMEN MECANISMOS DE TRANSICIÓN.

Nombre	Tipo de Mecanismo	Conectividad	Descripción	Ventajas	Desventajas
Doble Pila	Dual Stack(Doble Pila)	Solo entre sistemas del mismo tipo (IPv4-IPv4 e IPv6-IPv6)	- Trabaja con ambos protocolos (IPv4 e IPv6). - Procesa solo los encabezados IP. - Uno de los más populares dentro de su tipo. - Se basa en DHCP y direcciones compatibles para la asignación de direcciones.	- Fácil de implementar. - Solución inminente y accesible. - Permite a los nuevos dispositivos IPv6 relacionarse rápidamente con el resto de los dispositivos.	- No trabaja en ambientes mixtos (IPv4 sobre IPv6 y viceversa). - Si la red no es IPv6, no se ve beneficiada de las características de esta versión.
6to4	Túneles	IPv6 a IPv6 sobre IPv4	- Crea túneles automáticamente. - Algoritmo más popular	- Ayuda a conectar redes IPv6 aisladas entre sí.	- Difícil controlar el tráfico circulante. - Vulnerable a ataques de

			dentro de su clase.		DoS y Spoofing.
6over4	Túneles	IPv6 a IPv6 sobre IPv4	Se comporta como una red virtual.	- Permite la autoconfiguración. - Conserva todas las características de IPv6.	- Necesita soporte de ruteo multicast (IPv4 raramente cuenta con este soporte).
SIIT(Stateless ip/icmp Translator)	Traducción	De IPv6 a IPv4 y de IPv4 a IPv6	- Para hacer dos protocolos "compatibles" realiza la traducción de encabezado. - Se necesita que lleve a cabo la tarea de traducción.	- Permite a nodos IPv4 comunicarse con nodos IPv6. - Fácil de soportar por un dispositivo. - No se afecta el Checksum de la capa de transporte. - Puede manejar paquetes encriptados, ya que no modifica capas superiores.	- Al realizar la traducción IPv6 a IPv4 se pierde muchos campos de la cabecera de IPv6 y con esto beneficios. - Se ignoran la mayoría de los encabezados de extensión. - Ya que se manejan dos protocolos, se necesita de utilizar dos tablas de ruteo diferentes. - Al trabajar con direcciones IPv4 compatibles, se reduce el campo de direccionamiento. - Se reduce el tamaño del MTU lo que genera mayor fragmentación.

6.2.3. Comparación de los Mecanismos de Transición

A los mecanismos de transición podemos evaluarlos bajo parámetros que hacen de cada mecanismo a utilizar único en su implementación, dando así una solución a los problemas encontrados en IPv4 con el despliegue de IPv6.

6.2.3.1. Parámetros a evaluar de los mecanismos de Transición

Para poder evaluar el mecanismo de transición más eficiente para el despliegue de IPv6 en el Switch CORE y Switchs de Distribución en la red de datos de la Universidad Nacional de Loja se han planteado los siguientes parámetros, resolviendo a lo siguiente:

- Escalabilidad.
- Configuración.
- Compatibilidad (hardware y software).
- Seguridad
- Interoperabilidad
- Movilidad
- Desempeño
- Aplicabilidad
- Usabilidad

Los parámetros citados son punto clave para desplegar IPv6 en la red de datos de la institución, por ello se describe cada uno a continuación:

Escalabilidad. IPv6 se puede ampliar fácilmente si se agregan Encabezados de Extensión tras el encabezado de IPv6. A diferencia del campo de opciones en el encabezado IPv4, el cual solo permite entre 0 y 10 palabras de 32 bits para las opciones, el tamaño de los encabezados de extensión de IPv6 solo está limitado por el tamaño del paquete IPv6.

Los encabezados de extensión se ubican entre el encabezado IPv6 y el encabezado del protocolo de la capa superior; esto se da, debido a los encabezados de extensión para garantizar soporte a las futuras aplicaciones, ya que si se requiere definir nuevas opciones, también nuevas cabeceras opcionales deberán ser definidas.

Configuración. Cada mecanismo de transición tiene su propia manera de estructurar sus procedimientos de comunicación con los dispositivos que soporten la utilización de un determinado mecanismo, que varía según el Sistema Operativo. Esta información ha sido recopilada en los respectivos RFC (RFC 2893, RFC 2765, RFC 2473, etc) que describen los pasos a seguir para lograr la integración de los protocolos IPv4 e IPv6.

Compatibilidad (hardware y software):

- **Hardware**. Debido al avance tecnológico, los equipos de última generación incorporan funcionalidades que facilitan la configuración de los mecanismos de

transición, es decir, soportan la utilización del protocolo IPv4 e IPv6 simultáneamente.

- **Software**. Los Sistemas Operativos actuales incorporan el soporte necesario en sus núcleos, para facilitar la configuración del mecanismo de transición más idóneo para ambos protocolos.

Seguridad. Aunque se han definido estándares de seguridad para IPv4 ninguno de ellos es obligatorio, es por esto que se han impuesto soluciones propietarias reduciendo así la estandarización de la seguridad de Internet. En IPv6 la compatibilidad con IPSec es un requisito. IPSec proporciona una solución basada en estándares en respuesta a las necesidades de seguridad de red y aumenta la interoperabilidad entre distintas implementaciones de IPv6, aporta confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública (RSA), algoritmos de cifrado (DES, 3DES, IDEA, Blowfish), algoritmos de hash (MD5, SHA-1) y certificados digitales.

Interoperabilidad. Ejecuta programas o transfiere datos entre distintas unidades funcionales de forma que se requiera el mínimo o nulo conocimiento del usuario sobre las características particulares de dichas unidades.

Este parámetro ha adquirido gran trascendencia porque la penetración de Internet a nivel universal ha hecho que se convierta en una importante necesidad la interacción entre todos los sitios conectados a la red de redes, en la actualidad se está dando una progresiva migración del protocolo IPv4 hacia IPv6 y es necesario encontrar el mecanismo de transición que cumpla esta tarea de una manera efectiva.

Movilidad. Gracias al amplio espacio de direccionamiento IPv6, es fácil asignar una dirección nueva en cada punto de conexión de los dispositivos móviles. Se introdujo la seguridad para el tráfico reencaminado y para los procesos de vinculación a las redes. La versión 6 del protocolo de internet móvil tiene una implementación más sólida que la versión 4 del protocolo de internet.

Desempeño. Se puede hacer referencia al comportamiento que tiene un mecanismo de transición específico, una vez que cumple con todos los argumentos y/o especificaciones establecidas para su utilización. Permitiendo de esta manera, comprobar su funcionalidad en entornos de producción reales.

Aplicabilidad. Este parámetro hace referencia al modo de aplicacar cada mecanismo para su evaluación, cumpliendo porcentajes estandarizados de modo que al momento

de implementar resulte beneficioso para manejar ambas pilas de protocolos tanto en IPv4 como en IPv6.

Usabilidad. Se menciona en base a los equipos que se deben y pueden utilizar para la transición, infraestructura tecnológica suficientemente alta en cuanto a equipos de red, parámetro importante que debe ser analizado ya que de eso se beneficiará el mecanismo elegido al momento de desplegar IPv6.

6.2.4. Análisis comparativo de los Mecanismos de Transición mediante sus parámetros

Para el análisis de los mecanismos de transición se toma en cuenta los parámetros propuestos (Escalabilidad, Configuración, Compatibilidad (hardware-software), Seguridad, Interoperabilidad, Movilidad, Desempeño, Aplicabilidad y Usabilidad) con los cuales se procede a determinar el mejor mecanismo de transición que permita la coexistencia de IPv4 e IPv6.

Se dio una valoración a cada uno de ellos, categorizándolos de la siguiente manera: 5-óptimo, 4-satisfactorio, 3-aceptable, 2-regular y 1-inaplicable, con lo cual obtenemos una matriz con los porcentajes de cada mecanismo, llegando a la elección del mejor.

A continuación se presenta la tabla matriz de los parámetros “Criterios de Evaluación” con su respectiva valoración.

TABLA XIV: CRITERIOS DE EVALUACIÓN.

FACTOR	ESCALA	PONDERACIÓN
Óptimo	5	Se cumplen los argumentos establecidos en su totalidad.
Satisfactorio	4	Se cumplen la mayoría de los argumentos establecidos.
Aceptable	3	Son cumplidos la mitad de los argumentos.
Regular	2	Cumple parcialmente ciertos argumentos.
Inaplicable	1	No cumple ningún argumento establecido.

Ahora se procede a evaluar cada parámetro con los mecanismos de transición seleccionados, su objetivo es realizar un análisis específico tomando como referencia la TABLA XIV, “Criterios de Evaluación”.

TABLA XV: EVALUACIÓN DE PARÁMETROS.

Parámetro	Mecanismo	Factor	Escala	Justificación
Escalabilidad	Doble Pila	Óptimo	5	Encabezados de extensión garantizan soporte a futuras aplicaciones [6].
	Túneles	Satisfactorio	4	Necesidad de configuración manual con host individuales [6].
	Traducción	Regular	2	Debe utilizar dispositivo que convierta paquetes de IPv4 a IPv6 y viceversa [41].
Configuración	Doble Pila	Óptimo	5	Consiste en tener soporte IPv6 en el kernel para su utilización [41].
	Túneles	Satisfactorio	4	Necesita que los equipos que actúen como extremos soporten IPv4 e IPv6 [6].
	Traducción	Aceptable	3	Tedioso, requiere de muchas configuraciones en los equipos [41].
Compatibilidad (Hardware)	Doble Pila	Óptimo	5	Dispositivos de última generación soportan ambos protocolos [41].
	Túneles	Óptimo	5	Dispositivos de última generación soportan ambos protocolos [41].
	Traducción	Óptimo	5	Dispositivos de última generación soportan ambos protocolos [41].
Compatibilidad (Software)	Doble Pila	Óptimo	5	El uso de versiones de S.O. actualizadas soporta IPv6.
	Túneles	Óptimo	5	El uso de versiones de S.O. actualizadas soporta IPv6.
	Traducción	Óptimo	5	El uso de versiones de S.O. actualizadas soporta IPv6.
Seguridad	Doble Pila	Óptimo	5	Los equipos que tengan habilitado doble pila, podrán transmitir información entre

				sí, sin ningún tipo de problema. Asegurando la integridad y destino sin terceros en los datos que se envíen [6].
	Túneles	Satisfactorio	4	Debido a que este mecanismo hace uso de períodos de tiempo para mantener su conectividad activa. Puede darse el caso, en que durante el envío de paquetes, el tiempo de actividad para el túnel se termine, perdiéndose la información que se estaba transmitiendo [6].
	Traducción	Satisfactorio	4	Este mecanismo también hace referencia al periodo de conectividad activo, dando así un lapso de tiempo para la pérdida de paquetes en la transmisión de los mismos [6].
Interoperabilidad	Doble Pila	Óptimo	5	Cualquier dispositivo de red administrable con soporte de IPv4 e IPv6, pueden utilizar el mecanismo.
	Túneles	Óptimo	5	Cualquier dispositivo de red administrable con soporte de IPv4 e IPv6, pueden utilizar el mecanismo.
	Traducción	Óptimo	5	Cualquier dispositivo de red administrable con soporte de IPv4 e IPv6, pueden utilizar el mecanismo.
Movilidad	Doble Pila	Satisfactorio	4	Cada nodo móvil tendrá una dirección de casa [41].
	Túneles	Satisfactorio	4	Si un nodo no es configurado no tiene acceso a peticiones en IPv6 [41].
	Traducción	Regular	2	Debe realizar la traducción en los dos sentidos para la comunicación [41].
Desempeño	Doble Pila	Satisfactorio	4	Debe verificar el tipo de dirección que se usa [6].

	Túneles	Satisfactorio	4	Tiempo influye en el encapsulado y desencapsulado de paquetes [6].
	Traducción	Regular	2	Debe tener red IPv6 nativa para llegar a sitios solo IPv4 [6].
Aplicabilidad	Doble Pila	Óptimo	5	Popular en su tipo, recomendado por empresas con años de experiencia en el manejo de protocolos IP [41].
	Túneles	Satisfactorio	4	Necesita tener configurado Doble Pila en los extremos del túnel creando complejidad al momento de ser aplicado [41].
	Traducción	Regular	2	No recomendado por expertos en desplegar IPv6. Obsoleto en su tipo [41].
Usabilidad	Doble Pila	Óptimo	5	Técnicamente no requiere equipos robustos, se utiliza la misma infraestructura física para ser desplegado [6] [41].
	Túneles	Aceptable	3	Si un equipo del extremo del túnel no cuenta con características físicas para soportar IPv6, la comunicación no se realiza [6].
	Traducción	Regular	2	Infraestructura física en equipos muy elevada, cada uno debe tener traductores incorporados para realizar la traducción de IPv4 a IPv6 y viceversa. Precios muy elevados de los equipos [41].

En la siguiente tabla se muestra la valoración individual obtenida de los parámetros para cada mecanismo de transición y que se pueda dar la coexistencia de IPv4 a IPv6.

TABLA XVI: VALORACIÓN INDIVIDUAL DE PARÁMETROS ESTABLECIDOS PARA LOS MECANISMOS DE TRANSICIÓN.

	Mecanismos de Transición para la coexistencia de IPv4 e IPv6 evaluados		
Parámetro	**Doble Pila**	**Túneles**	**Traducción**
Escalabilidad	5	4	2
Configuración	5	4	3
Compatibilidad (Hardware)	5	5	5
Compatibilidad (Software)	5	5	5
Seguridad	5	4	4
Interoperabilidad	5	5	5
Movilidad	4	4	2
Desempeño	4	4	2
Aplicabilidad	5	4	2
Usabilidad	5	3	2
Suma General	**48**	**42**	**32**
Porcentaje Total	**96%**	**84%**	**64%**

A continuación se presenta mediante gráficas los resultados obtenidos de la evaluación de cada parámetro con cada mecanismo de Transición.

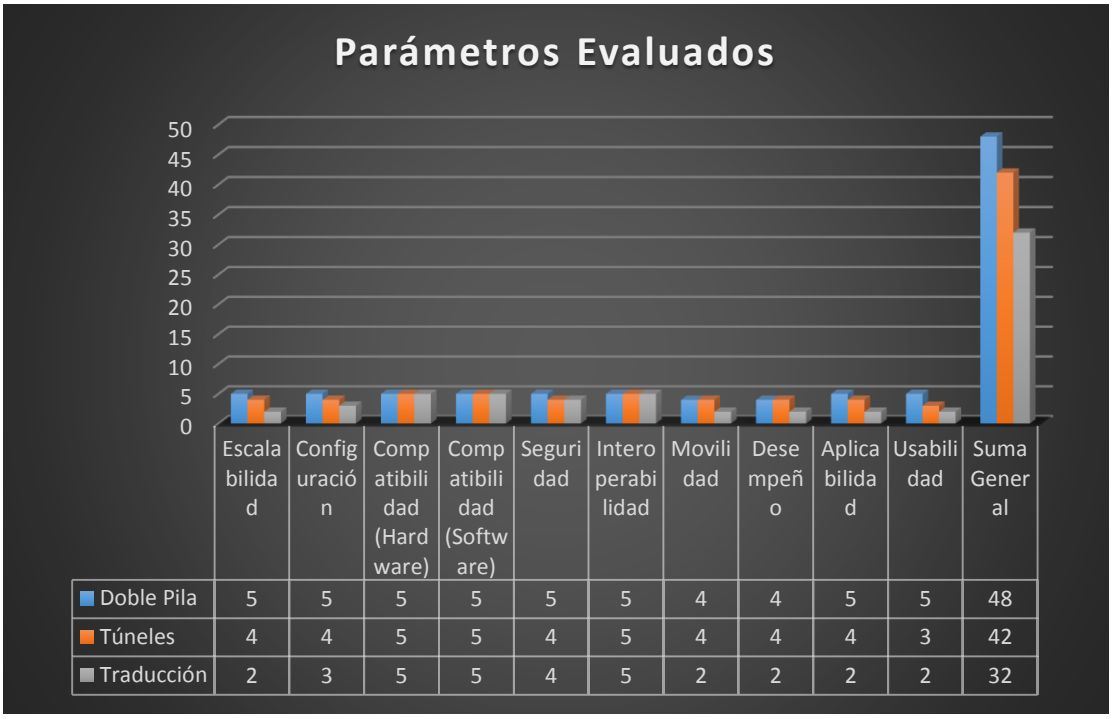


Figura 34: Valoración de parámetros de los Mecanismos de Transición.

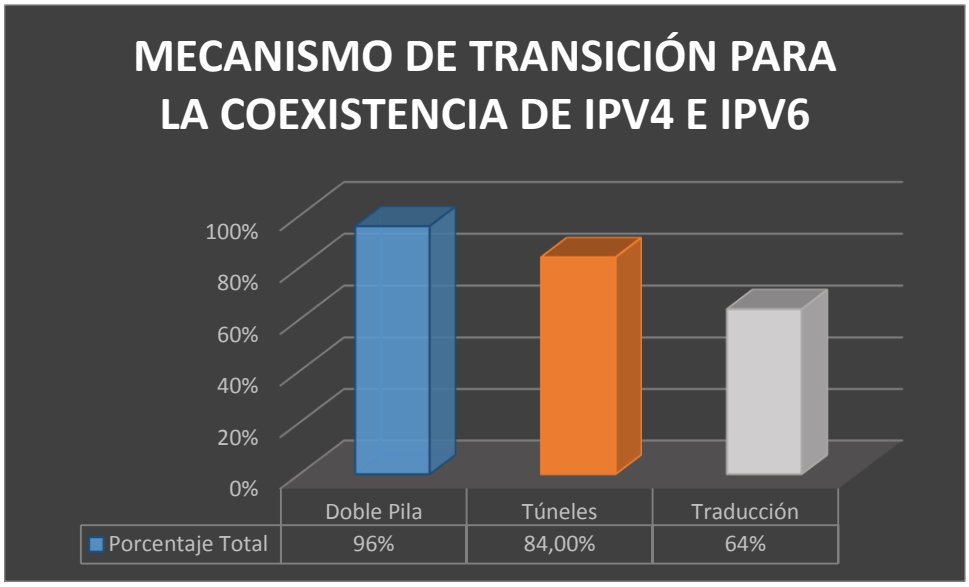


Figura 35: Porcentajes de los Mecanismos de Transición.

Los resultados obtenidos de la evaluación de los mecanismos de transición a IPv6, son los siguientes:

El mecanismo doble pila presenta el porcentaje más alto con un 96%, seguido por el mecanismo de túneles con un 84%, y finalmente con un porcentaje de 64% el mecanismo de traducción. Dichos porcentajes se los obtuvo de la suma general obtenido por cada mecanismo, comprobando así que Doble Pila es el mecanismo mejor puntuado para ser utilizado en el despliegue de IPv6 para los equipos de red de la Universidad Nacional de Loja.

Con los resultados obtenidos podemos decir que:

- Los argumentos y parámetros utilizados para los mecanismos de transición, cumplen con los requerimientos establecidos. Sin embargo, la diferencia está en los porcentajes totales de los mecanismos evaluados, donde se presentó argumentos que diferencian un mecanismo del otro. Por ejemplo, en la Seguridad de los datos el mecanismo "Túneles" y “Traducción” marca una diferencia respecto a "doble pila", debido a que su utilización se basa en períodos de tiempo y si dicho período de tiempo expira, los datos que se transmiten en ese momento tienen algún grado de alteración o pérdida. Con respecto a la Configuración de cada mecanismo; "doble pila" no presenta inconvenientes, porque para su utilización basta con tener el soporte IPv6 en el kernel, mientras que el mecanismo "Túneles" debe incorporar equipos con doble pila en sus extremos, para efectuar posteriormente la configuración que el mecanismo

túneles usa y en el mecanismo “Traducción” sus configuraciones son demasiado extensas y tediosas en los equipos a utilizar. En cuanto a la Usabilidad y Aplicabilidad varía por el equipamiento tecnológico adecuado ya que en el mecanismo de “Traducción” su infraestructura debe ser demasiada robusta e incluir traductores en los equipos de red a utilizar, mencionando que su costo es económicamente elevado para ser adquiridos. Por estas razones, los mecanismos se distinguen uno de otro, de ahí la diferencia existente en los porcentajes finales entre los mecanismos de transición evaluados.

- Se debe mencionar que la utilización del mecanismo "Doble-Pila" es apto para entornos donde se conoce explícitamente la cantidad de equipos que se usa o la infraestructura donde se realizará la implementación. Como el despliegue de IPv6 se enfoca en el dispositivo Core y en los Switchs de Distribución, "doble pila" cumple satisfactoriamente con lo requerido, proporcionando que ambos protocolos IPv4 e IPv6 trabajen al mismo tiempo, pero también se lo realizó pensando en futuras incorporaciones de equipos de red para la institución.

6.2.5. Caso de estudio aplicando el Mecanismo Doble Pila para IPv6

Se puede observar que el mecanismo para una transición en estos momentos es Doble Pila o Dual Stack, a continuación se detalla mediante la siguiente tabla algunos casos de éxito implementando IPv6 mediante el mecanismo elegido y presentando un estudio profundo en la Universidad Salesiana de Cuenca del Protocolo de Internet versión 6.

Dichos casos de éxito se los describe a continuación:

TABLA XVII: CASOS DE ÉXITO – IMPLEMENTACIÓN DOBLE PILA.

Caso de éxito	Resumen
Universidad Nacional de Chimborazo (UNACH) [50]	La universidad UNACH como entidad de educación superior en el año 2011 – 2012, puso en marcha la ejecución de un plan de estudio e implementación para la transición de IPv4 a IPv6. Al momento de la implementación, el mecanismo Dual Stack es el idóneo logrando que los servicios y equipos trabajen con IPv4 e IPv6, sin crear impacto notable para los usuarios, debido a que trabaja de manera transparente, facilitando el cambio de red sin perder

	conectividad lo que permite mejorar la calidad de servicio (QoS). Estableciendo que el tiempo de respuesta mediante consultas IPv6 sea más rápido debido a que la fragmentación se la realiza en el nodo origen y el reensamblado en los nodos finales y no en los routers como en el caso de IPv4.
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 [51]	Este trabajo refleja el impulso de promover la utilización de las nuevas tecnologías como lo es IPv6, primeramente establecer una cultura hacia el uso de buenas prácticas a nivel de seguridad de la Información llevando de forma adecuada y ordenada el proceso de transición de IPv4 a IPv6. Uno de los problemas existentes que tiene esta entidad es el agotamiento ya de sus direcciones IPv4, mediante la implementación de IPv6 lo resuelve pudiendo observar el aumento en la seguridad a nivel de capa de red, ya que el protocolo IPsec se vuelve obligatorio, y esto permite que se cree una estructura de seguridad más fuerte y por ende aplicaciones más seguras.
Propuesta de un Plan de Implementación para la migración a IPv6 en la red de la Universidad Politécnica Salesiana Sede-Cuenca [52]	Esta propuesta si bien es cierto es un Plan de implementación pero con resultados favorables para la utilización de Doble Pila como mecanismo de transición, sus resultados fueron: 1. Simulación de toda la red de la universidad mediante doble pila utilizando Packet Tracer. 2. Factible implementación por lo que sus equipos cuentan con soporte en IPv6. 3. La migración a IPv6 debe hacerse de forma gradual, establecer un periodo de transición y coexistencia entre los protocolos con el fin de reducir el impacto sobre el funcionamiento de la red.

	4. Con el plan de implementación se determinó aspectos como implementar niveles de seguridad y aspectos relevantes como la escalabilidad de la red, seguridad, configuración y administración de redes, soporte para QoS, movilidad, políticas de enrutamiento, etc.

Todos los tres casos planteados y analizados apuntan a una transición de coexistencia entre el protocolo IPv4 y el protocolo IPv6, su demanda en el aumento de dispositivos, mantener la seguridad de las redes, consultas en ambos protocolos, son aspectos importantes y necesarios, destacando como mecanismo de transición Doble Pila o Dual Stack para la implementación ya sea de forma gradual o de forma masiva.

6.3. OBJETIVO 3: Diseñar el esquema de Direccionamiento utilizando IPv6 para la red privada de la Universidad Nacional de Loja

La Universidad Nacional de Loja como entidad de Educación Superior y por la prestación de servicios mediante sus instalaciones a la comunidad universitaria tiene establecido un esquema de direccionamiento con el Protocolo de Internet versión 4 (IPv4).

Dentro del trabajo de titulación se desarrolla un esquema de direccionamiento con el nuevo Protocolo de Internet versión 6 (IPv6) tomando en cuenta la dirección IPv6 que la Universidad Nacional de Loja posee asignada por parte de CEDIA (Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado) y mostrando el esquema que actualmente está en marcha como es IPv4.

6.3.1. Direccionamiento IPv4 de la Universidad Nacional de Loja

La dirección otorgada en IPv4 para la UNL por el ISP (Proveedor de Servicios de Internet) Telconet S.A, es la subred clase B 172.16.32.0/19 para toda la intranet en el campus universitario, de la cual la Unidad de Telecomunicaciones de Información (UTI), encargado de las interconexiones de red, ha hecho uso desglosándola por rangos conforme a los requerimientos de la institución, al equipamiento de los dispositivos de networking, a las Facultades Académico Administrativas (FAA) y a sus dependencias.

También cuenta con una red de clase C 192.188.49.0/24 en IPv4 para los servicios de Internet públicos que brinda y que pueden ser accedidos desde toda la internet.

La distribución de direcciones IPv4 realizada en la institución está dada de la siguiente manera:

TABLA XVIII: DIRECCIONAMIENTO IPV4 DE LA UNIVERSIDAD NACIONAL DE LOJA.

	DATOS VLAN		DATOS RED
DISPOSITIVO	NOMBRE VLAN	ID VLAN	RED / PREFIJO
	SUBREDES: 10.X.X.X/X – 10.X.X.X/X		
SW-CORE CISCO WS-C6506-E	DEFAULT-DMZ	1	172.16.32.0/19
	ENLACE MPLS	ROUTE	10. X.X.X/X
	VLAN_ADM_B2	2	10. X.X.X/X
	UTI	3	10. X.X.X/X
	RED-ISOLADA	5	192. X.X.X/X
	ADMINISTRATIVO	10	10. X.X.X/X
	PROFESORES	20	10. X.X.X/X
	ESTUDIANTES	30	10. X.X.X/X
	VoIP	40	10. X.X.X/X
	RELOJ/IMPRESORAS	50	10. X.X.X/X
	CAMARAS	60	10. X.X.X/X
	LABORATORIOS	70	10. X.X.X/X
	EDUROAM	100	10. X.X.X/X
	UNL	101	10. X.X.X/X
	INVITADOS	102	10. X.X.X/X
	CAMPUS	103	10. X.X.X/X
	BIBLIOTECA	120	no ipaddress
	RESTRINGIDAS	200	10. X.X.X/X
	WIRELESS	210	10. X.X.X/X
	SUBREDES: 10. X.X.X/X – 10. X.X.X/X		
SW-L3-ADMCENTRAL-B2_1.0 CISCO WS-C3750X-24	**ENLACE**	ROUTE	10. X.X.X/X
	DEFAULT	1	10. X.X.X/X
	UTI	3	10. X.X.X/X
	ADMINISTRATIVO	10	10. X.X.X/X
	DOCENTES	20	10. X.X.X/X
	ESTUDIANTES	30	10. X.X.X/X
	TELEFONIA	40	10. X.X.X/X
	RELOJ/IMPRESORAS	50	10. X.X.X/X
	CAMARAS	60	10. X.X.X/X
	LABORATORIOS	70	10. X.X.X/X
	BIBLIOTECA	120	10. X.X.X/X
	RESTRINGIDO	200	10. X.X.X/X
	WIRELESS	210	10. X.X.X/X
	SUBREDES: 10. X.X.X/X – 10. X.X.X/X		
	ENLACE	ROUTE	10. X.X.X/X
	DEFAULT	1	10. X.X.X/X

SW-L3-MED_1.0 CISCO WS-C3750X-24	ADMINISTRATIVO	10	10. X.X.X/X
	PROFESORES	20	10. X.X.X/X
	ESTUDIANTES	30	10. X.X.X/X
	VoIP	40	10. X.X.X/X
	RELOJ/IMPRESORAS	50	10. X.X.X/X
	CAMARAS	60	10. X.X.X/X
	LABORATORIOS	70	10. X.X.X/X
	BIBLIOTECA	120	10. X.X.X/X
	DEFAULT/LINKSYS	200	10. X.X.X/X
	WIRELESS	210	10. X.X.X/X
	SUBREDES: 10. X.X.X/X – 10. X.X.X/X		
SW-L3-EDUCATIVA_1.0 CISCO WS-C3750X-24	ENLACE	ROUTE	10. X.X.X/X
	DEFAULT	1	10. X.X.X/X
	ADMINISTRATIVO	10	10. X.X.X/X
	PROFESORES	20	10. X.X.X/X
	ESTUDIANTES	30	10. X.X.X/X
	VoIP	40	10. X.X.X/X
	RELOJ/IMPRESORAS	50	10. X.X.X/X
	CAMARAS	60	10. X.X.X/X
	LABORATORIOS	70	10. X.X.X/X
	BIBLIOTECA	120	10. X.X.X/X
	DEFAULT/LINKSYS	200	10. X.X.X/X
	WIRELESS	210	10. X.X.X/X
	SUBREDES: 10. X.X.X/X – 10. X.X.X/X		
SW-L3-JURIDICA_1.0 CISCO WS-C3750X-24	ENLACE	ROUTE	10. X.X.X/X
	DEFAULT	1	10. X.X.X/X
	ADMINISTRATIVO	10	10. X.X.X/X
	PROFESORES	20	10. X.X.X/X
	ESTUDIANTES	30	10. X.X.X/X
	VoIP	40	10. X.X.X/X
	RELOJ/IMPRESORAS	50	10. X.X.X/X
	CAMARAS	60	10. X.X.X/X
	LABORATORIOS	70	10. X.X.X/X
	BIBLIOTECA	120	10. X.X.X/X
	DEFAULT/LINKSYS	200	10. X.X.X/X
	WIRELESS	210	10. X.X.X/X
	SUBREDES: 10. X.X.X/X – 10. X.X.X/X		
SW-L3_JURIDICA_B10_1.0 CISCO WS-C3750X-24	ENLACE	ROUTE	10. X.X.X/X
	DEFAULT	1	10. X.X.X/X
	ADMINISTRATIVO	10	10. X.X.X/X
	PROFESORES	20	10. X.X.X/X
	ESTUDIANTES	30	10. X.X.X/X
	VoIP	40	10. X.X.X/X
	RELOJ/IMPRESORAS	50	10. X.X.X/X
	CAMARAS	60	10. X.X.X/X
	LABORATORIOS	70	10. X.X.X/X
	BIBLIOTECA	120	10. X.X.X/X

	DEFAULT/LINKSYS	200	10.1 X.X.X/X
	WIRELESS	210	10. X.X.X/X
	SUBREDES: 10. X.X.X/X – 10. X.X.X/X		
SW-L3-AGROPECUARIA_1.0 CISCO WS-C3750X-24	ENLACE	ROUTE	10. X.X.X/X
	DEFAULT	1	10. X.X.X/X
	ADMINISTRATIVO	10	10. X.X.X/X
	PROFESORES	20	10. X.X.X/X
	ESTUDIANTES	30	10. X.X.X/X
	VoIP	40	10. X.X.X/X
	RELOJ/IMPRESORAS	50	10. X.X.X/X
	CAMARAS	60	10. X.X.X/X
	LABORATORIOS	70	10. X.X.X/X
	BIBLIOTECA	120	10. X.X.X/X
	DEFAULT/LINKSYS	200	10. X.X.X/X
	WIRELESS	210	10. X.X.X/X
	SUBREDES: 10. X.X.X/X – 10. X.X.X/X		
SW-L3-ENERGIA_1.0 CISCO WS-C3750X-24	ENLACE	ROUTE	10. X.X.X/X
	DEFAULT	1	10. X.X.X/X
	ADMINISTRATIVO	10	10. X.X.X/X
	DOCENTES	20	10. X.X.X/X
	ESTUDIANTES	30	10. X.X.X/X
	TELEFONIA	40	10. X.X.X/X
	IMPRESORAS-RELOJ	50	10. X.X.X/X
	CAMARAS	60	10. X.X.X/X
	LABORATORIOS	70	10. X.X.X/X
	BIBLIOTECA	120	10. X.X.X/X
	WIRELESS-NO	200	10. X.X.X/X
	WIRELESS	210	10. X.X.X/X
	SUBREDES: 10. X.X.X/X – 10. X.X.X/X		
SW-L3-LAB-ENERGIA_1.0 CISCO WS-C3750X-48PF-S	ENLACE	ROUTE	10. X.X.X/X
	DEFAULT	1	10. X.X.X/X
	ADMINISTRATIVO	10	10. X.X.X/X
	DOCENTES	20	10. X.X.X/X
	ESTUDIANTES	30	10. X.X.X/X
	TELEFONIA	40	10. X.X.X/X
	IMPRESORAS-RELOJ	50	10. X.X.X/X
	CAMARAS	60	10. X.X.X/X
	LABORATORIOS	70	10. X.X.X/X
	BIBLIOTECA	120	10. X.X.X/X
	DEFAULT/LINKSYS	200	10. X.X.X/X
	SERVIDORES	300	10. X.X.X/X
	WIRELESS	210	10. X.X.X/X
	SUBREDES: 10. X.X.X/X – 10. X.X.X/X - 10. X.X.X/X		
SW-L3-SALUD_1.0 CISCO WS-3750X-24	ENLACE-ADM-SAL	ROUTE	10. X.X.X/X
	ENLACE MPLS	ROUTE	10. X.X.X/X
	DEFAULT	1	10. X.X.X/X

	ADMINISTRATIVO	10	10. X.X.X/X
	DOCENTES	20	10. X.X.X/X
	ESTUDIANTES	30	10. X.X.X/X
	TELEFONIA	40	10. X.X.X/X
	IMPRESORAS-RELOJ	50	10. X.X.X/X
	CAMARAS	60	10. X.X.X/X
	LABORATORIOS	70	10. X.X.X/X
	BIBLIOTECA	120	10. X.X.X/X
	WIRELESS-NO	200	10. X.X.X/X
	WIRELESS	210	10. X.X.X/X
	WIRELLES-WLC		10. X.X.X/X
	SUBREDES: 10. X.X.X/X		
SW-L3-CON_MOTUPE_1.0 MIKROTIK CRS125-24G-1S-RM	ENLACE WIRELESS		10. X.X.X/X
	ENLACE MPLS		10. X.X.X/X
	MOTUPE	97	10. X.X.X/X
	MOTUPE		10. X.X.X/X
	MOTUPE		10. X.X.X/X
	MOTUPE		10. X.X.X/X
	SUBREDES: 10. X.X.X/X		
SW-L3-CON_JURIDICO_1.0 MIKROTIK CRS125-24G-1S-RM	ENLACE		10. X.X.X/X
	ADMINISTRATIVOS	10	10. X.X.X/X
	ESTUDIATES	30	10. X.X.X/X
	RELOJ/IMPRESORAS	50	10. X.X.X/X
	WIRELESS	210	10. X.X.X/X
	SUBREDES: 10. X.X.X/X - CAMPUS PRINCIPAL UNL		
MKT-JAR-BOT_1.0	ENLACE		10. X.X.X/X
	JARDIN BOTANICO		10. X.X.X/X
	JARDIN BOTANICO		10. X.X.X/X
MKT-OBELISCO_1.0	ENLACE		10. X.X.X/X
	OBELISCO		10. X.X.X/X
	OBELISCO		10. X.X.X/X
MKT-PUNZARA_1.0	ENLACE		10. X.X.X/X
	PUNZARA		10. X.X.X/X
	PUNZARA		10. X.X.X/X
	PUNZARA		10. X.X.X/X

Dentro de cada Facultad Académico Administrativa que tiene la Universidad Nacional de Loja se asigna un equipo, en este caso un Switch de Capa 3 (L3) para la conexión y envío de información dentro de la institución, si bien es cierto la distribución está dada mediante VLAN creando su respectivo rango de direcciones con el protocolo dinámico DHCP. El enrutamiento se maneja mediante el Protocolo OSPFv2 en los equipos de red de la Capa de Núcleo y la Capa de Distribución.

6.3.2. Asignación de la dirección IPv6 a la Universidad Nacional de Loja

La Universidad Nacional de Loja ya tiene asignado una dirección IPv6, a continuación se detalla cómo es asignada dicha dirección.

6.3.2.1. Requisitos en la Asignación de una dirección IPv6[8]

Existen una serie de pasos a seguir para recibir y solicitar recursos a LACNIC (Registros de Direcciones de Internet para Latinoamérica y el Caribe), también se debe cumplir una serie de requisitos para cada tipo de solicitud como:

1. Ser una organización ubicada en la región de América Latina y Caribe.
2. Se pueden solicitar: ASN (Sistema de Número Autónomo), IPv4/IPv6 por parte de ISP, IPv4/IPv6 por parte de usuarios finales.
3. Rellenar el formulario correspondiente y enviar a hostmaster@lacnic.net
4. Aprobación de la solicitud por parte de LACNIC.
5. Pago del recurso solicitado.
6. Firma de un Acuerdo de Servicios con LACNIC.

Para la asignación de direcciones a un Proveedor de Servicio de Internet (ISP) como lo es Telconet S.A y como bloque mínimo asignado es un /32, debe cumplir algunos requisitos como:

1. Ser un LIR (Registrador Local de Internet) que asigna direcciones a sus usuarios.
2. No ser un usuario final.
3. Documentar un plan detallado sobre servicios y conectividad en IPv6 a ofrecer a clientes.
4. Anunciar en el sistema de rutas inter-dominio de Internet el bloque asignado, con mínima desagregación posible, en un plazo no mayor a 12 meses.
5. Ofrecer servicios en IPv6 a clientes localizados físicamente en la región de LACNIC en un plazo no mayor de 24 meses.

Para la asignación de un bloque de direcciones a un usuario final se entrega como bloque mínimo un /48 y máximo un /32 debiendo cumplir con una serie de requisitos y haciendo hincapié a dos tipos de usuarios finales como:

Usuarios finales con asignaciones IPv4 portables previas de LACNIC:

1. LACNIC asignará bloques de direcciones IPv6 portables directamente.

[8] http://www.lacnic.net/web/lacnic/manual-4

Usuarios finales sin asignaciones IPv4 portables previas de LACNIC, prefijo IPv6 para la Universidad Nacional de Loja.

1. No ser un LIR o ISP.
2. En caso de anunciar el bloque designado en el sistema de rutas inter-dominio de internet, la organización receptora deberá anunciar un único bloque, que agregue toda la asignación de direcciones IPv6 recibida.
3. Proveer información detallada mostrando como el bloque solicitado será utilizado dentro de tres, seis y doce meses.
4. Entregar planes de direccionamiento por al menos un año, y números de terminales sobre cada subred.
5. Entregar una descripción detallada de la topología de la red.
6. Realizar una descripción detallada de los planes de encaminamiento de la red, incluyendo los protocolos de encaminamiento a ser usados, así también como cualquier limitación existente.

Prefijo IPv6 2800:68::/32. CEDIA (Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado)[9] dispone del prefijo IPv6 2800:68::/32 asignado por LACNIC, es decir igual que un LIR, este rango se ha subdividido en bloques más pequeños para las instituciones miembros del CEDIA, estos bloques son /48.

Estas asignaciones se han realizado tomando en cuenta el RFC (Request for Comment, Petición de Comentarios) 3177. CEDIA puede tener hasta 65536 instituciones con redes diferentes, para que se acabe el /32 asignado (por algo se dice que IPv6 tiene IP para todo mundo).

Prefijo IPv6 2800:68:7::/48. El prefijo IPv6 asignado por CEDIA a la Universidad Nacional de Loja es 2800:68:7::/48, con ello la institución cuenta con 65536 redes internas diferentes de prefijo IPv6 /64 y cada uno de estos puede tener un total de 18446744073709551616 direcciones IPv6, un número difícil de leer.

En el análisis realizado de los Mecanismos de Transición y llegando a la conclusión de que Doble Pila es el mejor para su implementación dentro de la Universidad Nacional de Loja, cada nodo contendrá dos direcciones de red una en IPv4 y la otra en IPv6, con esto se asegura la conectividad entre los nodos es decir cuando no sea posible

[9] https://www.cedia.edu.ec/es/

comunicar con un nodo IPv6 se lo podrá realizar mediante el nodo IPv4 y viceversa ya que en la red estarán funcionando ambas pilas (IPv4 e Ipv6).

6.3.3. Plan de direccionamiento de IPv6 en la Universidad Nacional de Loja

La Universidad Nacional de Loja como se lo mencionó anteriormente tiene asignado un prefijo por parte de su proveedor CEDIA, que es: 2800:0068:0007:0:0:0:0:0/48, dirección que a simple vista se ve difícil de leer e interpretar pero aplicando las técnicas expuestas en la Sección 4.1.5 acerca de la sintaxis que se puede manejar en las direcciones IPv6 podemos agrupar los ceros y obviar los que estén a la izquierda quedando de la siguiente manera: 2800:68:7::/48 lo que permite a la institución contar con 65536 redes en IPv6.

El direccionamiento se lo realizó pensando en el Modelo Jerárquico de la institución distribuido en el campus universitario lo cual fue expuesto y estudiado en el apartado de la Situación Actual dentro del Objetivo 1, considerando las FAA (Facultades Académico Administrativas) y las dependencias con las que cuenta la Universidad.

En reunión mantenida con el personal encargado de la Unidad de Telecomunicaciones e Información (UTI) se tomó como referencia los dispositivos de red como estructura principal para el despliegue de IPv6 en la intranet, empezando a desglosar la dirección asignada /48 en un /56 para cada Facultad llegando a un /64 para las redes locales (LAN), usuarios finales; agrupando en este rango de direcciones las suficientes para cada facultad y también el poder asignar nuevas direcciones si en un futuro aumentan nuevas facultades y equipos de red para la institución. Se tomó en consideración los consejos dados por parte de la IETF quien recomienda para una institución educativa de nivel superior el esquema que se planteó.

6.3.4. Direccionamiento IPv6 en el dispositivo Core y Switchs de Distribución para la Universidad Nacional de Loja

La siguiente tabla muestra el direccionamiento IPv6 realizado para la institución desglosándola por Facultades, tomando como referencia en la mayor parte los nombres asignados mediante el direccionamiento IPv4 que actualmente está en marcha descrito en la TABLA XVIII de la Sección 6.3.1.

En IPv6 como en IPv4 también existe un prefijo específicamente utilizado para documentación (Prefijo de documentación: 2001:db8::/32) estudiado en la Sección 4.1.6.1 y es el que se está utilizando para elaborar su direccionamiento y mostrar los resultados obtenidos.

TABLA XIX: DIRECCIONAMIENTO IPV6 PARA LA UNIVERSIDAD NACIONAL DE LOJA.

	DATOS VLAN	DATOS RED	
DISPOSITIVO	NOMBRE VLAN	RED / PREFIJO	GATEWAY/SVI
	IPv6: 2001:DB8:3003:AC::/56		
SW-CORE CISCO WS-C6506-E	LIBRE	2001:DB8:3003:ACA1::/64	
	ROUTE ASA	2001:DB8:3003:ACA2::/64	2001:DB8:3003:ACA2::FEFF/64
	MPLS	2001:DB8:3003:ACA3::/64	
	GESTIÓN	2001:DB8:3003:ACA4::/64	
	DMZ	2001:DB8:3003:ACA5::/64	
	EDUROAM	2001:DB8:3003:ACA6::/64	
	UNL	2001:DB8:3003:ACA7::/64	
	INVITADOS	2001:DB8:3003:ACA8::/64	
	CAMPUS	2001:DB8:3003:ACA9::/64	
	RED WLAN	2001:DB8:3003:ACAA::/64	2001:DB8:3003:ACAA::FEFF/64
	IPv6: 2001:DB8:3003:AD::/56		
ENLACE - ROUTE SWITCH CORE - SWITCH DISTRIBUCIÓN	LIBRE	2001:DB8:3003:ADA1::/64	
	ADMS1MA0204SD01_1.0	2001:DB8:3003:ADA2::/64	2001:DB8:3003:ADA2::FFFF/64
	EDUS1MB0101SD01_1.0	2001:DB8:3003:ADA3::/64	2001:DB8:3003:ADA3::FFFF/64
	JURS2MC0801SD01_1.0	2001:DB8:3003:ADA4::/64	2001:DB8:3003:ADA4::FFFF/64
	JURS2MD0602SD01_1.0	2001:DB8:3003:ADA5::/64	2001:DB8:3003:ADA5::FFFF/64
	AGRS1MG0301SD01_1.0	2001:DB8:3003:ADA6::/64	2001:DB8:3003:ADA6::FFFF/64
	MEDS2MD0101SD01_1.0	2001:DB8:3003:ADA7::/64	2001:DB8:3003:ADA7::FFFF/64
	ENES2MD0301SD01_1.0	2001:DB8:3003:ADA8::/64	2001:DB8:3003:ADA8::FFFF/64
	ENES2MD1202SD01_1.0	2001:DB8:3003:ADA9::/64	2001:DB8:3003:ADA9::FFFF/64
	SALS1MA0302SD01_1.0	2001:DB8:3003:ADAA::/64	2001:DB8:3003:ADAA::FFFF/64
	MKT-JAR-BOT_1.0	2001:DB8:3003:ADAB::/64	2001:DB8:3003:ADAB::FFFF/64
	MKT-OBELISCO_1.0	2001:DB8:3003:ADAC::/64	2001:DB8:3003:ADAC::FFFF/64
	MKT-PUNZARA_1.0	2001:DB8:3003:ADAD::/64	2001:DB8:3003:ADAD::FFFF/64
	MKT-CON-JUR_1.0	2001:DB8:3003:ADAE::/64	2001:DB8:3003:ADAE::FFFF/64
	MKT-MOTUPE_1.0	2001:DB8:3003:ADAF::/64	2001:DB8:3003:ADAF::FFFF/64
	CENTRO DE FORMACIÓN ZAPOTEPAMBA	2001:DB8:3003:AD10::/64	2001:DB8:3003:AD10::FFFF/64
	EL PADMI	2001:DB8:3003:AD11::/64	2001:DB8:3003:AD11::FFFF/64
	IPV6: 2001:DB8:3003:1::/56		
SW-L3-ADMCENTRAL-B1_1.0 CISCO WS-C3750X-24	ENLACE	2001:DB8:3003:ADA2::/64	2001:DB8:3003:ADA2::FFFE/64
	LIBRE	2001:DB8:3003:1A1::/64	
	LIBRE	2001:DB8:3003:1A2::/64	
	GESTIÓN (Nativa)	2001:DB8:3003:1A3::/64	2001:DB8:3003:1A3::FFFF/64
	UTI	2001:DB8:3003:1A4::/64	2001:DB8:3003:1A4::FFFF/64
	ADMINISTRATIVO	2001:DB8:3003:1A5::/64	2001:DB8:3003:1A5::FFFF/64
	DOCENTES	2001:DB8:3003:1A6::/64	2001:DB8:3003:1A6::FFFF/64
	ESTUDIANTES	2001:DB8:3003:1A7::/64	2001:DB8:3003:1A7::FFFF/64
	VoIP	2001:DB8:3003:1A8::/64	2001:DB8:3003:1A8::FFFF/64
	IMPRESORAS	2001:DB8:3003:1A9::/64	2001:DB8:3003:1A9::FFFF/64
	CAMARAS	2001:DB8:3003:1AA::/64	2001:DB8:3003:1AA::FFFF/64
	LABORATORIOS	2001:DB8:3003:1AB::/64	2001:DB8:3003:1AB::FFFF/64
	BIBLIOTECA	2001:DB8:3003:1AC::/64	2001:DB8:3003:1AC::FFFF/64

	WIFI-MULTIMARCA	2001:DB8:3003:1AD::/64	2001:DB8:3003:1AD::FFFF/64
	WIFI-WLC	2001:DB8:3003:1AE::/64	2001:DB8:3003:1AE::FFFF/64
	IPV6: 2001:DB8:3003:2::/56		
SW-L3-EDUCATIVA_1.0 CISCO WS-C3750X-24	ENLACE	2001:DB8:3003:ADA3::/64	2001:DB8:3003:ADA3::FFFE/64
	LIBRE	2001:DB8:3003:2A1::/64	
	LIBRE	2001:DB8:3003:2A2::/64	
	GESTIÓN (Nativa)	2001:DB8:3003:2A3::/64	2001:DB8:3003:2A3::FFFF/64
	ADMINISTRATIVO	2001:DB8:3003:2A4::/64	2001:DB8:3003:2A4::FFFF/64
	DOCENTES	2001:DB8:3003:2A5::/64	2001:DB8:3003:2A5::FFFF/64
	ESTUDIANTES	2001:DB8:3003:2A6::/64	2001:DB8:3003:2A6::FFFF/64
	VoIP	2001:DB8:3003:2A7::/64	2001:DB8:3003:2A7::FFFF/64
	IMPRESORAS	2001:DB8:3003:2A8::/64	2001:DB8:3003:2A8::FFFF/64
	CAMARAS	2001:DB8:3003:2A9::/64	2001:DB8:3003:2A9::FFFF/64
	LABORATORIOS	2001:DB8:3003:2AA::/64	2001:DB8:3003:2AA::FFFF/64
	BIBLIOTECA	2001:DB8:3003:2AB::/64	2001:DB8:3003:2AB::FFFF/64
	WIFI-MULTIMARCA	2001:DB8:3003:2AC::/64	2001:DB8:3003:2AC::FFFF/64
	WIFI-WLC	2001:DB8:3003:2AD::/64	2001:DB8:3003:2AD::FFFF/64
	IPV6: 2001:DB8:3003:3::/56		
SW-L3-JURIDICA_01_BIBLIOTECA CISCO WS-C3750X-24	ENLACE	2001:DB8:3003:ADA4::/64	2001:DB8:3003:ADA4::FFFE/64
	LIBRE	2001:DB8:3003:3A1::/64	
	LIBRE	2001:DB8:3003:3A2::/64	
	GESTIÓN (Nativa)	2001:DB8:3003:3A3::/64	2001:DB8:3003:3A3::FFFF/64
	ADMINISTRATIVO	2001:DB8:3003:3A4::/64	2001:DB8:3003:3A4::FFFF/64
	DOCENTES	2001:DB8:3003:3A5::/64	2001:DB8:3003:3A5::FFFF/64
	ESTUDIANTES	2001:DB8:3003:3A6::/64	2001:DB8:3003:3A6::FFFF/64
	VoIP	2001:DB8:3003:3A7::/64	2001:DB8:3003:3A7::FFFF/64
	IMPRESORAS	2001:DB8:3003:3A8::/64	2001:DB8:3003:3A8::FFFF/64
	CAMARAS	2001:DB8:3003:3A9::/64	2001:DB8:3003:3A9::FFFF/64
	LABORATORIOS	2001:DB8:3003:3AA::/64	2001:DB8:3003:3AA::FFFF/64
	BIBLIOTECA	2001:DB8:3003:3AB::/64	2001:DB8:3003:3AB::FFFF/64
	WIFI-MULTIMARCA	2001:DB8:3003:3AC::/64	2001:DB8:3003:3AC::FFFF/64
	WIFI-WLC	2001:DB8:3003:3AD::/64	2001:DB8:3003:3AD::FFFF/64
	IPV6: 2001:DB8:3003:4::/56		
SW-L3_JURIDICA_B10_02 CISCO WS-C3750X-24	ENLACE	2001:DB8:3003:ADA5::/64	2001:DB8:3003:ADA5::FFFE/64
	LIBRE	2001:DB8:3003:4A1::/64	
	LIBRE	2001:DB8:3003:4A2::/64	
	GESTIÓN (Nativa)	2001:DB8:3003:4A3::/64	2001:DB8:3003:4A3::FFFF/64
	ADMINISTRATIVO	2001:DB8:3003:4A4::/64	2001:DB8:3003:4A4::FFFF/64
	DOCENTES	2001:DB8:3003:4A5::/64	2001:DB8:3003:4A5::FFFF/64
	ESTUDIANTES	2001:DB8:3003:4A6::/64	2001:DB8:3003:4A6::FFFF/64
	VoIP	2001:DB8:3003:4A7::/64	2001:DB8:3003:4A7::FFFF/64
	IMPRESORAS	2001:DB8:3003:4A8::/64	2001:DB8:3003:4A8::FFFF/64
	CAMARAS	2001:DB8:3003:4A9::/64	2001:DB8:3003:4A9::FFFF/64
	LABORATORIOS	2001:DB8:3003:4AA::/64	2001:DB8:3003:4AA::FFFF/64
	BIBLIOTECA	2001:DB8:3003:4AB::/64	2001:DB8:3003:4AB::FFFF/64
	WIFI-MULTIMARCA	2001:DB8:3003:4AC::/64	2001:DB8:3003:4AC::FFFF/64
	WIFI-WLC	2001:DB8:3003:4AD::/64	2001:DB8:3003:4AD::FFFF/64

	IPV6: 2001:DB8:3003:5::/56		
SW-L3-AGROPECUARIA_1.0 CISCO WS-C3750X-24	ENLACE	2001:DB8:3003:ADA6::/64	2001:DB8:3003:ADA6::FFFE/64
	LIBRE	2001:DB8:3003:5A1::/64	
	LIBRE	2001:DB8:3003:5A2::/64	
	GESTIÓN (Nativa)	2001:DB8:3003:5A3::/64	2001:DB8:3003:5A3::FFFF/64
	ADMINISTRATIVO	2001:DB8:3003:5A4::/64	2001:DB8:3003:5A4::FFFF/64
	DOCENTES	2001:DB8:3003:5A5::/64	2001:DB8:3003:5A5::FFFF/64
	ESTUDIANTES	2001:DB8:3003:5A6::/64	2001:DB8:3003:5A6::FFFF/64
	VoIP	2001:DB8:3003:5A7::/64	2001:DB8:3003:5A7::FFFF/64
	IMPRESORAS	2001:DB8:3003:5A8::/64	2001:DB8:3003:5A8::FFFF/64
	CAMARAS	2001:DB8:3003:5A9::/64	2001:DB8:3003:5A9::FFFF/64
	LABORATORIOS	2001:DB8:3003:5AA::/64	2001:DB8:3003:5AA::FFFF/64
	BIBLIOTECA	2001:DB8:3003:5AB::/64	2001:DB8:3003:5AB::FFFF/64
	WIFI-MULTIMARCA	2001:DB8:3003:5AC::/64	2001:DB8:3003:5AC::FFFF/64
	WIFI-WLC	2001:DB8:3003:5AD::/64	2001:DB8:3003:5AD::FFFF/64
	IPV6: 2001:DB8:3003:6::/56		
SW-L3-MED_1.0 CISCO WS-C3750X-24	ENLACE	2001:DB8:3003:ADA7::/64	2001:DB8:3003:ADA7::FFFE/64
	LIBRE	2001:DB8:3003:6A1::/64	
	LIBRE	2001:DB8:3003:6A2::/64	
	GESTIÓN (Nativa)	2001:DB8:3003:6A3::/64	2001:DB8:3003:6A3::FFFF/64
	ADMINISTRATIVO	2001:DB8:3003:6A4::/64	2001:DB8:3003:6A4::FFFF/64
	DOCENTES	2001:DB8:3003:6A5::/64	2001:DB8:3003:6A5::FFFF/64
	ESTUDIANTES	2001:DB8:3003:6A6::/64	2001:DB8:3003:6A6::FFFF/64
	VoIP	2001:DB8:3003:6A7::/64	2001:DB8:3003:6A7::FFFF/64
	IMPRESORAS	2001:DB8:3003:6A8::/64	2001:DB8:3003:6A8::FFFF/64
	CAMARAS	2001:DB8:3003:6A9::/64	2001:DB8:3003:6A9::FFFF/64
	LABORATORIOS	2001:DB8:3003:6AA::/64	2001:DB8:3003:6AA::FFFF/64
	BIBLIOTECA	2001:DB8:3003:6AB::/64	2001:DB8:3003:6AB::FFFF/64
	WIFI-MULTIMARCA	2001:DB8:3003:6AC::/64	2001:DB8:3003:6AC::FFFF/64
	WIFI-WLC	2001:DB8:3003:6AD::/64	2001:DB8:3003:6AD::FFFF/64
	IPV6: 2001:DB8:3003:7::/56		
SW-L3-ENERGIA_1.0 CISCO WS-C3750X-24	ENLACE	2001:DB8:3003:ADA8::/64	2001:DB8:3003:ADA8::FFFE/64
	LIBRE	2001:DB8:3003:7A1::/64	
	LIBRE	2001:DB8:3003:7A2::/64	
	GESTIÓN (Nativa)	2001:DB8:3003:7A3::/64	2001:DB8:3003:7A3::FFFF/64
	ADMINISTRATIVO	2001:DB8:3003:7A4::/64	2001:DB8:3003:7A4::FFFF/64
	DOCENTES	2001:DB8:3003:7A5::/64	2001:DB8:3003:7A5::FFFF/64
	ESTUDIANTES	2001:DB8:3003:7A6::/64	2001:DB8:3003:7A6::FFFF/64
	VoIP	2001:DB8:3003:7A7::/64	2001:DB8:3003:7A7::FFFF/64
	IMPRESORAS	2001:DB8:3003:7A8::/64	2001:DB8:3003:7A8::FFFF/64
	CAMARAS	2001:DB8:3003:7A9::/64	2001:DB8:3003:7A9::FFFF/64
	LABORATORIOS	2001:DB8:3003:7AA::/64	2001:DB8:3003:7AA::FFFF/64
	BIBLIOTECA	2001:DB8:3003:7AB::/64	2001:DB8:3003:7AB::FFFF/64
	WIFI-MULTIMARCA	2001:DB8:3003:7AC::/64	2001:DB8:3003:7AC::FFFF/64
	WIFI-WLC	2001:DB8:3003:7AD::/64	2001:DB8:3003:7AD::FFFF/64
	IPV6: 2001:DB8:3003:8::/56		

SW-L3-LAB-ENERGIA_B12_1.0 CISCO WS-C3750X-48PF-S	ENLACE	2001:DB8:3003:ADA9::/64	2001:DB8:3003:ADA9::FFFE/64
	LIBRE	2001:DB8:3003:8A1::/64	
	LIBRE	2001:DB8:3003:8A2::/64	
	GESTIÓN (Nativa)	2001:DB8:3003:8A3::/64	2001:DB8:3003:8A3::FFFF/64
	ADMINISTRATIVO	2001:DB8:3003:8A4::/64	2001:DB8:3003:8A4::FFFF/64
	DOCENTES	2001:DB8:3003:8A5::/64	2001:DB8:3003:8A5::FFFF/64
	ESTUDIANTES	2001:DB8:3003:8A6::/64	2001:DB8:3003:8A6::FFFF/64
	VoIP	2001:DB8:3003:8A7::/64	2001:DB8:3003:8A7::FFFF/64
	IMPRESORAS	2001:DB8:3003:8A8::/64	2001:DB8:3003:8A8::FFFF/64
	CAMARAS	2001:DB8:3003:8A9::/64	2001:DB8:3003:8A9::FFFF/64
	LABORATORIOS	2001:DB8:3003:8AA::/64	2001:DB8:3003:8AA::FFFF/64
	BIBLIOTECA	2001:DB8:3003:8AB::/64	2001:DB8:3003:8AB::FFFF/64
	WIFI-MULTIMARCA	2001:DB8:3003:8AC::/64	2001:DB8:3003:8AC::FFFF/64
	SERVIDORES	2001:DB8:3003:8AD::/64	2001:DB8:3003:8AD::FFFF/64
	WIFI-WLC	2001:DB8:3003:8AE::/64	2001:DB8:3003:8AE::FFFF/64
	IPV6: 2001:DB8:3003:9::/56		
SW-L3-SALUD_1.0 CISCO WS-3750X-24	ENLACE	2001:DB8:3003:ADAA::/64	2001:DB8:3003:ADAA::FFFE/64
	LIBRE	2001:DB8:3003:9A1::/64	
	LIBRE	2001:DB8:3003:9A2::/64	
	MPLS	2001:DB8:3003:9A3::/64	
	GESTIÓN (Nativa)	2001:DB8:3003:9A4::/64	2001:DB8:3003:9A4::FFFF/64
	ADMINISTRATIVO	2001:DB8:3003:9A5::/64	2001:DB8:3003:9A5::FFFF/64
	DOCENTES	2001:DB8:3003:9A6::/64	2001:DB8:3003:9A6::FFFF/64
	ESTUDIANTES	2001:DB8:3003:9A7::/64	2001:DB8:3003:9A7::FFFF/64
	VoIP	2001:DB8:3003:9A8::/64	2001:DB8:3003:9A8::FFFF/64
	IMPRESORAS	2001:DB8:3003:9A9::/64	2001:DB8:3003:9A9::FFFF/64
	CAMARAS	2001:DB8:3003:9AA::/64	2001:DB8:3003:9AA::FFFF/64
	LABORATORIOS	2001:DB8:3003:9AB::/64	2001:DB8:3003:9AB::FFFF/64
	BIBLIOTECA	2001:DB8:3003:9AC::/64	2001:DB8:3003:9AC::FFFF/64
	WIFI-MULTIMARCA	2001:DB8:3003:9AD::/64	2001:DB8:3003:9AD::FFFF/64
	WIFI-WLC	2001:DB8:3003:9AE::/64	2001:DB8:3003:9AE::FFFF/64
	IPV6: 2001:DB8:3003:A::/56		
MKT-JAR-BOT_1.0	ENLACE	2001:DB8:3003:ADAB::/64	2001:DB8:3003:ADAB::FFFE/64
	LIBRE	2001:DB8:3003:AA1::/64	
	LIBRE	2001:DB8:3003:AA2::/64	
	MPLS	2001:DB8:3003:AA3::/64	
	GESTIÓN (Nativa)	2001:DB8:3003:AA4::/64	2001:DB8:3003:AA4::FFFF/64
	ADMINISTRATIVO	2001:DB8:3003:AA5::/64	2001:DB8:3003:AA5::FFFF/64
	DOCENTES	2001:DB8:3003:AA6::/64	2001:DB8:3003:AA6::FFFF/64
	ESTUDIANTES	2001:DB8:3003:AA7::/64	2001:DB8:3003:AA7::FFFF/64
	VoIP	2001:DB8:3003:AA8::/64	2001:DB8:3003:AA8::FFFF/64
	IMPRESORAS	2001:DB8:3003:AA9::/64	2001:DB8:3003:AA9::FFFF/64
	CAMARAS	2001:DB8:3003:AAA::/64	2001:DB8:3003:AAA::FFFF/64
	LABORATORIOS	2001:DB8:3003:AAB::/64	2001:DB8:3003:AAB::FFFF/64
	BIBLIOTECA	2001:DB8:3003:AAC::/64	2001:DB8:3003:AAC::FFFF/64
	WIFI-MULTIMARCA	2001:DB8:3003:AAD::/64	2001:DB8:3003:AAD::FFFF/64
	WIFI-WLC	2001:DB8:3003:AAE::/64	2001:DB8:3003:AAE::FFFF/64

	IPV6: 2001:DB8:3003:B::/56		
MKT-OBELISCO_1.0	ENLACE	2001:DB8:3003:ADAC::/64	2001:DB8:3003:ADAC::FFFE/64
	LIBRE	2001:DB8:3003:BA1::/64	
	LIBRE	2001:DB8:3003:BA2::/64	
	GESTION (Nativa)	2001:DB8:3003:BA3::/64	2001:DB8:3003:BA3::FFFF/64
	ADMINISTRATIVOS	2001:DB8:3003:BA4::/64	2001:DB8:3003:BA4::FFFF/64
	DOCENTES	2001:DB8:3003:BA5::/64	2001:DB8:3003:BA5::FFFF/64
	ESTUDIANTES	2001:DB8:3003:BA6::/64	2001:DB8:3003:BA6::FFFF/64
	VoIP	2001:DB8:3003:BA7::/64	2001:DB8:3003:BA7::FFFF/64
	IMPRESORAS	2001:DB8:3003:BA8::/64	2001:DB8:3003:BA8::FFFF/64
	CAMARAS	2001:DB8:3003:BA9::/64	2001:DB8:3003:BA9::FFFF/64
	LABORATORIOS	2001:DB8:3003:BAA::/64	2001:DB8:3003:BAA::FFFF/64
	BIBLIOTECA	2001:DB8:3003:BAB::/64	2001:DB8:3003:BAB::FFFF/64
	WIFI-MULTIMARCA	2001:DB8:3003:BAC::/64	2001:DB8:3003:BAC::FFFF/64
	WIFI-WLC	2001:DB8:3003:BAD::/64	2001:DB8:3003:BAD::FFFF/64
	IPV6: 2001:DB8:3003:C::/56		
MKT-PUNZARA_1.0	ENLACE	2001:DB8:3003:ADAD::/64	2001:DB8:3003:ADAD::FFFE/64
	LIBRE	2001:DB8:3003:CA1::/64	
	LIBRE	2001:DB8:3003:CA2::/64	
	GESTION (Nativa)	2001:DB8:3003:CA3::/64	2001:DB8:3003:CA3::FFFF/64
	ADMINISTRATIVOS	2001:DB8:3003:CA4::/64	2001:DB8:3003:CA4::FFFF/64
	DOCENTES	2001:DB8:3003:CA5::/64	2001:DB8:3003:CA5::FFFF/64
	ESTUDIANTES	2001:DB8:3003:CA6::/64	2001:DB8:3003:CA6::FFFF/64
	VoIP	2001:DB8:3003:CA7::/64	2001:DB8:3003:CA7::FFFF/64
	IMPRESORAS	2001:DB8:3003:CA8::/64	2001:DB8:3003:CA8::FFFF/64
	CAMARAS	2001:DB8:3003:CA9::/64	2001:DB8:3003:CA9::FFFF/64
	LABORATORIOS	2001:DB8:3003:CAA::/64	2001:DB8:3003:CAA::FFFF/64
	BIBLIOTECA	2001:DB8:3003:CAB::/64	2001:DB8:3003:CAB::FFFF/64
	WIFI-MULTIMARCA	2001:DB8:3003:CAC::/64	2001:DB8:3003:CAC::FFFF/64
	WIFI-WLC	2001:DB8:3003:CAD::/64	2001:DB8:3003:CAD::FFFF/64
	IPV6: 2001:DB8:3003:D::/56		
MKT-CON-JUR_1.0	ENLACE	2001:DB8:3003:ADAE::/64	2001:DB8:3003:ADAE::FFFE/64
	LIBRE	2001:DB8:3003:DA1::/64	
	LIBRE	2001:DB8:3003:DA2::/64	
	GESTION (Nativa)	2001:DB8:3003:DA3::/64	2001:DB8:3003:DA3::FFFF/64
	ADMINISTRATIVOS	2001:DB8:3003:DA4::/64	2001:DB8:3003:DA4::FFFF/64
	DOCENTES	2001:DB8:3003:DA5::/64	2001:DB8:3003:DA5::FFFF/64
	ESTUDIANTES	2001:DB8:3003:DA6::/64	2001:DB8:3003:DA6::FFFF/64
	VoIP	2001:DB8:3003:DA7::/64	2001:DB8:3003:DA7::FFFF/64
	IMPRESORAS	2001:DB8:3003:DA8::/64	2001:DB8:3003:DA8::FFFF/64
	CAMARAS	2001:DB8:3003:DA9::/64	2001:DB8:3003:DA9::FFFF/64
	LABORATORIOS	2001:DB8:3003:DAA::/64	2001:DB8:3003:DAA::FFFF/64
	BIBLIOTECA	2001:DB8:3003:DAB::/64	2001:DB8:3003:DAB::FFFF/64
	WIFI-MULTIMARCA	2001:DB8:3003:DAC::/64	2001:DB8:3003:DAC::FFFF/64
	WIFI-WLC	2001:DB8:3003:DAD::/64	2001:DB8:3003:DAD::FFFF/64
	IPV6: 2001:DB8:3003:E::/56		
MKT-MOTUPE_1.0	ENLACE	2001:DB8:3003:ADAF::/64	2001:DB8:3003:ADAF::FFFE/64

	LIBRE	2001:DB8:3003:EA1::/64	
	LIBRE	2001:DB8:3003:EA2::/64	
	GESTIÓN (Nativa)	2001:DB8:3003:EA3::/64	2001:DB8:3003:EA3::FFFF/64
	ADMINISTRATIVOS	2001:DB8:3003:EA4::/64	2001:DB8:3003:EA4::FFFF/64
	DOCENTES	2001:DB8:3003:EA5::/64	2001:DB8:3003:EA5::FFFF/64
	ESTUDIANTES	2001:DB8:3003:EA6::/64	2001:DB8:3003:EA6::FFFF/64
	VoIP	2001:DB8:3003:EA7::/64	2001:DB8:3003:EA7::FFFF/64
	IMPRESORAS	2001:DB8:3003:EA8::/64	2001:DB8:3003:EA8::FFFF/64
	CAMARAS	2001:DB8:3003:EA9::/64	2001:DB8:3003:EA9::FFFF/64
	LABORATORIOS	2001:DB8:3003:EAA::/64	2001:DB8:3003:EAA::FFFF/64
	BIBLIOTECA	2001:DB8:3003:EAB::/64	2001:DB8:3003:EAB::FFFF/64
	WIFI-MULTIMARCA	2001:DB8:3003:EAC::/64	2001:DB8:3003:EAC::FFFF/64
	WIFI-WLC	2001:DB8:3003:EAD::/64	2001:DB8:3003:EAD::FFFF/64
	IPV6: 2001:DB8:3003:F::/56		
CENTRO DE FORMACIÓN ZAPOTEPAMBA	ENLACE	2001:DB8:3003:AD10::/64	2001:DB8:3003:AD10::FFFE/64
	LIBRE	2001:DB8:3003:FA1::/64	
	LIBRE	2001:DB8:3003:FA2::/64	
	GESTION (Nativa)	2001:DB8:3003:FA3::/64	2001:DB8:3003:FA3::FFFF/64
	ADMINISTRATIVOS	2001:DB8:3003:FA4::/64	2001:DB8:3003:FA4::FFFF/64
	DOCENTES	2001:DB8:3003:FA5::/64	2001:DB8:3003:FA5::FFFF/64
	ESTUDIANTES	2001:DB8:3003:FA6::/64	2001:DB8:3003:FA6::FFFF/64
	VoIP	2001:DB8:3003:FA7::/64	2001:DB8:3003:FA7::FFFF/64
	IMPRESORAS	2001:DB8:3003:FA8::/64	2001:DB8:3003:FA8::FFFF/64
	CAMARAS	2001:DB8:3003:FA9::/64	2001:DB8:3003:FA9::FFFF/64
	LABORATORIOS	2001:DB8:3003:FAA::/64	2001:DB8:3003:FAA::FFFF/64
	BIBLIOTECA	2001:DB8:3003:FAB::/64	2001:DB8:3003:FAB::FFFF/64
	WIFI-MULTIMARCA	2001:DB8:3003:FAC::/64	2001:DB8:3003:FAC::FFFF/64
	WIFI-WLC	2001:DB8:3003:FAD::/64	2001:DB8:3003:FAD::FFFF/64
	IPV6: 2001:DB8:3003:10::/56		
EL PADMI	ENLACE	2001:DB8:3003:AD11::/64	2001:DB8:3003:AD11::FFFE/64
	LIBRE	2001:DB8:3003:10A1::/64	
	LIBRE	2001:DB8:3003:10A2::/64	2001:DB8:3003:10A2::FFFF/64
	GESTION (Nativa)	2001:DB8:3003:10A3::/64	2001:DB8:3003:10A3::FFFF/64
	ADMINISTRATIVOS	2001:DB8:3003:10A4::/64	2001:DB8:3003:10A4::FFFF/64
	DOCENTES	2001:DB8:3003:10A5::/64	2001:DB8:3003:10A5::FFFF/64
	ESTUDIANTES	2001:DB8:3003:10A6::/64	2001:DB8:3003:10A6::FFFF/64
	VoIP	2001:DB8:3003:10A7::/64	2001:DB8:3003:10A7::FFFF/64
	IMPRESORAS	2001:DB8:3003:10A8::/64	2001:DB8:3003:10A8::FFFF/64
	CAMARAS	2001:DB8:3003:10A9::/64	2001:DB8:3003:10A9::FFFF/64
	LABORATORIOS	2001:DB8:3003:10AA::/64	2001:DB8:3003:10AA::FFFF/64
	BIBLIOTECA	2001:DB8:3003:10AB::/64	2001:DB8:3003:10AB::FFFF/64
	WIFI-MULTIMARCA	2001:DB8:3003:10AC::/64	2001:DB8:3003:10AC::FFFF/64
	WIFI-WLC	2001:DB8:3003:10AD::/64	2001:DB8:3003:10AD::FFFF/64

En la TABLA XIX se presenta ya el direccionamiento con el Protocolo de Internet versión 6 (IPv6) agregando los lugares de: Centro de Formación Zapotepamba y para el sector del Padmi, que son parte de la Universidad Nacional de Loja, dejando asignado a cada

sector sus VLAN con su respectiva dirección IPv6, se debe mencionar que no hay equipos existentes en estos lugares solo se está dejando el esquema de direccionamiento para futuras implementaciones.

Se establecen las direcciones IPv6 agregando las VLAN necesarias para el correcto funcionamiento en los sectores de: Motupe (SW-L3-CON_MOTUPE_1.0), Consultorio Jurídico (SW-L3-CON_JURIDICO_1.0), Obelisco (OBELISCO_1.0), Punzara (PUNZARA_1.0) y Jardín Botánico (JAR-BOT_1.0) teniendo en cuenta que en estos sectores a excepción de Motupe, se opera con Equipos Mikrotik de capa 3 para la configuración y prestación de sus servicios en el campus universitario.

Se toma en cuenta para el direccionamiento IPv6 los servidores públicos, realizando un direccionamiento muy independiente pero ya asignando una dirección IPv6 para que trabajen con el nuevo protocolo de internet.

6.3.5. Topología de Red del Backbone de la Universidad Nacional de Loja en IPv6

Luego de haber desarrollado el direccionamiento con el nuevo protocolo IPv6, se presenta un esquema topológico adicionando la ruta de comunicación y la dirección establecida para cada equipo en el Backbone de la Red de Datos de la Universidad Nacional de Loja.

Como se observa en la Figura 36, se indica las direcciones IPv6 de los enlaces desde el CORE hacia los equipos de distribución. Las demás direcciones para cada enlace se muestran en la TABLA XIX correspondiente al direccionamiento IPv6 para la institución.

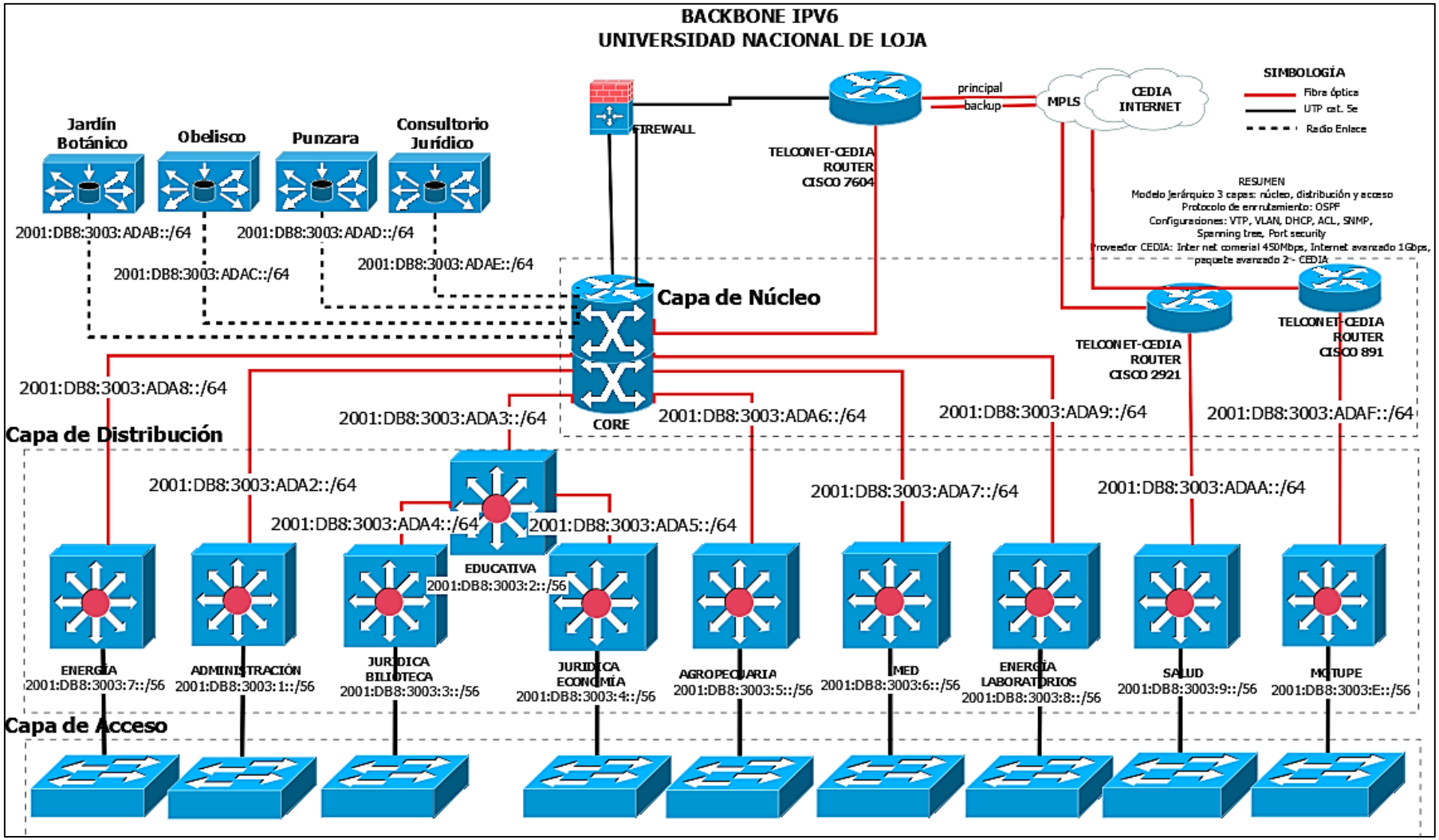


Figura 36: Backbone Universidad Nacional de Loja en IPv6.

6.4. OBJETIVO 4: Establecer un escenario de pruebas de acuerdo al Mecanismo de Transición seleccionado

Dentro del desarrollo del Objetivo 4 se debe mencionar que se levantó dos escenarios de pruebas, gracias a la facilidad de los equipos con los que se pudo contar por parte de la Unidad de Telecomunicaciones e Información (UTI), como también por los simuladores que hoy en día se los puede utilizar, permitiendo de esta manera realizar las configuraciones necesarias con el direccionamiento IPv6 y simulando así los equipos necesarios para realizar las pruebas pertinentes con los dos protocolos de internet.

A continuación se detalla cada escenario utilizado y debidamente configurado con el mecanismo de transición seleccionado: Mecanismo Doble-Pila.

6.4.1. ESCENARIO DE PRUEBAS 1: Equipos Mikrotik y Equipo CISCO

6.4.1.1. Requerimientos para el Escenario de Pruebas 1

Antes de empezar con las configuraciones necesarias se debe tomar en cuenta los requisitos para la utilización de la tecnología Mikrotik y como es su funcionamiento.

6.4.1.2. Instalación de la Herramienta Winbox

La herramienta Winbox para Mikrotik se lo descarga de la página oficial www.mikrotik.com, damos clic en la parte superior derecha “Software” y nos dirigimos a la sección de “Useful tools and utilities”, damos clic nuevamente en “Winbox versión 3.11” (el número de versión se encuentra actualizada) y se descargará automáticamente de nuestro navegador como se lo muestra en la siguiente figura.

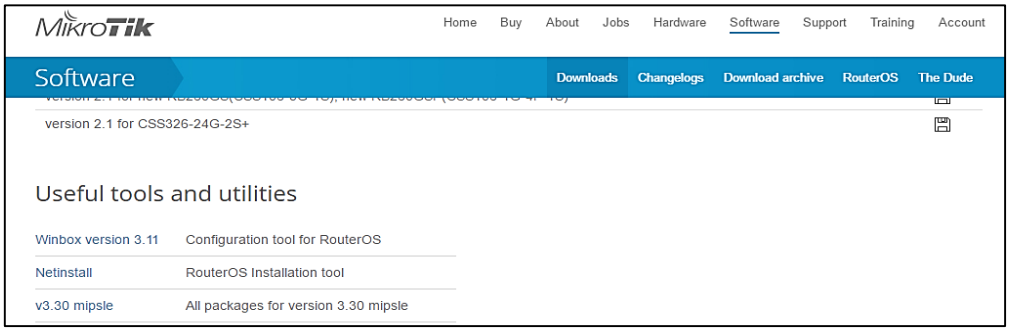


Figura 37: Descargar Winbox para Mikrotik.

Una vez descargado lo buscamos en nuestro computador y nos dará el siguiente resultado.

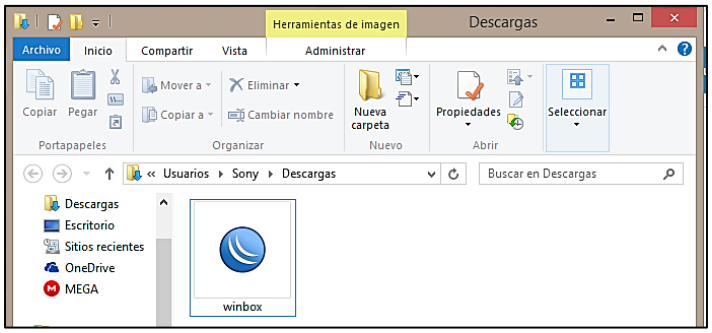


Figura 38: Ejecutable Winbox.

Procedemos a instalarlo dando doble clic o dando clic derecho “Abrir” y nos mostrará la siguiente interfaz donde podremos acceder mediante dirección IP o mediante dirección MAC del equipo, por lo general y en la mayoría de los casos se accede por dirección MAC y una vez configurado su dirección IP podremos ingresar mediante su dirección.

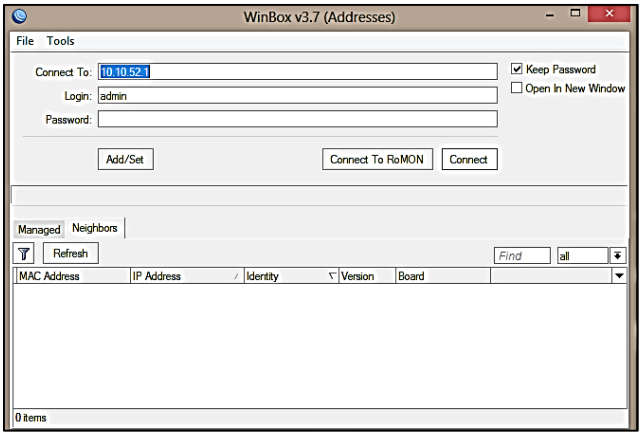


Figura 39: Interfaz Gráfica de Winbox.

Materiales adiciones:

TABLA XX: MATERIALES ADICIONALES.

Nombre	Material
Cable de Conexión (Patch Cord)	
Cable Consola ***NOTA: solo para el switch de acceso cisco 2960.***	

Cable Serial a RJ45 ***NOTA: solo para el switch de acceso cisco 2960.***	

6.4.1.3. SWITCH CORE: Configuración Protocolo de Internet versión 4 (IPv4)

El equipo Mikrotik utilizado no se encuentra con ninguna configuración realizada por eso para simular el Switch Core tenemos:

- **Equipo utilizado:** Mikrotik CCR1016 – 12G

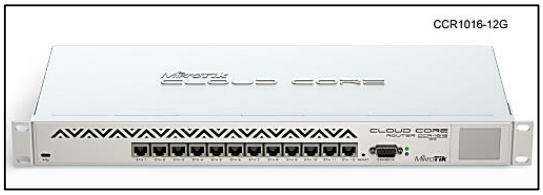


Figura 40: Equipo CCR1016 – 12G.

Antes de realizar cualquier configuración en IPv4, por defecto no viene instalado el paquete para IPv6 para ello hay que verificar que los equipos Mikrotik tengan soporte para IPv6 y en su página oficial (www.mikrotik.com) se puede obtener documentación importante para cualquier configuración y soporte que se desee realizar.

La tecnología Mikrotik funciona de la siguiente manera para el soporte de IPv6:

1. **Ingreso para activar IPv6:**

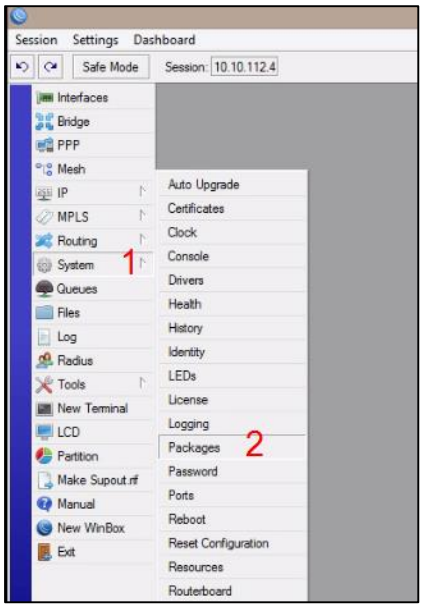


Figura 41: Ingreso para activar IPv6.

2. Activar paquete IPv6

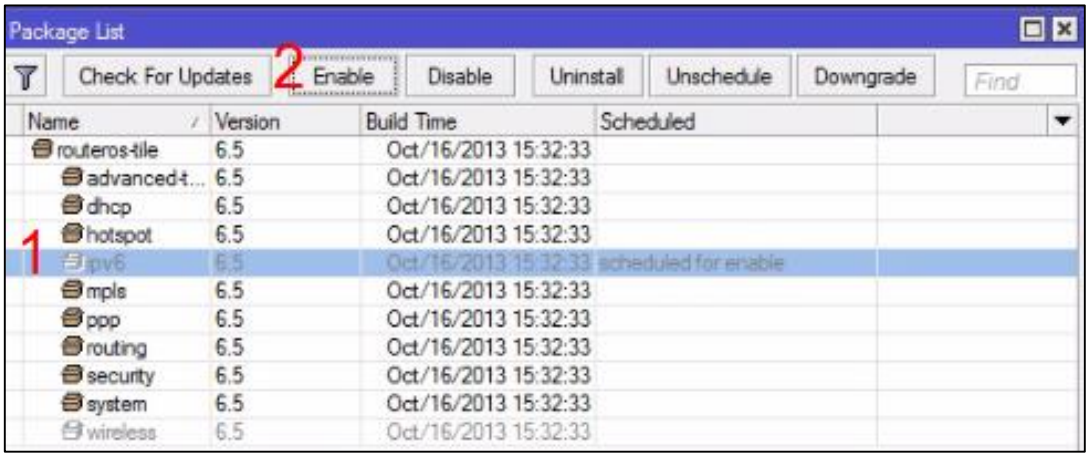


Figura 42: Activar paquete IPv6.

3. Reiniciar el equipo

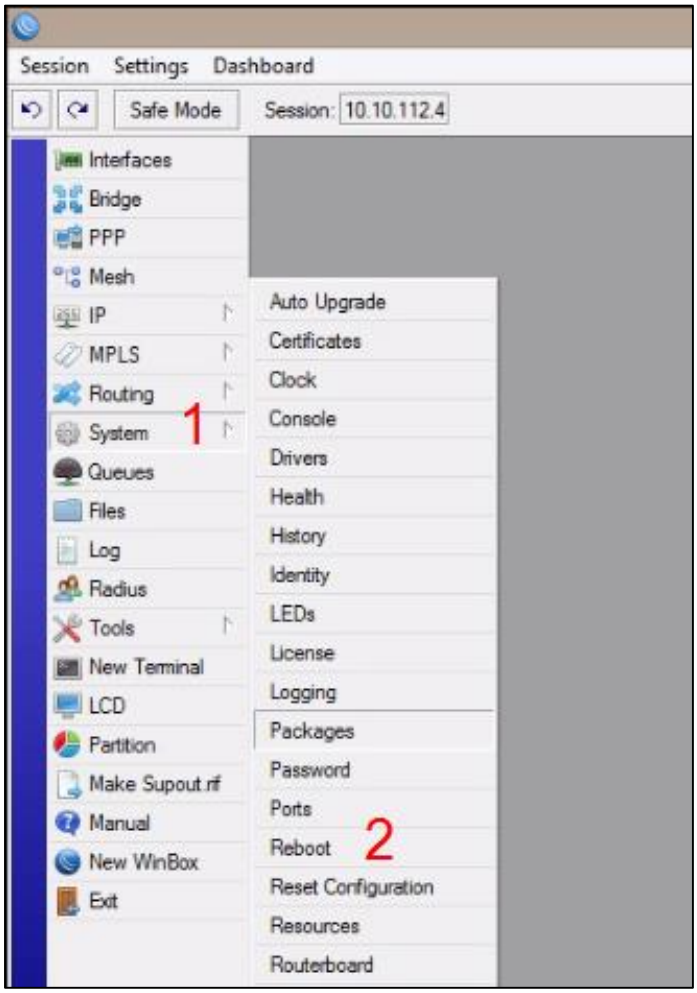


Figura 43: Reiniciar equipo Mikrotik.

4. Verificar soporte para IPv6

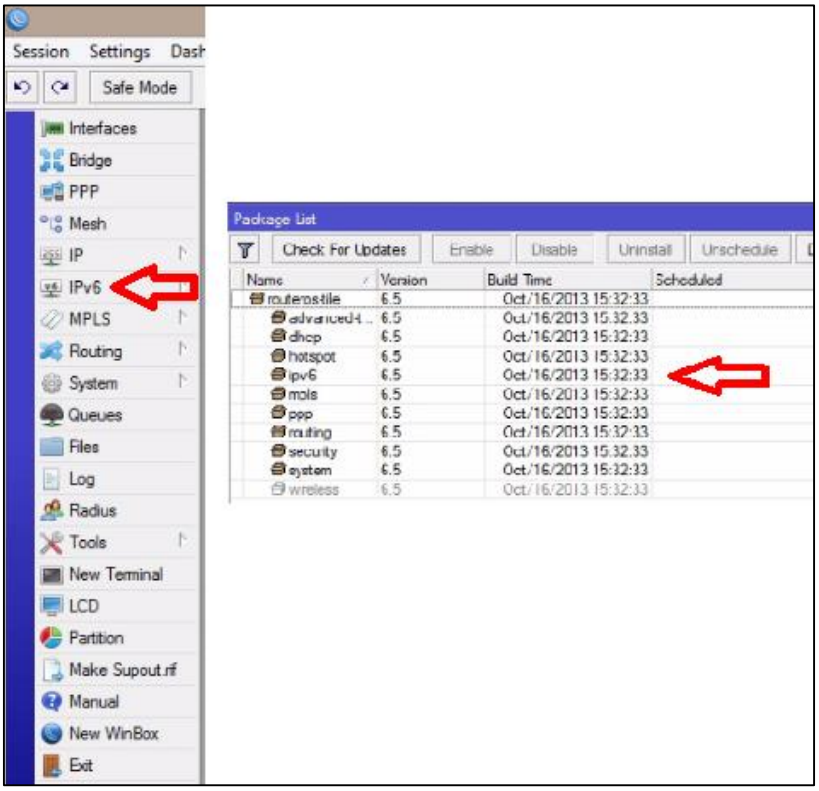


Figura 44: Verificar paquete IPv6 instalado.

- **Configuraciones.** El equipo consta de 12 interfaces Ethernet como se lo aprecia en la figura.

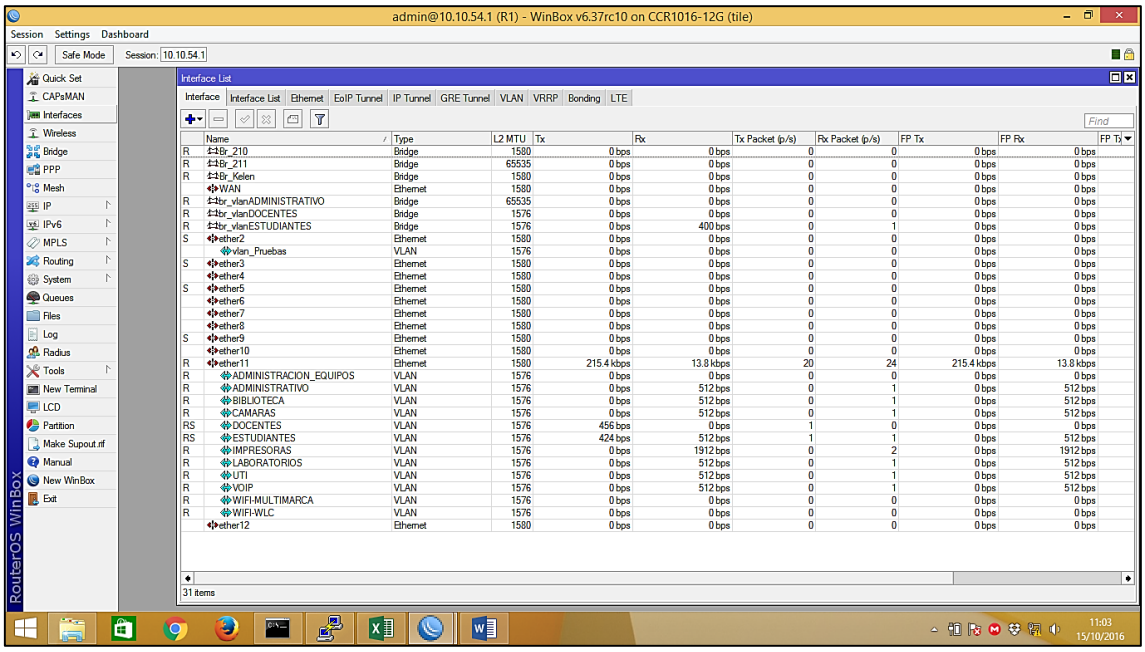


Figura 45: Interfaces equipo CCR1016 – 12G – Switch Core.

- **Crear Vlan.** Dentro de la misma pestaña de “Interfaces” se encuentra la pestaña “VLAN” damos clic y procedemos a crear las respectivas VLAN.

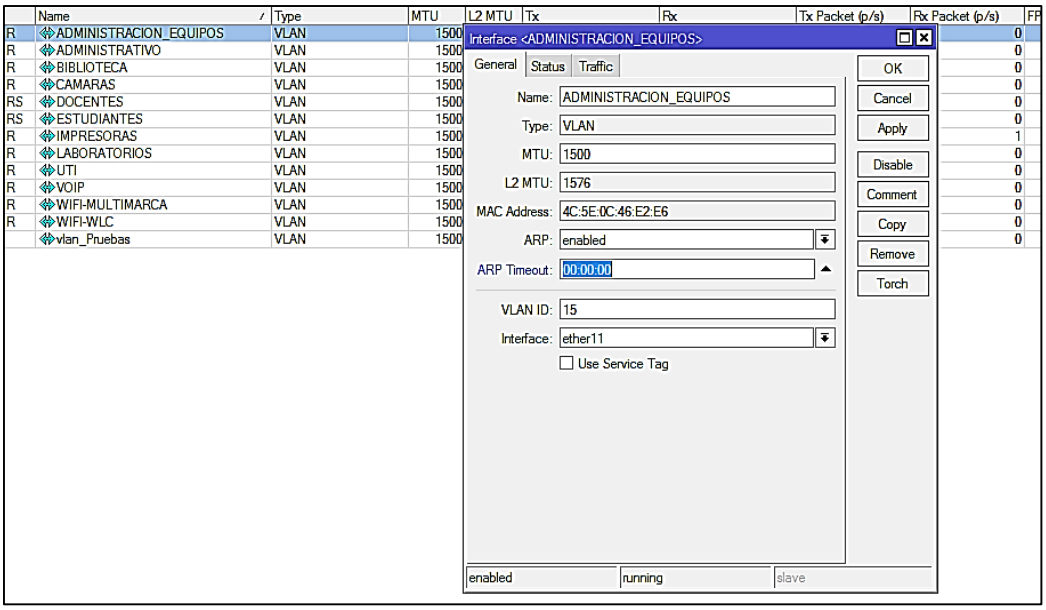


Figura 46: Crear VLAN – Switch Core.

- **Agregar direcciones IPv4.** En la parte lateral izquierda se encuentra el item “IP”, luego damos clic en “Addresses”, nos aparecerá la siguiente ventana damos clic en el símbolo “+” y empezamos a agregar las direcciones IPv4 asignándolas a sus respectivas VLAN creadas.

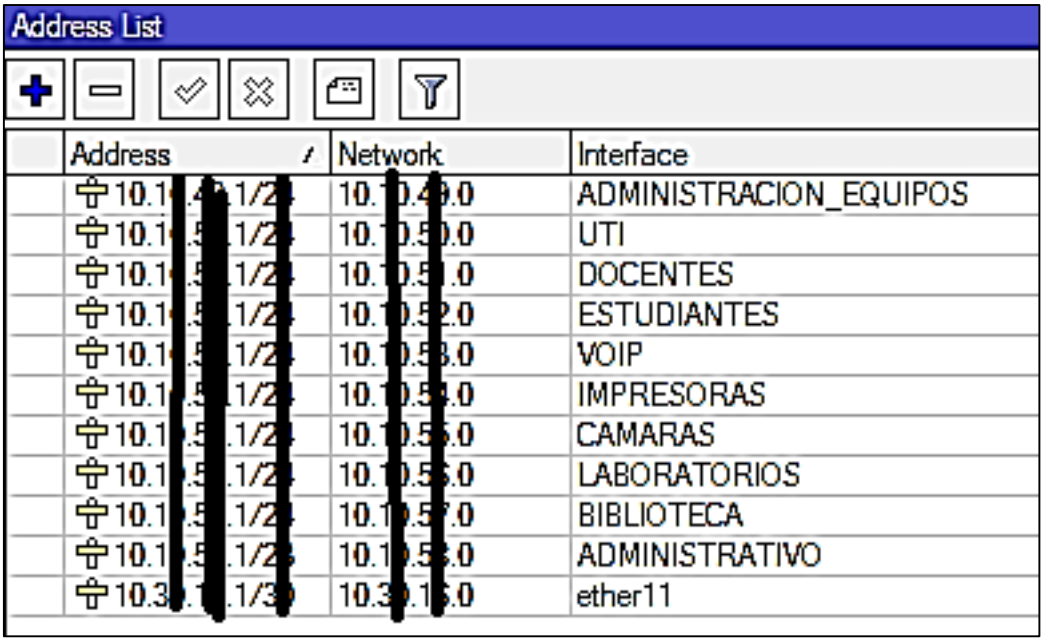


Figura 47: Agregar Dirección IPv4 – Switch Core.

- **Crear Pool-DHCP.** En la siguiente figura se presenta la creación de los pool (Piscina de Direcciones) mediante el protocolo dinámico DHCP.

IP Pool

Pools | Used Addresses

Name	Addresses	Next Pool
dhcp_pool1	10.1[redacted].10-10.10.5[redacted].250	none
dhcp_pool20	10.1[redacted].10-10.10.5[redacted].250	none
dhcp_pool21	10.1[redacted].10-10.10.5[redacted].250	none
dhcp_pool22	10.1[redacted].10-10.10.5[redacted].250	none
dhcp_pool23	10.1[redacted].10-10.10.5[redacted].250	none
dhcp_pool24	10.1[redacted].10-10.10.5[redacted].250	none
dhcp_pool28	10.1[redacted].10-10.10.5[redacted].250	none
dhcp_pool29	10.1[redacted].10-10.10.5[redacted].250	none
dhcp_pool30	10.1[redacted].10-10.10.5[redacted].250	none
dhcp_pool31	10.1[redacted]2-10.10.52[redacted]254	none

Figura 48: Crear Pool de direcciones IPv4 – Switch Core.

- **Crear DHCP Server.** Luego de crear los "Pool" se procede a crear los "DHCP Server" y en la siguiente figura se muestra como es su procedimiento.

DHCP Server

DHCP | Networks | Leases | Options | Option Sets | Alerts

DHCP Config | DHCP Setup

Name	Interface	Relay	Lease Time	Address Pool	Add AR...
dhcp1	UTI		00:10:00	dhcp_pool20	no
dhcp2	ADMINISTRATIVO		00:10:00	dhcp_pool21	no
dhcp3	br_vlanDOCENTES		00:10:00	dhcp_pool1	no
dhcp4	br_vlanESTUDIANTES		00:10:00	dhcp_pool31	no
dhcp5	VOIP		00:10:00	dhcp_pool23	no
dhcp6	IMPRESORAS		00:10:00	dhcp_pool24	no
dhcp7	CAMARAS		00:10:00	dhcp_pool28	no
dhcp8	LABORATORIOS		00:10:00	dhcp_pool29	no
dhcp9	BIBLIOTECA		00:10:00	dhcp_pool30	no

Figura 49: Crear DHCP Server en IPv4 – Switch Core.

Conforme se realizó la configuración anterior, en la figura siguiente podemos observar cómo se van agregando los "Networks" para cada DHCP Server creado.

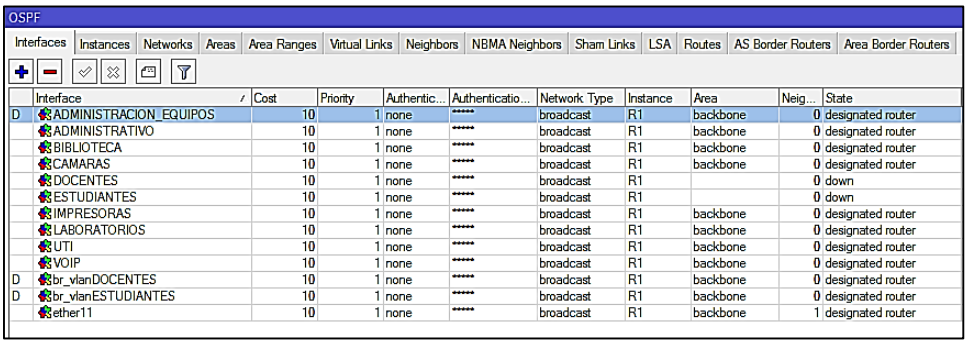
DHCP Server

DHCP | Networks | Leases | Options | Option Sets | Alerts

Address	Gateway	DNS Servers
10.1[redacted].50[redacted]0/2[redacted]	10.1[redacted]0.1	172.[redacted]6.3[redacted]2.8[redacted]
10.1[redacted].51[redacted]0/2[redacted]	10.1[redacted].5[redacted].1	172.[redacted]6.3[redacted]2.1[redacted]
10.1[redacted].52[redacted]0/2[redacted]	10.1[redacted].5[redacted].1	172.[redacted]6.3[redacted]2.1
10.1[redacted].53[redacted]0/2[redacted]	10.1[redacted].5[redacted].1	172.[redacted]6.3[redacted]2.1[redacted]
10.1[redacted].54[redacted]0/2[redacted]	10.1[redacted].5[redacted].1	172.[redacted]6.3[redacted]2.1[redacted]
10.1[redacted].55[redacted]0/2[redacted]	10.1[redacted].55[redacted]1	172.[redacted]6.3[redacted]2.1[redacted]
10.1[redacted].56[redacted]0/2[redacted]	10.1[redacted].56[redacted]1	172.[redacted]6.3[redacted]2.1[redacted]
10.1[redacted].57[redacted]0/2[redacted]	10.1[redacted].57[redacted]1	172.[redacted]6.3[redacted]2.1[redacted]
10.1[redacted].58[redacted]0/2[redacted]	10.1[redacted].58[redacted]1	172.[redacted]6.3[redacted]2.9[redacted]

Figura 50: Networks agregadas en IPv4 – Switch Core.

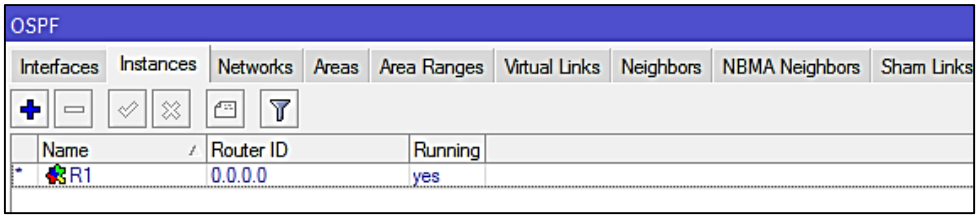
- **OSPF - Interfaces.** Procedemos a configurar el protocolo OSPF ingresando a la opción “Routing”, luego a la opción “OSPF”, se presenta la pantalla con la pestaña “Interfaces” donde se agrega las interfaces que intervienen en el enrutamiento.



	Interface	Cost	Priority	Authentic...	Authenticatio...	Network Type	Instance	Area	Neig...	State
D	ADMINISTRACION_EQUIPOS	10	1	none	*****	broadcast	R1	backbone	0	designated router
	ADMINISTRATIVO	10	1	none	*****	broadcast	R1	backbone	0	designated router
	BIBLIOTECA	10	1	none	*****	broadcast	R1	backbone	0	designated router
	CAMARAS	10	1	none	*****	broadcast	R1	backbone	0	designated router
	DOCENTES	10	1	none	*****	broadcast	R1		0	down
	ESTUDIANTES	10	1	none	*****	broadcast	R1		0	down
	IMPRESORAS	10	1	none	*****	broadcast	R1	backbone	0	designated router
	LABORATORIOS	10	1	none	*****	broadcast	R1	backbone	0	designated router
	UTI	10	1	none	*****	broadcast	R1	backbone	0	designated router
	VOIP	10	1	none	*****	broadcast	R1	backbone	0	designated router
D	br_vlanDOCENTES	10	1	none	*****	broadcast	R1	backbone	0	designated router
D	br_vlanESTUDIANTES	10	1	none	*****	broadcast	R1	backbone	0	designated router
	ether11	10	1	none	*****	broadcast	R1	backbone	1	designated router

Figura 51: OSPF Interfaces en IPv4 – Switch Core.

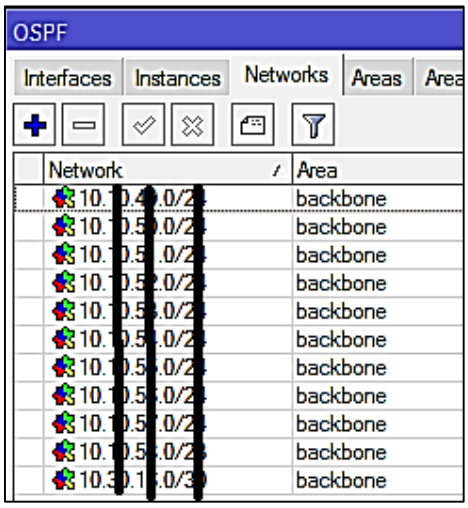
- **OSPF – Instances.** En este caso se da clic en “Instances” y se agrega el Router ID. Como se puede observar OSPFv2 está ejecutándose “Runnig = yes”.



	Name	Router ID	Running
*	R1	0.0.0.0	yes

Figura 52: OSPF Instances en IPv4 – Switch Core.

- **OSPF – Networks.** En la siguiente figura se agrega las redes que intervienen en OSPF tomando en cuenta la respectiva área en este caso Backbone.



Network	Area
10.[redacted]	backbone
10.[redacted]	backbone
10.[redacted]	backbone
10.[redacted]	backbone
10.[redacted]	backbone
10.[redacted]	backbone
10.[redacted]	backbone
10.[redacted]	backbone
10.[redacted]	backbone
10.[redacted]	backbone
10.[redacted]	backbone

Figura 53: OSPF - Networks en IPv4 – Switch Core.

- **OSPF – Áreas.** Se toma en cuenta el área en la que se trabajará como es el área Backbone y su área ID.

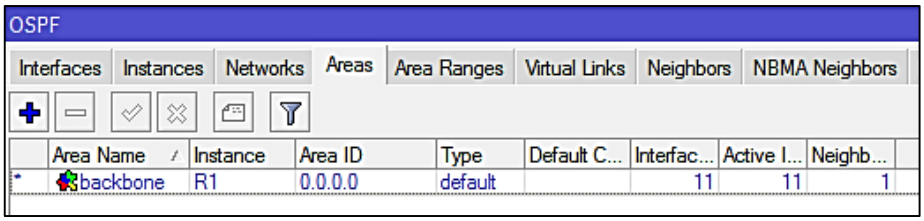


Figura 54: OSPF - Áreas en IPv4 – Switch Core.

En las siguientes figuras se presenta las configuraciones del OSPF que se han relizado teniendo en cuenta que ya está hecha la conexión desde el Switch Core al Switch de Distribución (L3), apreciando las rutas aprendidas mediante el protocolo de enrutamiento antes mencionado así:

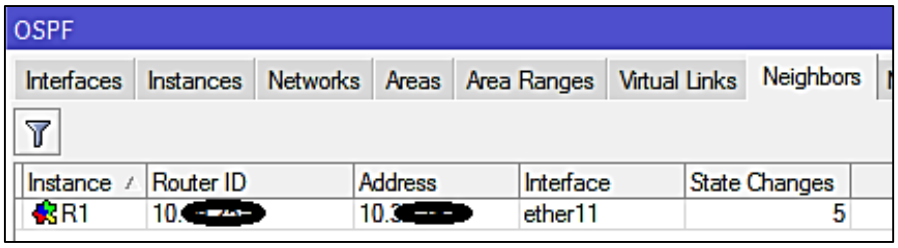


Figura 55: OSPF - Neighbors en IPv4 – Switch Core.

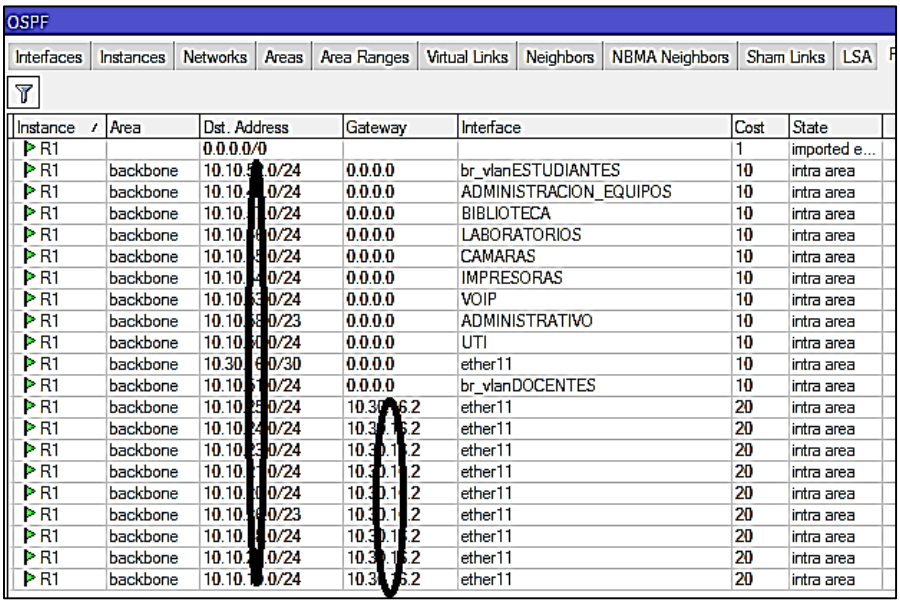
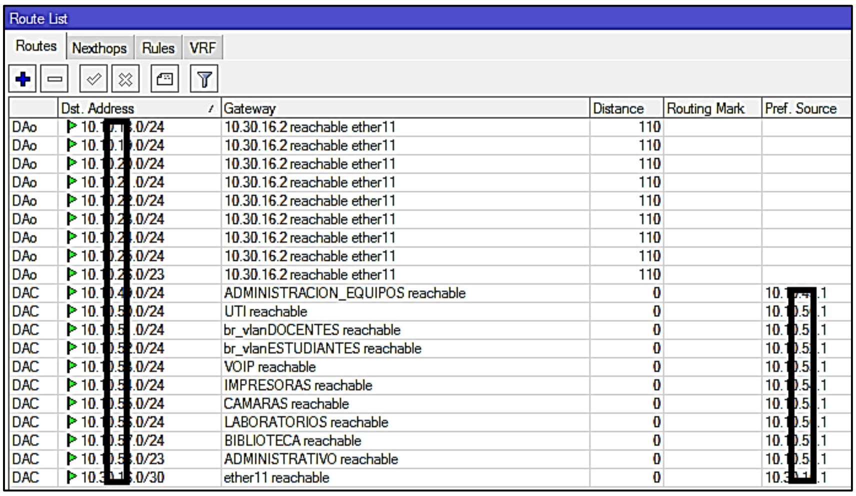


Figura 56: OSPF - Routes en IPv4 – Switch Core.



	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAo	10.[redacted].0/24	10.30.16.2 reachable ether11	110		
DAo	10.[redacted].0/24	10.30.16.2 reachable ether11	110		
DAo	10.[redacted].0/24	10.30.16.2 reachable ether11	110		
DAo	10.[redacted].0/24	10.30.16.2 reachable ether11	110		
DAo	10.[redacted].0/24	10.30.16.2 reachable ether11	110		
DAo	10.[redacted].0/24	10.30.16.2 reachable ether11	110		
DAo	10.[redacted].0/24	10.30.16.2 reachable ether11	110		
DAo	10.[redacted].0/24	10.30.16.2 reachable ether11	110		
DAo	10.[redacted].0/23	10.30.16.2 reachable ether11	110		
DAC	10.[redacted].0/24	ADMINISTRACION_EQUIPOS reachable	0		10.[redacted].1
DAC	10.[redacted].0/24	UTI reachable	0		10.[redacted].1
DAC	10.[redacted].0/24	br_vlanDOCENTES reachable	0		10.[redacted].1
DAC	10.[redacted].0/24	br_vlanESTUDIANTES reachable	0		10.[redacted].1
DAC	10.[redacted].0/24	VOIP reachable	0		10.[redacted].1
DAC	10.[redacted].0/24	IMPRESORAS reachable	0		10.[redacted].1
DAC	10.[redacted].0/24	CAMARAS reachable	0		10.[redacted].1
DAC	10.[redacted].0/24	LABORATORIOS reachable	0		10.[redacted].1
DAC	10.[redacted].0/24	BIBLIOTECA reachable	0		10.[redacted].1
DAC	10.[redacted].0/23	ADMINISTRATIVO reachable	0		10.[redacted].1
DAC	10.3[redacted].0/30	ether11 reachable	0		10.3[redacted].1

Figura 57: OSPF – Lista de Rutas aprendidas en IPv4 – Switch Core.

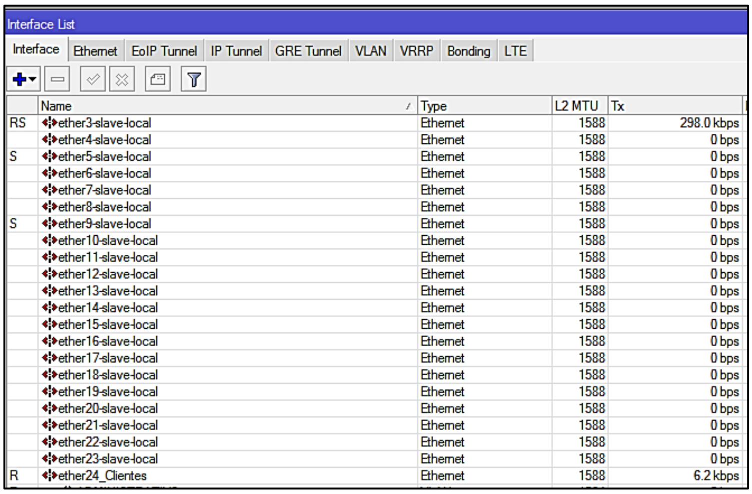
6.4.1.4. SWITCH DISTRIBUCIÓN L3: Configuración Protocolo de Internet versión 4 (IPv4)

El siguiente equipo Mikrotik se lo utilizó como Switch de Distribución constando de las siguientes interfaces y teniendo en cuenta que el acceso al equipo mencionado se lo realizó de la misma manera que el equipo anteriormente utilizado como Switch Core.

- **Equipo utilizado:** Mikrotik CRS125 – 24G – 1S

Figura 58: Equipo CRS125 – 24G – 1S.

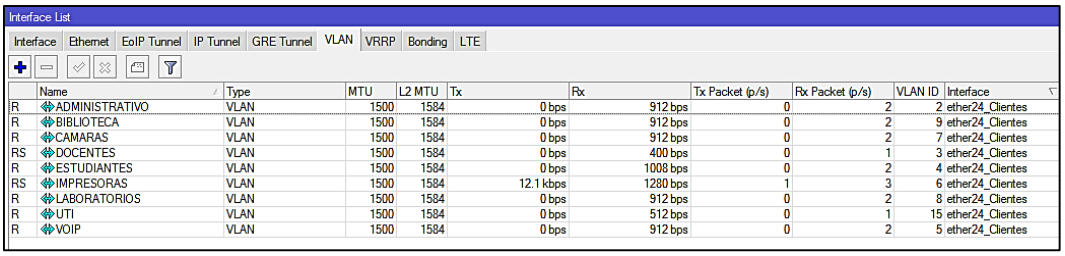
- **Configuraciones.** El equipo consta de 24 interfaces Ethernet.



	Name	Type	L2 MTU	Tx
RS	ether3-slave-local	Ethernet	1588	298.0 kbps
	ether4-slave-local	Ethernet	1588	0 bps
S	ether5-slave-local	Ethernet	1588	0 bps
	ether6-slave-local	Ethernet	1588	0 bps
	ether7-slave-local	Ethernet	1588	0 bps
	ether8-slave-local	Ethernet	1588	0 bps
S	ether9-slave-local	Ethernet	1588	0 bps
	ether10-slave-local	Ethernet	1588	0 bps
	ether11-slave-local	Ethernet	1588	0 bps
	ether12-slave-local	Ethernet	1588	0 bps
	ether13-slave-local	Ethernet	1588	0 bps
	ether14-slave-local	Ethernet	1588	0 bps
	ether15-slave-local	Ethernet	1588	0 bps
	ether16-slave-local	Ethernet	1588	0 bps
	ether17-slave-local	Ethernet	1588	0 bps
	ether18-slave-local	Ethernet	1588	0 bps
	ether19-slave-local	Ethernet	1588	0 bps
	ether20-slave-local	Ethernet	1588	0 bps
	ether21-slave-local	Ethernet	1588	0 bps
	ether22-slave-local	Ethernet	1588	0 bps
	ether23-slave-local	Ethernet	1588	0 bps
R	ether24_Clientes	Ethernet	1588	6.2 kbps

Figura 59: Interfaces equipo Switch Distribución.

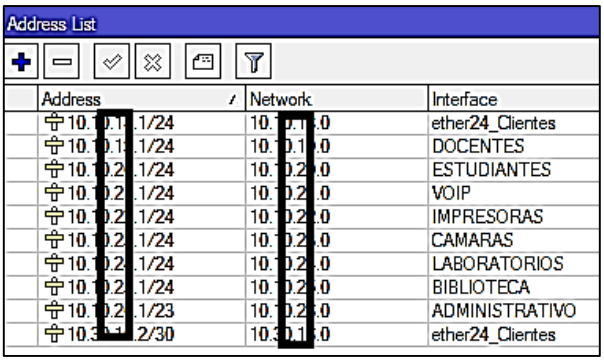
- **Crear VLAN.** Se procede a crear “VLAN” y ubicarlas en la interfaz 24 para su utilización.



	Name	Type	MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	VLAN ID	Interface
R	ADMINISTRATIVO	VLAN	1500	1584	0 bps	912 bps	0	2	2	ether24_Clientes
R	BIBLIOTECA	VLAN	1500	1584	0 bps	912 bps	0	2	9	ether24_Clientes
R	CAMARAS	VLAN	1500	1584	0 bps	912 bps	0	2	7	ether24_Clientes
RS	DOCENTES	VLAN	1500	1584	0 bps	400 bps	0	1	3	ether24_Clientes
R	ESTUDIANTES	VLAN	1500	1584	0 bps	1008 bps	0	2	4	ether24_Clientes
RS	IMPRESORAS	VLAN	1500	1584	12.1 kbps	1280 bps	1	3	6	ether24_Clientes
R	LABORATORIOS	VLAN	1500	1584	0 bps	912 bps	0	2	8	ether24_Clientes
R	UTI	VLAN	1500	1584	0 bps	512 bps	0	1	15	ether24_Clientes
R	VOIP	VLAN	1500	1584	0 bps	912 bps	0	2	5	ether24_Clientes

Figura 60: Crear VLAN en IPv4 - Switch Distribución.

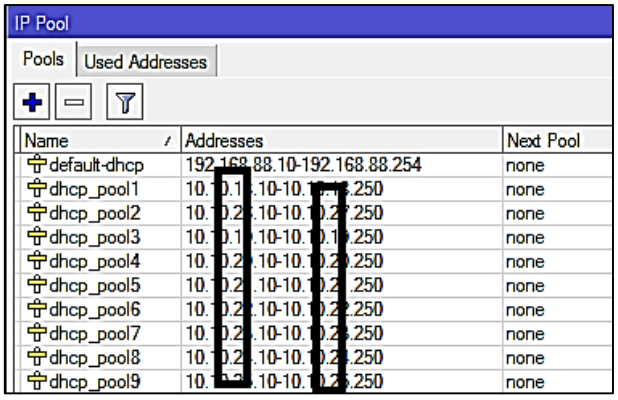
- **Agregar direcciones IPv4.** Así mismo empezamos agregar las direcciones IP en el item “IP”, luego damos clic en “Addresses”, nos aparecerá la siguiente ventana damos clic en el símbolo “+” y empezamos a agregar las direcciones IPv4 asignándolas a las VLAN creadas.



Address	Network	Interface
10.[redacted]1/24	10.[redacted]0	ether24_Clientes
10.[redacted]1/24	10.[redacted]0	DOCENTES
10.[redacted]1/24	10.[redacted]0	ESTUDIANTES
10.[redacted]1/24	10.[redacted]0	VOIP
10.[redacted]1/24	10.[redacted]0	IMPRESORAS
10.[redacted]1/24	10.[redacted]0	CAMARAS
10.[redacted]1/24	10.[redacted]0	LABORATORIOS
10.[redacted]1/24	10.[redacted]0	BIBLIOTECA
10.[redacted]1/23	10.[redacted]0	ADMINISTRATIVO
10.[redacted]2/30	10.[redacted]0	ether24_Clientes

Figura 61: Dirección IPv4 para VLAN - Switch Distribución.

- **Crear Pool-DHCP.** En la siguiente figura se presenta la creación de los pool (Piscina de Direcciones) mediante el protocolo dinámico DHCP y el rango que podrán tomar los equipos finales.



Name	Addresses	Next Pool
default-dhcp	192.168.88.10-192.168.88.254	none
dhcp_pool1	10.[redacted].250	none
dhcp_pool2	10.[redacted].250	none
dhcp_pool3	10.[redacted].250	none
dhcp_pool4	10.[redacted].250	none
dhcp_pool5	10.[redacted].250	none
dhcp_pool6	10.[redacted].250	none
dhcp_pool7	10.[redacted].250	none
dhcp_pool8	10.[redacted].250	none
dhcp_pool9	10.[redacted].250	none

Figura 62: Crear Pool de direcciones IPv4 - Switch Distribución.

- **Crear DHCP Server.** Se crea los “DHCP Server” como se muestra en la figura y se los asigna a los Pool creados anteriormente.

DHCP Server

DHCP | Networks | Leases | Options | Option Sets | Alerts

DHCP Config | DHCP Setup

Name	Interface	Relay	Lease Time	Address Pool	Add AR...
dhcp2	ADMINISTRATIVO		3d 00:00:00	dhcp_pool2	no
dhcp3	br_vlanDOCENTES		3d 00:00:00	dhcp_pool3	no
dhcp4	ESTUDIANTES		3d 00:00:00	dhcp_pool4	no
dhcp5	VOIP		3d 00:00:00	dhcp_pool5	no
dhcp6	br_vlanIMPRESORAS		3d 00:00:00	dhcp_pool6	no
dhcp7	CAMARAS		3d 00:00:00	dhcp_pool7	no
dhcp8	LABORATORIOS		3d 00:00:00	dhcp_pool8	no
dhcp9	BIBLIOTECA		3d 00:00:00	dhcp_pool9	no

Figura 63: Crear DHCP Server en IPv4 - Switch Distribución.

Mediante la configuración anterior, en la figura siguiente podemos observar cómo se van agregando los “Networks” para cada DHCP Server creado.

DHCP Server

DHCP | Networks | Leases | Options | Option Sets | Alerts

Address	Gateway	DNS Servers
10.[redacted].0/24	10.[redacted].1	172.[redacted].8
10.[redacted].0/24	10.[redacted].1	172.[redacted].10
10.[redacted].0/24	10.[redacted].1	172.[redacted].11
10.[redacted].0/24	10.[redacted].1	172.[redacted].12
10.[redacted].0/24	10.[redacted].1	172.[redacted].13
10.[redacted].0/24	10.[redacted].1	172.[redacted].14
10.[redacted].0/24	10.[redacted].1	172.[redacted].15
10.[redacted].0/24	10.[redacted].1	172.[redacted].16
10.[redacted].0/23	10.[redacted].1	172.[redacted].9

Figura 64: Networks agregadas en IPv4 - Switch Distribución.

- **OSPF - Interfaces.** Procedemos a configurar el protocolo OSPF ingresando las interfaces que intervienen en el enrutamiento.

OSPF

Interfaces | Instances | Networks | Areas | Area Ranges | Virtual Links | Neighbors | NBMA Neighbors | Sham Links | LSA | Routes | AS Border Routers | Area Border

	Interface	Cost	Priority	Authentic...	Authenticatio...	Network Type	Instance	Area	Neig...	State
	ADMINISTRATIVO	10	1	none	*****	broadcast	SW1	backbone	0	designated router
	BIBLIOTECA	10	1	none	*****	broadcast	SW1	backbone	0	designated router
	CAMARAS	10	1	none	*****	broadcast	SW1	backbone	0	designated router
	DOCENTES	10	1	none	*****	broadcast	SW1	unknown	0	down
	ESTUDIANTES	10	1	none	*****	broadcast	SW1	backbone	0	designated router
	IMPRESORAS	10	1	none	*****	broadcast	SW1	unknown	0	down
	LABORATORIOS	10	1	none	*****	broadcast	SW1	backbone	0	designated router
	UTI	10	1	none	*****	broadcast	SW1	unknown	0	down
	VOIP	10	1	none	*****	broadcast	SW1	backbone	0	designated router
D	br_vlanDOCENTES	10	1	none	*****	broadcast	SW1	backbone	0	designated router
D	br_vlanIMPRESORAS	10	1	none	*****	broadcast	SW1	backbone	0	designated router
	ether24_Clientes	10	1	none	*****	broadcast	SW1	backbone	1	backup
D	ether24_Clientes	10	1	none	*****	broadcast	SW1	backbone	0	designated router

Figura 65: OSPF Interfaces en IPv4 - Switch Distribución.

- **OSPF – Instances.** En este caso se da clic en “Instances” y se agrega el Router ID.

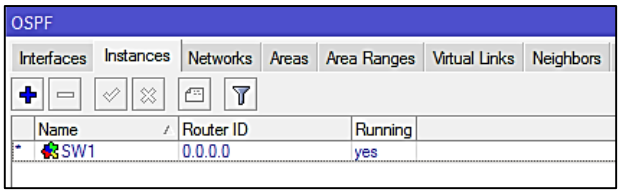


Figura 66: OSPF Instances en IPv4 - Switch Distribución.

- **OSPF – Networks.** En la siguiente figura se agrega las redes que intervienen en OSPF tomando en cuenta la respectiva área en la que se trabaja Backbone.

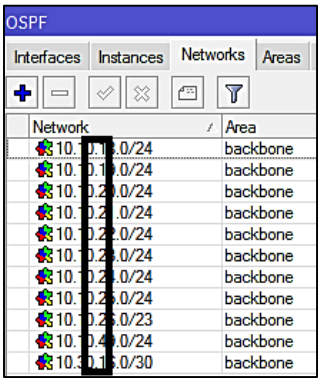


Figura 67: OSPF - Networks en IPv4 - Switch Distribución.

- **OSPF – Áreas.** Se toma en cuenta el área (Backbone) y su área ID.

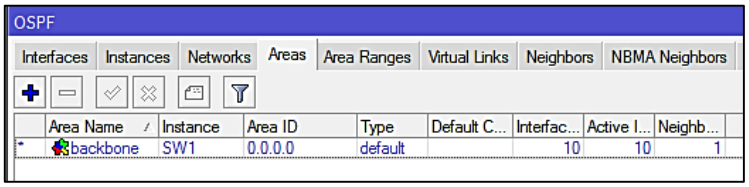


Figura 68: OSPF - Áreas en IPv4 - Switch Distribución.

En las siguientes figuras se presenta las configuraciones del OSPF que se han configurado, apreciando las rutas aprendidas mediante el protocolo de enrutamiento antes mencionado:

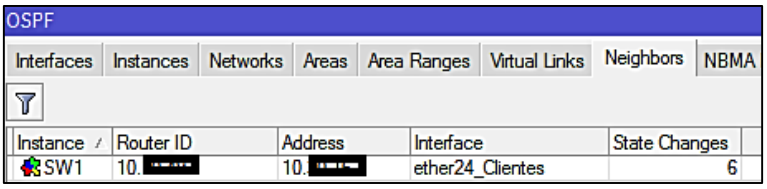
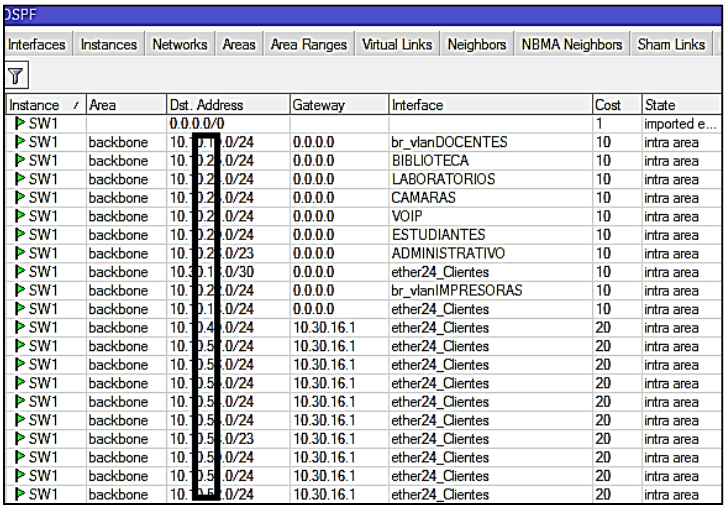
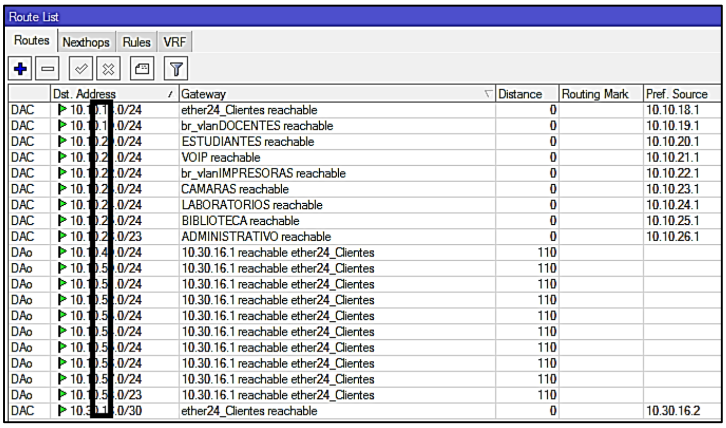


Figura 69: OSPF - Neighbors en IPv4 - Switch Distribución.



Instance	Area	Dst. Address	Gateway	Interface	Cost	State
SW1		0.0.0.0/0			1	imported e...
SW1	backbone	10.1[redacted].1[redacted].0/24	0.0.0.0	br_vlanDOCENTES	10	intra area
SW1	backbone	10.1[redacted].2[redacted].0/24	0.0.0.0	BIBLIOTECA	10	intra area
SW1	backbone	10.1[redacted].2[redacted].0/24	0.0.0.0	LABORATORIOS	10	intra area
SW1	backbone	10.1[redacted].2[redacted].0/24	0.0.0.0	CAMARAS	10	intra area
SW1	backbone	10.1[redacted].2[redacted].0/24	0.0.0.0	VOIP	10	intra area
SW1	backbone	10.1[redacted].2[redacted].0/24	0.0.0.0	ESTUDIANTES	10	intra area
SW1	backbone	10.1[redacted].2[redacted].0/23	0.0.0.0	ADMINISTRATIVO	10	intra area
SW1	backbone	10.3[redacted].1[redacted].0/30	0.0.0.0	ether24_Clientes	10	intra area
SW1	backbone	10.1[redacted].2[redacted].0/24	0.0.0.0	br_vlanIMPRESORAS	10	intra area
SW1	backbone	10.1[redacted].1[redacted].0/24	0.0.0.0	ether24_Clientes	10	intra area
SW1	backbone	10.1[redacted].4[redacted].0/24	10.30.16.1	ether24_Clientes	20	intra area
SW1	backbone	10.1[redacted].5[redacted].0/24	10.30.16.1	ether24_Clientes	20	intra area
SW1	backbone	10.1[redacted].5[redacted].0/24	10.30.16.1	ether24_Clientes	20	intra area
SW1	backbone	10.1[redacted].5[redacted].0/24	10.30.16.1	ether24_Clientes	20	intra area
SW1	backbone	10.1[redacted].5[redacted].0/24	10.30.16.1	ether24_Clientes	20	intra area
SW1	backbone	10.1[redacted].5[redacted].0/24	10.30.16.1	ether24_Clientes	20	intra area
SW1	backbone	10.1[redacted].5[redacted].0/23	10.30.16.1	ether24_Clientes	20	intra area
SW1	backbone	10.1[redacted].5[redacted].0/24	10.30.16.1	ether24_Clientes	20	intra area
SW1	backbone	10.1[redacted].5[redacted].0/24	10.30.16.1	ether24_Clientes	20	intra area
SW1	backbone	10.1[redacted].5[redacted].0/24	10.30.16.1	ether24_Clientes	20	intra area

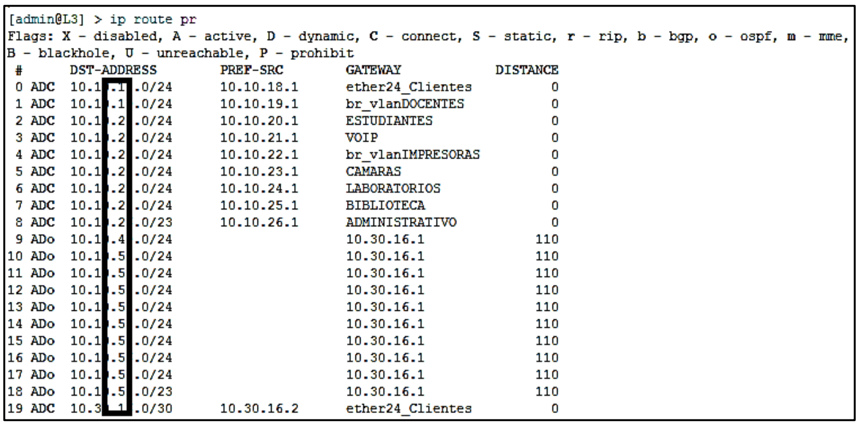
Figura 70: OSPF - Routes en IPv4 - Switch Distribución.



	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAC	10.1[redacted].1[redacted].0/24	ether24_Clientes reachable	0		10.10.18.1
DAC	10.1[redacted].1[redacted].0/24	br_vlanDOCENTES reachable	0		10.10.19.1
DAC	10.1[redacted].2[redacted].0/24	ESTUDIANTES reachable	0		10.10.20.1
DAC	10.1[redacted].2[redacted].0/24	VOIP reachable	0		10.10.21.1
DAC	10.1[redacted].2[redacted].0/24	br_vlanIMPRESORAS reachable	0		10.10.22.1
DAC	10.1[redacted].2[redacted].0/24	CAMARAS reachable	0		10.10.23.1
DAC	10.1[redacted].2[redacted].0/24	LABORATORIOS reachable	0		10.10.24.1
DAC	10.1[redacted].2[redacted].0/24	BIBLIOTECA reachable	0		10.10.25.1
DAC	10.1[redacted].2[redacted].0/23	ADMINISTRATIVO reachable	0		10.10.26.1
DAo	10.1[redacted].4[redacted].0/24	10.30.16.1 reachable ether24_Clientes	110		
DAo	10.1[redacted].5[redacted].0/24	10.30.16.1 reachable ether24_Clientes	110		
DAo	10.1[redacted].5[redacted].0/24	10.30.16.1 reachable ether24_Clientes	110		
DAo	10.1[redacted].5[redacted].0/24	10.30.16.1 reachable ether24_Clientes	110		
DAo	10.1[redacted].5[redacted].0/24	10.30.16.1 reachable ether24_Clientes	110		
DAo	10.1[redacted].5[redacted].0/24	10.30.16.1 reachable ether24_Clientes	110		
DAo	10.1[redacted].5[redacted].0/24	10.30.16.1 reachable ether24_Clientes	110		
DAo	10.1[redacted].5[redacted].0/24	10.30.16.1 reachable ether24_Clientes	110		
DAo	10.1[redacted].5[redacted].0/24	10.30.16.1 reachable ether24_Clientes	110		
DAo	10.1[redacted].5[redacted].0/23	10.30.16.1 reachable ether24_Clientes	110		
DAC	10.3[redacted].1[redacted].0/30	ether24_Clientes reachable	0		10.30.16.2

Figura 71: OSPF – Lista de Rutas aprendidas en IPv4 - Switch Distribución.

También se puede hacer uso mediante consola en equipos Mikrotik si usted así lo prefiere y mediante el siguiente comando se muestra las rutas aprendidas en OSPF desde el equipo de Distribución hacia el equipo Core.



```
[admin@L3] > ip route pr
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADC  10.1[redacted].1[redacted].0/24       10.10.18.1      ether24_Clientes          0
 1 ADC  10.1[redacted].1[redacted].0/24       10.10.19.1      br_vlanDOCENTES           0
 2 ADC  10.1[redacted].2[redacted].0/24       10.10.20.1      ESTUDIANTES               0
 3 ADC  10.1[redacted].2[redacted].0/24       10.10.21.1      VOIP                      0
 4 ADC  10.1[redacted].2[redacted].0/24       10.10.22.1      br_vlanIMPRESORAS         0
 5 ADC  10.1[redacted].2[redacted].0/24       10.10.23.1      CAMARAS                   0
 6 ADC  10.1[redacted].2[redacted].0/24       10.10.24.1      LABORATORIOS              0
 7 ADC  10.1[redacted].2[redacted].0/24       10.10.25.1      BIBLIOTECA                0
 8 ADC  10.1[redacted].2[redacted].0/23       10.10.26.1      ADMINISTRATIVO            0
 9 ADo  10.1[redacted].4[redacted].0/24                       10.30.16.1              110
10 ADo  10.1[redacted].5[redacted].0/24                       10.30.16.1              110
11 ADo  10.1[redacted].5[redacted].0/24                       10.30.16.1              110
12 ADo  10.1[redacted].5[redacted].0/24                       10.30.16.1              110
13 ADo  10.1[redacted].5[redacted].0/24                       10.30.16.1              110
14 ADo  10.1[redacted].5[redacted].0/24                       10.30.16.1              110
15 ADo  10.1[redacted].5[redacted].0/24                       10.30.16.1              110
16 ADo  10.1[redacted].5[redacted].0/24                       10.30.16.1              110
17 ADo  10.1[redacted].5[redacted].0/24                       10.30.16.1              110
18 ADo  10.1[redacted].5[redacted].0/23                       10.30.16.1              110
19 ADC  10.3[redacted]1[redacted].0/30        10.30.16.2      ether24_Clientes          0
```

Figura 72: Comando “ip routing print” – Switch Distribución.

Comprobación de la conexión entre el Switch Core y el Switch de Distribución, realizando un ping a la interface “ether 11” mediante su dirección IPv4.

```
[admin@L3] >
[admin@L3] > ping 10.30.16.1
HOST                                     SIZE TTL TIME  STATUS
10.30.16.1                                 56  64 0ms
10.30.16.1                                 56  64 0ms
10.30.16.1                                 56  64 0ms
10.30.16.1                                 56  64 0ms
10.30.16.1                                 56  64 0ms
10.30.16.1                                 56  64 0ms
10.30.16.1                                 56  64 0ms
10.30.16.1                                 56  64 0ms
10.30.16.1                                 56  64 0ms
10.30.16.1                                 56  64 0ms
10.30.16.1                                 56  64 0ms
    sent=11 received=11 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

Figura 73: Comprobación de conexión Switch Distribución al Switch Core.

Así mismo se realizó una comprobación de conexión hacia una de las VLAN creadas, se tomó como referencia la “VLAN-Estudiantes”.

```
[admin@L3] >
[admin@L3] > ping 10.10.52.1
HOST                                     SIZE TTL TIME  STATUS
10.10.52.1                                 56  64 0ms
10.10.52.1                                 56  64 0ms
10.10.52.1                                 56  64 0ms
10.10.52.1                                 56  64 0ms
10.10.52.1                                 56  64 0ms
10.10.52.1                                 56  64 0ms
10.10.52.1                                 56  64 0ms
10.10.52.1                                 56  64 0ms
10.10.52.1                                 56  64 0ms
10.10.52.1                                 56  64 0ms
10.10.52.1                                 56  64 0ms
10.10.52.1                                 56  64 0ms
10.10.52.1                                 56  64 0ms
10.10.52.1                                 56  64 0ms
10.10.52.1                                 56  64 0ms
10.10.52.1                                 56  64 0ms
    sent=16 received=16 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

Figura 74: Comprobación de conexión hacia VLAN.

6.4.1.5. SWITCH ACCESO L2: Configuración Protocolo de Internet versión 4 (IPv4)

Para las configuraciones del equipo de acceso se utilizó un Switch de marca Cisco 2960, funcionando como L2.

- **Equipo utilizado:** Switch de Acceso Catalyst 2960X-Series.

Figura 75: Switch Acceso Catalyst 2960X-Series.

- **Crear VLAN:** Se crea las VLAN conforme se crearon en los equipos Core y L3. Se ingresa a la configuración global de equipo mediante el comando “configure

terminal” y se crea la VLAN con mediante el comando “vlan 10”, para luego dar un nombre con el comando “name UTI”. La siguiente figura muestra las VLAN creadas.

```
!
!
vlan internal allocation policy ascending
!
vlan 2
 name ADMINISTRATIVO
!
vlan 3
 name DOCENTES
!
vlan 4
 name ESTUDIANTES
!
vlan 5
 name VOIP
!
vlan 6
 name IMPRESORAS
!
vlan 7
 name CAMARAS
!
vlan 8
 name LABORATORIOS
!
vlan 9
 name BIBLIOTECA
!
vlan 15
 name ADMIN_EQUIPOS
!
 --More--
```

Figura 76: Crear VLAN – Switch Acceso.

En la siguiente Figura se procede a realizar la asignación de las VLAN a los puertos de las interfaces en modo de acceso mediante los siguientes comandos:

switch(config)#interface fa0/0
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 2

```
!
interface GigabitEthernet0/2
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet0/3
 switchport access vlan 3
 switchport mode access
!
interface GigabitEthernet0/4
 switchport access vlan 4
 switchport mode access
!
interface GigabitEthernet0/5
 switchport access vlan 5
 switchport mode access
 spanning-tree portfast
!
```

Figura 77. Asignar VLAN a interfaz – Switch Acceso.

Luego se habilita el puerto en modo trunk a la interface GigabitEthernet 0/24 como se ve en la Figura 72 mediante los siguientes comandos:

switch(config)#interface GigabitEthernet0/24
switch(config-if)#switchport trunk vlan 15
switch(config-if)#switchport trunk allowed vlan 1-15
switch(config-if)#switchport mode trunk
switch(config-if)#exit

```
!
interface GigabitEthernet0/24
 switchport access vlan 15
 switchport trunk native vlan 15
 switchport trunk allowed vlan 1-15
 switchport mode trunk
 speed 100
 duplex full
```

Figura 78: Habilitar modo trunk – Switch Acceso.

Se asigna una dirección IPv4 a la VLAN de Administración de Equipos y un Gateway por defecto como se muestra en la siguiente figura.

```
interface Vlan15
 ip address 10.10.18.2 255.255.255.0
!
interface Vlan16
 no ip address
!
ip default-gateway 10.10.18.1
ip http server
ip http secure-server
!
```

Figura 79: IPv4 para VLAN nativa – Switch Acceso.

Se realiza las pruebas de conexión desde el Switch de acceso al Switch de Distribución y al Switch Core.

```
Switch_Acceso#
Switch_Acceso#ping 10.30.16.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.30.16.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Switch_Acceso#
Switch_Acceso#
Switch_Acceso#pin 10.10.53.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.53.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/10 ms
Switch_Acceso#
Switch_Acceso#
Switch_Acceso#ping 10.30.16.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.30.16.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Switch_Acceso#
Switch_Acceso#ping 10.10.21.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Switch_Acceso#
Switch_Acceso#
Switch_Acceso#
```

Figura 80: Comprobando conexión hacia Switch Distribución y Switch Core.

- **Usuario Final:** se conecta la PC y verificamos que nos genere la respectiva dirección IPv4 con el comando “ipconfig” mediante el protocolo DHCP.

```
Adaptador de Ethernet Ethernet 1:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::2c24:152b:4c82:6ea1%4
   Dirección IPv4. . . . . . . . . . . . . . : 10.10.22.250
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::4e5e:cff:fe46:e2e6%4
                                               192.168.30.1
                                               10.10.22.1
```

Figura 81: Dirección IPv4 en usuario final.

Se comprueba la conectividad desde el Usuario Final hacia los Switch Acceso-Distribución-Core.

```
C:\Users\Walter-Agusto>ping 10.10.26.1

Haciendo ping a 10.10.26.1 con 32 bytes de datos:
Respuesta desde 10.10.26.1: bytes=32 tiempo<1m TTL=63
Respuesta desde 10.10.26.1: bytes=32 tiempo<1m TTL=63
Respuesta desde 10.10.26.1: bytes=32 tiempo<1m TTL=63
Respuesta desde 10.10.26.1: bytes=32 tiempo<1m TTL=63

Estadísticas de ping para 10.10.26.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Walter-Agusto>ping 10.10.54.1

Haciendo ping a 10.10.54.1 con 32 bytes de datos:
Respuesta desde 10.10.54.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.10.54.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.10.54.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.10.54.1: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 10.10.54.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Walter-Agusto>ping 10.30.16.1

Haciendo ping a 10.30.16.1 con 32 bytes de datos:
Respuesta desde 10.30.16.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.30.16.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.30.16.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.30.16.1: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 10.30.16.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Walter-Agusto>ping 10.30.16.2

Haciendo ping a 10.30.16.2 con 32 bytes de datos:
Respuesta desde 10.30.16.2: bytes=32 tiempo<1m TTL=63
Respuesta desde 10.30.16.2: bytes=32 tiempo<1m TTL=63
Respuesta desde 10.30.16.2: bytes=32 tiempo<1m TTL=63
Respuesta desde 10.30.16.2: bytes=32 tiempo<1m TTL=63

Estadísticas de ping para 10.30.16.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Figura 82: Conectividad hacia los Swtichs Acceso-Distribución-Core.

Como ya se levantó toda la configuración con el Protocolo de Internet versión 4 (IPv4), se comprobó su funcionamiento; ahora procedemos a configurar en los mismos equipos el Protocolo de Internet versión 6 (IPv6) para así tener las dos pilas en marcha aplicando el Mecanismo de Transición Doble Pila (Dual Stack) conforme se lo estudió anteriormente y siendo el idóneo para la implementación en los equipos y estructura que maneja la Universidad Nacional de Loja.

6.4.1.6. SWITCH CORE: Configuración Protocolo de Internet versión 6 (IPv6)

En el equipo Core procedemos a configurar una dirección IPv6 tomando en cuenta el Esquema de direccionamiento realizado en la Sección 6.3.4 para poder tener conectividad y mediante esta dirección poder llegar al Switch de Distribución como se lo indica en la Figura 77.

- **Agregar dirección IPv6:** en la parte izquierda encontramos la opción "IPv6", damos clic en "Addresses", nos aparecerá la siguiente ventana damos clic en el símbolo "+" y empezamos a agregar las direcciones IPv6 asignándolas a las VLAN que se crearon con anterioridad.

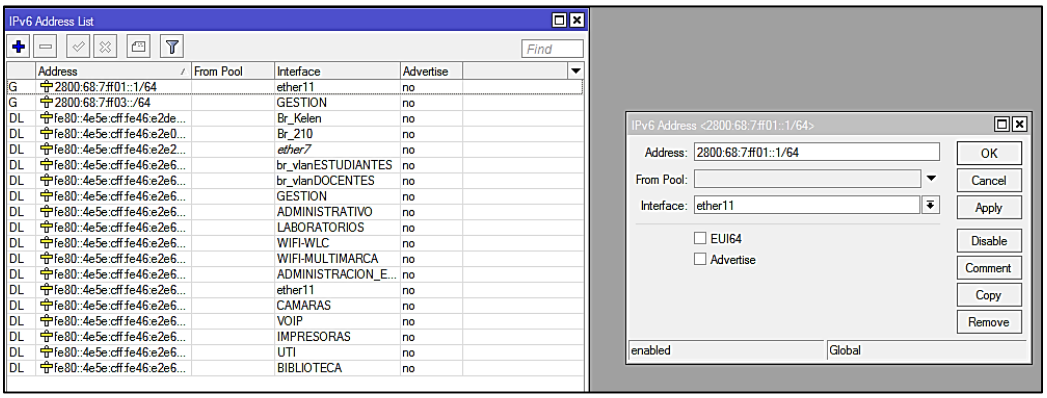


Figura 83: Dirección IPv6 – Switch Core.

- **OSPFv3 – Interfaces:** se configura el protocolo OSPFv3, ingresando las interfaces que intervienen en el enrutamiento.

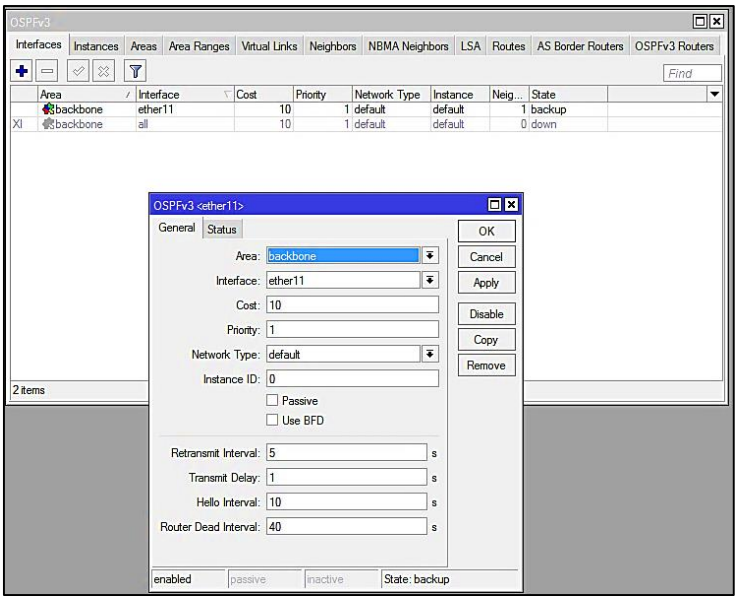


Figura 84: Configuración OSPFv3 – Switch Core.

- **OSPFv3 – Instances:** se da clic en la pestaña “Instances” y se agrega el Router ID para IPv6.

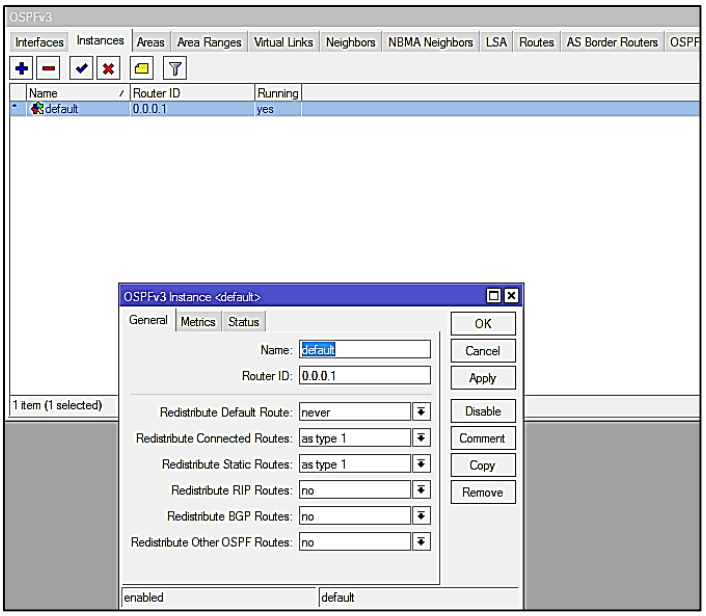


Figura 85: OSPFv3 Instances IPv6 – Switch Core.

- **OSPFv3 – Áreas:** como se realizó la configuración para IPv4 así mismo, se toma en cuenta el área (Backbone) y su área ID.

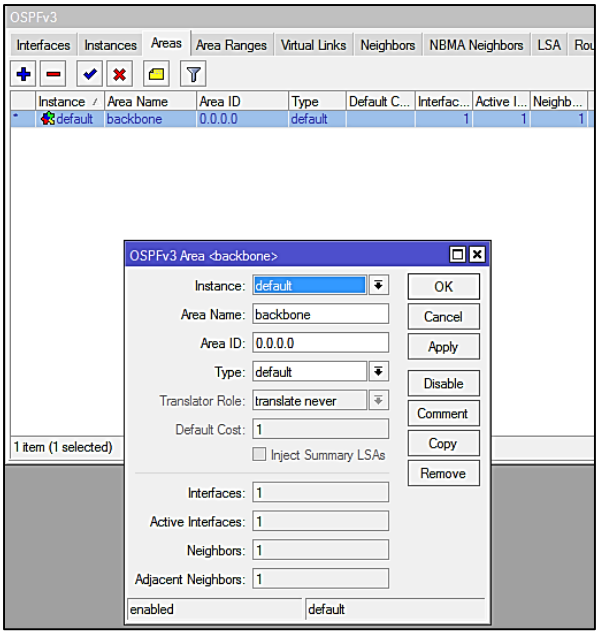
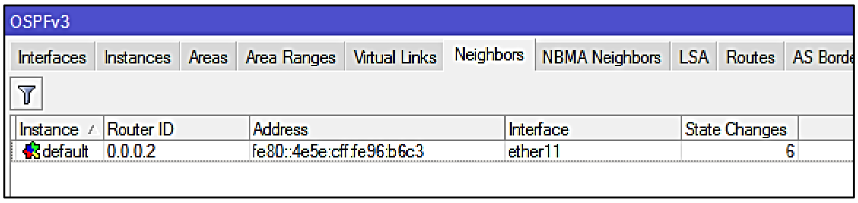


Figura 86: OSPFv3 - Áreas en IPv6 – Switch Core.

Una vez levantado el protocolo de enrutamiento OSPFv3 con las interfaces que intervienen para IPv6, se empiezan a mostrar los “Neighbors” (Nodos Vecinos) y

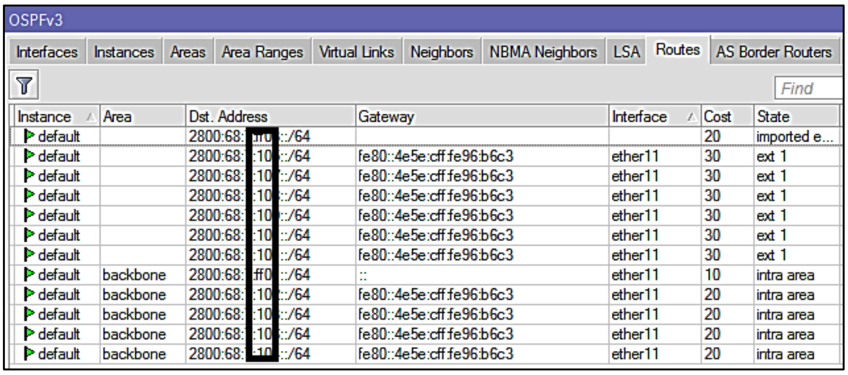
también empieza aprender las rutas para el envío de paquetes y la comunicación entre los equipos.



Instance	Router ID	Address	Interface	State Changes
default	0.0.0.2	fe80::4e5e:cff:fe96:b6c3	ether11	6

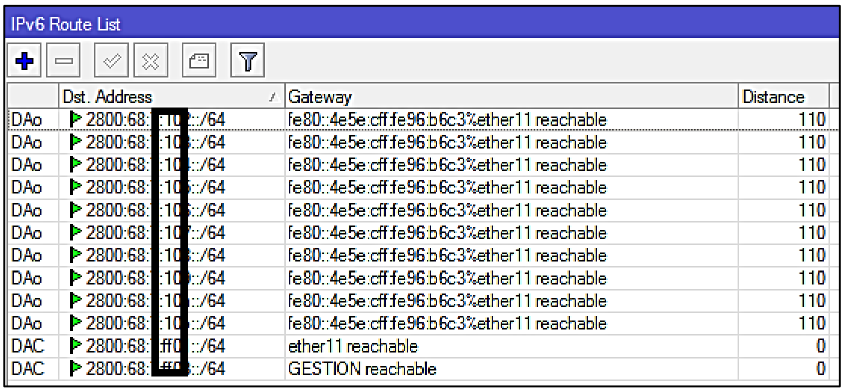
Figura 87: OSPFv3 Neighbors IPv6 – Switch Core.

Para OSPFv3 también se puede apreciar del protocolo de enrutamiento en las siguientes Figuras:



Instance	Area	Dst. Address	Gateway	Interface	Cost	State
default		2800:68:[redacted]::/64			20	imported e...
default		2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3	ether11	30	ext 1
default		2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3	ether11	30	ext 1
default		2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3	ether11	30	ext 1
default		2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3	ether11	30	ext 1
default		2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3	ether11	30	ext 1
default		2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3	ether11	30	ext 1
default	backbone	2800:68:[redacted]::/64	::	ether11	10	intra area
default	backbone	2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3	ether11	20	intra area
default	backbone	2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3	ether11	20	intra area
default	backbone	2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3	ether11	20	intra area
default	backbone	2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3	ether11	20	intra area

Figura 88: OSPFv3 Routes en IPv6 – Switch Core.



	Dst. Address	Gateway	Distance
DAo	2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3%ether11 reachable	110
DAo	2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3%ether11 reachable	110
DAo	2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3%ether11 reachable	110
DAo	2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3%ether11 reachable	110
DAo	2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3%ether11 reachable	110
DAo	2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3%ether11 reachable	110
DAo	2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3%ether11 reachable	110
DAo	2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3%ether11 reachable	110
DAo	2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3%ether11 reachable	110
DAo	2800:68:[redacted]::/64	fe80::4e5e:cff:fe96:b6c3%ether11 reachable	110
DAC	2800:68:[redacted]::/64	ether11 reachable	0
DAC	2800:68:[redacted]::/64	GESTION reachable	0

Figura 89: OSPFv3 Route List en IPv6 – Switch Core.

6.4.1.7. SWITCH DISTRIBUCIÓN: Configuración Protocolo de Internet versión 6 (IPv6)

Para el Switch de Distribución o L3, su configuración queda de la siguiente manera:

- **Agregar dirección IPv6:** se agrega las direcciones “IPv6”, como se lo hizo en el Switch Core en este caso para cada VLAN conforme se muestra en la Figura 86.

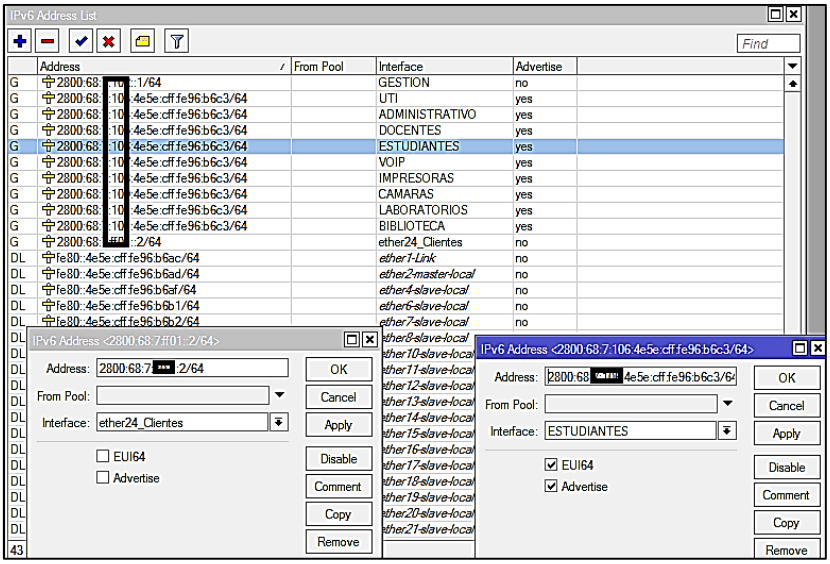


Figura 90: Direcciones IPv6 – Switch Distribución.

- **Crear Pool-DHCPv6:** la siguiente figura presenta la creación de los “Pool” (Piscina de Direcciones) mediante el protocolo dinámico DHCPv6 añadiendo en esta configuración la Técnica EUI-64 para que los usuarios puedan tomar y formar su dirección final combinando la dirección MAC de su equipo y la dirección IPv6 asignada como se lo estudió en la Sección 4.1.9.

Nótese que en el Switch Core no se realizó alguna configuración con el Protocolo Dinámico DHCPv6, la razón; no es necesario ya que el nuevo protocolo IPv6 presenta una de la facilidades de configuración donde solo deba existir la comunicación mediante una sola dirección IPv6 desde el Switch Core hacia el Switch de Distribución.

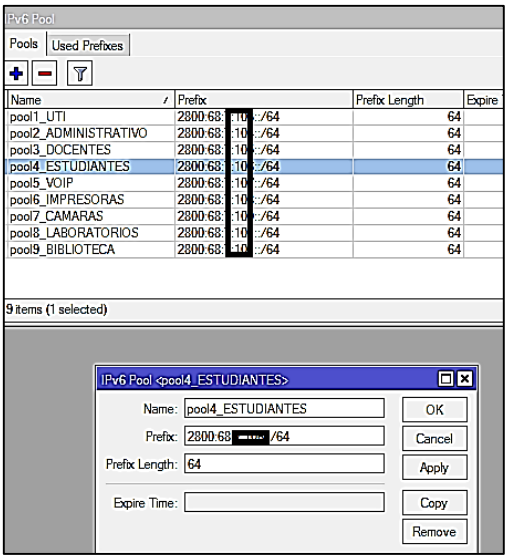


Figura 91: Crear Pool de direcciones IPv6 - Switch Distribución.

- **Crear DHCPv6 Server.** Se crea los "DHCPv6 Server" como se muestra en la figura y se los asigna a los Pool creados anteriormente.

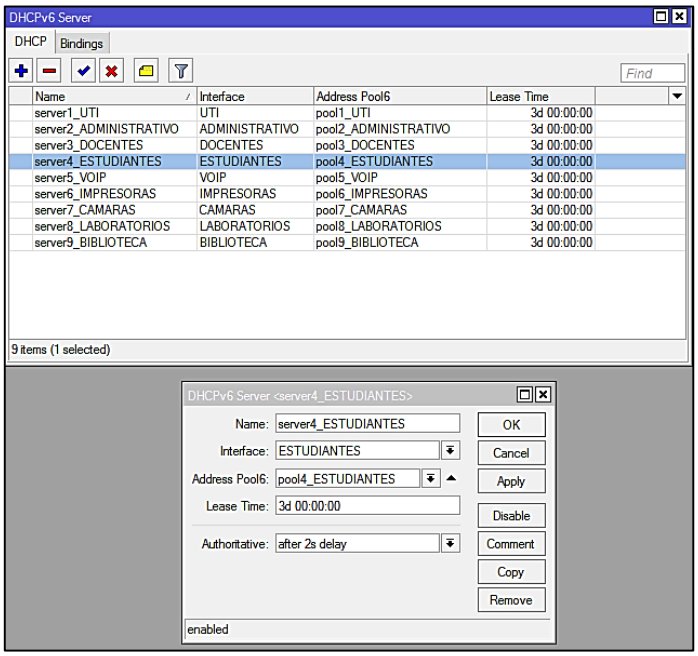


Figura 92: DHCPv6 Server en IPv6 - Switch Distribución.

- **OSPFv3 – Interfaces:** se configura el protocolo OSPFv3, ingresando las interfaces que intervienen en el enrutamiento.

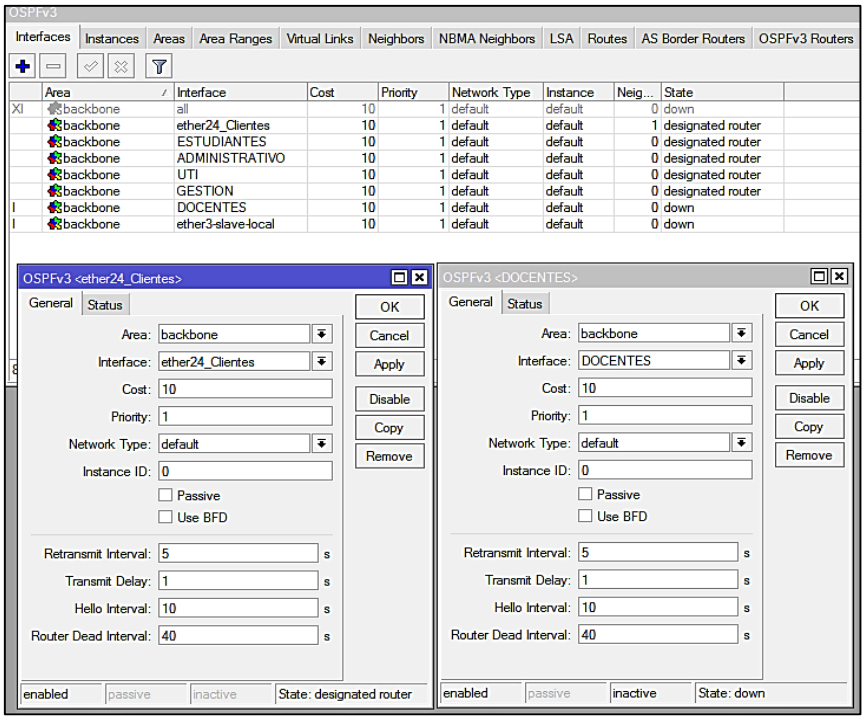


Figura 93: OSPFv3 Interfaces IPv6– Switch Distribución.

- **OSPFv3 – Instances:** se da clic en la pestaña “Instances” y se agrega el Router ID para IPv6.

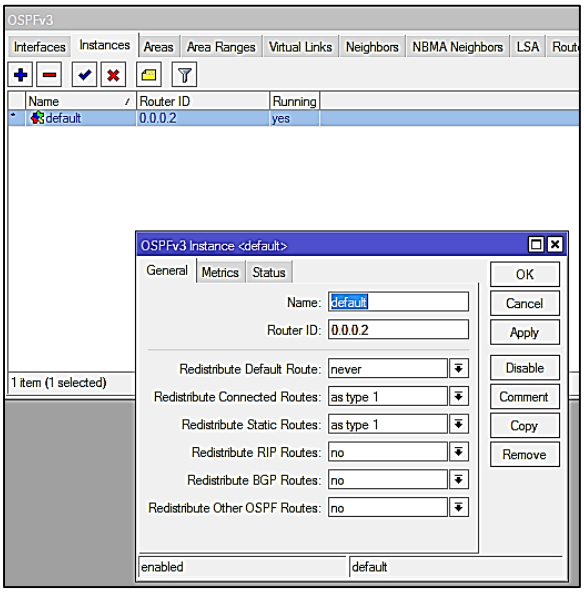


Figura 94: OSPFv3 Instances IPv6 – Switch Distribución.

- **OSPFv3 – Áreas:** como se realizó la configuración para IPv4 así mismo, se toma en cuenta el área (Backbone) y su área ID.

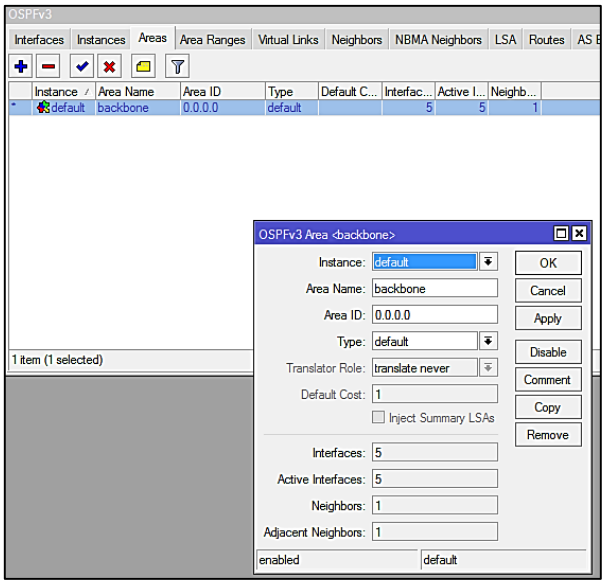


Figura 95: OSPFv3 - Áreas en IPv6 – Switch Distribución.

Una vez levantado el protocolo de enrutamiento OSPFv3 con las interfaces que intervienen para IPv6, se empiezan a mostrar los “Neighbors” (Nodos Vecinos) y también empieza aprender las rutas para el envío de paquetes y la comunicación entre los equipos.

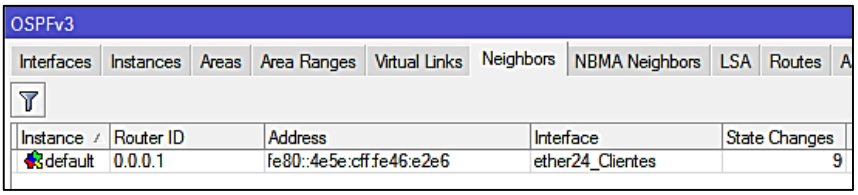


Figura 96: OSPFv3 Neighbors IPv6 – Switch Distribución.

Para OSPFv3 también se puede apreciar las direcciones por el protocolo de enrutamiento y en las siguientes Figuras las podemos observar.

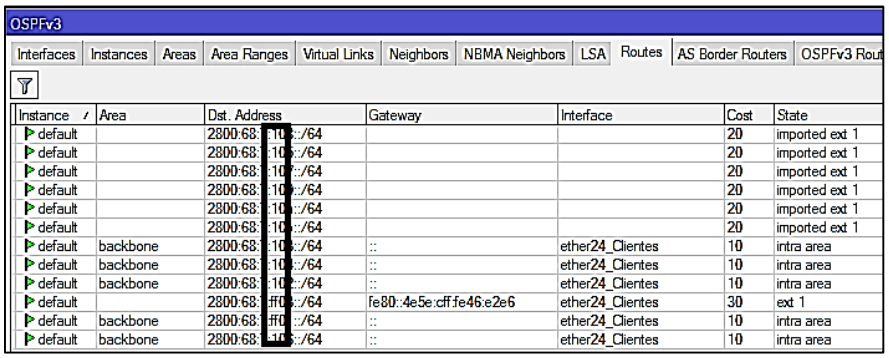


Figura 97: OSPFv3 Routes en IPv6 – Switch Distribución.

IPv6 Route List

	Dst. Address	Gateway	Distance
DAC	2800:68: [redacted] ::/64	GESTION reachable	0
DAC	2800:68: [redacted] ::/64	UTI reachable	0
DAC	2800:68: [redacted] ::/64	ADMINISTRATIVO reachable	0
DAC	2800:68: [redacted] ::/64	br_vlanDOCENTES reachable	0
DAC	2800:68: [redacted] ::/64	ESTUDIANTES reachable	0
DAC	2800:68: [redacted] ::/64	VOIP reachable	0
DAC	2800:68: [redacted] ::/64	br_vlanIMPRESORAS reachable	0
DAC	2800:68: [redacted] ::/64	CAMARAS reachable	0
DAC	2800:68: [redacted] ::/64	LABORATORIOS reachable	0
DAC	2800:68: [redacted] ::/64	BIBLIOTECA reachable	0
DAC	2800:68: [redacted] ::/64	ether24_Clientes reachable	0
DAo	2800:68: [redacted] ::/64	fe80::4e5e:cff:fe46:e2e6%ether24_Clientes reachable	110

Figura 98: OSPFv3 Route List en IPv6 – Switch Distribución.

6.4.1.8. SWITCH ACCESO: Configuración Protocolo de Internet versión 6 (IPv6)

Dentro del contexto de configuración del Switch de Acceso lo único que se procedió a realizar es la ubicación de una dirección IPv6 única y exclusivamente para la VLAN nativa o VLAN de Administración de Equipos ya que no es necesario configurar las demás VLAN creadas con direcciones IPv6 porque en el Switch de Distribución se realiza todas las configuraciones necesarias con el nuevo Protocolo de Internet versión 6.

Se realizaron varias pruebas y comprobaciones mediante el comando “ping -6” desde el usuario final hacia el Switch de Acceso, Switch de Distribución y Switch Core. En las siguientes figuras se detalla.

C:\Windows\system32\cmd.exe

```
Configuración IP de Windows


Adaptador de Ethernet Conexión de red Bluetooth:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Dirección IPv6 . . . . . . . . . . . . : 2800:68:7:106:81aa:9a8d:1f90:f255
   Dirección IPv6 temporal. . . . . . . . : 2800:68:7:106:d85f:301f:2096:ca11
   Vínculo: dirección IPv6 local. . . . : fe80::81aa:9a8d:1f90:f255%12
   Dirección IPv4. . . . . . . . . . . . . . : 10.10.52.254
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::4e5e:cff:fe96:b6c3%12
                                               10.10.52.1

Adaptador de túnel isatap.{035F0857-F9C5-4225-B023-CEEBB832820A}:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

C:\Users\Sony>_
```

Figura 99: Dirección IPv4 e IPv6 usuario final.

```
C:\Users\Sony>
C:\Users\Sony>ping -6 2800:68:7:109:4e5e:cff:fe96:b6c3

Haciendo ping a 2800:68:7:109:4e5e:cff:fe96:b6c3 con 32 bytes de datos:
Respuesta desde 2800:68:7:109:4e5e:cff:fe96:b6c3: tiempo=1ms
Respuesta desde 2800:68:7:109:4e5e:cff:fe96:b6c3: tiempo<1m
Respuesta desde 2800:68:7:109:4e5e:cff:fe96:b6c3: tiempo<1m
Respuesta desde 2800:68:7:109:4e5e:cff:fe96:b6c3: tiempo<1m

Estadísticas de ping para 2800:68:7:109:4e5e:cff:fe96:b6c3:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

Figura 100: Ping -6 VLAN-Cámaras.

```
C:\Users\Sony>
C:\Users\Sony>ping -6 2800:68:7:102::1

Haciendo ping a 2800:68:7:102::1 con 32 bytes de datos:
Respuesta desde 2800:68:7:102::1: tiempo<1m
Respuesta desde 2800:68:7:102::1: tiempo<1m
Respuesta desde 2800:68:7:102::1: tiempo<1m
Respuesta desde 2800:68:7:102::1: tiempo<1m

Estadísticas de ping para 2800:68:7:102::1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Figura 101: Ping -6 Switch Distribución.

```
C:\Users\Sony>
C:\Users\Sony>ping -6 2800:68:7:ff01::1

Haciendo ping a 2800:68:7:ff01::1 con 32 bytes de datos:
Respuesta desde 2800:68:7:ff01::1: tiempo<1m
Respuesta desde 2800:68:7:ff01::1: tiempo<1m
Respuesta desde 2800:68:7:ff01::1: tiempo<1m
Respuesta desde 2800:68:7:ff01::1: tiempo<1m

Estadísticas de ping para 2800:68:7:ff01::1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Figura 102: Ping -6 Switch Core.

Como se puede apreciar, queda levantado ambas pilas de los protocolos de internet tanto para la versión 4 (IPv4) como para la versión 6 (IPv6) funcionando con normalidad con el Mecanismo de Transición utilizado como es Doble Pila; dentro del primer escenario de pruebas planteado.

6.4.1.9. WIRESHARK: Captura de paquetes IPv4 e IPv6

Mediante la herramienta libre Wireshark se puede apreciar con mayor amplitud y conocimiento cada paquete respectivamente de su pila habilitada tanto en IPv4 como en IPv6 así mismo ejecutándose varios de los protocolos de enrutamiento como son: ICMPv4, ICMPv6, ARP, DHCPv6, OSPFv2, OSPFv3; a continuación se analizará ambos Protocolos de Internet para mayor entendimiento:

- **Paquetes ARP en IPv4:** el Protocolo de Resolución de Direcciones encuentra la dirección de hardware o MAC que corresponda al equipo de una determinada dirección IP como se observa en la figura:

  (1) El paquete viaja desde el campo "*Source*"

  (2) Hacia el campo "*Destination*"

  (3) Mediante el protocolo ARP

  (4) Accediendo por su puerta de enlace en el campo "*Info*".

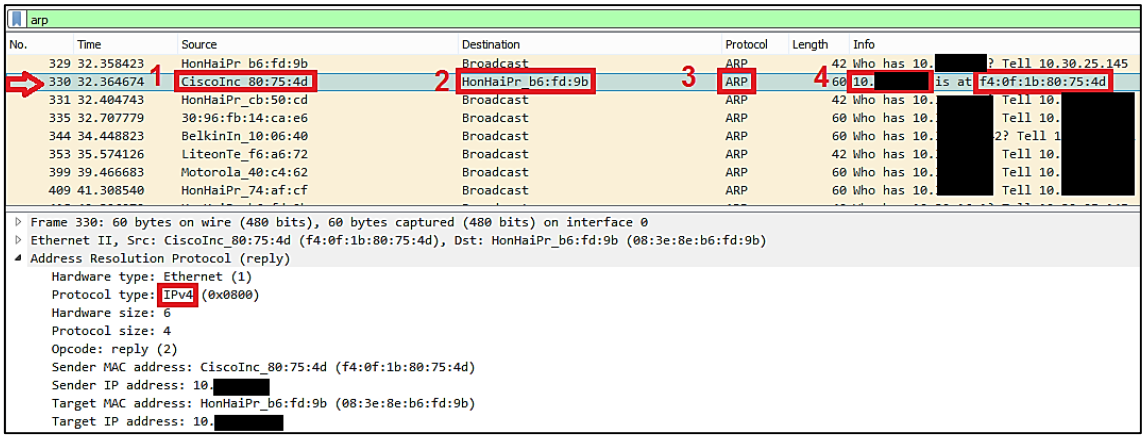


Figura 103: Direcciones Broadcast en IPv4.

- **Paquete DHCPv6:** tomando como referencia la TABLA VI donde menciona los diferentes tipos de mensajes que maneja DHCPv6, la máquina origen envía un mensaje de solicitud para la asignación de un dirección IPv6 al host, esta configuración se da

  (1) Mediante la puerta de enlace predeterminada campo "*Source*" configurada automáticamente por el router.

  (2) Hacia la dirección multicast campo "*Destination*".

  (3) Realizado mediante el protocolo DHCPv6.

  (4) Recibiendo el mensaje de "*Solicit*" en el campo "*Info*".

  En la imagen se observa que identifica al cliente desde donde proviene el mensaje "Solicit" para asignar una dirección IPv6.

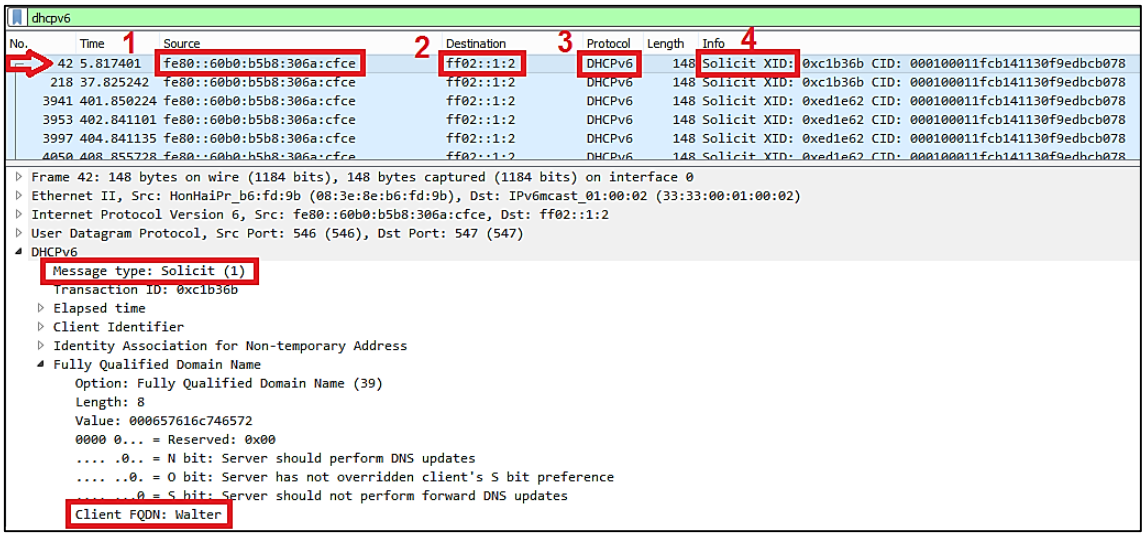


Figura 104: Paquete DHCPv6 para IPv6.

- **Paquetes ICMPv4 - ICMPv6:** con las pruebas de ping realizadas tanto para IPv4 e IPv6 se puede observar el funcionamiento del Protocolo de Control de Mensajes ICMP pudiendo observar las mejoras en el paquete para la versión 6, ya que su cabecera en notablemente simplificada con respecto al paquete de la versión 4 indicando esta diferencia bajo las siguientes figuras.

  (1) Dirección de host origen campo "*Source*".

  (2) Dirección host destino campo "*Destination*"

  (3) Protocolo campo "*Protocol*" "*ICMP*".

  (4) Obtiene solicitud de ping "*request*" campo "*Info*".

  Contestación de solicitud:

  (5) Dirección host destino campo "*Source*".

  (6) Dirección de host origen campo "*Destination*".

  (7) Protocolo campo "*Protocol*" "*ICMP*".

  (8) Obtiene respuesta de ping "*reply*" campo "*Info*".

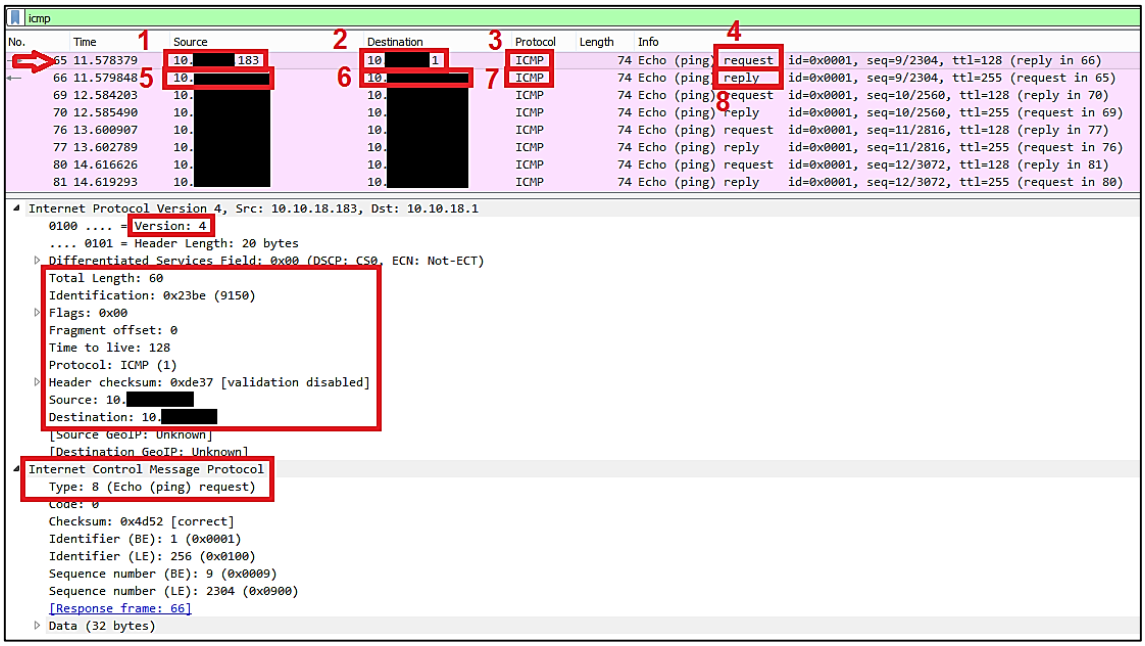


Figura 105: Paquete ICMPv4 para IPv4.

En las siguientes imagenes se observa los diferentes mensajes en funcionamiento con el protocolo ICMPv6: RS (Router Advertisement), RA (Router Solicitation), NA (Neighbor Solicitation), NS (Neighbor Advertisement) y contrarestando la información obtenida de la sección 4.1.11 Principales Protocolos en IPv6, específicamente 4.1.11.2 Neighbor Discovery, podemos observar que al momento de que un host se conecta a la red se proceden a enviar dichos mensajes y recibir contestaciones por parte de los equipos de red configurados con IPv6 llegando a obtener las siguientes capturas de paquetes.

Solicitud de Router (Router Solicitation): lo genera las interfaces de los routers cuando son activadas, pidiendo que se "anuncien" inmediatamente. Este tipo de paquete ICMPv6 tiene el valor de 133.

Anunciación de Router (Router Advertisement): mediante la siguiente figura se realizó el seguimiento del paquete obteniendo los siguientes resultados:

(1) Puerta de enlace campo "*Source*".

(2) Dirección multicast indica todos los nodos del enlace local campo "*Destination*".

(3) Protocolo "*ICMPv6*" campo "*Destination*".

(4) Mensaje RA "*Router Advertisement*" campo "*Info*".

(5) Valor del mensaje ICMPv6 = 134

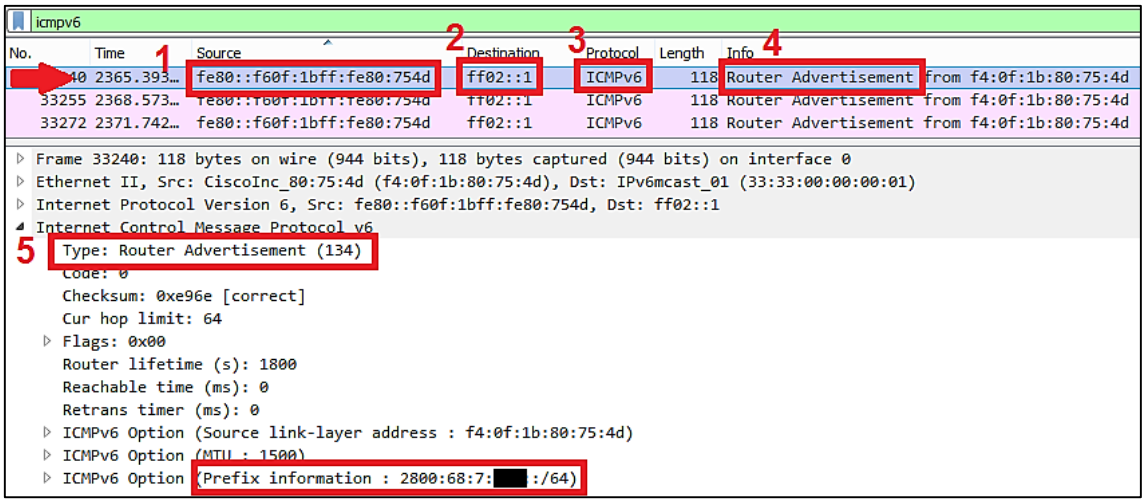


Figura 106: Tipo de mensaje ICMPv6 - RA

Solicitud de Vecino (Neighbor Solicitation): mediante la siguiente imagen se observa como funciona el mensaje NS y que valor debería tomar dicho mensaje.

(1) Desde la puerta de enlace campo "*Source*".

(2) Hacia la dirección de host IPv6 campo "*Destination*".

(3) Protocolo utilizado "*ICMPv6*" campo "*Protocol*".

(4) Tipo de mensaje obtenido NS "*Neighbor Solicitation*" campo "*Info*".

(5) Valor del mensaje ICMPv6 = 135.

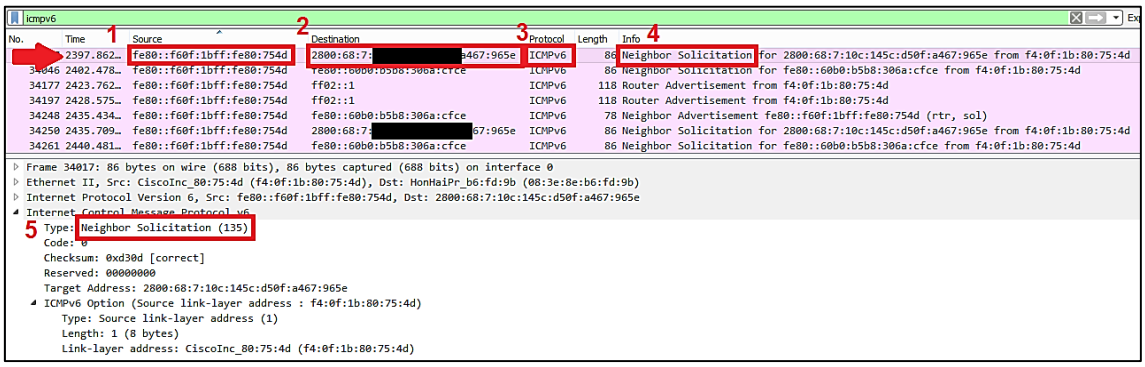


Figura 107: Tipo de mensaje ICMPv6 – NS.

Anunciación de Vecino (Neighbor Advertisement): en la siguiente figura se indica el funcionamiento del mensaje NA.

(1) Desde la puerta de enlace router campo "*Source*".

(2) Hacia la dirección de host IPv6 campo "*Destination*".

(3) Protocolo utilizado "*ICMPv6*" campo "*Protocol*".

(4) Tipo de mensaje obtenido NA "*Neighbor Advertisement*" campo "*Info*".

(5) Valor del mensaje ICMPv6 = 136.

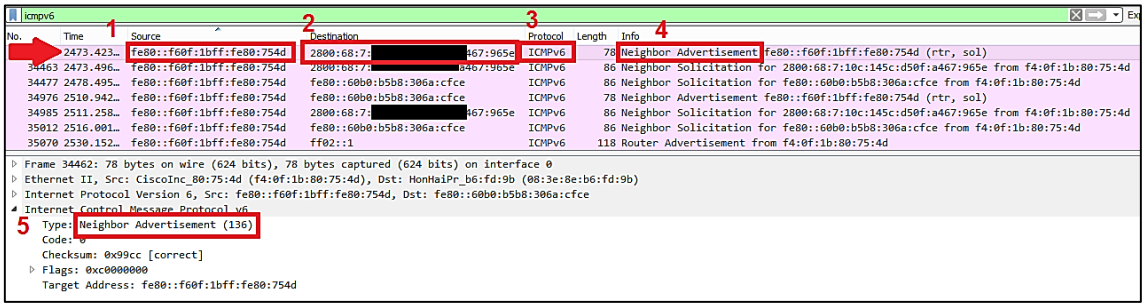


Figura 108: Tipo de mensaje ICMPv6 - NA.

Realizando prueba de ping desde host conectado a la VLAN – Wifi hacia host conectado a la VLAN - Uti directamente con las direcciones IPv6 asignadas a cada host:

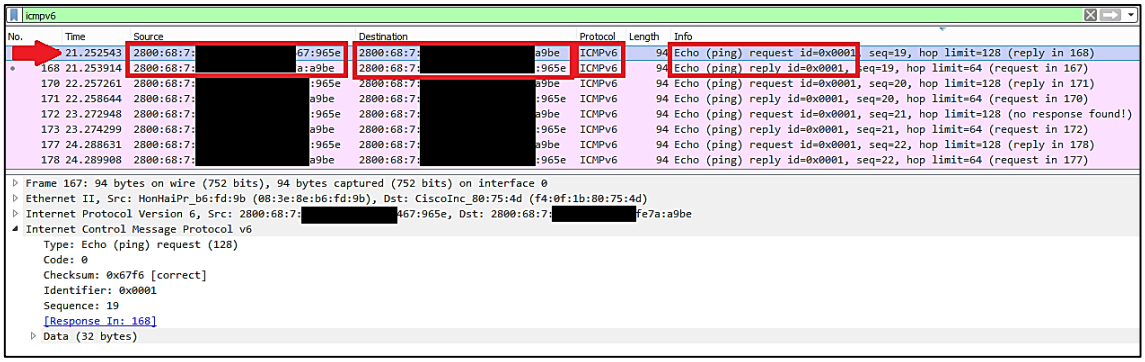


Figura 109: Paquete ICMPv6: IPv6 prueba de ping -6.

- **Paquetes OSPFv2 y OSPFv3:** en este tipo de paquetes la diferencia se da en la versión del protocolo que esta utilizando, los mesajes de “Hello” que realiza en la versión 4 los mismos mensajes se dan para la versión 6 como se muestran en las siguientes figuras.

ospf

No.	Time	Source	Destination	Protocol	Length	Info
14	3.846291	fe80::f60f:1bff:fe80:7543	ff02::5	OSPF	90	Hello Packet
26	6.534824	10.[redacted]	224.0.0.5	OSPF	90	Hello Packet
55	12.977013	fe80::f60f:1bff:fe80:7543	ff02::5	OSPF	90	Hello Packet
67	15.635807	10[redacted]	224.0.0.5	OSPF	90	Hello Packet

```
▷ Frame 26: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
▷ Ethernet II, Src: CiscoInc_80:75:43 (f4:0f:1b:80:75:43), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
▷ Internet Protocol Version 4, Src: 10.[redacted], Dst: 224.0.0.5
◢ Open Shortest Path First
  ◢ OSPF Header
      Version: 2
      Message Type: Hello Packet (1)
      Packet Length: 44
      Source OSPF Router: 10.[redacted]
      Area ID: 0.0.0.0 (Backbone)
      Checksum: 0xb674 [correct]
      Auth Type: Null (0)
      Auth Data (none): 0000000000000000
  ◢ OSPF Hello Packet
      Network Mask: 255.255.255.0
      Hello Interval [sec]: 10
    ▷ Options: 0x12 ((L) LLS Data block, (E) External Routing)
      Router Priority: 1
      Router Dead Interval [sec]: 40
      Designated Router: 10.[redacted]
      Backup Designated Router: 0.0.0.0
  ◢ OSPF LLS Data Block
      Checksum: 0xfff6
      LLS Data Length: 12 bytes
    ▷ Extended options TLV
```

Figura 110: Protocolo OSPFv2 para IPv4.

ospf

No.	Time	Source	Destination	Protocol	Length	Info
14	3.846291	fe80::f60f:1bff:fe80:7543	ff02::5	OSPF	90	Hello Packet
26	6.534824	10.10.18.1	224.0.0.5	OSPF	90	Hello Packet
55	12.977013	fe80::f60f:1bff:fe80:7543	ff02::5	OSPF	90	Hello Packet
67	15.635807	10.10.18.1	224.0.0.5	OSPF	90	Hello Packet

```
▷ Frame 14: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
▷ Ethernet II, Src: CiscoInc_80:75:43 (f4:0f:1b:80:75:43), Dst: IPv6mcast_05 (33:33:00:00:00:05)
▷ Internet Protocol Version 6, Src: fe80::f60f:1bff:fe80:7543, Dst: ff02::5
◢ Open Shortest Path First
  ◢ OSPF Header
      Version: 3
      Message Type: Hello Packet (1)
      Packet Length: 36
      Source OSPF Router: 1.1.1.1
      Area ID: 0.0.0.0 (Backbone)
      Checksum: 0x6ba1 [correct]
      Instance ID: IPv6 unicast AF (0)
      Reserved: 00
  ◢ OSPF Hello Packet
      Interface ID: 2071
      Router Priority: 1
    ▷ Options: 0x000013 (R, E, V6)
      Hello Interval [sec]: 10
      Router Dead Interval [sec]: 40
      Designated Router: 1.1.1.1
      Backup Designated Router: 0.0.0.0
```

Figura 111: Protocolo OSPFv3 para IPv6.

- **Comparación cabecera IPv4 e IPv6:** una vez obtenidos ambos paquetes tanto de IPv4 como de IPv6 procedemos a realizar el siguiente análisis comparando los campos eliminados, los campos que no se utilizan y los campos que han cambiado de nombre y posición de IPv4 frente al nuevo protocolo IPv6 mediante la información y colores de cada campo obtenidos de la revisión literaria en la Sección 4.1.3 Formato de cabecera IPv6. La Figura 112 muestra lo expuesto:

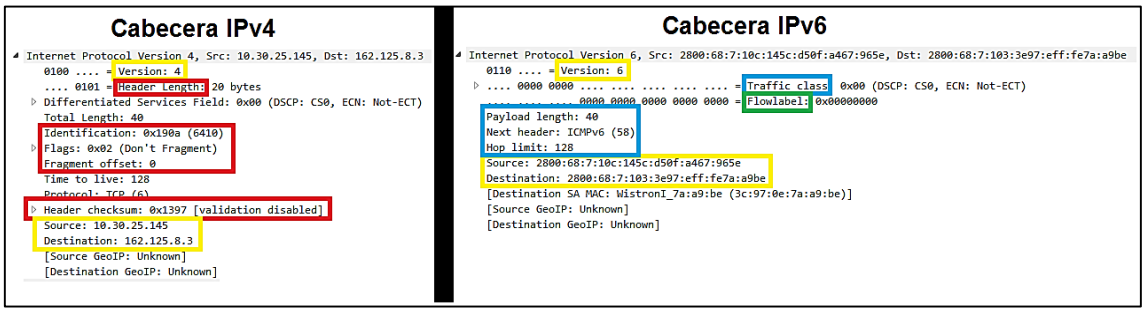


Figura 112: Comparativa Cabeceras IPv4 – IPv6.

- **Comparación cabecera IPv4 e IPv6 Protocolo OSPF:** así mismo se realiza una comparativa entre las cabeceras de los paquetes con el protocolo OSPF tanto en la versión 4 como en la versión 6 y se observa como en IPv6 su cabecera es mucho mas simplificada que en IPv4, indicándonos:

  Cabecera IPv4 - OSPFv2:

  (1) Versión = 2 “IPv4 – OSPFv2”.

  (2) Longitud de paquete = 44

  (3) Source = asignado por puerta de enlace de router.

  (4) Área de Backbone “0.0.0.0”.

  (5) Designated = asignado por puerta de enlace de router.

  Cabecera IPv6 – OSPFv3:

  (1) Versión = 3; “IPv4 – OSPFv3”.

  (2) Longitud de paquete = 36.

  (3) Source = asignado por el “*Router-ID*” configurado en el router.

  (4) Área de Backbone “0.0.0.0”.

  (5) Designated = asignado por el “*Router-ID*” configurado en el router.

  Notamos que en la cabecera del paquete IPv6 del protocolo OSPFv3 estudiado el campo de “*OSPF LLS Data Block*” se elimina, dando mayor velocidad de respuesta.

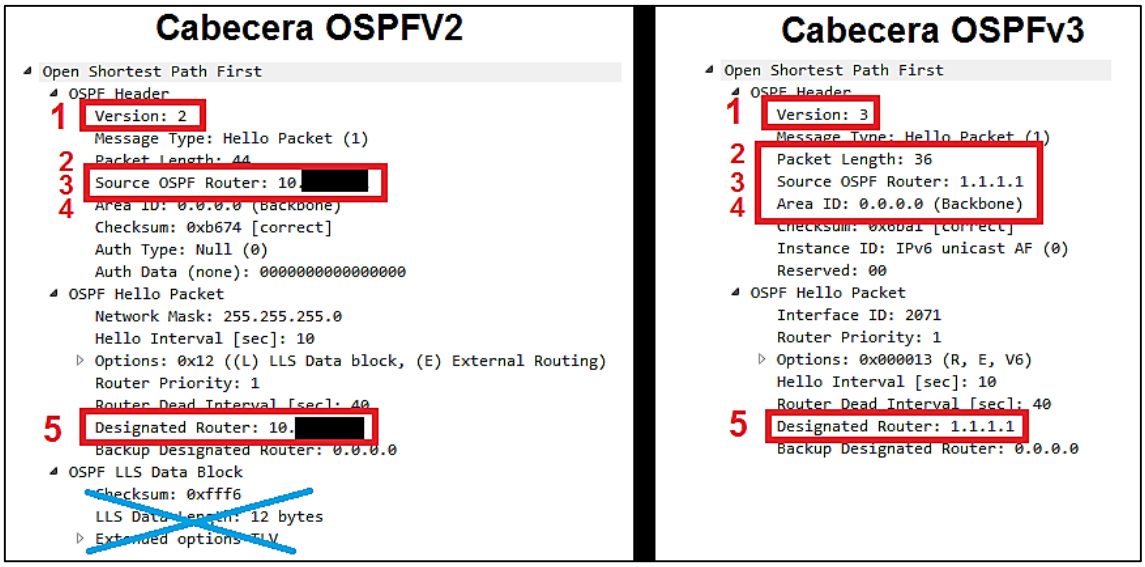


Figura 113: Comparativa Cabecera OSPFv2 – OSPFv3.

6.4.2. ESCENARIO DE PRUEBAS 2: Simulador de Redes GNS3

Para el escenario de Pruebas 2 se utilizó lo que es el Simulador de Redes GNS3, realizando una tabla comparativa de los simuladores populares y más utilizados por los administradores de redes.

TABLA XXI: COMPARACIÓN DE SIMULADORES DE REDES.

Simulador	Soporte IPv6	Sistema operativo	Protocolos de ruteo	RAM mínima requerida	Espacio en disco	Tipo licencia
NEST	No	Unix	Los más básicos	256 MB	400 MB	Libre
MaRS	No	Unix y Windows	RIP, IS-IS y OSPF	512 MB	400 MB	Libre
SSF	No	Linux y Windows	RIP, OSPF, IGRP, IS-IS y BGP	512 MB	300 MB	Libre y propietario
J-Sim	No	Multiplataforma	RIP, OSPFv2, DVMRP, MOSPF y CBT	256 MB	200 MB	Libre
Ns-2	No	Linux, Mac OS y Windows	RIP, IS-IS y OSPF	256 MB	320 MB	Libre

Real	No	Linux	RIP, IS-IS y OSPF	512 MB	300 MB	Libre y propietario
NCTUns 2.0	No	Windows y Linux	RIP, OSPF y EIGRP	256 MB	400 MB	Propietario
Packet Tracer	Si	Linux y Windows	RIP,RIPng, EIGRP OSPF, OSPFv3	256 MB	400 MB	Propietario
OPNET IT Guru Academic	No	Windows	BGP,EIGRP, IGMP, IS-IS, IGRP, OSPF, RIP.	256 MB	400 MB	Libre
OPNET Modeler	Si	Windows	BGP,EIGRP, IGMP, IS-IS, IGRP, OSPF, RIP, MPLS y OSPFv3.	512 MB	600 MB	Propietario
GNS3	Si	Linux, Windows y Mac OS	IGRP, OSPF, RIP, RIPng, BGP, OSPF y OSPFv3.	512 MB	100 MB	Libre

El poder contar con un ambiente de simulación lo más apegado a la realidad, es el objetivo principal de un simulador. GNS3[10] es un simulador gráfico de redes que permite diseñar fácilmente topologías de red y luego ejecutar simulaciones de las mismas. Es ejecutado sobre Dynamips (programa básico que permite la emulación de imágenes de sistemas operativos de ruteadores y switches) para crear un entorno gráfico, haciéndolo más amigable de usar.

Como se lo puede apreciar en la TABLA XXI, GNS3 es el simulador accesible acorde a los requerimientos que se necesitan para la implementación de IPv6 en la Universidad Nacional de Loja y consta de lo necesario para poder simular ambos protocolos IPv4 e IPv6.

Es ampliamente conocido para la simulación de redes y de fácil uso ya que cuenta con una interfaz gráfica, trabaja bajo múltiples plataformas de software Windows, Linux, MacOS X. GNS3 a través de Dynamips, permite emular el IOS real de Cisco de los

[10] http://www.gns3.net

cuales soporta c1700 serie, c2600 serie, c3620, c3640, c3660, c2691, c3725, c3745, c7200 serie, Cisco Catalyst Switches.

Para la simulación de la red se hace uso de 5 enrutadores c3725 los cuales cuentan con interfaces fastEthernet y con el IOS 15.2 (4) M8, características necesarias para soportar tanto para IPv4/IPv6 y 2 PC para comprobar las direcciones IPv6 asignadas. Así mismo las facultades que vamos a enrutar son: Facultad de Administración – Departamento UTI y Facultad de Energía – Departamento Biblioteca.

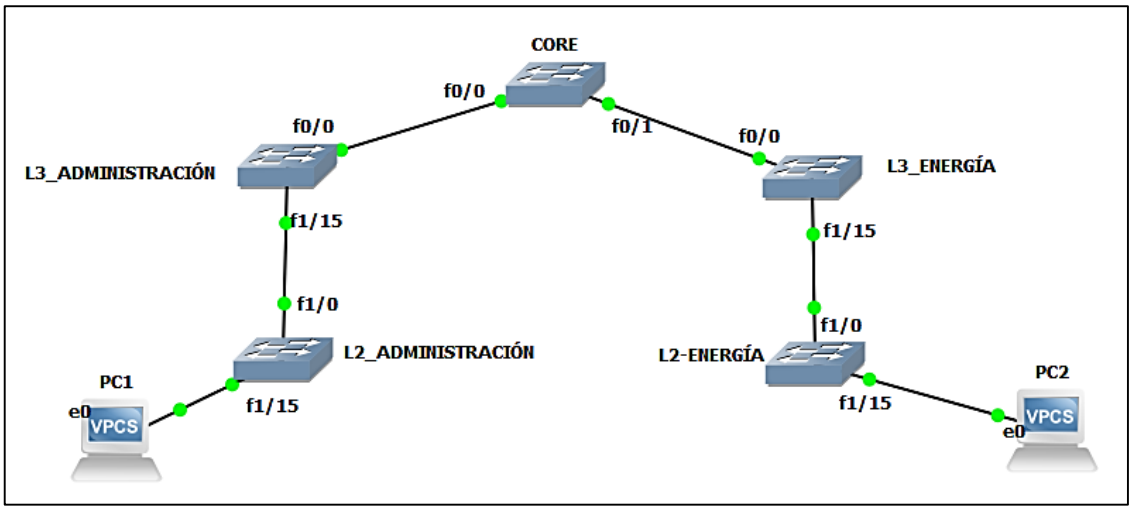


Figura 114: Topología de Red para el despliegue de IPv6 – GNS3.

Tomando en cuenta para las configuraciones necesarias se optó por utilizar las direcciones IPv6 reales y para su documentación se tomó en cuenta el direccionamiento realizado bajo el prefijo de documentación de IPv6.

6.4.2.1. Configuración Switch CORE

Como los equipos que se utilizan en el simulador son de la marca CISCO, no tendremos problemas en los comandos a utilizar.

Sus configuraciones quedan de la siguiente manera.

- **Configuración interfaz fa0/0**

```
CORE#configure terminal
CORE(config)#ipv6 unicast-routing
CORE (config)#interface fastEthernet 0/0
CORE (config-if)#ipv6 address 2001:DB8:3003:ADA2::FFFF/64
CORE (config-if)#no shutdown
CORE (config-if)#exit
```

- **Configuración interfaz fa0/1**

```
CORE#configure terminal
CORE(config)#ipv6 unicast-routing
CORE(config)#interface fastEthernet 0/1
```

```
CORE(config-if)#ipv6 address 2001:DB8:3003:ADA8::FFFF/64
CORE(config-if)#no shutdown
CORE(config-if)#exit
```

- **Configuración OSPFv3**

```
CORE#configure terminal
CORE(config)#ipv6 router ospf 1
CORE(config-rtr)#router-id 1.1.1.1
CORE(config-rtr)#exit

CORE(config)#interface fastEthernet 0/0
CORE(config-if)#ipv6 enable
CORE(config-if)#ipv6 ospf 1 area 0
CORE(config-if)#exit

CORE(config)#interface fastEthernet 0/1
CORE(config-if)#ipv6 enable
CORE(config-if)#ipv6 ospf 1 area 0
CORE(config-if)#exit
```

6.4.2.2. Configuración de Switch L3 Facultad Administración - Departamento UTI

Para el Switch de Distribución o L3 de Administración se realiza las siguientes configuraciones:

- **Configuración interfaz fa0/0**

```
ADMINISTRACIÓN_L3#configure terminal
ADMINISTRACIÓN_L3(config)#ipv6 unicast-routing
ADMINISTRACIÓN_L3(config)#interface fastEthernet 0/0
ADMINISTRACIÓN_L3(config-if)#ipv6 address 2001:DB8:3003:ADA2::FFFE/64
ADMINISTRACIÓN_L3(config-if)#no shutdown
ADMINISTRACIÓN_L3(config-if)#exit
```

- **Configuración VLAN de Administración de Equipos (VLAN-Nativa)**

```
ADMINISTRACIÓN_L3(config)#interface vlan 2
ADMINISTRACIÓN_L3(config-if)#ipv6 address 2001:DB8:3003:1A3::FFFF/64
ADMINISTRACIÓN_L3(config-if)#no shutdown
ADMINISTRACIÓN_L3(config-if)#exit
```

- **Crear y configurar VLAN 4: TESIS_IPV6**

```
ADMINISTRACIÓN_L3(config)#vlan 4
ADMINISTRACIÓN_L3(config-if)#name TESIS_IPV6
ADMINISTRACIÓN_L3(config-if)#exit
ADMINISTRACIÓN_L3(config)#interface vlan 4
ADMINISTRACIÓN_L3(config-if)#ipv6 address 2001:DB8:3003:1A4::FFFF/64
ADMINISTRACIÓN_L3(config-if)#no shutdown
ADMINISTRACIÓN_L3(config-if)#exit

ADMINISTRACIÓN_L3(config)#interface fasttEthernet1/15
ADMINISTRACIÓN_L3(config-if)#swicthport trunk encapsulation dot1q
ADMINISTRACIÓN_L3(config-if)#switchport trunk native vlan 2
ADMINISTRACIÓN_L3(config-if)#switchport trunk allowed vlan 2,4
ADMINISTRACIÓN_L3(config-if)#switchport mode trunk
ADMINISTRACIÓN_L3(config-if)#no shutdown
ADMINISTRACIÓN_L3(config-if)#exit
```

- **Configuración DHCPv6 STATELES y STATEFUL**

```
ADMINISTRACIÓN_L3(config)#ipv6 dhcp pool STATEFUL_TESIS_IPV6
ADMINISTRACIÓN_L3(config-dhcpv6)#prefix-delegation 2001:DB8:3003:1A4::/64 600
```

```
ADMINISTRACIÓN_L3(config-dhcpv6)#dns-server 2001:DB8:3003:ACA5::1234
ADMINISTRACIÓN_L3(config-dhcpv6)#domain-name TESIS_IPV6.COM
ADMINISTRACIÓN_L3(config-dhcpv6)#exit

ADMINISTRACIÓN_L3(config)#interface vlan 4
ADMINISTRACIÓN_L3(config-if)#ipv6 enable
ADMINISTRACIÓN_L3(config-if)#ipv6 address 2001:DB8:3003:1A4::FFFF/64 eui-64
ADMINISTRACIÓN_L3(config-if)#ipv6 dhcp server STATEFUL_TESIS_IPV6
ADMINISTRACIÓN_L3(config-if)#ipv6 nd managed-config-flag
ADMINISTRACIÓN_L3(config-if)#ipv6 nd other-config-flag
ADMINISTRACIÓN_L3(config-dhcpv6)#exit
```

- **Configuración OSPFv3**

```
ADMINISTRACIÓN_L3#configure terminal
ADMINISTRACIÓN_L3(config)#ipv6 router ospf 1
ADMINISTRACIÓN_L3(config-rtr)#router-id 2.2.2.2
ADMINISTRACIÓN_L3(config-rtr)#exit

ADMINISTRACIÓN_L3(config)#interface fastEthernet1/15
ADMINISTRACIÓN_L3(config-if)#ipv6 enable
ADMINISTRACIÓN_L3(config-if)#ipv6 ospf 1 area 0
ADMINISTRACIÓN_L3(config-if)#exit

ADMINISTRACIÓN_L3(config)#interface vlan 2
ADMINISTRACIÓN_L3(config-if)#ipv6 enable
ADMINISTRACIÓN_L3(config-if)#ipv6 ospf 1 area 0
ADMINISTRACIÓN_L3(config-if)#exit

ADMINISTRACIÓN_L3(config)#interface vlan 4
ADMINISTRACIÓN_L3(config-if)#ipv6 enable
ADMINISTRACIÓN_L3(config-if)#ipv6 ospf 1 area 0
ADMINISTRACIÓN_L3(config-if)#exit
```

6.4.2.3. Configuración Switch L2 Facultad Administración - Departamento UTI

Configuraciones necesarias para el Protocolo de Internet versión 6 (IPv6).

- **Configuración VLAN de Administración de Equipos (VLAN-Nativa)**

```
ADMINISTRACIÓN_L2#configure terminal
ADMINISTRACIÓN_L2(config)#interface vlan 2
ADMINISTRACIÓN_L2(config-if)#ipv6 address 2001:DB8:3003:1A3::FFFE/64
ADMINISTRACIÓN_L2(config-if)#no shutdown
ADMINISTRACIÓN_L2(config-if)#exit
```

- **Habilitar puerto Troncal**

```
ADMINISTRACIÓN_L2(config)#interface fastEthernet1/0
ADMINISTRACIÓN_L2(config-if)#switchport trunk native vlan 2
ADMINISTRACIÓN_L2(config-if)#switchport trunk allowed vlan 2-4
ADMINISTRACIÓN_L2(config-if)#switchport mode trunk
ADMINISTRACIÓN_L2(config-if)#no shutdown
ADMINISTRACIÓN_L2(config-if)#exit
```

- **Asignar puertos de VLAN 4 a la interfaz**

```
ADMINISTRACIÓN_L2(config)#interface fastEthernet1/15
ADMINISTRACIÓN_L2(config-if)#switchport mode access
ADMINISTRACIÓN_L2(config-if)#switch access vlan 4
ADMINISTRACIÓN_L2(config-if)#exit
```

6.4.2.4. PC1: Usuario Final - Administración

Se verifica la asignación de la dirección IPv6 asignada dinámicamente mediante DHCPv6.

```
PC1> show ipv6

NAME               : PC1[1]
LINK-LOCAL SCOPE   : fe80::250:79ff:fe66:6800/64
GLOBAL SCOPE       : 2800:68:7:103:2050:79ff:fe66:6800/64
ROUTER LINK-LAYER  : c2:01:11:90:00:00
MAC                : 00:50:79:66:68:00
LPORT              : 10002
RHOST:PORT         : 127.0.0.1:10003
MTU:               : 1500
```

Figura 115: Asignación de Dirección IPv6 Administración.

Se menciona que hay algunas limitantes con respecto a los simuladores ya que en este escenario de pruebas como se ve en la figura nos indica su dirección IPv6 con la técnica EUI-64, su puerta de enlace que viene hacer “LINK-LOCAL SCOPE” pero más no lo que es información del DNS y nombre de dominio que están configurados en DHCPv6.

6.4.2.5. Pruebas de conectividad

Se pudo comprobar la conectividad que existe desde el PC de usuario final de Administración hacia todas las rutas llegando al Switch CORE como se muestra en la siguiente figura.

```
PC1> ping 2800:68:7:ff01::ffff

2800:68:7:ff01::ffff icmp6_seq=1 ttl=63 time=78.495 ms
2800:68:7:ff01::ffff icmp6_seq=2 ttl=63 time=47.436 ms
2800:68:7:ff01::ffff icmp6_seq=3 ttl=63 time=48.962 ms
2800:68:7:ff01::ffff icmp6_seq=4 ttl=63 time=47.090 ms
2800:68:7:ff01::ffff icmp6_seq=5 ttl=63 time=47.194 ms

PC1> ping 2800:68:7:ff01::fffe

2800:68:7:ff01::fffe icmp6_seq=1 ttl=64 time=16.111 ms
2800:68:7:ff01::fffe icmp6_seq=2 ttl=64 time=15.955 ms
2800:68:7:ff01::fffe icmp6_seq=3 ttl=64 time=17.525 ms
2800:68:7:ff01::fffe icmp6_seq=4 ttl=64 time=15.799 ms
2800:68:7:ff01::fffe icmp6_seq=5 ttl=64 time=15.664 ms

PC1> ping 2800:68:7:102::ffff

2800:68:7:102::ffff icmp6_seq=1 ttl=64 time=16.056 ms
2800:68:7:102::ffff icmp6_seq=2 ttl=64 time=16.253 ms
2800:68:7:102::ffff icmp6_seq=3 ttl=64 time=14.797 ms
2800:68:7:102::ffff icmp6_seq=4 ttl=64 time=15.939 ms
2800:68:7:102::ffff icmp6_seq=5 ttl=64 time=16.204 ms

PC1> ping 2800:68:7:102::fffe

2800:68:7:102::fffe icmp6_seq=1 ttl=63 time=47.569 ms
2800:68:7:102::fffe icmp6_seq=2 ttl=63 time=47.271 ms
2800:68:7:102::fffe icmp6_seq=3 ttl=63 time=47.252 ms
2800:68:7:102::fffe icmp6_seq=4 ttl=63 time=47.182 ms
2800:68:7:102::fffe icmp6_seq=5 ttl=63 time=47.268 ms

PC1> ping 2800:68:7:103::ffff

2800:68:7:103::ffff icmp6_seq=1 ttl=64 time=15.854 ms
2800:68:7:103::ffff icmp6_seq=2 ttl=64 time=15.834 ms
2800:68:7:103::ffff icmp6_seq=3 ttl=64 time=15.879 ms
2800:68:7:103::ffff icmp6_seq=4 ttl=64 time=15.926 ms
2800:68:7:103::ffff icmp6_seq=5 ttl=64 time=16.386 ms

PC1>
```

Figura 116: Conectividad desde PC1-Administración hacia Switch CORE.

6.4.2.6. Configuración de Switch L3 Facultad Energía - Departamento Biblioteca

Para el Switch de Distribución o L3 de Energía se realiza las siguientes configuraciones:

- **Configuración interfaz fa0/0**

```
ENERGIA_L3#configure terminal
ENERGIA_L3(config)#ipv6 unicast-routing
ENERGIA_L3(config)#interface fastEthernet 0/0
ENERGIA_L3(config-if)#ipv6 address 2001:DB8:3003:ADA8::FFFE/64
ENERGIA_L3(config-if)#no shutdown
ENERGIA_L3(config-if)#exit
```

- **Configuración VLAN de Administración de Equipos (VLAN-Nativa)**

```
ENERGIA_L3(config)#interface vlan 2
ENERGIA_L3(config-if)#ipv6 address 2001:DB8:3003:7A3::FFFF/64
ENERGIA_L3(config-if)#no shutdown
ENERGIA_L3(config-if)#exit
```

- **Crear y configurar VLAN 4: TESIS_IPV6**

```
ENERGIA_L3(config)#vlan 4
ENERGIA_L3(config-if)#name TESIS_IPV6
ENERGIA_L3(config-if)#exit
ENERGIA_L3(config)#interface vlan 4
ENERGIA_L3(config-if)#ipv6 address 2001:DB8:3003:7A6::FFFF/64
ENERGIA_L3(config-if)#no shutdown
ENERGIA_L3(config-if)#exit

ENERGIA_L3(config)#interface fasttEthernet1/15
ENERGIA_L3(config-if)#swicthport trunk encapsulation dot1q
ENERGIA_L3(config-if)#switchport trunk native vlan 2
ENERGIA_L3(config-if)#switchport trunk allowed vlan 2,4
ENERGIA_L3(config-if)#switchport mode trunk
ENERGIA_L3(config-if)#no shutdown
ENERGIA_L3(config-if)#exit
```

- **Configuración DHCPv6 STATELES y STATEFUL**

```
ENERGIA_L3(config)#ipv6 dhcp pool STATEFUL_TESIS_IPV6
ENERGIA_L3(config-dhcpv6)#prefix-delegation 2001:DB8:3003:7A6::/64 600
ENERGIA_L3(config-dhcpv6)#dns-server 2001:DB8:3003:ACA5::1234
ENERGIA_L3(config-dhcpv6)#domain-name TESIS_IPV6.COM
ENERGIA_L3(config-dhcpv6)#exit

ENERGIA_L3(config)#interface vlan 4
ENERGIA_L3(config-if)#ipv6 enable
ENERGIA_L3(config-if)#ipv6 address 2001:DB8:3003:7A6::FFFF/64 eui-64
ENERGIA_L3(config-if)#ipv6 dhcp server STATEFUL_TESIS_IPV6
ENERGIA_L3(config-if)#ipv6 nd managed-config-flag
ENERGIA_L3(config-if)#ipv6 nd other-config-flag
ENERGIA_L3(config-dhcpv6)#exit
```

- **Configuración OSPFv3**

```
ENERGIA_L3#configure terminal
ENERGIA_L3(config)#ipv6 router ospf 1
ENERGIA_L3(config-rtr)#router-id 3.3.3.3
ENERGIA_L3(config-rtr)#exit

ENERGIA_L3(config)#interface fastEthernet1/15
ENERGIA_L3(config-if)#ipv6 enable
ENERGIA_L3(config-if)#ipv6 ospf 1 area 0
```

ENERGIA_L3(config-if)#exit

ENERGIA_L3(config)#interface vlan 2
ENERGIA_L3(config-if)#ipv6 enable
ENERGIA_L3(config-if)#ipv6 ospf 1 area 0
ENERGIA_L3(config-if)#exit

ENERGIA_L3(config)#interface vlan 4
ENERGIA_L3(config-if)#ipv6 enable
ENERGIA_L3(config-if)#ipv6 ospf 1 area 0
ENERGIA_L3(config-if)#exit

6.4.2.7. Configuración Switch L2 Facultad Energía - Departamento Biblioteca

Se debe realizar para el Switch L2 las siguientes configuraciones:

- **Configuración VLAN de Administración de Equipos (VLAN-Nativa)**

ENERGIA_L2#configure terminal
ENERGIA_L2(config)#interface vlan 2
ENERGIA_L2(config-if)#ipv6 address 2001:DB8:3003:7A3::FFFE/64
ENERGIA_L2(config-if)#no shutdown
ENERGIA_L2(config-if)#exit

- **Habilitar puerto Troncal**

ENERGIA_L2(config)#interface fastEthernet1/0
ENERGIA_L2(config-if)#switchport trunk native vlan 2
ENERGIA_L2(config-if)#switchport trunk allowed vlan 2-4
ENERGIA_L2(config-if)#switchport mode trunk
ENERGIA_L2(config-if)#no shutdown
ENERGIA_L2(config-if)#exit

- **Asignar puertos de VLAN 4 a la interfaz**

ENERGIA_L2(config)#interface fastEthernet1/15
ENERGIA_L2(config-if)#switchport mode access
ENERGIA_L2(config-if)#switch access vlan 4
ENERGIA_L2(config-if)#exit

6.4.2.8. PC1: Usuario Final – Energía

Se verifica la dirección IPv6 asignada a usuario final de la Facultad de Energía.

```
PC2> show ipv6

NAME               : PC2[1]
LINK-LOCAL SCOPE   : fe80::250:79ff:fe66:6801/64
GLOBAL SCOPE       : 2800:68:7:705:2050:79ff:fe66:6801/64
ROUTER LINK-LAYER  : c2:01:11:90:00:00
MAC                : 00:50:79:66:68:01
LPORT              : 10004
RHOST:PORT         : 127.0.0.1:10005
MTU:               : 1500
```

Figura 117: Asignación de Dirección IPv6 Energía.

6.4.2.9. Pruebas de conectividad

La conectividad se la realizó desde el PC de usuario final de Energía hacia todas las rutas llegando al Switch CORE como se muestra en la siguiente figura.

```
PC1> ping 2800:68:7:ff07::ffff

2800:68:7:ff07::ffff icmp6_seq=1 ttl=63 time=78.495 ms
2800:68:7:ff07::ffff icmp6_seq=2 ttl=63 time=47.436 ms
2800:68:7:ff07::ffff icmp6_seq=3 ttl=63 time=48.962 ms
2800:68:7:ff07::ffff icmp6_seq=4 ttl=63 time=47.090 ms
2800:68:7:ff07::ffff icmp6_seq=5 ttl=63 time=47.194 ms

PC1> ping 2800:68:7:ff07::fffe

2800:68:7:ff07::fffe icmp6_seq=1 ttl=64 time=16.111 ms
2800:68:7:ff07::fffe icmp6_seq=2 ttl=64 time=15.955 ms
2800:68:7:ff07::fffe icmp6_seq=3 ttl=64 time=17.525 ms
2800:68:7:ff07::fffe icmp6_seq=4 ttl=64 time=15.799 ms
2800:68:7:ff07::fffe icmp6_seq=5 ttl=64 time=15.664 ms

PC1> ping 2800:68:7:702::ffff

2800:68:7:702::ffff icmp6_seq=1 ttl=64 time=16.056 ms
2800:68:7:702::ffff icmp6_seq=2 ttl=64 time=16.253 ms
2800:68:7:702::ffff icmp6_seq=3 ttl=64 time=14.797 ms
2800:68:7:702::ffff icmp6_seq=4 ttl=64 time=15.939 ms
2800:68:7:702::ffff icmp6_seq=5 ttl=64 time=16.204 ms

PC1> ping 2800:68:7:702::fffe

2800:68:7:702::fffe icmp6_seq=1 ttl=63 time=47.569 ms
2800:68:7:702::fffe icmp6_seq=2 ttl=63 time=47.271 ms
2800:68:7:702::fffe icmp6_seq=3 ttl=63 time=47.252 ms
2800:68:7:702::fffe icmp6_seq=4 ttl=63 time=47.182 ms
2800:68:7:702::fffe icmp6_seq=5 ttl=63 time=47.268 ms

PC1> ping 2800:68:7:705::ffff

2800:68:7:705::ffff icmp6_seq=1 ttl=64 time=15.854 ms
2800:68:7:705::ffff icmp6_seq=2 ttl=64 time=15.834 ms
2800:68:7:705::ffff icmp6_seq=3 ttl=64 time=15.879 ms
2800:68:7:705::ffff icmp6_seq=4 ttl=64 time=15.926 ms
2800:68:7:705::ffff icmp6_seq=5 ttl=64 time=16.386 ms

2800:68:7:705::ffff icmp6_seq=3 ttl=64 time=15.879 ms
2800:68:7:705::ffff icmp6_seq=4 ttl=64 time=15.926 ms
2800:68:7:705::ffff icmp6_seq=5 ttl=64 time=16.386 ms
```

Figura 118: Conectividad desde PC1-Energía hacia Switch CORE.

6.5. OBJETIVO 5: Realizar las configuraciones necesarias para la implementación del Protocolo de Internet versión 6 (IPv6) en la Universidad Nacional de Loja

En el contexto del Objetivo 5, la Universidad Nacional de Loja ya está funcionando con el Protocolo de Internet versión 4 (IPv4); tornándose las nuevas configuraciones algo más sencillas, por la razón de que tocaría realizar las configuraciones solamente para el nuevo Protocolo de Internet versión 6 (IPv6).

Algunas de las configuraciones realizadas en los equipos Swtich Core, Switch de Distribución y Switch de Acceso en IPv4; nos servirán también para las configuraciones en IPv6 como por ejemplo los puertos Trunk que ya se encuentran habilitados, las VLAN que ya están creadas y 100% funcionales a lo largo de toda la Universidad.

Lo que se va a requerir, es identificar las interfaces que intervienen en el enrutamiento desde un switch a otro para así levantar todo el enrutamiento en IPv6 y no provocar algún desperfecto en el enrutamiento IPv4 existente.

6.5.1. Plan de Implementación: Protocolo de Internet versión 6 (IPv6)

El esquema de configuración para la Capa de Núcleo (Switch CORE) y la capa de distribución (Switch de Distribución) queda de la siguiente manera, mencionando que para el sector de Motupe y de Salud no se realizó ninguna configuración puesto que estos sectores constan de la tecnología MPLS y se debería gestionar los permisos necesarios para realizar dichas configuraciones.

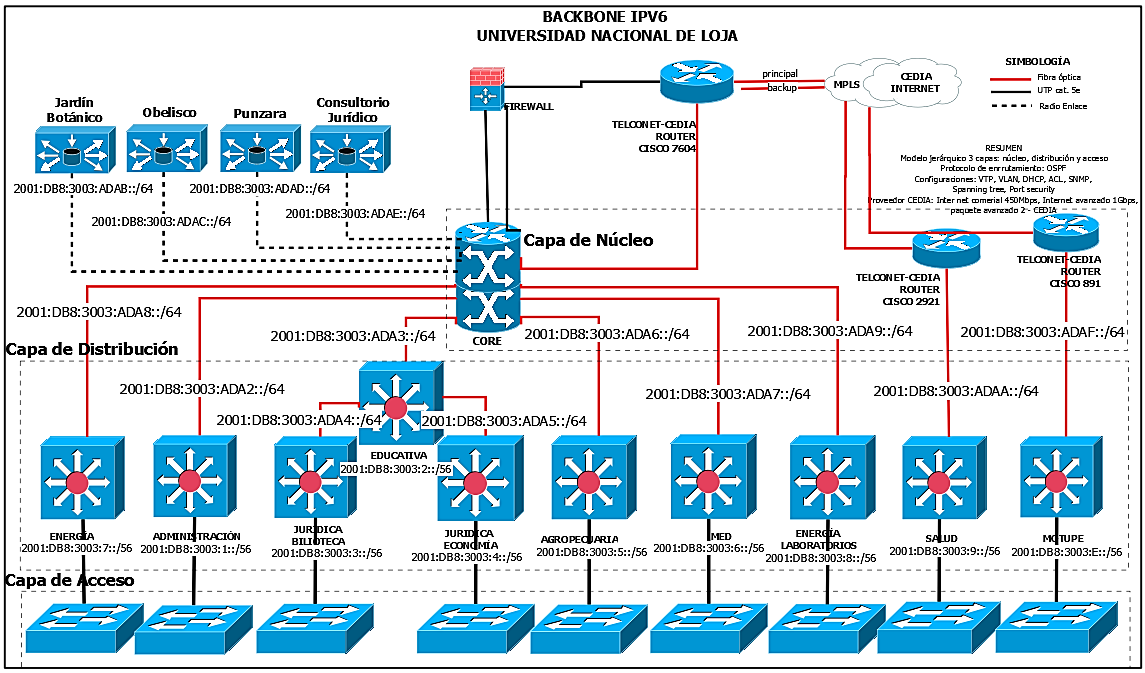


Figura 119: Topología implementación IPv6.

Conjuntamente en reunión mantenida con el Subdirector de la Unidad de Telecomunicaciones e Información Ing. Jhon Calderón y mediante la apertura por parte del Director de dicha unidad Ing. Milton Lavanda se planteó el siguiente esquema de implementación para IPv6 con el fin de llegar hasta el usuario final y comprobar las configuraciones realizas y los parámetros asignados, mostrado en la siguiente figura.

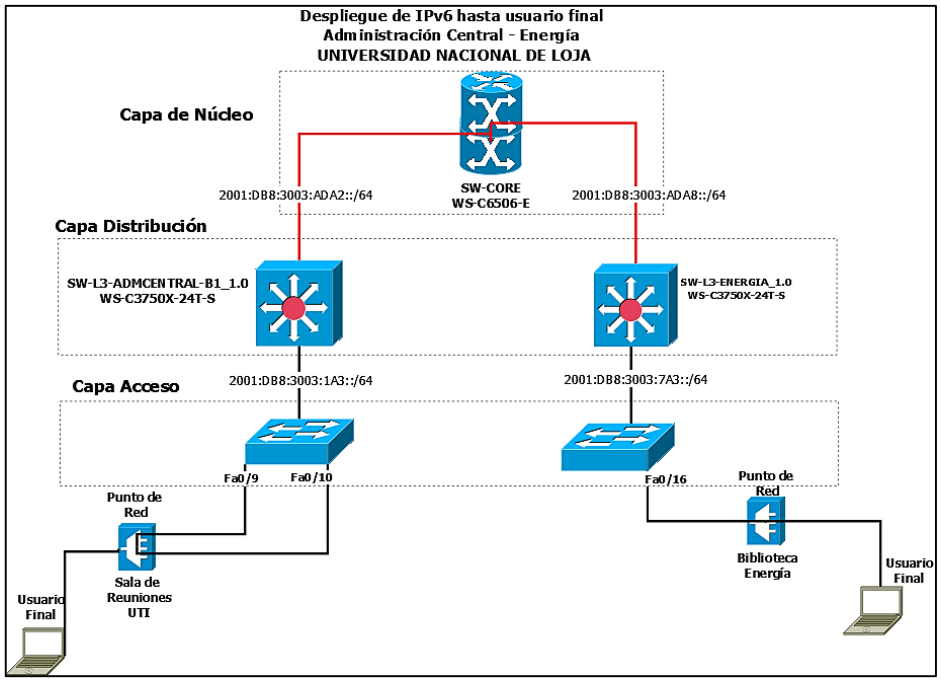


Figura 120: Esquema Facultad Administración - Facultad Energía en IPv6.

En el planteamiento del Escenario 2 de Pruebas se tomó como referencia dos facultades así mismo para la implementación de IPv6 se tomó dichas Facultades hasta llegar al usuario final y poder comprobar las configuraciones y parámetros asignados con el nuevo protocolo, que son: Facultad Administración Departamento UTI y Facultad de Energía Departamento de Biblioteca, para las demás facultades se desplegó IPv6 en todo lo que es Capa de Núcleo y Capa de Distribución utilizando autoconfiguración para lo que son usuarios finales, mediante el direccionamiento real que se realizó con IPv6 para el trabajo de titulación y dando a conocer sus configuraciones mediante el prefijo de documentación de IPv6.

Pasos a seguir: para realizar la transición y coexistencia de ambos protocolos se plantearon algunos pasos a seguir recalcando que no son pasos estrictamente secuenciales sino más bien una guía a tomar en consideración para la implementación de IPv6, quedando de la siguiente manera:

1. Verificar conexión física.
2. Verificar las direcciones IPv6 a utilizar.
3. Configuración de las direcciones IPv6 en el Switch Core y de Distribución (L3).
    a. Probar conectividad.
4. Configurar las direcciones IPv6 en las interfaces del Switch L3 y L2.
    a. Asignar dirección IPv6 a “VLAN-Nativa” en Switch L3 y L2.

b. Asignar puertos en Switch L2 para “VLAN [VLAN-ID]”.

c. Probar conectividad.

5. Autoconfiguración STATELESS o STATEFUL en L3.

a. Verificar asignación de dirección IPv6 y parámetros en Usuario Final.

b. Probar conectividad.

6. Configurar protocolo de enrutamiento OSPFv3 en Switch Core y L3.

a. Agregar las interfaces que intervienen en OSPFv3.

b. Probar conectividad.

Para poder acceder a los equipos reales y realizar las configuraciones necesarias se me otorgó un usuario, una contraseña y las direcciones IPv4 necesarias para iniciar sesión mediante SSH (Secure Shell – Intérprete de Órdenes Seguro) utilizando el programa Putty[11], obteniendo los siguientes resultados.

6.5.2. Configuración Switch Core (Facultad Administración-UTI / Facultad Energía-Biblioteca)

Se procede a realizar el acceso al equipo ejecutando el programa antes mencionado Putty con su dirección IPv4 como se aprecia en la figura.

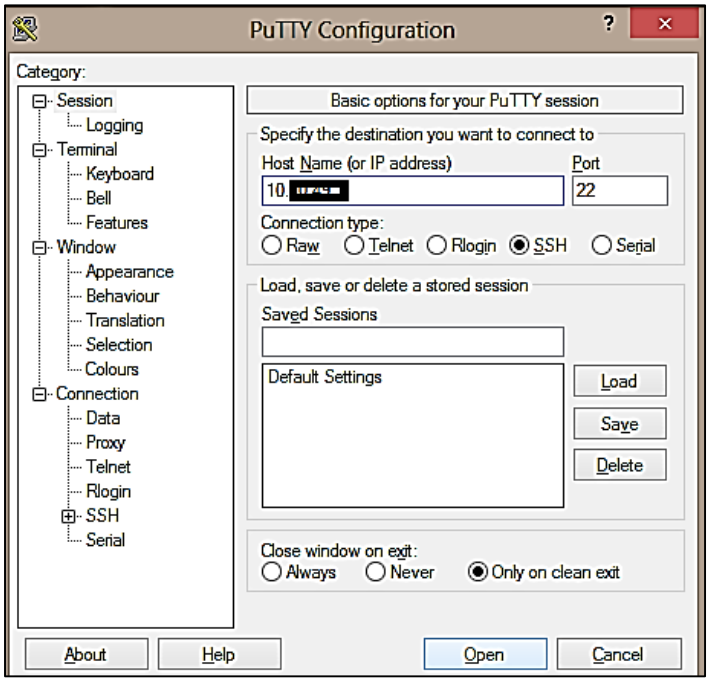


Figura 121: Acceso Switch Core.

[11] http://www.putty.org/

Una vez ingresado nos pedirá el Usuario y Password.

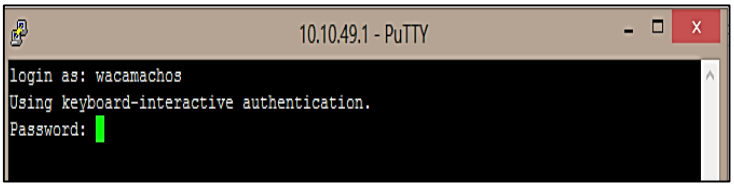


Figura 122: Inicio Sesión Switch Core.

Ya realizado el inicio de sesión del Switch Core se procede a la configuración:

- **Configuración interfaz GiX/X**

S1MA0204CO01#configure terminal
S1MA0204CO01(config)#ipv6 unicast-routing
S1MA0204CO01(config)#interface gigabitEthernet X/X
S1MA0204CO01(config-if)#ipv6 address 2001:DB8:3003:ADA2::FFFF/64
S1MA0204CO01(config-if)#no shutdown
S1MA0204CO01(config-if)#exit

- **Configuración interfaz GiX/X**

S1MA0204CO01#configure terminal
S1MA0204CO01(config)#ipv6 unicast-routing
S1MA0204CO01(config)#interface gigabitEthernet X/X
S1MA0204CO01(config-if)#ipv6 address 2001:DB8:3003:ADA8::FFFF/64
S1MA0204CO01(config-if)#no shutdown
S1MA0204CO01(config-if)#exit

- **Configuración OSPFv3**

S1MA0204CO01#configure terminal
S1MA0204CO01(config)#ipv6 router ospf 1
S1MA0204CO01(config-rtr)#router-id 1.1.1.0
S1MA0204CO01(config-rtr)#exit

S1MA0204CO01(config)#interface gigabitEthernetX/X
S1MA0204CO01(config-if)#ipv6 enable
S1MA0204CO01(config-if)#ipv6 ospf 1 area 0
S1MA0204CO01(config-if)#exit

S1MA0204CO01(config)#interface gigabitEthernetX/X
S1MA0204CO01(config-if)#ipv6 enable
S1MA0204CO01(config-if)#ipv6 ospf 1 area 0
S1MA0204CO01(config-if)#exit

En la siguiente figura se muestra las rutas aprendidas por medio de enrutamiento OSPFv3 señalando que las direcciones con la primera inicial “O” serían las rutas tanto del Switch de Administración como del Switch de Energía.

```
ADMS1MA0204CO01#sh ipv6 route
IPv6 Routing Table - default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       R - RIP, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2800:68:7:[redacted]::/64 [110/2]
     via FE80::F60F:1BFF:FE80:754E, GigabitEthernet2/46
O   2800:68:7:[redacted]::/64 [110/2]
     via FE80::F60F:1BFF:FE80:754E, GigabitEthernet2/46
O   2800:68:7:[redacted]::/64 [110/2]
     via FE80::225:83FF:FE9E:3AC1, GigabitEthernet1/4
O   2800:68:7:[redacted]::/64 [110/2]
     via FE80::225:83FF:FE9E:3AC1, GigabitEthernet1/4
C   2800:68:7:FF01::/64 [0/0]
     via GigabitEthernet2/46, directly connected
L   2800:68:7:FF01::FFFF/128 [0/0]
     via GigabitEthernet2/46, receive
C   2800:68:7:FF07::/64 [0/0]
     via GigabitEthernet1/4, directly connected
L   2800:68:7:FF07::FFFF/128 [0/0]
     via GigabitEthernet1/4, receive
L   FF00::/8 [0/0]
     via Null0, receive
ADMS1MA0204CO01#
```

Figura 123: Rutas Aprendidas OSPFv3 Switch CORE.

6.5.3. Configuración Switch Distribución o L3 (Facultad Administración – Departamento UTI)

Para la configuración del equipo L3 se inicia de sesión conforme se ingresó en el Switch Core, a continuación se muestra su acceso.

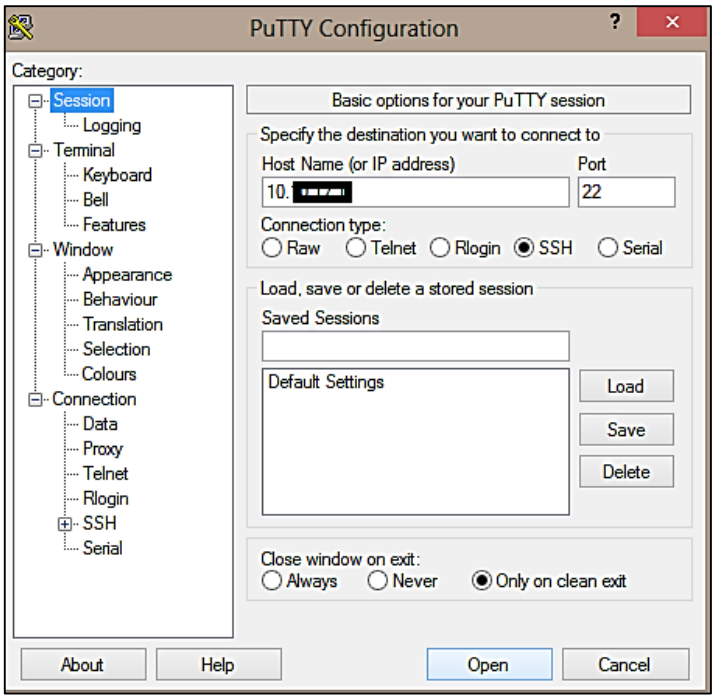


Figura 124: Acceso Switch Distribución o L3 - Administración.

Así mismo no pedirá ingresar nombre de Usuario y Password.

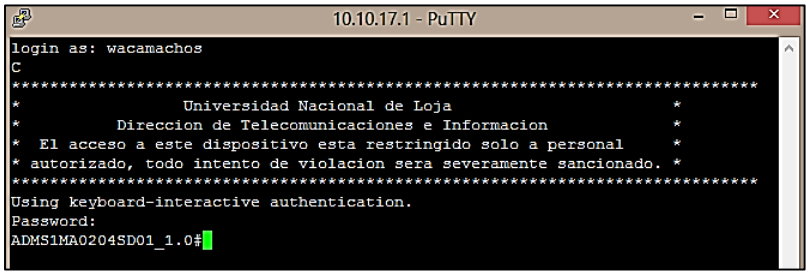


Figura 125: Inicio Sesión Switch L3 - Administración.

Luego se procede a configurar las direcciones IPv6 para las interfaces que se requieren con los mismos comandos utilizados anteriormente.

- **Configuración interfaz GiX/X/X**

S1MA0204SD01_1.0#configure terminal
S1MA0204SD01_1.0(config)#ipv6 unicast-routing
S1MA0204SD01_1.0(config)#interface gigabitEthernet X/X/X
S1MA0204SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:ADA2::FFFE/64
S1MA0204SD01_1.0(config-if)#no shutdown
S1MA0204SD01_1.0(config-if)#exit

- **Configuración VLAN Nativa**

S1MA0204SD01_1.0(config)#interface vlan 2
S1MA0204SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:1A3::FFFF/64
S1MA0204SD01_1.0(config-if)#no shutdown
S1MA0204SD01_1.0(config-if)#exit

- **Configurar VLAN-UTI**

S1MA0204SD01_1.0(config)#interface vlan 3
S1MA0204SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:1A4::FFFF/64
S1MA0204SD01_1.0(config-if)#no shutdown
S1MA0204SD01_1.0(config-if)#exit

S1MA0204SD01_1.0(config)#interface gigabitEthernetX/X/X
S1MA0204SD01_1.0(config-if)#description TESIS_IPV6
S1MA0204SD01_1.0(config-if)#swicthport trunk encapsulation dot1q
S1MA0204SD01_1.0(config-if)#switchport trunk native vlan 2
S1MA0204SD01_1.0(config-if)#switchport trunk allowed vlan
1-3,10,20,30,40,50,60,70,120,200,210
S1MA0204SD01_1.0(config-if)#switchport mode trunk
S1MA0204SD01_1.0(config-if)#no shutdown
S1MA0204SD01_1.0(config-if)#exit

- **Configuración DHCPv6: STATELESS y STATEFUL**

S1MA0204SD01_1.0(config)#ipv6 dhcp pool STATEFUL_TESIS_IPV6
S1MA0204SD01_1.0(config-dhcpv6)#address prefix 2001:DB8:3003:1A4::/64 lifetime 1800
600
S1MA0204SD01_1.0(config-dhcpv6)#dns-server 2001:DB8:3003:ACA5::1234
S1MA0204SD01_1.0(config-dhcpv6)#domain-name TESIS_IPV6.COM
S1MA0204SD01_1.0(config-dhcpv6)#exit

S1MA0204SD01_1.0(config)#interface vlan 3
S1MA0204SD01_1.0(config-if)#ipv6 enable
S1MA0204SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:1A4::FFFF/64 eui-64

S1MA0204SD01_1.0(config-if)#ipv6 dhcp server STATEFUL_TESIS_IPV6
S1MA0204SD01_1.0(config-if)#ipv6 nd managed-config-flag
S1MA0204SD01_1.0(config-if)#ipv6 nd other-config-flag
S1MA0204SD01_1.0(config-dhcpv6)#exit

- **Configuración OSPFv3**

S1MA0204SD01_1.0#configure terminal
S1MA0204SD01_1.0(config)#ipv6 router ospf 1
S1MA0204SD01_1.0(config-rtr)#router-id 1.1.1.1
S1MA0204SD01_1.0(config-rtr)#exit

S1MA0204SD01_1.0(config)#interface gigabitEthernetX/X/X
S1MA0204SD01_1.0(config-if)#ipv6 enable
S1MA0204SD01_1.0(config-if)#ipv6 ospf 1 area 0
S1MA0204SD01_1.0(config-if)#exit

S1MA0204SD01_1.0(config)#interface vlan 2
S1MA0204SD01_1.0(config-if)#ipv6 enable
S1MA0204SD01_1.0(config-if)#ipv6 ospf 1 area 0
S1MA0204SD01_1.0(config-if)#exit

S1MA0204SD01_1.0(config)#interface vlan 3
S1MA0204SD01_1.0(config-if)#ipv6 enable
S1MA0204SD01_1.0(config-if)#ipv6 ospf 1 area 0
S1MA0204SD01_1.0(config-if)#exit

Rutas aprendidas en Switch de Distribución de la Facultad de Administración:

```
ADMS1MA0204SD01_1.0#sh ipv6 route
IPv6 Routing Table - default - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       R - RIP, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2800:68:7:102::/64 [0/0]
     via Vlan2, directly connected
L   2800:68:7:102::FFFF/128 [0/0]
     via Vlan2, receive
C   2800:68:7:103::/64 [0/0]
     via Vlan4, directly connected
L   2800:68:7:103::FFFF/128 [0/0]
     via Vlan4, receive
L   2800:68:7:103:F60F:1BFF:FE80:7550/128 [0/0]
     via Vlan4, receive
O   2800:68:7:[redacted]::/64 [110/3]
     via FE80::7ADA:6EFF:FE19:2D00, GigabitEthernet1/0/21
O   2800:68:7:[redacted]::/64 [110/3]
     via FE80::7ADA:6EFF:FE19:2D00, GigabitEthernet1/0/21
C   2800:68:7:FF01::/64 [0/0]
     via GigabitEthernet1/0/21, directly connected
L   2800:68:7:FF01::FFFE/128 [0/0]
     via GigabitEthernet1/0/21, receive
O   2800:68:7:[redacted]::/64 [110/2]
     via FE80::7ADA:6EFF:FE19:2D00, GigabitEthernet1/0/21
L   FF00::/8 [0/0]
     via Null0, receive
ADMS1MA0204SD01_1.0#
```

Figura 126: Rutas Aprendidas OSPFv3 Switch L3 Administración.

6.5.4. Configuración Switch Acceso o L2 (Facultad Administración – Departamento UTI)

Se accede conforme se lo realizó con los equipos anteriores.

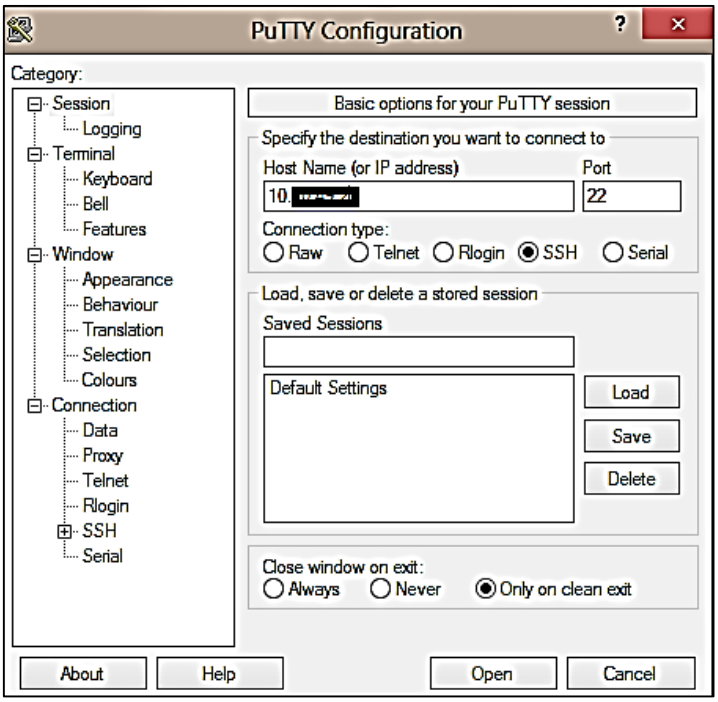


Figura 127: Acceder Switch de Acceso o L2.

Luego se precede a iniciar sesión con nombre de Usuario y password.

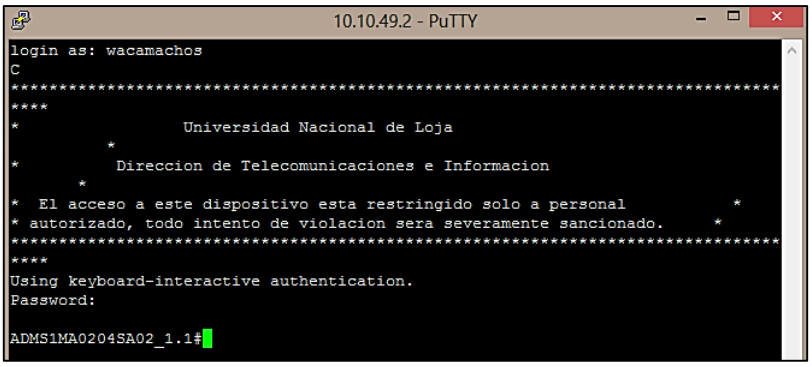


Figura 128: Inicio Sesión Switch L2.

Antes de realizar alguna configuración se debe tomar en cuenta y verificar la plantilla “dual-ipv4-and-ipv6 default”, mediante el comando (show sdm prefer) la cual debe estar habilitada para poder trabajar con ambas pilas de protocolos IPv4 e IPv6; si no lo esta se procede a realizar las siguientes configuraciones:

- **Configuración SDM**

```
S1MA0204SA02_1.1#configure terminal
S1MA0204SA02_1.1(config)#sdm prefer dual-ipv4-and-ipv6 default
S1MA0204SA02_1.1(config)#exit
S1MA0204SA02_1.1#reload
```

Configuraciones necesarias para el Protocolo de Internet versión 6 (IPv6).

- **Configuración VLAN de Gestión (VLAN-Nativa)**

```
S1MA0204SA02_1.1#configure terminal
S1MA0204SA02_1.1(config)#interface vlan 2
S1MA0204SA02_1.1(config-if)#ipv6 address 2001:DB8:3003:1A3::FFFE/64
S1MA0204SA02_1.1(config-if)#no shutdown
S1MA0204SA02_1.1(config-if)#exit
```

- **Habilitar puerto Troncal**

```
S1MA0204SA02_1.1(config)#interface fastEthernetX/X
S1MA0204SA02_1.1(config-if)#description USUARIO_FINAL_IPV6
S1MA0204SA02_1.1(config-if)#switchport trunk native vlan 2
S1MA0204SA02_1.1(config-if)#switchport trunk allowed vlan
1-3,10,20,30,40,50,60,70,120,200,210
S1MA0204SA02_1.1(config-if)#switchport mode trunk
S1MA0204SA02_1.1(config-if)#no shutdown
S1MA0204SA02_1.1(config-if)#exit
```

- **Asignar puertos: Acceso VLAN 3 a la interfaz**

```
S1MA0204SA02_1.1(config)#interface fastEthernet0/9
S1MA0204SA02_1.1(config-if)#switchport mode access
S1MA0204SA02_1.1(config-if)#switch access vlan 3
S1MA0204SA02_1.1(config-if)#exit

S1MA0204SA02_1.1(config)#interface fastEthernet0/10
S1MA0204SA02_1.1(config-if)#switchport mode access
S1MA0204SA02_1.1(config-if)#switch access vlan 3
S1MA0204SA02_1.1(config-if)#exit
```

6.5.5. USUARIO FINAL (Facultad Administración - Departamento UTI): Asignación de dirección IPv6

Para comprobar la asignación correcta de la dirección IPv6 con la técnica EUI-64 hacia el usuario final en la Facultad de Administración – Departamento UTI, se capturó la siguiente imagen indicando todos los parámetros requeridos y necesarios para su funcionalidad en el envío de paquetes mediante OSPFv3 con el Protocolo de Internet versión 6.

Se observa también el nombre de dominio y dirección IPv6 que se configuraron con el protocolo dinámico DHCPv6 Stateful.

```
Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . : Adaptador de red inalámbrica Qual
comm Atheros AR9485WB-EG
   Dirección física. . . . . . . . . . . . : 08-3E-8E-B6-FD-9B
   DHCP habilitado . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Dirección IPv6 . . . . . . . . . . . : 2800:68:7:[redacted]:cfce(Prefer
ido)
   Dirección IPv6 temporal. . . . . . . : 2800:68:7:[redacted]:965e(Prefer
ido)
   Vínculo: dirección IPv6 local. . . : fe80::60b0:b5b8:306a:cfce%13(Preferido)

   Dirección IPv4. . . . . . . . . . . . . : 10.30.25.145(Preferido)
   Máscara de subred . . . . . . . . . . . : 255.255.240.0
   Concesión obtenida. . . . . . . . . . . : miércoles, 5 de julio de 2017 9:0
3:40
   La concesión expira . . . . . . . . . . : viernes, 7 de julio de 2017 11:51
:34
   Puerta de enlace predeterminada . . . . . : fe80::f60f:1bff:fe80:754d%13
                                       10.30.16.1
   Servidor DHCP . . . . . . . . . . . . . : 10.30.16.1
   IAID DHCPv6 . . . . . . . . . . . . . . : 319307406
   DUID de cliente DHCPv6. . . . . . . . . : 00-01-00-01-1F-CB-14-11-30-F9-ED-
BC-B0-78
   Servidores DNS. . . . . . . . . . . . . : 172.16.32.2
                                       172.16.32.3
   NetBIOS sobre TCP/IP. . . . . . . . . . : habilitado

Adaptador de Ethernet Ethernet:

   Estado de los medios. . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . : unl.edu.ec
   Descripción . . . . . . . . . . . . . . : Controladora Realtek PCIe GBE Fam
ily
   Dirección física. . . . . . . . . . . . : 30-F9-ED-BC-B0-78
   DHCP habilitado . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
```

Figura 129: Asignación de dirección IPv6 a usuario final – Facultad Administración.

6.5.6. Pruebas de Conectividad

6.5.6.1. Switch CORE

- Conectividad Switch Core – Switch L3 (Administración)

```
ADMS1MA0204CO01#ping 2800:68:7:ff01::fffe
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:FF01::FFFE, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/11/40 ms
ADMS1MA0204CO01#tracer 2800:68:7:ff01::fffe
Type escape sequence to abort.
Tracing the route to 2800:68:7:FF01::FFFE

  1 2800:68:7:FF01::FFFE 4 msec 0 msec 4 msec
ADMS1MA0204CO01#
```

Figura 130: Conectividad Core – L3 (Administración).

- Conectividad Switch Core - Switch L3 (Administración-Interface VLAN 2)

```
ADMS1MA0204CO01#ping 2800:68:7:102::ffff
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:102::FFFF, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms
ADMS1MA0204CO01#tracer 2800:68:7:102::ffff
Type escape sequence to abort.
Tracing the route to 2800:68:7:102::FFFF

  1 2800:68:7:FF01::FFFE 0 msec 4 msec 0 msec
ADMS1MA0204CO01#
```

Figura 131: Conectividad Core - Switch L3 (Administración-Interface VLAN 2).

- Conectividad Switch Core - Switch L2 (Administración-Interface VLAN 2)

```
ADMS1MA0204CO01#ping 2800:68:7:102::fffe
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:102::FFFE, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
ADMS1MA0204CO01#tracer 2800:68:7:102::fffe
Type escape sequence to abort.
Tracing the route to 2800:68:7:102::FFFE

  1 2800:68:7:FF01::FFFE 4 msec 0 msec 4 msec
  2 2800:68:7:102::FFFE 0 msec 0 msec 0 msec
ADMS1MA0204CO01#
```

Figura 132: Conectividad Switch Core - Switch L2 (Administración-Interface VLAN 2).

- Conectividad Switch Core - Switch L3 (Administración-Interface VLAN 3)

```
ADMS1MA0204CO01#ping 2800:68:7:103::ffff
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:103::FFFF, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms
ADMS1MA0204CO01#tracer 2800:68:7:103::ffff
Type escape sequence to abort.
Tracing the route to 2800:68:7:103::FFFF

  1 2800:68:7:FF01::FFFE 4 msec 0 msec 4 msec
ADMS1MA0204CO01#
```

Figura 133: Conectividad Switch Core - Switch L3 (Administración-Interface VLAN 3).

- Conectividad Switch Core – Usuario Final (Administración)

```
ADMS1MA0204CO01#ping 2800:68:7:10c:60b0:b5b8:306a:cfce
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:10C:60B0:B5B8:306A:CFCE, timeout is 2
 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/12/52 ms
ADMS1MA0204CO01#traceroute 2800:68:7:10c:60b0:b5b8:306a:cfce
Type escape sequence to abort.
Tracing the route to 2800:68:7:10C:60B0:B5B8:306A:CFCE

  1 2800:68:7:FF01::FFFE 4 msec 0 msec 4 msec
```

Figura 134: Conectividad Switch Core – Usuario Final (Administración).

6.5.6.2. Switch Distribución o L3 (Facultad Administración)

- Conectividad Switch L3 (Administración) - Switch CORE

```
ADMS1MA0204SD01_1.0#ping 2800:68:7:ff01::ffff
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:FF01::FFFF, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/8 ms
ADMS1MA0204SD01_1.0#tracer 2800:68:7:ff01::ffff
Type escape sequence to abort.
Tracing the route to 2800:68:7:FF01::FFFF

  1 2800:68:7:FF01::FFFF 0 msec 0 msec 8 msec
ADMS1MA0204SD01_1.0#
```

Figura 135: Conectividad Switch L3 (Administración) - Switch CORE.

- Conectividad Switch L3 (Administración) - Switch L2 (Administración-Interface VLAN 2)

```
ADMS1MA0204SD01_1.0#ping 2800:68:7:102::fffe
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:102::FFFE, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/10/34 ms
ADMS1MA0204SD01_1.0#tracer 2800:68:7:102::fffe
Type escape sequence to abort.
Tracing the route to 2800:68:7:102::FFFE

  1 2800:68:7:102::FFFE 8 msec 9 msec 0 msec
ADMS1MA0204SD01_1.0#
```

Figura 136: Conectividad Switch L3 (Administración) - Switch L2 (Administración-Interface VLAN 2).

- Conectividad Switch L3 (Administración) – Usuario Final (Administración)

```
ADMS1MA0204SD01_1.0#ping 2800:68:7:103:81aa:9a8d:1f90:f255
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:103:81AA:9A8D:1F90:F255, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/8 ms
ADMS1MA0204SD01_1.0#
```

Figura 137: Conectividad Switch Distribución – Usuario Final.

6.5.6.3. Switch Acceso o L2 (Facultad Administración)

- Conectividad Switch L2 (Administración) – Switch CORE (Interface GiX/X)

```
ADMS1MA0204SA02_1.1#ping 2800:68:7:ff01::ffff
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:FF01::FFFF, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
ADMS1MA0204SA02_1.1#tracer 2800:68:7:ff01::ffff
Type escape sequence to abort.
Tracing the route to 2800:68:7:FF01::FFFF

  1 2800:68:7:102::FFFF 0 msec 8 msec 0 msec
  2 2800:68:7:FF01::FFFF 9 msec 0 msec 0 msec
ADMS1MA0204SA02_1.1#
```

Figura 138: Conectividad Switch L2 (Administración) – SwitchCORE (Interface GiX/X).

- Conectividad Switch L2 (Administración) – Switch L3 (Administración-Interface GiX/X/X)

```
ADMS1MA0204SA02_1.1#ping 2800:68:7:ff01::fffe
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:FF01::FFFE, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/9 ms
ADMS1MA0204SA02_1.1#tracer 2800:68:7:ff01::fffe
Type escape sequence to abort.
Tracing the route to 2800:68:7:FF01::FFFE

  1 2800:68:7:102::FFFF 0 msec 9 msec 0 msec
ADMS1MA0204SA02_1.1#
```

Figura 139: Conectividad Switch L2 (Administración) – Switch L3 (Administración-Interface GiX/X/X).

- Conectividad Switch L2 (Administración) – Switch L3 (Administración-Interface VLAN 2)

```
ADMS1MA0204SA02_1.1#ping 2800:68:7:102::ffff
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:102::FFFF, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/6/25 ms
ADMS1MA0204SA02_1.1#tracer 2800:68:7:102::ffff
Type escape sequence to abort.
Tracing the route to 2800:68:7:102::FFFF

  1 2800:68:7:102::FFFF 9 msec 0 msec 0 msec
ADMS1MA0204SA02_1.1#
```

Figura 140: Conectividad Switch L2 (Administración) – Switch L3 (Administración-Interface VLAN 2).

- Conectividad Switch L2 (Administración) – Switch L3 (Administración-Interface VLAN 3)

```
ADMS1MA0204SA02_1.1#ping 2800:68:7:103::ffff
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:103::FFFF, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/9 ms
ADMS1MA0204SA02_1.1#tracer 2800:68:7:103::ffff
Type escape sequence to abort.
Tracing the route to 2800:68:7:103::FFFF

  1 2800:68:7:102::FFFF 0 msec 8 msec 0 msec
ADMS1MA0204SA02_1.1#
```

Figura 141: Conectividad Switch L2 (Administración) – Switch L3 (Administración-Interface VLAN 3).

- Conectividad Switch L2 (Administración) – Usuario Final (Administración)

```
ADMS1MA0204SA02_1.1#ping 2800:68:7:103:81aa:9a8d:1f90:f255
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:103:81AA:9A8D:1F90:F255, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/17 ms
ADMS1MA0204SA02_1.1#
```

Figura 142: Conectividad Switch L2 (Administración) – Usuario Final (Administración).

6.5.6.4. Usuario Final o PC en IPv6 (Administración)

- Conectividad PC (Administración) – Switch CORE (Interface GiX/X)

```
C:\Users\Sony>ping 2800:68:7:ff01::ffff

Haciendo ping a 2800:68:7:ff01::ffff con 32 bytes de datos:
Respuesta desde 2800:68:7:ff01::ffff: tiempo=3ms
Respuesta desde 2800:68:7:ff01::ffff: tiempo=13ms
Respuesta desde 2800:68:7:ff01::ffff: tiempo=1ms
Respuesta desde 2800:68:7:ff01::ffff: tiempo=1ms

Estadísticas de ping para 2800:68:7:ff01::ffff:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 13ms, Media = 4ms

C:\Users\Sony>tracert 2800:68:7:ff01::ffff

Traza a 2800:68:7:ff01::ffff sobre caminos de 30 saltos como máximo.

  1     1 ms    <1 ms     1 ms  2800:68:7:103::ffff
  2     1 ms    <1 ms    <1 ms  2800:68:7:ff01::ffff

Traza completa.
```

Figura 143: Conectividad PC (Administración) – Switch CORE (Interface GiX/X).

- Conectividad PC (Administración) – Switch L3 (Administración-Interface GiX/X/X)

```
C:\Users\Sony>ping 2800:68:7:ff01::fffe

Haciendo ping a 2800:68:7:ff01::fffe con 32 bytes de datos:
Respuesta desde 2800:68:7:ff01::fffe: tiempo=1ms
Respuesta desde 2800:68:7:ff01::fffe: tiempo=1ms
Respuesta desde 2800:68:7:ff01::fffe: tiempo=1ms
Respuesta desde 2800:68:7:ff01::fffe: tiempo=3ms

Estadísticas de ping para 2800:68:7:ff01::fffe:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 3ms, Media = 1ms

C:\Users\Sony>tracert 2800:68:7:ff01::fffe

Traza a 2800:68:7:ff01::fffe sobre caminos de 30 saltos como máximo.

  1     2 ms     1 ms     1 ms  2800:68:7:ff01::fffe

Traza completa.
```

Figura 144: Conectividad PC (Administración) – Switch L3 (Administración-Interface GiX/X/X).

- Conectividad PC (Administración) – Switch L3 (Administración-Interface VLAN 2)

```
C:\Users\Sony>ping 2800:68:7:102::ffff

Haciendo ping a 2800:68:7:102::ffff con 32 bytes de datos:
Respuesta desde 2800:68:7:102::ffff: tiempo=3ms
Respuesta desde 2800:68:7:102::ffff: tiempo=2ms
Respuesta desde 2800:68:7:102::ffff: tiempo=1ms
Respuesta desde 2800:68:7:102::ffff: tiempo=1ms

Estadísticas de ping para 2800:68:7:102::ffff:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 3ms, Media = 1ms

C:\Users\Sony>tracert 2800:68:7:102::ffff

Traza a 2800:68:7:102::ffff sobre caminos de 30 saltos como máximo.

  1     1 ms     1 ms     1 ms  2800:68:7:102::ffff

Traza completa.
```

Figura 145: Conectividad PC (Administración) – Switch L3 (Administración-Interface VLAN 2)

- Conectividad PC (Administración) – Switch L3 (Administración-Interface VLAN 3)

```
C:\Users\Sony>ping 2800:68:7:103::ffff

Haciendo ping a 2800:68:7:103::ffff con 32 bytes de datos:
Respuesta desde 2800:68:7:103::ffff: tiempo=12ms
Respuesta desde 2800:68:7:103::ffff: tiempo=2ms
Respuesta desde 2800:68:7:103::ffff: tiempo=5ms
Respuesta desde 2800:68:7:103::ffff: tiempo=1ms

Estadísticas de ping para 2800:68:7:103::ffff:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 12ms, Media = 5ms

C:\Users\Sony>tracert 2800:68:7:103::ffff

Traza a 2800:68:7:103::ffff sobre caminos de 30 saltos como máximo.

  1     1 ms     1 ms     1 ms  2800:68:7:103::ffff

Traza completa.
```

Figura 146: Conectividad PC (Administración) – Switch L3 (Administración-Interface VLAN 3).

- Conectividad PC (Administración) – Switch L2 (Administración-Interface VLAN 2)

```
C:\Users\Sony>ping -6 2800:68:7:102::fffe

Haciendo ping a 2800:68:7:102::fffe con 32 bytes de datos:
Respuesta desde 2800:68:7:102::fffe: tiempo<1m
Respuesta desde 2800:68:7:102::fffe: tiempo=1ms
Respuesta desde 2800:68:7:102::fffe: tiempo<1m
Respuesta desde 2800:68:7:102::fffe: tiempo=1ms

Estadísticas de ping para 2800:68:7:102::fffe:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\Sony>tracert 2800:68:7:102::fffe

Traza a 2800:68:7:102::fffe sobre caminos de 30 saltos como máximo.

  1     2 ms     2 ms     1 ms  2800:68:7:103::ffff
  2     1 ms    <1 ms     1 ms  2800:68:7:102::fffe

Traza completa.
```

Figura 147: Conectividad PC (Administración) – Switch L2 (Administración-Interface VLAN 2).

6.5.7. Configuración Switch Distribución o L3 (Facultad Energía – Departamento Biblioteca)

En este apartado se omite lo que es el inicio de sesión a los equipos, su acceso es el mismo mediante los pasos que se realizaron en los equipos de la Facultad de Administración, se tornará algo repetitivo las configuraciones pero necesarias para poder comprobar la conectividad desde una facultad a otra. Las configuraciones quedan de la siguiente manera:

- **Configuración interfaz GiX/X/X**

S2MD0301SD01_1.0#configure terminal
S2MD0301SD01_1.0(config)#ipv6 unicast-routing
S2MD0301SD01_1.0(config)#interface gigabitEthernet X/X/X
S2MD0301SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:ADA8::FFFE/64
S2MD0301SD01_1.0(config-if)#no shutdown
S2MD0301SD01_1.0(config-if)#exit

- **Configuración VLAN Nativa**

S2MD0301SD01_1.0(config)#interface vlan 2

```
S2MD0301SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:7A3::FFFF/64
S2MD0301SD01_1.0(config-if)#no shutdown
S2MD0301SD01_1.0(config-if)#exit
```

- **Configurar VLAN Estudiantes**

```
S2MD0301SD01_1.0(config)#interface vlan 30
S2MD0301SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:7A6::FFFF/64
S2MD0301SD01_1.0(config-if)#no shutdown
S2MD0301SD01_1.0(config-if)#exit

S2MD0301SD01_1.0(config)#interface gigabitEthernetX/X/X
S2MD0301SD01_1.0(config-if)#description TESIS_IPV6
S2MD0301SD01_1.0(config-if)#switchport trunk allowed vlan
1,2,10,20,30,40,50,60,70,80,90,100,110,120,200,210
S2MD0301SD01_1.0(config-if)#no shutdown
S2MD0301SD01_1.0(config-if)#exit
```

NOTA: como la interfaz se encuentra activa no es necesario habilitar el puerto en modo trunk.

- **Configuración DHCPv6 STATEFUL**

```
S2MD0301SD01_1.0(config)#ipv6 dhcp pool STATEFUL_TESIS_IPV6
S2MD0301SD01_1.0(config-dhcpv6)#address prefix 2001:DB8:3003:7A6::/64 lifetime 1800
600
S2MD0301SD01_1.0(config-dhcpv6)#dns-server 2001:DB8:3003:ACA5::1234
S2MD0301SD01_1.0(config-dhcpv6)#domain-name TESIS_IPV6.COM
S2MD0301SD01_1.0(config-dhcpv6)#exit

S2MD0301SD01_1.0(config)#interface vlan 30
S2MD0301SD01_1.0(config-if)#ipv6 enable
S2MD0301SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:7A6::FFFF/64 eui-64
S2MD0301SD01_1.0(config-if)#ipv6 dhcp server STATEFUL_TESIS_IPV6
S2MD0301SD01_1.0(config-if)#ipv6 nd managed-config-flag
S2MD0301SD01_1.0(config-if)#ipv6 nd other-config-flag
S2MD0301SD01_1.0(config-dhcpv6)#exit
```

- **Configuración OSPFv3**

```
S2MD0301SD01_1.0#configure terminal
S2MD0301SD01_1.0(config)#ipv6 router ospf 1
S2MD0301SD01_1.0(config-rtr)#router-id 1.1.1.7
S2MD0301SD01_1.0(config-rtr)#exit

S2MD0301SD01_1.0(config)#interface gigabitEthernetX/X/X
S2MD0301SD01_1.0(config-if)#ipv6 enable
S2MD0301SD01_1.0(config-if)#ipv6 ospf 1 area 0
S2MD0301SD01_1.0(config-if)#exit

S2MD0301SD01_1.0(config)#interface vlan 2
S2MD0301SD01_1.0(config-if)#ipv6 enable
S2MD0301SD01_1.0(config-if)#ipv6 ospf 1 area 0
S2MD0301SD01_1.0(config-if)#exit

S2MD0301SD01_1.0(config)#interface vlan 30
S2MD0301SD01_1.0(config-if)#ipv6 enable
S2MD0301SD01_1.0(config-if)#ipv6 ospf 1 area 0
S2MD0301SD01_1.0(config-if)#exit
```

Rutas aprendidas en Switch de Distribución de la Facultad de Energía:

```
ENES2MD0301SD01_1.0#sh ipv6 route
IPv6 Routing Table - default - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       R - RIP, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2800:68:7:[redacted]::/64 [110/3]
     via FE80::7ADA:6EFF:FE19:2D00, GigabitEthernet1/1/4
O   2800:68:7:[redacted]::/64 [110/3]
     via FE80::7ADA:6EFF:FE19:2D00, GigabitEthernet1/1/4
C   2800:68:7:602::/64 [0/0]
     via Vlan2, directly connected
L   2800:68:7:602::FFFF/128 [0/0]
     via Vlan2, receive
C   2800:68:7:605::/64 [0/0]
     via Vlan4, directly connected
L   2800:68:7:605::FFFF/128 [0/0]
     via Vlan4, receive
L   2800:68:7:605:225:83FF:FE9E:3ACD/128 [0/0]
     via Vlan4, receive
O   2800:68:7:[redacted]::/64 [110/2]
     via FE80::7ADA:6EFF:FE19:2D00, GigabitEthernet1/1/4
C   2800:68:7:FF07::/64 [0/0]
     via GigabitEthernet1/1/4, directly connected
L   2800:68:7:FF07::FFFE/128 [0/0]
     via GigabitEthernet1/1/4, receive
L   FF00::/8 [0/0]
     via Null0, receive
ENES2MD0301SD01_1.0#
```

Figura 148: Rutas Aprendidas OSPFv3 Switch L3 Energía.

6.5.8. Configuración Switch Acceso o L2 (Facultad Energía – Departamento Biblioteca)

Así mismo se procede habilitar la plantilla “dual-ipv4-and-ipv6 default”, para que trabajen ambos protocolos IPv4 e IPv6.

- **Configuración SDM**

S2MD1001SA01_1.5##configure terminal
S2MD1001SA01_1.5(config)#sdm prefer dual-ipv4-and-ipv6 default
S2MD1001SA01_1.5(config)#exit
S2MD1001SA01_1.5#reload

Configuraciones necesarias para el Protocolo de Internet versión 6 (IPv6).

- **Configuración VLAN de Administración de Equipos (VLAN-Nativa)**

S2MD1001SA01_1.5#configure terminal
S2MD1001SA01_1.5(config)#interface vlan 2
S2MD1001SA01_1.5(config-if)#ipv6 address 2001:DB8:3003:7A3::FFFE/64
S2MD1001SA01_1.5(config-if)#no shutdown
S2MD1001SA01_1.5(config-if)#exit

- **Habilitar puerto Troncal**

S2MD1001SA01_1.5(config)#interface gigabitEthernetX/X
S2MD1001SA01_1.5(config-if)#description USUARIO_FINAL_IPV6
S2MD1001SA01_1.5(config-if)#switchport trunk allowed vlan
1,2,10,20,30,40,50,60,70,80,90,100,110,120,200,210

S2MD1001SA01_1.5(config-if)#no shutdown
S2MD1001SA01_1.5(config-if)#exit

- **Asignar puerto de VLAN 30 a la interfaz**

S2MD1001SA01_1.5(config)#interface fastEthernet0/16
S2MD1001SA01_1.5(config-if)#switchport mode access
S2MD1001SA01_1.5(config-if)#switch access vlan 30
S2MD1001SA01_1.5(config-if)#exit

6.5.9. USUARIO FINAL (Facultad Energía - Departamento Biblioteca): Asignación de dirección IPv6

Asignación correcta de la dirección IPv6 con la técnica EUI-64 hacia el usuario final en la Facultad de Energía – Departamento Biblioteca. También la asignación del nombre de dominio y dirección IPv6 que se configuraron mediante DHCPv6.

```
Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . : STATEFUL_TESIS_IPV6.COM
   Descripción . . . . . . . . . . . . . . . : Controladora Realtek PCIe GBE Fam
ily
   Dirección física. . . . . . . . . . . . . : 30-F9-ED-BC-B0-78
   DHCP habilitado . . . . . . . . . . . . . : no
   Configuración automática habilitada . . . : sí
   Dirección IPv6 . . . . . . . . . . . : 2800:68:7:[redacted]:f255(Prefer
ido)
   Dirección IPv6 . . . . . . . . . . . : 2800:68:7:[redacted]:3b45(Prefer
ido)
   Concesión obtenida. . . . . . . . . . . . : lunes, 8 de mayo de 2017 8:37:14
   La concesión expira . . . . . . . . . . . : miércoles, 10 de mayo de 2017 8:3
7:13
   Dirección IPv6 temporal. . . . . . . : 2800:68:7:[redacted]:2010(Prefer
ido)
   Vínculo: dirección IPv6 local. . . : fe80::81aa:9a8d:1f90:f255%12(Preferido)

   Dirección IPv4. . . . . . . . . . . . . . : 10.10.14.172(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::225:83ff:fe9e:3acd%12
                                               10.10.14.1
   IAID DHCPv6 . . . . . . . . . . . . . . . : 254867949
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-1F-CB-14-11-30-F9-ED-
BC-B0-78
   Servidores DNS. . . . . . . . . . . . . . : 2800:68:7:ff04::1234
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
   Lista de búsqueda de sufijos DNS específicos de conexión:
                                               STATEFUL_TESIS_IPV6.COM
```

Figura 149: Asignación de dirección IPv6 a usuario final – Facultad Energía.

6.5.10. Pruebas de Conectividad

6.5.10.1. Switch CORE

- Conectividad Switch Core – Switch L3 (Energía)

```
ADMS1MA0204CO01#ping 2800:68:7:ff07::fffe
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:FF07::FFFE, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/4/12 ms
ADMS1MA0204CO01#tracer 2800:68:7:ff07::fffe
Type escape sequence to abort.
Tracing the route to 2800:68:7:FF07::FFFE

  1 2800:68:7:FF07::FFFE 0 msec 8 msec 0 msec
ADMS1MA0204CO01#
```

Figura 150: Conectividad Core – L3 (Energía).

- Conectividad Switch Core - Switch L3 (Energía-Interface VLAN 2)

```
ADMS1MA0204CO01#ping 2800:68:7:702::ffff
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:702::FFFF, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms
ADMS1MA0204CO01#tracer 2800:68:7:702::ffff
Type escape sequence to abort.
Tracing the route to 2800:68:7:702::FFFF

  1 2800:68:7:FF07::FFFE 4 msec 0 msec 4 msec
ADMS1MA0204CO01#
```

Figura 151: Conectividad Core - Switch L3 (Energía-Interface VLAN 2).

- Conectividad Switch Core - Switch L2 (Energía-Interface VLAN 2)

```
ADMS1MA0204CO01#ping 2800:68:7:702::fffe
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:702::FFFE, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
ADMS1MA0204CO01#tracer 2800:68:7:702::fffe
Type escape sequence to abort.
Tracing the route to 2800:68:7:702::FFFE

  1 2800:68:7:FF07::FFFE 4 msec 0 msec 4 msec
  2 2800:68:7:702::FFFE 8 msec 0 msec 0 msec
ADMS1MA0204CO01#
```

Figura 152: Conectividad Switch Core - Switch L2 (Energía-Interface VLAN 2).

- Conectividad Switch Core - Switch L3 (Energía-Interface VLAN 30)

```
ADMS1MA0204CO01#ping 2800:68:7:705::ffff
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:705::FFFF, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/4 ms
ADMS1MA0204CO01#tracer 2800:68:7:705::ffff
Type escape sequence to abort.
Tracing the route to 2800:68:7:705::FFFF

  1 2800:68:7:FF07::FFFE 4 msec 0 msec 4 msec
ADMS1MA0204CO01#
```

Figura 153: Conectividad Switch Core - Switch L3 (Energía-Interface VLAN 30).

- Conectividad Switch Core – Usuario Final (Energía)

```
ADMS1MA0204CO01#ping 2800:68:7:705:bc0f:4feb:7955:3b45
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:705:BC0F:4FEB:7955:3B45, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
ADMS1MA0204CO01#tracer 2800:68:7:705:bc0f:4feb:7955:3b45
Type escape sequence to abort.
Tracing the route to 2800:68:7:705:BC0F:4FEB:7955:3B45

  1 2800:68:7:FF07::FFFE 8 msec 4 msec 0 msec
```

Figura 154: Conectividad Switch Core – Usuario Final (Energía).

6.5.10.2. Switch Distribución o L3 (Energía)

- Conectividad Switch L3 (Energía) - Switch CORE

```
ENES2MD0301SD01_1.0#ping 2800:68:7:ff07::ffff
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:FF07::FFFF, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
ENES2MD0301SD01_1.0#tracer 2800:68:7:ff07::ffff
Type escape sequence to abort.
Tracing the route to 2800:68:7:FF07::FFFF

  1 2800:68:7:FF07::FFFF 0 msec 8 msec 0 msec
ENES2MD0301SD01_1.0#
```

Figura 155: Conectividad Switch Distribución - Switch CORE.

- Conectividad Switch L3 (Energía) - Switch L2 (Energía-Interface VLAN 2)

```
ENES2MD0301SD01_1.0#ping 2800:68:7:702::fffe
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:702::FFFE, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/8/25 ms
ENES2MD0301SD01_1.0#tracer 2800:68:7:702::fffe
Type escape sequence to abort.
Tracing the route to 2800:68:7:702::FFFE

  1 2800:68:7:702::FFFE 8 msec 8 msec 0 msec
ENES2MD0301SD01_1.0#
```

Figura 156: Conectividad Switch L3 (Energía) - Switch L2 (Energía-Interface VLAN 2).

- Conectividad Switch L3 (Energía) – Usuario Final (Energía)

```
ENES2MD0301SD01_1.0#ping 2800:68:7:705:bc0f:4feb:7955:3b45
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:705:BC0F:4FEB:7955:3B45, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/17 ms
```

Figura 157: Conectividad Switch L3 (Energía) – Usuario Final (Energía).

6.5.10.3. Switch Acceso o L2 (Energía)

- Conectividad Switch L2 (Energía) – Switch CORE

```
ENES2MD1001SA01_1.5#ping 2800:68:7:ff07::ffff
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:FF07::FFFF, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
ENES2MD1001SA01_1.5#tracer 2800:68:7:ff07::ffff
Type escape sequence to abort.
Tracing the route to 2800:68:7:FF07::FFFF

  1 2800:68:7:702::FFFF 0 msec 8 msec 0 msec
  2 2800:68:7:FF07::FFFF 8 msec 0 msec 0 msec
ENES2MD1001SA01_1.5#
```

Figura 158: Conectividad Switch L2 (Energía) – Switch CORE.

- Conectividad Switch L2 (Energía) – Switch L3 (Energía)

```
ENES2MD1001SA01_1.5#ping 2800:68:7:ff07::fffe
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:FF07::FFFE, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
ENES2MD1001SA01_1.5#tracer 2800:68:7:ff07::fffe
Type escape sequence to abort.
Tracing the route to 2800:68:7:FF07::FFFE

  1 2800:68:7:702::FFFF 9 msec 0 msec 8 msec
ENES2MD1001SA01_1.5#
```

Figura 159: Conectividad Switch L2 (Energía) – Switch L3 (Energía).

- Conectividad Switch L2 (Energía) – Switch L3 (Energía-Interface VLAN 2)

```
ENES2MD1001SA01_1.5#ping 2800:68:7:702::ffff
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:702::FFFF, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/9 ms
ENES2MD1001SA01_1.5#tracer 2800:68:7:702::ffff
Type escape sequence to abort.
Tracing the route to 2800:68:7:702::FFFF

  1 2800:68:7:702::FFFF 17 msec 0 msec 8 msec
ENES2MD1001SA01_1.5#
```

Figura 160: Conectividad Switch L2 (Energía) – Switch L3 (Energía-Interface VLAN 2).

- Conectividad Switch L2 (Energía) – Switch L3 (Energía-Interface VLAN 30)

```
ENES2MD1001SA01_1.5#ping 2800:68:7:705::ffff
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:705::FFFF, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/5/16 ms
ENES2MD1001SA01_1.5#tracer 2800:68:7:705::ffff
Type escape sequence to abort.
Tracing the route to 2800:68:7:705::FFFF

  1 2800:68:7:702::FFFF 8 msec 0 msec 9 msec
ENES2MD1001SA01_1.5#
```

Figura 161: Conectividad Switch L2 (Energía) – Switch L3 (Energía-Interface VLAN 30).

- Conectividad Switch L2 (Energía) – Usuario Final (Energía)

```
ENES2MD1001SA01_1.5#ping 2800:68:7:705:bc0f:4feb:7955:3b45
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:705:BC0F:4FEB:7955:3B45, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/8 ms
ENES2MD1001SA01_1.5#
```

Figura 162: Conectividad Switch L2 (Energía) – Usuario Final (Energía).

6.5.10.4. Usuario Final o PC en IPv6 (Energía)

- Conectividad PC (Energía) – Switch CORE

```
C:\Users\Sony>ping -6 2800:68:7:ff07::ffff

Haciendo ping a 2800:68:7:ff07::ffff con 32 bytes de datos:
Respuesta desde 2800:68:7:ff07::ffff: tiempo<1m
Respuesta desde 2800:68:7:ff07::ffff: tiempo=1ms
Respuesta desde 2800:68:7:ff07::ffff: tiempo=1ms
Respuesta desde 2800:68:7:ff07::ffff: tiempo=1ms

Estadísticas de ping para 2800:68:7:ff07::ffff:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\Sony>tracert 2800:68:7:ff07::ffff

Traza a 2800:68:7:ff07::ffff sobre caminos de 30 saltos como máximo.

  1     1 ms     3 ms     4 ms  2800:68:7:705::ffff
  2     1 ms     1 ms     1 ms  2800:68:7:ff07::ffff

Traza completa.
```

Figura 163: Conectividad PC (Energía) – Switch CORE.

- Conectividad PC (Energía) – Switch L3 (Energía)

```
C:\Users\Sony>ping -6 2800:68:7:ff07::fffe

Haciendo ping a 2800:68:7:ff07::fffe con 32 bytes de datos:
Respuesta desde 2800:68:7:ff07::fffe: tiempo=3ms
Respuesta desde 2800:68:7:ff07::fffe: tiempo=3ms
Respuesta desde 2800:68:7:ff07::fffe: tiempo=2ms
Respuesta desde 2800:68:7:ff07::fffe: tiempo=1ms

Estadísticas de ping para 2800:68:7:ff07::fffe:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 3ms, Media = 2ms

C:\Users\Sony>tracert 2800:68:7:ff07::fffe

Traza a 2800:68:7:ff07::fffe sobre caminos de 30 saltos como máximo.

  1     3 ms     1 ms     1 ms  2800:68:7:ff07::fffe

Traza completa.
```

Figura 164: Conectividad PC (Energía) – Switch L3 (Energía-Interface Gi1/1/4).

- Conectividad PC (Energía) – Switch L3 (Energía-Interface VLAN 2)

```
C:\Users\Sony>ping -6 2800:68:7:702::ffff

Haciendo ping a 2800:68:7:702::ffff con 32 bytes de datos:
Respuesta desde 2800:68:7:702::ffff: tiempo=1ms
Respuesta desde 2800:68:7:702::ffff: tiempo=2ms
Respuesta desde 2800:68:7:702::ffff: tiempo=2ms
Respuesta desde 2800:68:7:702::ffff: tiempo=4ms

Estadísticas de ping para 2800:68:7:702::ffff:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 4ms, Media = 2ms

C:\Users\Sony>tracert 2800:68:7:702::ffff

Traza a 2800:68:7:702::ffff sobre caminos de 30 saltos como máximo.

  1     2 ms     1 ms     1 ms  2800:68:7:702::ffff

Traza completa.
```

Figura 165: Conectividad PC (Energía) – Switch L3 (Energía-Interface VLAN 2)

- Conectividad PC (Energía) – Switch L3 (Energía-Interface VLAN 30)

```
C:\Users\Sony>ping -6 2800:68:7:705::ffff

Haciendo ping a 2800:68:7:705::ffff con 32 bytes de datos:
Respuesta desde 2800:68:7:705::ffff: tiempo=53ms
Respuesta desde 2800:68:7:705::ffff: tiempo=1ms
Respuesta desde 2800:68:7:705::ffff: tiempo=1ms
Respuesta desde 2800:68:7:705::ffff: tiempo=4ms

Estadísticas de ping para 2800:68:7:705::ffff:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 53ms, Media = 14ms

C:\Users\Sony>tracert 2800:68:7:705::ffff

Traza a 2800:68:7:705::ffff sobre caminos de 30 saltos como máximo.

  1     2 ms     1 ms     3 ms  2800:68:7:705::ffff

Traza completa.
```

Figura 166: Conectividad PC (Energía) – Switch L3 (Energía-Interface VLAN 30).

- Conectividad PC (Energía) – Switch L2 (Energía-Interface VLAN 2)

```
C:\Users\Sony>ping -6 2800:68:7:702::fffe

Haciendo ping a 2800:68:7:702::fffe con 32 bytes de datos:
Respuesta desde 2800:68:7:702::fffe: tiempo=17ms
Respuesta desde 2800:68:7:702::fffe: tiempo=9ms
Respuesta desde 2800:68:7:702::fffe: tiempo=4ms
Respuesta desde 2800:68:7:702::fffe: tiempo=1ms

Estadísticas de ping para 2800:68:7:702::fffe:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 17ms, Media = 7ms

C:\Users\Sony>tracert 2800:68:7:702::fffe

Traza a 2800:68:7:702::fffe sobre caminos de 30 saltos como máximo.

  1     1 ms    <1 ms     1 ms  2800:68:7:705::ffff
  2     1 ms    <1 ms    <1 ms  2800:68:7:702::fffe

Traza completa.
```

Figura 167: Conectividad PC (Energía) – Switch L2 (Energía-Interface VLAN 2).

6.5.11. Pruebas de Conectividad entre Facultades

Se realiza la siguiente prueba para constatar su conectividad desde un área a otra mostrada en la siguiente figura, recalcando que se encuentran habilitadas ambas pilas de protocolo de internet como son IPv4 e IPv6:

- Conectividad Facultad Administración – Facultad Energía

```
C:\Users\Sony>ping -6 2800:68:7:702::fffe

Haciendo ping a 2800:68:7:702::fffe con 32 bytes de datos:
Respuesta desde 2800:68:7:702::fffe: tiempo<1m
Respuesta desde 2800:68:7:702::fffe: tiempo=1ms
Respuesta desde 2800:68:7:702::fffe: tiempo=3ms
Respuesta desde 2800:68:7:702::fffe: tiempo=1ms

Estadísticas de ping para 2800:68:7:702::fffe:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 3ms, Media = 1ms

C:\Users\Sony>tracert 2800:68:7:702::fffe

Traza a 2800:68:7:602::fffe sobre caminos de 30 saltos como máximo.

  1     1 ms    <1 ms     2 ms  2800:68:7:103::ffff
  2     1 ms    <1 ms    <1 ms  2800:68:7:ff01::ffff
  3     1 ms     2 ms     1 ms  2800:68:7:ff07::fffe
  4     1 ms     1 ms     5 ms  2800:68:7:702::fffe

Traza completa.
```

Figura 168: Conectividad Facultad Administración – Facultad Energía.

- Conectividad Facultad Energía – Facultad Administración

```
C:\Users\Sony>ping -6 2800:68:7:102::fffe

Haciendo ping a 2800:68:7:102::fffe con 32 bytes de datos:
Respuesta desde 2800:68:7:102::fffe: tiempo<1m
Respuesta desde 2800:68:7:102::fffe: tiempo=1ms
Respuesta desde 2800:68:7:102::fffe: tiempo=3ms
Respuesta desde 2800:68:7:102::fffe: tiempo=1ms

Estadísticas de ping para 2800:68:7:102::fffe:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 3ms, Media = 1ms

C:\Users\Sony>tracert 2800:68:7:102::fffe

Traza a 2800:68:7:102::fffe sobre caminos de 30 saltos como máximo.

  1     1 ms    <1 ms     2 ms  2800:68:7:705::ffff
  2     1 ms    <1 ms    <1 ms  2800:68:7:ff07::ffff
  3     1 ms     2 ms     1 ms  2800:68:7:ff01::fffe
  4     1 ms     1 ms     5 ms  2800:68:7:102::fffe

Traza completa.
```

Figura 169: Conectividad Facultad Energía – Facultad Administración.

Una vez realizado todas las configuraciones observamos que ambas pilas IPv4 e IPv6 quedan totalmente levantadas y en funcionamiento, como institución la Universidad Nacional de Loja queda lista para dar el primer paso al nuevo protocolo de internet versión 6 (IPv6) y no poseer ninguna limitante en su navegación ni problemas con el agotamiento de las direcciones IPv4.

Adicionando un poco el despliegue de IPv6 en la Universidad Nacional de Loja, se toma para la implementación equipos Mikrotik ya que en el escenario de pruebas 1 se trabajó con esta tecnología, entonces también se reliza configuraciones en IPv6 en los sectores de Jardín Botánico y de Obelisco.

6.5.12. Configuración Equipos Mikrotik[12]

Durante la realización de las pruebas se mencionó la utilización de tecnología mikrotik, su manejo y configuración, en el desarrollo del proyecto de titulación por pedido de la Unidad de Telecomunicaciones e Información y para reafirmar y sustentar el despliegue de IPv6 se pudo llegar e implementar en equipos Mikrotik en producción, se tomó como referencia lo que es Jardín Botánico y el Sector de Obelisco, sin mayores complicaciones se logró obtener las siguientes configuraciones y capturas realizando el despliegue de IPv6 en los sectores mencionados.

6.5.12.1. Configuración enlace Switch CORE hacia: Jardín Botánico y Obelisco

Las configuraciones en el equipo CORE resultaran ser las mismas que las configuraciones realizadas en todos los Switch de Distribución, así:

- **Configuración interfaz GiX/X (Jardín Botánico)**

```
S1MA0204CO01(config)#interface gigabitEthernet X/X
S1MA0204CO01(config-if)#ipv6 address 2001:DB8:3003:ADAB::FFFF/64
S1MA0204CO01(config-if)#no shutdown
S1MA0204CO01(config-if)#exit
```

- **Configuración interfaz GiX/X (Obelisco)**

```
S1MA0204CO01(config)#interface gigabitEthernet X/X
S1MA0204CO01(config-if)#ipv6 address 2001:DB8:3003:ADAC::FFFF/64
S1MA0204CO01(config-if)#no shutdown
S1MA0204CO01(config-if)#exit
```

Ambos sectores se encuentran conectados mediante radio enlace, conectados por dos antenas, una antena funciona como emisor y la otra antena como receptor llegando así hacia los equipos Mikrotik ubicados en dichos sectores, en la Figura 170 se muestra un esquema de cómo se encuentra estructurada la comunicación hacia Jardín Botánico y Obelisco, de igual manera se conécta lo que es el sector de Punzara quien también se comunica mediante radio enlace.

[12] https://mikrotik.com/

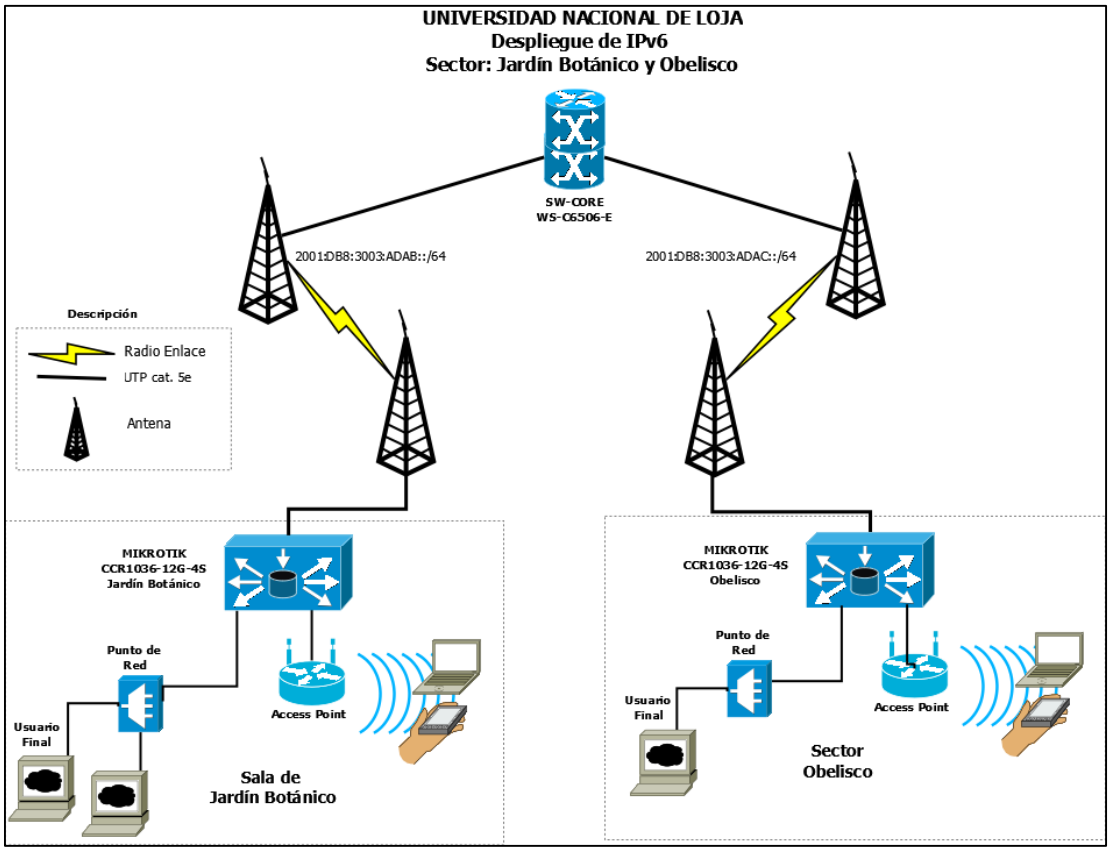


Figura 170: Esquema Switch CORE hacia Jardín Botánico y Obelisco.

Las configuraciones realizadas en el equipo mikrotik del sector de Jardín Botánico quedan de la siguiente manera:

6.5.12.2. Configuración Mikrotik – Jardín Botánico

Su ingreso es realizado mediante la herramienta Winbox una herramienta libre sin mayor impedimento para ejecutarla, al igual como se expuso en la sección 6.4.1 Escenario de Pruebas 1 Equipos Mikrotik. El modelo del equipo es: Mikrotik CCR1036-12G-4S, constando de 12 interfaces Gigabit Ethernet.

El inicio de sesión y acceso a los equipos se dio con los permisos otorgados por el Subdirector de Redes y Equipos Informáticos, “Usuario” y “Contraseña” para la realización de las configuraciones respectivas, con las capturas mostradas a continuación se indica paso a paso el desarrollo quedando configuradas ambas pilas de protocolos en IPv4 e IPv6.

- Ingresar dirección IPv6

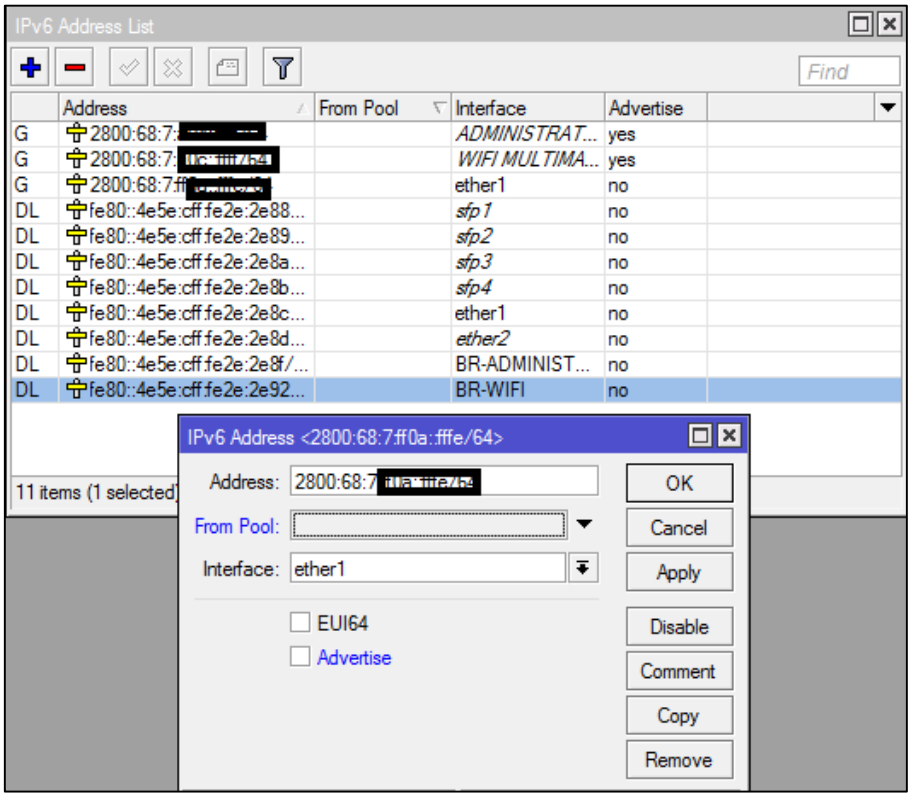


Figura 171: Configurar dirección IPv6.

Configurar DHCPv6: como las VLAN ya se encuentran creadas procedemos a configurar los requisitos para DHCPv6.

- Crear Pool con el prefijo IPv6 para cada Vlan

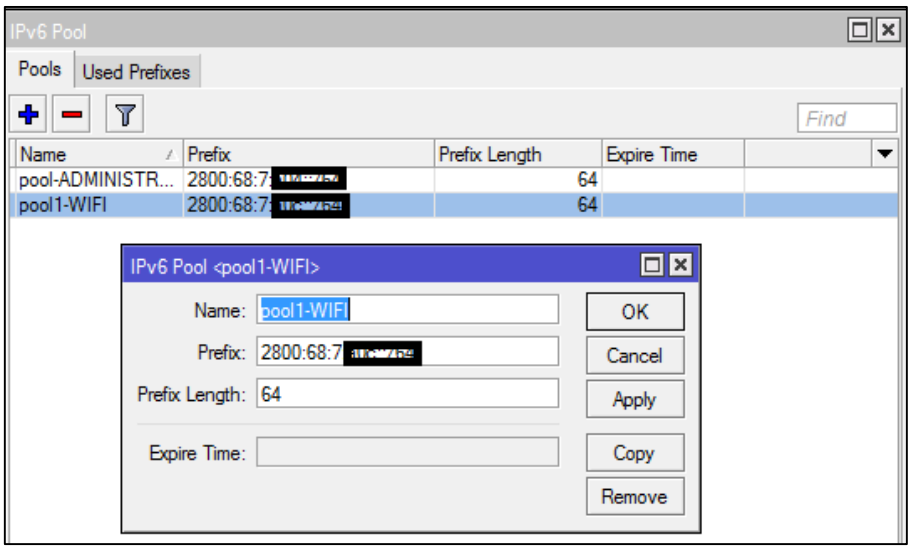


Figura 172: Pool DHCPv6.

- Configurar DHCPv6 Server

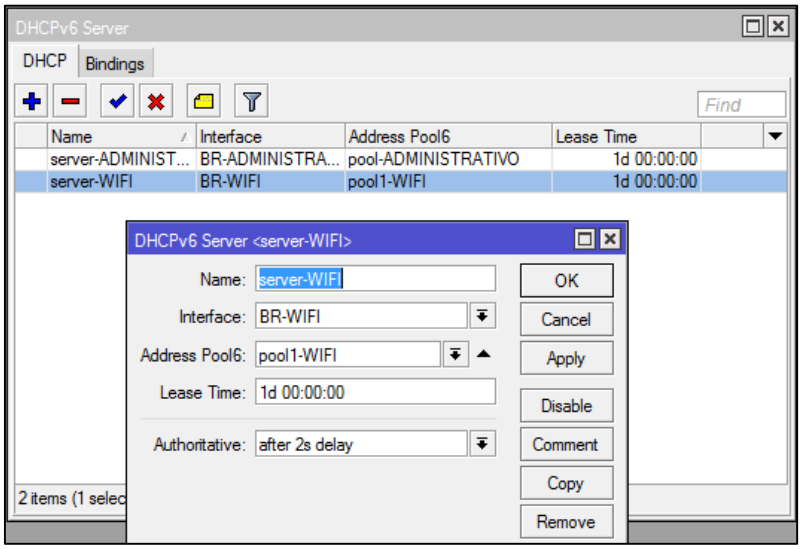


Figura 173: Configuración DHCPv6 server.

- Configurar OSPFv3: "*Interfaces*"

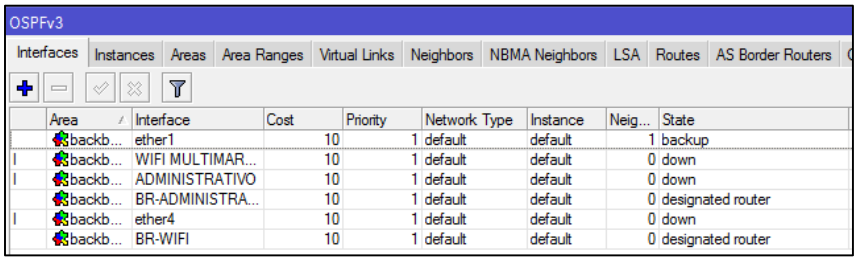


Figura 174: OSPFv3: Interfaces.

- Configurar OSPFv3: "*Instances*"

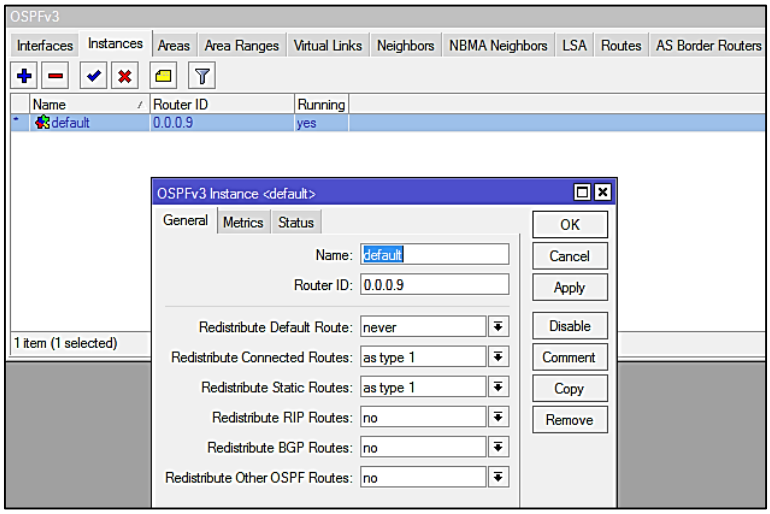


Figura 175: OSPFv3: Instances.

- OSPFv3: “*Areas*”

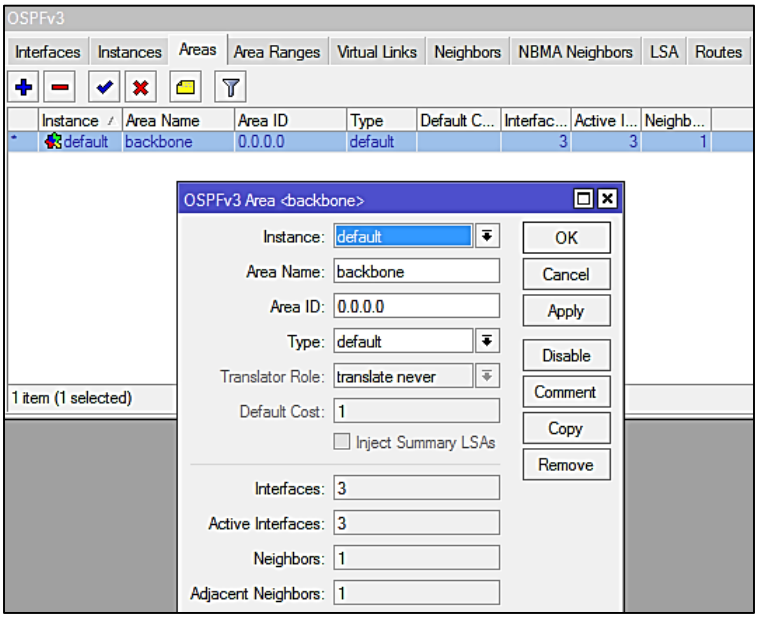


Figura 176: OSPFv3: Areas.

- OSPFv3: “*Neighbors*”

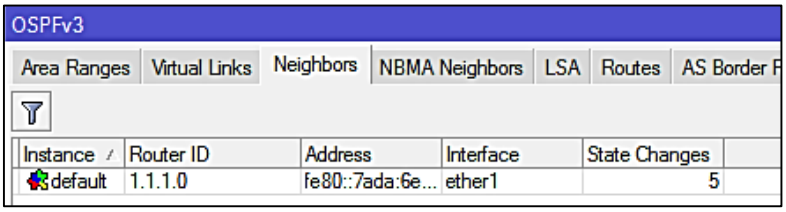


Figura 177: OSPFv3: Neighbors.

- Rutas aprendidas por OSPFv3

```
[uti@JBOS2MC0101SM01_1.0] /ipv6 route> print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, o - ospf, b - bgp, U - unreachable
#      DST-ADDRESS                GATEWAY                    DISTANCE
0 ADo  2800:68:7:[redacted]2::/64      fe80::7ada:6eff:fe19:...      110
1 ADo  2800:68:7:[redacted]3::/64      fe80::7ada:6eff:fe19:...      110
2 ADo  2800:68:7:[redacted]4::/64      fe80::7ada:6eff:fe19:...      110
3 ADo  2800:68:7:[redacted]5::/64      fe80::7ada:6eff:fe19:...      110
4 ADo  2800:68:7:[redacted]6::/64      fe80::7ada:6eff:fe19:...      110
5 ADo  2800:68:7:[redacted]7::/64      fe80::7ada:6eff:fe19:...      110
6 ADo  2800:68:7:[redacted]8::/64      fe80::7ada:6eff:fe19:...      110
7 ADo  2800:68:7:[redacted]9::/64      fe80::7ada:6eff:fe19:...      110
8 ADo  2800:68:7:[redacted]a::/64      fe80::7ada:6eff:fe19:...      110
9 ADo  2800:68:7:[redacted]b::/64      fe80::7ada:6eff:fe19:...      110
```

Figura 178: Rutas aprendidas por OSPFv3.

- Asignación de dirección IPv6 a usuario final

```
Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : Controladora Realtek PCIe GBE Fam
ily
   Dirección física. . . . . . . . . . . . . : 30-F9-ED-BC-B0-78
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Dirección IPv6 . . . . . . . . . . . : 2800:68:7:[redacted]:1f90:f255(Prefer
ido)
   Dirección IPv6 temporal. . . . . . . : 2800:68:7:[redacted]:d19f:2148(Prefer
ido)
   Vínculo: dirección IPv6 local. . . : fe80::81aa:9a8d:1f90:f255%12(Preferido)

   Dirección IPv4. . . . . . . . . . . . . . : 10.10.121.252(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Concesión obtenida. . . . . . . . . . . . : miércoles, 24 de mayo de 2017 11:
24:30
   La concesión expira . . . . . . . . . . . : jueves, 25 de mayo de 2017 11:27:
16
   Puerta de enlace predeterminada . . . . . : fe80::4e5e:cff:fe2e:2e8f%12
                                               10.10.121.1
   Servidor DHCP . . . . . . . . . . . . . . : 10.10.121.1
   IAID DHCPv6 . . . . . . . . . . . . . . . : 254867949
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-1F-CB-14-11-30-F9-ED-
BC-B0-78
   Servidores DNS. . . . . . . . . . . . . . : 172.16.32.2
                                               172.16.32.3
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado

C:\Users\Sony>
```

Figura 179: Asignación IPv6 a Usuario Final.

6.5.12.3. Configuración Mikrotik – Obelisco

El equipo a utilizar es el siguiente: Mikrotik CCR1016-12G, consta de 12 interfaces Gigabit Ethernet.

Las configuraciones realizadas en el sector de Obelisco son las mismas comparadas con el sector de Jardín Botánico la única diferencia será en las direcciones IPv6 a utilizar, la asignación correcta de las direcciones a los equipos, la creación de su correspondiente DHCPv6 para las VLAN que se encuentren trabajando y levantando el proceso de enrutamiento mediante el protocolo OSPFv3, todo aquello conlleva a resumir un poco sus configuraciones por ser las mismas y presentando las rutas aprendidas por medio del protocolo de enrutamiento configurado, completamente en funcionamiento y quedando levantadas ambas pilas de protocolos de internet, IPv4 e IPv6.

- Rutas aprendidas OSPFv3

```
[uti@B10S2MD1002SM01_1.0] > ipv6 route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static,
 #      DST-ADDRESS                GATEWAY                    DISTANCE
 0 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
 1 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
 2 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
 3 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
 4 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
 5 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
 6 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
 7 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
 8 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
 9 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
10 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
11 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
12 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
13 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
14 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
15 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
16 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
17 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
18 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
19 ADo  2800:68:7:[redacted]:/64   fe80::7ada:6eff:fe19:...       110
```

Figura 180: Rutas aprendidas con OSPFv3.

De esta manera queda desplegado el nuevo protocolo de internet versión 6 (IPv6) y el actual protocolo que está en marcha IPv4, en los sectores mencionados con anterioridad dejando así mismo una guía de implementación para los demás sectores en los que se comuniquen mediante radio enlace, observando ambas pilas de protocolos mediante el mecanismo de transición escogido como es Doble Pila.

Como es una transición, las configuraciones no realizadas en los equipos faltantes poco a poco se las irá realizando. Pudiendo observar que tanto para la tecnología CISCO como para la tecnología MIKROTIK se realizó el despliegue de IPv6 quedando así en funcionamiento, estos lugares no serán diferentes tornándose repetitivas y siendo las mismas para los equipos de red faltante.

7. DISCUSIÓN

7.1. Evaluación del objeto de investigación

El presente trabajo de titulación denominado **"Despliegue del Protocolo de Internet versión 6 (IPv6) para los dispositivos Core y Switchs de distribución en la red de datos de la Universidad Nacional de Loja"** dio como resultado final la implementación en los equipos reales configurando IPv6 dentro de la institución.

El desarrollo de la propuesta alternativa se basa en el cumplimiento de cada uno de los objetivos específicos que fueron abarcados en su totalidad tal y como se describe a continuación:

- **Objetivo específico 1.** Analizar la situación actual de los dispositivos Core y Switchs de distribución en la red de datos de la Universidad Nacional de Loja.

Este objetivo se lo abordó en primer lugar realizando una entrevista escogiendo a la persona idónea para que me proporcione información confiable y segura Ing. Jhon Calderón - Subdirector de Telecomunicaciones e Información y administrador de la red de datos de la UNL, pudiendo de esta manera empaparme de la estructura principal "Backbone", servicios, tecnología; observando los equipos con los que la institución cuenta. Luego ya con la información pertinente y como es de conocimiento para el trabajo de titulación comprobar en fuentes confiables si el equipo Switch Core WS-C6506-E y los Switchs de distribución WS-C3750X-24T-S y WS-C3750X-48PF-S, soportan el nuevo y mejorado protocolo de internet IPv6 obteniendo de la misma empresa de creación de los equipos resultados positivos para desplegar IPv6.

- **Objetivo específico 2.** Determinar el mecanismo de transición a utilizar entre IPv4 a IPv6.

El objetivo mencionado se lo abordó en tres partes:

Investigación Bibliográfica

Se realizó una investigación bibliográfica para conocer los mecanismos de transición más utilizados para la correcta transición y que de esta manera puedan coexistir ambos protocolos tanto IPv4 como IPv6, siendo la transición la opción adecuada hasta el momento porque la estructura de internet en gran porcentaje trabajo con IPv4 acoplando de esta manera IPv6 para su utilización.

Parámetros para los Mecanismos de Transición

El estudio profundo de los mecanismos de transición nos dio como resultado tres, creados por la IETF que son: Doble Pila, Túneles y Traducción, cada uno de ellos fue evaluado mediante parámetros establecidos acorde con su funcionamiento y características importantes para la implementación como es: escalabilidad, configuración, compatibilidad (hardware y software), seguridad, interoperabilidad, movilidad, desempeño, aplicabilidad y usabilidad. No obstante nos dio como resultado que Doble Pila con un porcentaje del 96% es el mecanismo apropiado para poderlo aplicar en los equipos de red de la Universidad Nacional de Loja.

Caso de estudio

Después de realizar la selección del mecanismo de transición Doble Pila o Dual Satck, se describió 3 casos de éxito: el primero de ellos se ve reflejado el estudio y la implementación en los equipos reales en la Universidad Nacional del Chimborazo, en el segundo caso también se despliega IPv6 enfocándose ya en el agotamiento y escasez de sus direcciones IPv4 y tomando en consideración al nuevo protocolo y la seguridad que IPv6 presta mediante IPsec; y en el tercer caso se observa no un caso de éxito sino más bien un plan detallado y a profundidad del estudio de equipos y soporte de IPv6, infraestructura interna de la red, externa, protocolos de enrutamiento, etc., dejando un plan trazado pero a su vez utilizando el mecanismo Doble Pila ya que también se realizan pruebas en toda la Universidad Salesiana de Cuenca manteniendo ambas de protocolos IPv4 e IPv6, obteniendo en los tres casos resultados positivos referentes a la transición que hoy en día se viene dando.

- **Objetivo específico 3.** Diseñar el esquema de direccionamiento utilizando IPv6 para la red privada de la Universidad Nacional de Loja.

Para cumplir con el objetivo se tomó en cuenta el direccionamiento IPv4 con el que trabaja la UNL centrándome en los nombres que hasta el año 2016 se llamaban Áreas y ahora en el 2017 denominadas Facultad, creadas en toda la universidad, los equipos que posee y las VLAN creadas para cada departamento, dejando a un lado las direcciones IPv4 y centrando el estudio en la dirección IPv6 que posee la institución 2800:68:7::/48 y que a su vez para mostrar los resultados obtenidos el direccionamiento y algunas características mas serán expuestas mediante el prefijo de documentación 2001:db8::/32, resultando de esta manera fácil manejo y subneting para la asignación de direcciones IPv6.

- **Objetivo específico 4.** Establecer un escenario de pruebas de acuerdo al mecanismo de transición seleccionado.

Para el cumplimiento de este objetivo se lo abordó en dos partes:

Escenario de pruebas 1: Equipos físicos

Gracias a la ayuda prestada por el Departamento de Telecomunicaciones e Información, se pudo contar con un escenario de pruebas mediante equipos físicos; es decir, dos equipos en la tecnología mikrotik y un equipo en la tecnología cisco pudiendo así realizar las configuraciones necesarias para la implementación de IPv6. Comprobando el envio de paquetes mediante la herramienta Wireshark y realizando las respectivas comparativas entre la pila IPv4 y la pila IPv6 habilitadas.

Escenario de pruebas 2: Simulador de Redes

La creación de simuladores en este caso GNS3 dio la facilidad para poder realizar las pruebas y configuraciones como si se lo realizara en un ambiente real obteniendo resultados satisfactorios para poder abordar la implementación en los equipos reales.

- **Objetivo específico 5.** Realizar las configuraciones necesarias para la implementación del Protocolo de Internet versión 6 en los dispositivos Core y Switchs de distribución de la Universidad Nacional de Loja.

Finalmente para cumplir con este objetivo, las pruebas que se realizaron y los conocimientos obtenidos se los transmitieron hacia los equipos reales; para proceder a las configuraciones se optó por entregarme un usuario y contraseña por parte del director del departamento de UTI Ing. Milton Lavanda y mediante la supervisión para las configuraciones con el subdirector de UTI Ing. Jhon Calderón se tuvo acceso al Switch Core, Switch de distribución y Switch de acceso y directamente empezar a implementar IPv6 en la UNL, trabajando con mucho cuidado ya que hay que recordar que IPv4 se encuentra desplegado por toda la universidad tratando de mejor manera no ocasionar algún desperfecto en su red.

Adicionalmente también se desplegó IPv6 en los sectores de Jardín Botánico y de Obelisco, dichos sectores pertenecen a la Universidad Nacional de Loja pero se encuentran conectados mediante radio enlace al igual que el sector de Punzara, los equipos que están ubicados aquí son de la tecnología Mikrotik como se observó en la sección 6.5.12 y al igual que en los equipos CISCO quedan actualmente levantadas ambas pilas de protocolos IPv4 e IPv6.

7.2. Valoración Técnico – Económica – Ambiental

El presente trabajo de titulación se concluyó de manera satisfactoria porque se contó con todos los recursos humanos, económicos y tecnológicos. Tecnológicamente hablando el desarrollo del proyecto no implica el uso de equipos costosos, para la puesta en marcha se necesita de un computador donde funcionen programas básicos entre ellos podemos mencionar también Putty, Winbox, GNS3, los cuales no requieren de muchos recursos hardware, mientras que los equipos como Switch Core, Switch Distribución y Switch de Acceso en los que se trabajaría para las pruebas y luego para la implementación se dio facilidades por parte de Departamento de Telecomunicaciones e Información (UTI) quienes cuentan con tales equipos para las configuraciones. En el ámbito económico no hubo mayor inconveniente porque el software usado es en su mayoría libre y gratuito. Por las razones mencionadas fue factible el desarrollo del proyecto. Los materiales utilizados para el desarrollo del proyecto se detallan a continuación:

TABLA XXII: RECURSOS HUMANOS.

DESCRIPCIÓN	UNIDAD	CANTIDAD	COSTO UNITARIO	SUBTOTAL
Director de tesis	Hora	200	--	--
Tesista	Hora	400	4.00	1600.00
			TOTAL	1600.00

TABLA XXIII: RECURSOS MATERIALES.

DESCRIPCIÓN	UNIDAD	CANTIDAD	COSTO UNITARIO	SUBTOTAL
Copias	Unidad	440	0.02	8.80
Impresiones	Unidad	210	0.05	10.50
Anillados	Unidad	3	3.00	9.00
CD’s	Unidad	3	1.00	3.00
Empastados	Unidad	3	10.00	30.00
Transporte	--	--	40.00	40.00
Internet	Hora	1000	0.50	500.00
Refrigerio	Unidad	64	1.00	64.00
			TOTAL	665.30

TABLA XXIV: RECURSOS TÉCNICOS/TECNOLÓGICOS.

DESCRIPCIÓN	UNIDAD	CANTIDAD	COSTO UNITARIO	SUBTOTAL
Flash Memory	Unidad	1	8.00	8.00
Celular	--	--	30.00	30.00
Computador portátil SONY VAIO	Unidad	1	1300.00	1300.00
Winbox	Unidad	1	Free	--
Putty	Unidad	1	Free	--
Dia	Unidad	1	Free	--
Simulador de Redes GNS3	Unidad	1	Free	--
Paquete de Ofimática Microsoft	Unidad	1	250.00	250.00
Hyperterminal	Unidad	1	Free (Trial)	--
			TOTAL	1588.00

TABLA XXV: IMPREVISTOS.

DESCRIPCIÓN	SUBTOTAL
Valores posibles adicionales a los recursos necesarios	50.00
TOTAL	50.00

La TABLA XXIII, ilustra la suma total de todos los recursos: humanos, materiales, técnicos/tecnológicos y los imprevistos asignados al trabajo de titulación que nos brinda una aproximación real del coste del proyecto.

TABLA XXVI: RESUMEN DE PRESUPUESTO UTILIZADO.

DESCRIPCIÓN	SUBTOTAL
HUMANOS	1600.00
MATERIALES	665.300
TÉCNICOS/ TECNOLÓGICOS	1588.00
IMPREVISTOS	50.00
TOTAL	3903.30

8. CONCLUSIONES

Al finalizar el Despliegue del Protocolo de Internet versión 6 (IPv6) se puede concluir que:

- La motivación de desplegar IPv6 se dio por su característica relevante como es el alto número de disponibilidad de direcciones, permitiendo que todos los equipos que se conecten a la red dentro de la Universidad Nacional de Loja, no sufran del inminente agotamiento de direcciones IPv4 logrando una comunicación efectiva de extremo a extremo.

- En base a los parámetros establecidos (Escalabilidad, Configuración, Compatibilidad Hardware y Software, Seguridad, Interoperabilidad, Movilidad, Desempeño, Aplicabilidad y Usabilidad), se determinó que Doble Pila con un 96% es la mejor de las tres alternativas analizadas para la transición al nuevo protocolo de Internet (IPv6), ya que no requiere duplicidad en los equipos ni en sus interfaces de red, manteniendo la misma infraestructura dentro de la institución.

- Mediante la herramienta Wireshark se logró capturar paquetes tanto en IPv4 como en IPV6 con los protocolos habilitados como son: ICMPv4, ICMPv6, DHCPv4, DHCPv6, OSPFv2, OSPFv3, realizando de esta manera comparativas relevantes, obteniendo como resultado la simplificada cabecera que IPv6 maneja y la eliminación de campos como: Header Length, Identification, Flags, Fragment, Header Checksum, Options, Padding, campos innecesarios que IPv4 utilizaba.

- Con la creación del programa Dr. IPv6 gracias a LACNIC, se tomó en consideración puntos importantes dados por expertos en desplegar IPv6, como es, combinar las técnicas de: STATELES y STATEFUL que maneja el protocolo DHCPv6, obteniendo la asignación total de parámetros con las configuraciones realizadas en los equipos de red: dirección IPv6, Gateway o puerta de enlace, dirección IPv6 del DNS, nombre de dominio, técnica EUI-64 y el tiempo de vida de la dirección IPv6 asignada al usuario final.

- El ruteo en IPv6 se da en forma jerárquica, sin las clases que existen a lo largo de IPv4, de esta forma se observó que en el switch CORE y de Distribución las tablas de ruta no crecían, permitiendo disminuir sus tamaños, simplificando el ruteo, haciendo que los equipos sean eficientes al momento de enviar sus paquetes, dado que la fragmentación del mismo se lo realiza en el origen y el reensamblado en el destino, aumentando así la velocidad del paquete con el tráfico circundante.

9. RECOMENDACIONES

Dadas las conclusiones durante el Despliegue del Protocolo de Internet versión 6 (IPv6) me permito sugerir lo siguiente:

- Recomendar a la Unidad de Telecomunicaciones e Información (UTI), la capacitación del recurso humano para el manejo del nuevo protocolo, entendiendo cada configuración realizada en los equipos de red, puesto que la implantación de IPv6 requiere de un análisis cuidadoso, a pesar de que las funcionalidades son similares a las de IPv4, los mecanismos a utilizar son distintos.

- Revisar minuciosamente el soporte de IPv6 al momento de adquirir equipos nuevos, ya que los fabricantes se encuentran dedicados a la implantación de IPv6 en todos sus productos y redes, adquiriendo así recursos tecnológicos listos para continuar con su transición de IPv4 a IPv6.

- Tener en consideración varios puntos, entre ellos: tamaño de la red, diseño de la topología de red, distribución de las direcciones IPv6, metodología de implementación, protocolos de enrutamiento, etc. Con el fin de obtener los mejores resultados, al finalizar el despliegue de IPv6.

- Utilizar protocolos de enrutamiento dinámico, esto permitirá tener un mejor control y acceso a las rutas de manera sencilla; considerando que al aplicar un protocolo de red estático se puede terminar cometiendo errores o se podría omitir alguna ruta, ocasionando que la conectividad y los accesos a los nodos se pierdan, lo que produce una pérdida de tiempo.

- Obtener como referencia los prefijos de documentación expuestos en sus respectivos RFC (Request for Comments – Petición de Comentarios) tanto para IPv4 como para IPv6, en el instante de mostrar el direccionamiento interno realizado para la Universidad Nacional de Loja, con el fin de resguardar información crítica manejada por la institución y evitar daños e intrusiones por parte de terceras personas.

- Utilizar todas las herramientas que nos ofrece GNS3 como imágenes de IOS actualizadas, máquinas virtuales, asegurando de esta manera que las pruebas realizadas de conectividad y funcionalidad reflejen los resultados de una simulación apegada a un ambiente real donde se desea implementar.

- Impulsar y promover iniciativas para desplegar la versión 6 del Protocolo de Internet, tanto en empresas públicas como privadas por medio de la Universidad Nacional de Loja, Departamento de Unidad de Telecomunicaciones e Información, incluyendo como referente el presente trabajo para futuras implementaciones.

10. BIBLIOGRAFÍA

[1] M. D. Rey, «Internet Protocol, California: IETF. RFC 791,» California, 1981.

[2] L. M. S. Bracero, «Estudio y Análisis del estado actual de la Implantación de IPv6 en los proveedores de servicios de Internet a nivel Nacional.,» Quito, 2012.

[3] P. R. L. MIGUEL, «Simulación de funcionamiento del protocolo ipv6 entre una red WAN y LAN mediante el simulador GNS3,» Quito, 2014.

[4] L. Peralta, Agosto 2012. [En línea]. Available: http://www.cu.ipv6tf.org/pdf/ipv6.pdf.

[5] G. G. R. F. C. O. C. P. J. R. M. y. o. Cicileo, IPv6 para todos. Guía para uso y aplicación para diversos entornos., Buenos Aires, 2009.

[6] F. Contreras, «Guía para el aseguramiento del protocolo IPv6. Seguridad y Privacidad de la Información,» Mintic, Colombia, 2015.

[7] F. C. E. p. e. d. d. I. A. -. CEDIA, «Introducción a IPv6,» de *CEDIA-Ecuador*, Cuenca, 2010.

[8] Cisco, «Implementing IPv6 in an Enterprise Network,» Agosto 2012. [En línea]. Available: http://ciscodocuments.blogspot.com/2011/05/chapter-08-implementing-ipv6-in.html. [Último acceso: 15 Noviembre 2016].

[9] C. Taffernaberry, G. Mercado, A. Dantiacq, S. Pérez y R. Moralejo, «Implementación de Túnel 6to4,» Universidad Tecnológica Nacional, Mendoza Argentina, 2008.

[10] D. F. N. Lara, «Estudio para la Migración de IPv4 a IPv6 para la empresa proveedora de Internet Milltec S.A.,» , Quito, 2009.

[11] J. P. &. G. E. M. Barrera, «Implementación de TUNNELING entre redes IPV4 E IPV6 para la empresa NETXPERTS CONSULTING S.A. (Tesis de Grado),» Junio

2005. [En línea]. Available: http://repositorio.espe.edu.ec/bitstream/21000/406/1/T-ESPE-012631.pdf. [Último acceso: 1 Febrero 2017].

[12] CITEL, «Migración a IPv6,» Agosto 2012. [En línea]. Available: http://www.oas.org/en/citel/infocitel/2001/agosto/arin_e.asp. [Último acceso: 12 Enero 2017].

[13] J. S. F. Ernesto, «Estudio e Implementación de una red IPv6 en la UTFSM. (Tesis Ing. Civil Telemático),» Universidad Técnica Federico Santa María. Departamento de Electrónica., Valparaiso-Chile, 2009.

[14] A. Kaplan y T. Rhodes, «Capítulo 29. Networking avanzado,» 2010. [En línea]. Available: https://www.freebsd.org/doc/es/books/handbook/network-ipv6.html. [Último acceso: 20 Enero 2017].

[15] Microsoft, «IPv6 - General - Propiedades de la Interfaz,» Junio 2012. [En línea]. Available: http://technet.microsoft.com/es-es/library/cc772282(v=WS.10).aspx. [Último acceso: 15 Enero 2017].

[16] IETF, «Special-Use IPv6 Address,» RFC 5156, 2008.

[17] IETF, «Prefijo de dirección IPv6 IPv4-compatible,» RFCMX3.

[18] IETF, «Internet Protocol Version 6 (IPv6) Addressing Architecture,» RFC 3513, 2003.

[19] IETF, «6bone (IPv6 Testing Address Allocation) Phaseout,» RFC 3701, 2004.

[20] E. A. Martínez, «Supuesto práctico de análisis para la Transición de IPv4 a IPv6 en un entorno de redes empresariales WAN/LAN,» 10 Febrero 2013. [En línea]. [Último acceso: 12 Enero 2017].

[21] K. L. J. Abley, «Operation of Anycast Services,» Network Working Group, Diciembre 2006. [En línea]. Available: https://tools.ietf.org/html/rfc4786. [Último acceso: 17 Marzo 2017].

[22] M. D. G. García, «Estudio del direccionamiento y los Protocolos de enrutamiento basados en IPv6,» Universidad de San Buenaventura Cali, Cali-Colombia, 2010.

[23] IETF, «Unicast-Prefix-based IPv6 Multicast Address,» Network Working Group, Agosto 2002. [En línea]. Available: https://tools.ietf.org/html/rfc3306. [Último acceso: 11 Diciembre 2016].

[24] IETF, «IP Version 6 Addressing Architecture,» Network Working Group, Febrero 2006. [En línea]. Available: https://tools.ietf.org/html/rfc4291#appendix-A. [Último acceso: 23 Ferero 2017].

[25] S. Hagen, IPv6 Essentials 2da Edición, O´Reilly, 2006.

[26] F. R. F. Calahorrano, «Análisis y Emulación de Multihoming y de la Publicación al Internet de servicios WEB, Transferencia de Archivos y Correo a través de una red IPv6,» Quito, 2014.

[27] D. V. Silvia Duque, «Análisis del Protocolo IPv6 su evolución y aplicabilidad,» 5 Febrero 2013. [En línea]. Available: http://repositorio.utn.edu.ec/handle/123456789/1109. [Último acceso: 9 Enero 2017].

[28] Cisco, «ICMPV6 for IPv6,» IPv6 Addressing and Basic Connectivity Configuration Guide, Cisco IOS XE Release 3S, 2012.

[29] S. Hagen, IPv6 Essentials, O`Reilly & Associates Inc, 2002.

[30] A. P. S. Alamar, «Análisis, Diseño e Implementación de una red Prototipo utilizando el Protocolo IPv6 y QoS para la Empresa SANTANET,» Quito, 2014.

[31] C. Huitema, IPv6:The New Protocol, Prentice-Hall, 1998.

[32] A. C. A. Jordi Palet Martínez, «El Protocolo IPv6,» 5 Enero 2004. [En línea]. Available: http://www.6sos.org/documentos/6SOS_El_Protocolo_IPv6_v4_0.pdf. [Último acceso: 18 Febrero 2017].

[33] E. G. C. P. S. K. J. Veizades, «Service Location Protocol,» RFC Editor, Junio 1997. [En línea]. Available: https://tools.ietf.org/html/rfc2165. [Último acceso: 12 Noviembre 2016].

[34] «Word IPv6 Lunch,» Internet Society, 6 Junio 2012. [En línea]. Available: http://www.worldipv6launch.org/. [Último acceso: 3 Diciembre 2016].

[35] A. F. Alcántara, «TUTORIAL de IPv6 - IPv6 México - UNAM,» Septiembre 2010. [En línea]. Available: http://www.ipv6.unam.mx/documentos/Tutorial-IPv6-UNAM.pdf. [Último acceso: 4 Diciembre 2016].

[36] U. C. A. Javier, 24 Mayo 2007. [En línea]. Available: http://repositorio.espe.edu.ec/bitstream/21000/1172/1/T-ESPE-021890.pdf. [Último acceso: 5 Octubre 2016].

[37] C. Microsoft, IPv6/IPv4 Coexistence and Migration, 2001.

[38] E. N. R. Gilligan, Transition Mechanisms for IPv6 Hosts and Routers, RFC 2893, 2000.

[39] «Portal IPv6 - Dual Stack o Doble Pila,» LACNIC, [En línea]. Available: http://portalipv6.lacnic.net/dual-stack-o-pila-doble/. [Último acceso: 10 Diciembre 2016].

[40] J. Davies, «Understanding IPv6,» Washington USA, 2008.

[41] A. Acosta, S. Aggio, G. Cicileo, T. Lynch, A. Moreiras, A. Servin y S. Berenguer, «Ipv6 para Operadores de Red, 1ª Edición,» Transversal Branding, Buenos Aires, Argentina, 2014.

[42] C. Huitema, «Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs) IETF,» 2006. [En línea]. Available: http://tools.ietf.org/html/rfc4380. [Último acceso: 10 Diciembre 2016].

[43] «Internet Society,» Internet Hall of Fame, [En línea]. Available: http://www.isoc.org/. [Último acceso: 20 Enero 2017].

[44] D. Fernández, «Transition Mechanics BIA, TRT & Socks,» Departamento de Sistemas Telemáticos, Universidad Politécnica de Madrid, España, 2002.

[45] Cisco, «Cisco Catalyst 6506-E Switch,» [En línea]. Available: http://www.cisco.com/c/en/us/support/switches/catalyst-6506-e-switch/model.html. [Último acceso: 12 Marzo 2017].

[46] Cisco, «Cisco Catalyst 3750X-24T-S Switch,» [En línea]. Available: http://www.cisco.com/c/en/us/support/switches/catalyst-3750x-24t-s-switch/model.html. [Último acceso: 12 Marzo 2017].

[47] Cisco, «Cisco Catalyst 3750X-48PF-S Switch,» [En línea]. Available: http://www.cisco.com/c/en/us/support/switches/catalyst-3750x-48pf-s-switch/model.html. [Último acceso: 12 Marzo 2017].

[48] Mikrotik, «RouterBoard,» [En línea]. Available: https://routerboard.com/CCR1036-12G-4S. [Último acceso: 1 06 2017].

[49] Cisco, «Cisco Catalyst 2960-48TT-S Switch,» [En línea]. Available: http://www.cisco.com/c/en/us/support/switches/catalyst-2960-48tt-s-switch/model.html. [Último acceso: 12 Marzo 2017].

[50] G. Moreno y C. Orozco, «Universidad Nacional de Chimborazo,» 2011. [En línea]. Available: http://dspace.unach.edu.ec/bitstream/51000/3119/1/UNACH-ING-ELC-TEL-2016-0035.pdf. [Último acceso: 12 Marzo 2017].

[51] D. Ramírez, J. Guzmán y B. Jesús, «Universidad Católica de Colombia,» 2015. [En línea]. Available: http://repository.ucatolica.edu.co/bitstream/10983/2803/1/IPV6.pdf. [Último acceso: 12 Marzo 2017].

[52] D. Landy, «Universidad Politécnica Salesiana Sede Cuenca,» 2013. [En línea]. Available: http://dspace.ups.edu.ec/bitstream/123456789/5332/1/UPS-CT002767.pdf. [Último acceso: 12 Marzo 2017].

11. ANEXOS

ANEXO I: MANUAL TÉCNICO DE CONFIGURACIÓN EQUIPOS SWITCH CORE Y SWITCH DE DISTRIBUCIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA

Manual del Administrador
Versión 1.0

CONTROL DEL DOCUMENTO

DATOS GENERALES	
Código:	001
Versión:	1.0
Fecha de la versión:	2 de mayo de 2017
Páginas:	
Creado por:	Walter Agusto Camacho Saritama
Revisado por:	Ing. Jhon Calderón
Aprobado por:	
Nivel de confidencialidad:	Alto

CONTROL DE VERSIONES			
Código	**Versión**	**Fecha**	**Responsable**
001	1.0	02 de mayo de 2017	Walter Agusto Camacho Saritama

CONTROL DE MODIFICACIONES				
Código	**Versión**	**Fecha**	**Responsable**	**Descripción**
001	1.0	02 de mayo del 2017	Walter Camacho	

FIRMAS DE RESPONSABILIDAD			
Descripción	**Nombres y Apellidos**	**Cargo**	**Firma**
Creado por:	Walter Agusto Camacho Saritama	Egresado de la Carrera de Ingeniería en Sistemas	
Revisado por:	Ing. Jhon Calderón	Subdirector de Telecomunicación e Información	
Aprobado por:			

Ciudad Universitaria “Guillermo Falconí Espinosa”, La Argelia, Loja - Ecuador
Teléfonos: 07 2547252 Ext.: 125, Email: soporte.uti@unl.edu.ec, Web: http://www.unl.edu.ec

1. INTRODUCCIÓN

El presente manual detalla las configuraciones necesarias para poder desplegar el Protocolo de Internet versión 6 dentro de los equipos Switch Core, Switch de Distribución y Switch de Acceso, con el objetivo de ofrecer al usuario final una nueva alternativa de conexión con las características y ventajas que el nuevo protocolo de internet ofrece, enmarcado dentro de la Universidad Nacional de Loja.

2. DIRIGIDO A ADMINISTRADORES

Se detalla el proceso de despliegue del Protocolo de Internet versión 6 en el Switch Core, Switch de Distribución y Switch de Acceso a los administradores de redes del Departamento de Telecomunicaciones e Información (UTI).

3. OBJETIVO

Desplegar el Protocolo de Internet versión 6 (IPv6) con los nuevos protocolos de enrutamiento necesarios para la Universidad Nacional de Loja.

4. DEFINIR PROCEDIMIENTO PARA LA CONFIGURACIÓN DE IPV6

Pasos a seguir:

1. Verificar conexión física.
2. Verificar las direcciones IPv6 a utilizar.
3. Configuración de las direcciones IPv6 en el Switch Core y de Distribución (L3).
    a. Probar conectividad.
4. Configurar las direcciones IPv6 en las interfaces del Switch L3 y L2.
    a. Asignar dirección IPv6 a “VLAN-Nativa” en Switch L3 y L2.
    b. Asignar puertos en Switch L2 para “VLAN [ID-VLAN]”.
    c. Probar conectividad.
5. Autoconfiguración STATELESS o STATEFUL en L3.
    a. Verificar asignación de dirección IPv6 y parámetros en Usuario Final.
    b. Probar conectividad.
6. Configurar protocolo de enrutamiento OSPFv3 en Switch Core y L3.
    a. Agregar las interfaces que intervienen en OSPFv3.
    b. Probar conectividad.

Para realizar las configuraciones pertinentes, uno de los programas a utilizar para acceder es Putty, sesión iniciada por medio de SSH (Secure Shell – Intérprete de Órdenes Seguro); facilitando el manejo de los equipos.

En la siguiente sección se muestra las configuraciones correspondientes al equipo principal Switch Core WS-C6506-E, indicando la configuración de sus interfaces y se indica también las configuraciones del protocolo de enrutamiento para la versión 6 que es OSPFv3.

Ciudad Universitaria “Guillermo Falconí Espinosa”, La Argelia, Loja - Ecuador
Teléfonos: 07 2547252 Ext.: 125, Email: soporte.uti@unl.edu.ec, Web: http://www.unl.edu.ec

5. Configuración Switch CORE (Facultad Administración - UTI / Facultad Energía - Biblioteca)

Los siguientes comandos serán de forma general para el Switch CORE: ingresamos a modo de configuración global y luego habilitamos enrutamiento en todo el equipo para IPv6.

```
S1MA0204CO01#configure terminal
S1MA0204CO01(config)#ipv6 unicast-routing
```

Habilitar ruteo para IPv6 y configurar la dirección IPv6 en la interfaz de conexión entre el Switch CORE y Switch L3 Facultad de Administración.

- **Configuración interfaz GiX/X (Administración)**

```
S1MA0204CO01(config)#interface gigabitEthernet X/X
S1MA0204CO01(config-if)#ipv6 address 2001:DB8:3003:ADA2::FFFF/64
S1MA0204CO01(config-if)#no shutdown
S1MA0204CO01(config-if)#exit
```

Habilitar ruteo para IPv6 y configuración de la dirección IPv6 en la interfaz de conexión entre el Switch CORE y Switch L3 Facultad de Energía.

- **Configuración interfaz GiX/X (Energía)**

```
S1MA0204CO01(config)#interface gigabitEthernet X/X
S1MA0204CO01(config-if)#ipv6 address 2001:DB8:3003:ADA8::FFFF/64
S1MA0204CO01(config-if)#no shutdown
S1MA0204CO01(config-if)#exit
```

Configuración Switch CORE (Facultades restantes)

- **Configuración interfaz GiX/X (Educativa)**

```
S1MA0204CO01(config)#interface gigabitEthernet X/X
S1MA0204CO01(config-if)#ipv6 address 2001:DB8:3003:ADA3::FFFF/64
S1MA0204CO01(config-if)#no shutdown
S1MA0204CO01(config-if)#exit
```

- **Configuración interfaz GiX/X (Agropecuaria)**

```
S1MA0204CO01(config)#interface gigabitEthernet X/X
S1MA0204CO01(config-if)#ipv6 address 2001:DB8:3003:ADA6::FFFF/64
S1MA0204CO01(config-if)#no shutdown
S1MA0204CO01(config-if)#exit
```

- **Configuración interfaz GiX/X (MED)**

```
S1MA0204CO01(config)#interface gigabitEthernet X/X
S1MA0204CO01(config-if)#ipv6 address 2001:DB8:3003:ADA7::FFFF/64
S1MA0204CO01(config-if)#no shutdown
S1MA0204CO01(config-if)#exit
```

- **Configuración interfaz GiX/X (Energía-Laboratorios)**

```
S1MA0204CO01(config)#interface gigabitEthernet X/X
S1MA0204CO01(config-if)#ipv6 address 2001:DB8:3003:ADA9::FFFF/64
S1MA0204CO01(config-if)#no shutdown
S1MA0204CO01(config-if)#exit
```

Se define número de proceso para OSPFv3 y un ID tal como se lo realiza en IPv4, para encontrar routers vecinos desde el CORE.

- **Configuración OSPFv3**

Ciudad Universitaria "Guillermo Falconí Espinosa", La Argelia, Loja - Ecuador
Teléfonos: 07 2547252 Ext.: 125, Email: soporte.uti@unl.edu.ec, Web: http://www.unl.edu.ec

```
S1MA0204CO01#configure terminal
S1MA0204CO01(config)#ipv6 router ospf 1
S1MA0204CO01(config-rtr)#router-id 1.1.1.0
S1MA0204CO01(config-rtr)#exit
```

Se ingresa a la interfaz conectada desde el Core hacia el L3 de la Facultad de Administración y se levanta el proceso de OSPFv3.

```
S1MA0204CO01(config)#interface gigabitEthernetX/X
S1MA0204CO01(config-if)#ipv6 enable
S1MA0204CO01(config-if)#ipv6 ospf 1 area 0
S1MA0204CO01(config-if)#exit
```

Se ingresa a la interfaz de conexión entre el Switch CORE hacia Switch L3 Facultad Energía y se levanta el proceso de OSPFv3.

```
S1MA0204CO01(config)#interface gigabitEthernetX/X
S1MA0204CO01(config-if)#ipv6 enable
S1MA0204CO01(config-if)#ipv6 ospf 1 area 0
S1MA0204CO01(config-if)#exit
```

OSPFv3: CORE – Educativa

```
S1MA0204CO01(config)#interface gigabitEthernetX/X
S1MA0204CO01(config-if)#ipv6 enable
S1MA0204CO01(config-if)#ipv6 ospf 1 area 0
S1MA0204CO01(config-if)#exit
```

OSPFv3: CORE – Agropecuaria

```
S1MA0204CO01(config)#interface gigabitEthernetX/X
S1MA0204CO01(config-if)#ipv6 enable
S1MA0204CO01(config-if)#ipv6 ospf 1 area 0
S1MA0204CO01(config-if)#exit
```

OSPFv3: CORE – MED

```
S1MA0204CO01(config)#interface gigabitEthernetX/X
S1MA0204CO01(config-if)#ipv6 enable
S1MA0204CO01(config-if)#ipv6 ospf 1 area 0
S1MA0204CO01(config-if)#exit
```

OSPFv3: CORE – Energía Laboratorios

```
S1MA0204CO01(config)#interface gigabitEthernetX/X
S1MA0204CO01(config-if)#ipv6 enable
S1MA0204CO01(config-if)#ipv6 ospf 1 area 0
S1MA0204CO01(config-if)#exit
```

En la sección 6 se indica las configuraciones de uno de los equipos de distribución como el Switch WS-C3750X-24T-S, así mismo su configuración en las interfaces, protocolo de enrutamiento OSPFv3 y agregando en este punto la configuración de DHCPv6 donde se utilizó la configuración STATEFUL para poder obtener mayor descripción y asignación de sus parámetros como por ejemplo: dirección IPv6 del DNS, nombre de dominio, a parte de su puerta de enlace o gateway y su dirección IPv6.

Ciudad Universitaria “Guillermo Falconí Espinosa”, La Argelia, Loja - Ecuador
Teléfonos: 07 2547252 Ext.: 125, Email: soporte.uti@unl.edu.ec, Web: http://www.unl.edu.ec

6. Configuración Switch Distribución o L3 (Facultad Administración – Departamento UTI)

Habilitar ruteo para IPv6 y configuración de la dirección IPv6 en la interfaz de conexión entre el Switch L3 Facultad de Administración hacia el Switch CORE.

- **Configuración interfaz GiX/X/X**

```
S1MA0204SD01_1.0#configure terminal
S1MA0204SD01_1.0(config)#ipv6 unicast-routing
S1MA0204SD01_1.0(config)#interface gigabitEthernet X/X/X
S1MA0204SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:ADA2::FFFE/64
S1MA0204SD01_1.0(config-if)#no shutdown
S1MA0204SD01_1.0(config-if)#exit
```

Agregar dirección IPv6 para VLAN Nativa correspondiente a la administración de los equipos y levantar su interfaz.

- **Configuración VLAN Nativa**

```
S1MA0204SD01_1.0(config)#interface vlan 2
S1MA0204SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:1A3::FFFF/64
S1MA0204SD01_1.0(config-if)#no shutdown
S1MA0204SD01_1.0(config-if)#exit
```

Se configura la dirección IPv6 en la VLAN UTI.

- **Configurar VLAN-UTI**

```
S1MA0204SD01_1.0(config)#interface vlan 3
S1MA0204SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:1A4::FFFF/64
S1MA0204SD01_1.0(config-if)#no shutdown
S1MA0204SD01_1.0(config-if)#exit
```

Configuración VLAN restantes de la Facultad de Administración

```
S1MA0204SD01_1.0(config)#interface vlan 10
S1MA0204SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:1A5::FFFF/64
S1MA0204SD01_1.0(config-if)#no shutdown
S1MA0204SD01_1.0(config-if)#exit

S1MA0204SD01_1.0(config)#interface vlan 20
S1MA0204SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:1A6::FFFF/64
S1MA0204SD01_1.0(config-if)#no shutdown
S1MA0204SD01_1.0(config-if)#exit

S1MA0204SD01_1.0(config)#interface vlan 30
S1MA0204SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:1A7::FFFF/64
S1MA0204SD01_1.0(config-if)#no shutdown
S1MA0204SD01_1.0(config-if)#exit

S1MA0204SD01_1.0(config)#interface vlan 40
S1MA0204SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:1A8::FFFF/64
S1MA0204SD01_1.0(config-if)#no shutdown
S1MA0204SD01_1.0(config-if)#exit

S1MA0204SD01_1.0(config)#interface vlan 50
S1MA0204SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:1A9::FFFF/64
S1MA0204SD01_1.0(config-if)#no shutdown
S1MA0204SD01_1.0(config-if)#exit
```

```
S1MA0204SD01_1.0(config)#interface vlan 60
S1MA0204SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:1AA::FFFF/64
S1MA0204SD01_1.0(config-if)#no shutdown
S1MA0204SD01_1.0(config-if)#exit

S1MA0204SD01_1.0(config)#interface vlan 70
S1MA0204SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:1AB::FFFF/64
S1MA0204SD01_1.0(config-if)#no shutdown
S1MA0204SD01_1.0(config-if)#exit

S1MA0204SD01_1.0(config)#interface vlan 120
S1MA0204SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:1AC::FFFF/64
S1MA0204SD01_1.0(config-if)#no shutdown
S1MA0204SD01_1.0(config-if)#exit

S1MA0204SD01_1.0(config)#interface vlan 210
S1MA0204SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:1AD::FFFF/64
S1MA0204SD01_1.0(config-if)#no shutdown
S1MA0204SD01_1.0(config-if)#exit
```

Ingresar a la interfaz de conexión entre el Switch L3 Facultad de Administración y Switch L2 Facultad de Administración, se agrega una descripción, se realiza encapsulación dot1q para todas las VLAN, habilitar el puerto en modo troncal y hacer constar los ID de VLAN.

```
S1MA0204SD01_1.0(config)#interface gigabitEthernetX/X/X
S1MA0204SD01_1.0(config-if)#description TESIS_IPV6
S1MA0204SD01_1.0(config-if)#swicthport trunk encapsulation dot1q
S1MA0204SD01_1.0(config-if)#switchport trunk native vlan
S1MA0204SD01_1.0(config-if)#switchport trunk allowed vlan
1-3,10,20,30,40,50,60,70,120,200,210
S1MA0204SD01_1.0(config-if)#switchport mode trunk
S1MA0204SD01_1.0(config-if)#no shutdown
S1MA0204SD01_1.0(config-if)#exit
```

- **Configuración DHCPv6 STATELES y STATEFUL**

Crear DHCPv6 mediante la técnica establecida STATEFUL en Switch L3 Facultad de Administración, agregar la dirección IPv6 para el pool de direcciones y establecer un tiempo de vida de las direcciones, agregar la dirección IPv6 del DNS y fijar un nombre de dominio.

```
S1MA0204SD01_1.0(config)#ipv6 dhcp pool STATEFUL_TESIS_IPV6
S1MA0204SD01_1.0(config-dhcpv6)#address prefix 2001:DB8:3003:1A4::/64 lifetime 1800 600
S1MA0204SD01_1.0(config-dhcpv6)#dns-server 2001:DB8:3003:ACA5::1234
S1MA0204SD01_1.0(config-dhcpv6)#domain-name TESIS_IPV6.COM
S1MA0204SD01_1.0(config-dhcpv6)#exit
```

NOTA: *Se puede realizar la agregación si es necesario de otro DNS con dirección IPv6. En los parámetros del Usuario Final también se podrá observar ambos DNS establecidos.*
Las demás configuraciones de DHCPv6 serán las mismas, el único cambio es en la dirección IPv6 la cual debe corresponder al de la VLAN y poseer un pool diferente para cada una.

Ciudad Universitaria "Guillermo Falconí Espinosa", La Argelia, Loja - Ecuador
Teléfonos: 07 2547252 Ext.: 125, Email: soporte.uti@unl.edu.ec, Web: http://www.unl.edu.ec

Se ingresa a la interfaz de la VLAN 3, activar IPv6, ingresar dirección IPv6 seguido de la técnica EUI-64, asignar el DHCPv6 server con el mismo nombre que se lo creó y activar las dos banderas M y O.

```
S1MA0204SD01_1.0(config)#interface vlan 3
S1MA0204SD01_1.0(config-if)#ipv6 enable
S1MA0204SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:1A4::FFFF/64 eui-64
S1MA0204SD01_1.0(config-if)#ipv6 dhcp server STATEFUL_TESIS_IPV6
S1MA0204SD01_1.0(config-if)#ipv6 nd managed-config-flag          Flag M=1
S1MA0204SD01_1.0(config-if)#ipv6 nd other-config-flag            Flag O=1
S1MA0204SD01_1.0(config-dhcpv6)#exit
```

NOTA: *Las demás configuraciones son las mismas, se ingresa a cada una de las VLAN y se agrega su dirección IPv6 correspondiente a cada una se habilita las dos banderas en todos los casos.*

- **Configuración OSPFv3**

Definir número de proceso para OSPFv3 en Switch L3 Facultad de Administración y un ID tal como se lo realiza en IPv4, para encontrar routers vecinos.

```
S1MA0204SD01_1.0#configure terminal
S1MA0204SD01_1.0(config)#ipv6 router ospf 1
S1MA0204SD01_1.0(config-rtr)#router-id 1.1.1.1
S1MA0204SD01_1.0(config-rtr)#exit
```

Agregar la interfaz de conexión entre el Switch L3 Facultad de Administración y Switch Core para enrutamiento OSPFv3.

```
S1MA0204SD01_1.0(config)#interface gigabitEthernetX/X/X
S1MA0204SD01_1.0(config-if)#ipv6 enable
S1MA0204SD01_1.0(config-if)#ipv6 ospf 1 area 0
S1MA0204SD01_1.0(config-if)#exit
```

Ingresar interfaz nativa, activar IPv6 en la interfaz, agregar proceso OPSFv3 creado al área 0 (Backbone) para enrutamiento.

```
S1MA0204SD01_1.0(config)#interface vlan 2
S1MA0204SD01_1.0(config-if)#ipv6 enable
S1MA0204SD01_1.0(config-if)#ipv6 ospf 1 area 0
S1MA0204SD01_1.0(config-if)#exit
```

Ingresar interfaz VLAN 3, activar IPv6 en la interfaz, agregar proceso OPSFv3 creado al área 0 (Backbone) para enrutamiento.

```
S1MA0204SD01_1.0(config)#interface vlan 3
S1MA0204SD01_1.0(config-if)#ipv6 enable
S1MA0204SD01_1.0(config-if)#ipv6 ospf 1 area 0
S1MA0204SD01_1.0(config-if)#exit
```

NOTA: *Se agrega así mismo las demás interfaces de cada VLAN para enrutamiento OSPFv3 del mismo como la VLAN 3.*

En el Switch de Acceso WS-C2960-48TT-S, son muy pocas las configuraciones pero a la vez necesarias como por ejemplo la habilitación de la plantilla “dual-ipv4-and-ipv6” y la agregación de las direcciones IPv6.

Ciudad Universitaria “Guillermo Falconí Espinosa”, La Argelia, Loja - Ecuador
Teléfonos: 07 2547252 Ext.: 125, Email: soporte.uti@unl.edu.ec, Web: http://www.unl.edu.ec

7. Configuración Switch Acceso o L2 (Facultad Administración – Departamento UTI)

Elegir plantilla dual para que trabajen ambos protocolos IPv4 e IPv6, reiniciar el equipo.

- **Configuración SDM**

```
S1MA0204SA02_1.1#configure terminal
S1MA0204SA02_1.1(config)#sdm prefer dual-ipv4-and-ipv6 default
S1MA0204SA02_1.1(config)#exit
S1MA0204SA02_1.1#reload
```

Ingresar interfaz VLAN nativa, agregar dirección IPv6, levantar interfaz.

- **Configuración VLAN Nativa**

```
S1MA0204SA02_1.1#configure terminal
S1MA0204SA02_1.1(config)#interface vlan 2
S1MA0204SA02_1.1(config-if)#ipv6 address 2001:DB8:3003:1A3::FFFE/64
S1MA0204SA02_1.1(config-if)#no shutdown
S1MA0204SA02_1.1(config-if)#exit
```

Ingresar a la interfaz de conexión entre el Switch L2 Facultad de Administración y Switch L3 Facultad de Administración, se agrega una descripción, se realiza encapsulación dot1q para todas las VLAN, habilitar el puerto en modo troncal y hacer constar los ID de VLAN.

- **Habilitar puerto Troncal**

```
S1MA0204SA02_1.1(config)#interface fastEthernetX/X
S1MA0204SA02_1.1(config-if)#description USUARIO_FINAL_IPV6
S1MA0204SA02_1.1(config-if)#switchport trunk native vlan 2
S1MA0204SA02_1.1(config-if)#switchport trunk allowed vlan
1-3,10,20,30,40,50,60,70,120,200,210
S1MA0204SA02_1.1(config-if)#switchport mode trunk
S1MA0204SA02_1.1(config-if)#no shutdown
S1MA0204SA02_1.1(config-if)#exit
```

Ingresar interfaz de conexión Switch L2 Facultad Administración hacia los puntos de red de Sala de Conferencias UTI, activar ambos puertos en modo de acceso, dar paso a la VLAN 3.

- **Asignar puertos: Acceso VLAN 3 a la interfaz**

```
S1MA0204SA02_1.1(config)#interface fastEthernet0/9
S1MA0204SA02_1.1(config-if)#switchport mode access
S1MA0204SA02_1.1(config-if)#switch access vlan 3
S1MA0204SA02_1.1(config-if)#exit

S1MA0204SA02_1.1(config)#interface fastEthernet0/10
S1MA0204SA02_1.1(config-if)#switchport mode access
S1MA0204SA02_1.1(config-if)#switch access vlan 3
S1MA0204SA02_1.1(config-if)#exit
```

Las siguientes configuraciones serán una réplica de las configuraciones antes realizadas y se tornarán un poco repetitivas ya que los equipos serían los mismos y su estructura de red se mantendría igual. Para poder comprobar el enrutamiento mediante el protocolo OSPFv3 en IPv6 se tomó como referencia el Área de la Energía

Ciudad Universitaria "Guillermo Falconí Espinosa", La Argelia, Loja - Ecuador
Teléfonos: 07 2547252 Ext.: 125, Email: soporte.uti@unl.edu.ec, Web: http://www.unl.edu.ec

específicamente el departamento de Biblioteca, quedando las configuraciones de la siguiente manera y obteniendo resultados satisfactorios.

8. Configuración Switch Distribución o L3 (Facultad Energía – Departamento Biblioteca)

Habilitar ruteo para IPv6 y configuración de la dirección IPv6 en la interfaz de conexión entre el Switch L3 Facultad de Energía hacia el Switch CORE.

- **Configuración interfaz GiX/X/X**

```
S2MD0301SD01_1.0#configure terminal
S2MD0301SD01_1.0(config)#ipv6 unicast-routing
S2MD0301SD01_1.0(config)#interface gigabitEthernet X/X/X
S2MD0301SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:ADA8::FFFE/64
S2MD0301SD01_1.0(config-if)#no shutdown
S2MD0301SD01_1.0(config-if)#exit
```

Agregar dirección IPv6 para VLAN Nativa correspondiente a la administración de los equipos y levantar su interfaz.

- **Configuración VLAN Nativa**

```
S2MD0301SD01_1.0(config)#interface vlan 2
S2MD0301SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:7A3::FFFF/64
S2MD0301SD01_1.0(config-if)#no shutdown
S2MD0301SD01_1.0(config-if)#exit
```

Ingreso a la VLAN 30, asignar dirección IPv6. Levantar la interfaz.

- **Configurar VLAN Estudiantes**

```
S2MD0301SD01_1.0(config)#interface vlan 30
S2MD0301SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:7A6::FFFF/64
S2MD0301SD01_1.0(config-if)#no shutdown
S2MD0301SD01_1.0(config-if)#exit
```

Ingresar a la interfaz de conexión entre el Switch L3 Facultad Energía y Switch L2 Facultad Energía, se agrega una descripción, se realiza encapsulación dot1q para todas las VLAN, habilitar el puerto en modo troncal y hacer constar los ID de VLAN.

```
S2MD0301SD01_1.0(config)#interface gigabitEthernetX/X/X
S2MD0301SD01_1.0(config-if)#description TESIS_IPV6
S2MD0301SD01_1.0(config-if)#switchport trunk allowed vlan
1,2,10,20,30,40,50,60,70,80,90,100,110,120,200,210
S2MD0301SD01_1.0(config-if)#no shutdown
S2MD0301SD01_1.0(config-if)#exit
```

***NOTA**: como la interfaz se encuentra activa no es necesario habilitar el puerto en modo trunk solo se requiere incluir las VLAN que estaban trabajando.*

- **Configuración DHCPv6 STATELES y STATEFUL**

Crear DHCPv6 mediante la técnica establecida STATEFUL en Switch L3 Facultad Energía, agregar la dirección IPv6 para el pool de direcciones y establecer un tiempo de duración de dichas direcciones, agregar la dirección IPv6 del DNS y fijar un nombre de dominio.

```
S2MD0301SD01_1.0(config)#ipv6 dhcp pool STATEFUL_TESIS_IPV6
S2MD0301SD01_1.0(config-dhcpv6)#address prefix 2001:DB8:3003:7A6::/64 lifetime 1800 600
S2MD0301SD01_1.0(config-dhcpv6)#dns-server 2001:DB8:3003:ACA5::1234
```

```
S2MD0301SD01_1.0(config-dhcpv6)#domain-name TESIS_IPV6.COM
S2MD0301SD01_1.0(config-dhcpv6)#exit
```

Se ingresa a la interfaz de la VLAN 30, activar IPv6, ingresar dirección IPv6 seguido de la técnica EUI-64, asignar el DHCPv6 server con el mismo nombre que se lo creó y activar las dos banderas M y O.

```
S2MD0301SD01_1.0(config)#interface vlan 30
S2MD0301SD01_1.0(config-if)#ipv6 enable
S2MD0301SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:7A6::FFFF/64 eui-64
S2MD0301SD01_1.0(config-if)#ipv6 dhcp server STATEFUL_TESIS_IPV6
S2MD0301SD01_1.0(config-if)#ipv6 nd managed-config-flag          Flag M=1
S2MD0301SD01_1.0(config-if)#ipv6 nd other-config-flag            Flag O=1
S2MD0301SD01_1.0(config-dhcpv6)#exit
```

- **Configuración OSPFv3**

Definir número de proceso para OSPFv3 en Switch L3 Facultad Energía y un ID tal como se lo realiza en IPv4, para encontrar routers vecinos.

```
S2MD0301SD01_1.0#configure terminal
S2MD0301SD01_1.0(config)#ipv6 router ospf 1
S2MD0301SD01_1.0(config-rtr)#router-id 1.1.1.7
S2MD0301SD01_1.0(config-rtr)#exit
```

Agregar la interfaz de conexión entre el Switch L3 Facultad Energía y Switch Core para enrutamiento OSPFv3.

```
S2MD0301SD01_1.0(config)#interface gigabitEthernetX/X/X
S2MD0301SD01_1.0(config-if)#ipv6 enable
S2MD0301SD01_1.0(config-if)#ipv6 ospf 1 area 0
S2MD0301SD01_1.0(config-if)#exit
```

Ingresar interfaz nativa, activar IPv6 en la interfaz, agregar proceso OPSFv3 creado al área 0 (Backbone) para enrutamiento.

```
S2MD0301SD01_1.0(config)#interface vlan 2
S2MD0301SD01_1.0(config-if)#ipv6 enable
S2MD0301SD01_1.0(config-if)#ipv6 ospf 1 area 0
S2MD0301SD01_1.0(config-if)#exit
```

Ingresar interfaz VLAN de estudiantes, activar IPv6 en la interfaz, agregar proceso OPSFv3 creado al área 0 (Backbone) para enrutamiento.

```
S2MD0301SD01_1.0(config)#interface vlan 30
S2MD0301SD01_1.0(config-if)#ipv6 enable
S2MD0301SD01_1.0(config-if)#ipv6 ospf 1 area 0
 S2MD0301SD01_1.0(config-if)#exit
```

9. Configuración Switch Acceso o L2 (Facultad Energía – Departamento Biblioteca)

- **Configuración SDM**

Elegir plantilla dual para que trabajen ambos protocolos IPv4 e IPv6, reiniciar el equipo.

```
S2MD1001SA01_1.5##configure terminal
S2MD1001SA01_1.5(config)#sdm prefer dual-ipv4-and-ipv6 default
S2MD1001SA01_1.5(config)#exit
S2MD1001SA01_1.5#reload
```


Ciudad Universitaria “Guillermo Falconí Espinosa”, La Argelia, Loja - Ecuador
Teléfonos: 07 2547252 Ext.: 125, Email: soporte.uti@unl.edu.ec, Web: http://www.unl.edu.ec

- **Configuración VLAN de Administración de Equipos (VLAN-Nativa)**

Ingresar interfaz VLAN nativa, agregar dirección IPv6, levantar interfaz.

```
S2MD1001SA01_1.5#configure terminal
S2MD1001SA01_1.5(config)#interface vlan 2
S2MD1001SA01_1.5(config-if)#ipv6 address 2001:DB8:3003:7A3::FFFE/64
S2MD1001SA01_1.5(config-if)#no shutdown
S2MD1001SA01_1.5(config-if)#exit
```

- **Habilitar puerto Troncal**

Ingresar a la interfaz de conexión entre el Switch L2 Facultad Energía y Switch L3 Facultad Energía, se agrega una descripción, se realiza encapsulación dot1q para todas las VLAN, habilitar el puerto en modo troncal y hacer constar los ID de VLAN.

```
S2MD1001SA01_1.5(config)#interface gigabitEthernetX/X
S2MD1001SA01_1.5(config-if)#description USUARIO_FINAL_IPV6
S2MD1001SA01_1.5(config-if)#switchport trunk allowed vlan
1,2,10,20,30,40,50,60,70,80,90,100,110,120,200,210
S2MD1001SA01_1.5(config-if)#no shutdown
S2MD1001SA01_1.5(config-if)#exit
```

- **Asignar puertos de VLAN 30 a la interfaz**

Ingresar interfaz de conexión Switch L2 Facultad Energía hacia el punto de red de Biblioteca, activar puerto en modo de acceso, dar paso a la VLAN 30.

```
S2MD1001SA01_1.5(config)#interface fastEthernet0/16
S2MD1001SA01_1.5(config-if)#switchport mode access
S2MD1001SA01_1.5(config-if)#switch access vlan 30
S2MD1001SA01_1.5(config-if)#exit
```

Se adiciona dentro del Manual Técnico la configuración de DHCPv6 mediante la técnica STATELESS acotando que mediante esta técnica se torna incompleta la asignación de parámetros.

***NOTA**: la técnica STATELESS mediante DHCPv6 no fue implementada por lo motivos expuestos anteriormente en la sección 6. Sino se la conbinó con STATEFUL*

- **Configuración DHCPv6 STATELESS**

```
ADMS1MA0204SD01_1.0(config)#ipv6 dhcp pool STATELESS_TESIS_IPV6
ADMS1MA0204SD01_1.0(config-dhcpv6)#dns-server 2800:68:7:fe04::1234
ADMS1MA0204SD01_1.0(config-dhcpv6)#domain-name TESIS_IPV6.COM
ADMS1MA0204SD01_1.0(config-dhcpv6)#exit

ADMS1MA0204SD01_1.0(config)#interface vlan 30
ADMS1MA0204SD01_1.0(config-if)#ipv6 enable
ADMS1MA0204SD01_1.0(config-if)#ipv6 address 2001:DB8:3003:6A6::FFFF/64 eui-64
ADMS1MA0204SD01_1.0(config-if)#ipv6 dhcp server STATELESS_TESIS_IPV6
ADMS1MA0204SD01_1.0(config-if)#ipv6 nd other-config-flag          Flag O=1
ADMS1MA0204SD01_1.0(config-dhcpv6)#exit
```

Comandos adicionales:

Muestra las interfaces con direcciones IPv6.

#show ipv6 interface brief

Muestra las VLAN existentes

#show vlan

Muestra el DHCPv6 para IPv6

Ciudad Universitaria "Guillermo Falconí Espinosa", La Argelia, Loja - Ecuador
Teléfonos: 07 2547252 Ext.: 125, Email: soporte.uti@unl.edu.ec, Web: http://www.unl.edu.ec

#show ipv6 dhcp pool
Muestra la dirección IPv6 mediante la técnica EUI-64, datos de expiración de la dirección asignada.
#show ipv6 dhcp binding
Muestra el nombre del pool creado por DHCPv6
#show ipv6 dhcp interface
Muestra el identificador del router vecino.
#show ipv6 ospf neighbor
Muestra la tabla de rutas del OSPFv3
#show ipv6 route
Muestra la plantilla con la que está trabajando actualmente.
#show sdm prefer

10. CONCLUSIÓN

Con la elaboración del Manual Técnico se logrará con éxito implementar el nuevo protocolo de internet IPv6 en los equipos Switch Core, Switch Distribución y Switch de Acceso llegando al usuario final la implementación en todo el campus universitario.

Ciudad Universitaria "Guillermo Falconí Espinosa", La Argelia, Loja - Ecuador
Teléfonos: 07 2547252 Ext.: 125, Email: soporte.uti@unl.edu.ec, Web: http://www.unl.edu.ec

ANEXO II: CERTIFICADO DE IMPLEMENTACIÓN OTORGADO POR LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN (UTI)

Milton Leonardo Labanda Jaramillo
DIRECTOR DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN

Certifica

Que el señor **WALTER AUGUSTO CAMACHO SARITAMA** con cédula de ciudadanía número **0705383487** egresado de la Carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja, ha finalizado y socializado los resultados del proyecto de titulación denominado **"Despliegue del Protocolo de Internet versión 6 (IPv6) para los dispositivos Core y Switchs de distribución en la red de datos de la Universidad Nacional de Loja"**, bajo los lineamientos y requerimientos establecidos por esta unidad administrativa

Es cuanto puedo indicar en honor a la verdad, facultando al interesado hacer uso del presente documento en lo que creyere conveniente

Loja, 29 de mayo del 2017.

Milton Labanda, Mtr
DIRECTOR DE TELECOMUNICACIONES E INFORMACIÓN

ANEXO III: ENTREVISTA REALIZADA AL SUBDIRECTOR DE REDES Y EQUIPOS INFORMÁTICOS

CARRERA DE INGENIERÍA EN SISTEMAS

Entrevista realizada para la elaboración del Trabajo de Titulación correspondiente a desarrollar el proyecto: **"Despliegue del Protocolo de Internet Versión 6 (IPv6) para los dispositivos Core y Switchs de Distribución en la red de datos de la Universidad Nacional de Loja"**.

Nombre: Ing. Jhon Alexander Calderón.

Institución en la que labora: Universidad Nacional de Loja.

Cargo: Subdirector de Redes y Equipos Informáticos.

Fecha de Entrevista: 04 de enero de 2016.

Objetivo: Obtener los diferentes tipos de problemas que pueden surgir al no implementar el Protocolo de Internet Versión 6 (IPv6) en la red de datos de la Universidad Nacional de Loja.

Algunos inconvenientes que se visualizan a futuro y que pueden ocurrir si se continúa utilizando direccionamiento IPv4 es el agotamiento de direcciones IPv4 Públicas, como universidad y como ente académico no podemos hacernos a oídos sordos por lo que debemos adaptarnos a las nuevas tecnologías y una de ellas es IPv6; de no hacerlo, no podríamos acceder a sitios de internet que tengan habilitado solo para IPv6 en vista de que los protocolos IPv4 e IPv6 no son compatibles

Es importante el despliegue de IPv6 en la Universidad Nacional de Loja porque al tener instalado IPv6 nos va a permitir como Universidad innovar en nuevos proyecto de investigación en áreas como: seguridad, videoconferencia, telefonía IP, entre otros.

Al tener implementado IPv6 se eliminaría la técnica que se denomina NAT (Traducción de Direcciones de Red) que utiliza IPv4; se podría tener conexiones punto a punto (end to end) con cualquier equipo en todo el mundo, pero se debería tomar medidas de seguridad al implementar IPv6 ya que algún atacante podría hacer un ingreso no autorizado a mi computador.

Los beneficios que ofrecerá IPv6 en el caso que se diera su implementación se basa en todos nuestros servicios institucionales (servicios públicos) sean accesibles tanto en el protocolo IPv4 e IPv6, por ejemplo si ahora mismo hay una red en cualquier parte del mundo que solo tenga implementado IPv6 y quiere acceder a nuestra página no lo podría hacer por incompatibilidad de protocolos o si quiere comunicarse lo podría hacer utilizando alguna técnica como NAT64 o túneles.

Esto queda por analizar, ya que se dice que en IPv6 la latencia es menor pero se debería realizar las pruebas necesarias para comprobarlo, lo podría ser en la actualidad porque el tráfico de internet un 90% está por IPv4 aunque el tráfico por IPv6 está en aumento datos estadísticos del 2015 afirman q están en un 10% y al no implementar IPv6 nos podríamos estar quedando aislados de la red, pero recaería la responsabilidad en las personas que están al frente del departamento de telecomunicaciones de las universidades.

Se considera que es favorable y para iniciar hacer una transición entre los dos protocolos, es decir, que los dos protocolos estén funcionando en todos los equipos de red y servidores. En la transición de doble pila se analizaría la demanda de usuarios y ver la carga en los equipos, es decir son dos protocolos que van a estar implementados, por lo cual hay que tener en cuenta que el consumo de memoria incrementa por el procesamiento debido a que las peticiones serían a los dos protocolos.

La Migración a IPv6 no se tomaría en cuenta porque tocaría utilizar en algún equipo de borde alguna técnica para poder hacer la traducción.

Los dispositivos de red y los servidores con los que cuenta la Universidad Nacional de Loja soportan IPv6, el 90% si soportan IPv6 por ejemplo en servidores Debian y Centos desde varios años ya soporta IPv6, actualmente en la Universidad Nacional de Loja se está trabajando con un equipamiento CISCO y también soporta IPv6.

Los servicios de internet como Apache ya soportan IPv6 conjuntamente con el DNS, DHCP, FTP.

En la actualidad al no implementar IPv6 una de las causas sería el desconocimiento de las personas que están al frente de las redes, o tal vez porque no le ven algún beneficio o está funcionando todo bien en IPv4.

No hay que esperar a que los equipos, servicios sean accesibles a esta nueva tecnología o que tengamos algún inconveniente para recién ahí tomar medidas sino más bien ir innovando conforme avanza la tecnología.

NOTA: Los datos proporcionados se utilizarán únicamente con fines académicos y en particular para la tesis denominada: **"Despliegue del Protocolo de Internet Versión 6 (IPv6) para los dispositivos Core y Switchs de Distribución en la red de datos de la Universidad Nacional de Loja"**

Ing. Jhon Alexander Calderón

Subdirector de Redes y Equipos Informáticos.

ANEXO IV: ESPECIFICACIONES Y SOPORTE DE IPV6 EN EQUIPOS CISCO

Cisco Catalyst 6500/Cisco 7600 Series Supervisor Engine 720

Product Overview

The Cisco® Catalyst® 6500/Cisco 7600 Series Supervisor Engine 720 is a family of Supervisor Engine(s) designed to deliver scalable performance and rich set of IP features in hardware. Its hardware-based feature set enables applications such as traditional IP forwarding, Layer 2 and Layer 3 Multiprotocol Label Switching (MPLS) VPNs, Ethernet over MPLS (EoMPLS) with quality of service (QoS) and security features. The Supervisor engine 720 integrates a high-performance 720 Gbps crossbar switch fabric with a forwarding engine in a single module, delivering 40 Gbps of switching capacity per slot (enabling 4-port 10GE and 48-port 10/100/1000 density line cards). With hardware-enabled forwarding for IPv4, IPv6 and MPLS, the system performance is capable of 400 Mpps for IPv4, 200 Mpps for IPv6 traffic, with features and 1024 VRFs each populated with up to 700 routes/VRF for MPLS.

The Cisco Supervisor Engine 720 offers a strong set of security features. System security is hardened with support for features such as Port Security, CPU rate limiting, Multi-Path uRPF and a long list 802.1x extension. Extensive feature support such as QoS mechanisms, hardware-based generic-routing-encapsulation (GRE) tunneling, and access control lists (ACLs) enable customers to build high-performance, feature-rich campus networks, metropolitan (metro) aggregation, and various WAN edge networks.

With enhanced security, rich QoS and scalable performance for Gigabit and 10gigabit, the Sup720 is ideal for enterprise core and distribution and datacenters.

The Supervisor Engine 720 builds on the proven Cisco Express Forwarding (CEF) architecture, by supporting centralized forwarding (CEF) and distributed forwarding (dCEF). The variants of PFC3 distinguish the various Supervisor 720 families of engines. There are three flavors, PFC3A, PFC3B and PFC3BXL, correspond to WS-SUP720, WS-SUP720-3B and WS-SUP720-3BXL. The Supervisor Engine 720 family is supported on both operating systems–Cisco Catalyst OS® and Cisco IOS®.

Cisco Catalyst 3750 Series Switches

Product Overview

The Cisco® Catalyst® 3750 Series Switches (Figures 1 through 4) are innovative switches that improve LAN operating efficiency by combining industry-leading ease of use and high resiliency for stackable switches. This product series features Cisco StackWise™ technology, a 32-Gbps stack interconnect that allows customers to build a unified, highly resilient switching system, one switch at a time.

Figure 1. Cisco Catalyst 3750 Series Switches for 10/100 and 10/100/1000 Access and Aggregation

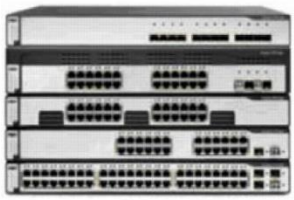


Figure 2. Cisco Catalyst 3750-24PS and Cisco Catalyst 3750-48PS Switches with IEEE 802.3af Power

Figure 3. Cisco Catalyst 3750G-16TD Switch

Figure 4. Cisco Catalyst 3750G-48TS Switch, Cisco Catalyst 3750G-48PS Switch with IEEE 802.3af Power, Cisco Catalyst 3750G-24TS-1U Switch, and Cisco Catalyst 3750G-24PS Switch with IEEE 802.3af Power

Cisco Catalyst 2960 Series Switches

Product Overview

Q. What is the Cisco Catalyst 2960PD-8TT-L compact switch?

A. The Cisco® Catalyst® 2960PD-8TT-L switch has eight 10/100 Mbps ports and receives power over the Gig uplink port from an upstream power over Ethernet (PoE) switch. The Cisco Catalyst 2960 powered device (PD) switch is ideal for deployments outside the wiring closet such as conference rooms and classrooms with spacing and wiring constraints.

Q. How can the Cisco Catalyst 2960PD-8TT-L compact switch be powered?

A. The Cisco Catalyst 2960PD-8TT-L can be powered by another PoE switch, a power adaptor or power injectors that support 802.3af, including AIR-PWRINJ4. The Cisco Catalyst 2960PD-8TT-L switch prioritizes the power adaptor over PoE input when both the power adaptor and the PoE input port are activated. The Cisco Catalyst 2960PD-8TT-L power adaptor and power cord are optional and sold separately

Q. What are the benefits of Power over Ethernet ?

A. Power over Ethernet can provide a lower total cost of ownership for deployments that incorporate Cisco IP phones and Cisco Aironet® wireless LAN access points, as well as any IEEE 802.3af compliant end device. Power over Ethernet removes the need for wall power to each PoE-enabled device and eliminates the cost for additional electrical cabling that would otherwise be necessary in IP phone and wireless LAN deployments. PoE switches also eliminate the need for power injectors and PoE mid-spans for powering IP devices.

Q. How many devices can the Cisco Catalyst 2960 Series power?

A. The Cisco Catalyst 2960-48PST-L can support 48 PoE ports with total PoE power output capacity at 370W. Taking advantage of Cisco Catalyst Intelligent Power Management, the Cisco Catalyst 2960-48PST-L configuration can deliver the necessary power to support 24 ports at 15.4W, 48 ports at 7.7W, or any combination in between. The Cisco Catalyst 2960-24PC-L can support 24 simultaneous full-powered PoE devices at 15.4W for maximum powered-device support. The Cisco Catalyst 2960-24LT-L can support eight PoE devices at 15.4W.

Q. Can Cisco Catalyst 2960 LAN Base switches support devices that require more than 15.4W?

A. No, Cisco Catalyst 2960 LAN Base switches support only up to 15.4W on PoE ports. The Cisco Catalyst 2960-24PC-L can support 24 simultaneous full-powered PoE port at 15.4W for maximum powered-device support. The Cisco Catalyst 2960-24LT-L24 has 24 10/100 ports with 8 simultaneous full-powered PoE ports at 15.4W. For support of higher than 15.4W, Cisco Catalyst 3560-E and 3750-E series switches are recommended.

Q. Does the Cisco Catalyst 2960 Series support standards-based Power over Ethernet?

A. Yes. The Cisco Catalyst 2960 Series supports IEEE 802.3af, and it provides investment protection for the installed base of Cisco IP phones and Cisco Aironet wireless LAN access points by also supporting the Cisco pre-standard Power over Ethernet (inline power).

Q. Can the Cisco Catalyst 2960 Series provide power to IEEE 802.3af and Cisco pre-standard Power over Ethernet simultaneously?

A. Yes. It automatically detects the end point to provide the appropriate power without any user intervention.

Q. What are the advantages of Cisco Catalyst 2960 Series Switches with the LAN Base software relative to Cisco Catalyst 2960 Series Switches with the LAN Lite software?

A. Cisco Catalyst 2960 LAN Base switches deliver intelligent services for branch offices and wiring closets. The LAN Base IOS software supports enhanced Layer 2+ security, quality of service (QoS), availability, and scalable management to enable new converged applications. Catalyst 2960 LAN Base switches include both 10/100 Fast Ethernet and 10/100/1000 Gigabit Ethernet connectivity in 8-, 24-, and 48-port configurations.

Cisco Catalyst 2960 LAN Lite switches are for entry-level branch office and wiring closet networks. They simplify the migration from nonintelligent hubs and unmanaged switches to a fully scalable and reliable network. The LAN Lite IOS software supports standard Layer 2 security, QoS, and availability while lowering the network total cost of ownership. Catalyst 2960 LAN Lite switches deliver 10/100 Fast Ethernet connectivity in 24- and 48-port configurations.

All Cisco Catalyst 2960 Series Switches have technical support service options available through Cisco SMARTNet® service. All come with a Limited Lifetime Hardware Warranty, and LAN Base and LAN Lite software updates are provided at no additional cost.

Q. What are the advantages of Cisco Catalyst 2960 PoE Series Switches and Cisco Catalyst 3560/3750 PoE Series Switches?

A. The Catalyst 2960 Series PoE switches with intelligent services are ideally suited for small branch offices that can benefit from converged networks. The Catalyst 2960 Series provides enhanced security, scalable management, and unified network services for applications such as unified communications and mobility. The Catalyst 3750 and 3560 with advanced intelligent services are better suited for enterprise and mid-market campus wiring closets as well as large branch offices. The Catalyst 3750 and 3560 Series switches provide investment protection and deliver increased availability and scalability through advanced L3 services, advanced security such as man-in-the-middle attack threat mitigation features, and increased control for applications like Telepresence.

Q. What are Cisco Catalyst 2960 Compact Switches?

A. Cisco Catalyst 2960 Compact Switches are small form-factor switches designed for deployments outside the wiring closet. They have a durable metal shell, no fan for silent operation, easy wall or under-the-desk mounting, a security lock to prevent theft, and an available cable guard to secure the Ethernet cables and switch. Now you can deliver intelligent services such as Network Admission Control for the office workspace, micro branch office, classroom, cruise ship, and other wiring-constrained environments. Table 1 describes the Cisco Catalyst 2960 Compact Switch portfolio.

ANEXO V: ACTA DE REUNIÓN NO. 034-UTI-2016 EXPOSICIÓN AVANCE DEL PROYECTO DE TITULACIÓN

Acta de Reunión No. 034-UTI-2016

Asunto:	Exposición del proyecto de titulación: **"Despliegue del Protocolo de Internet versión 6 (IPv6) para los dispositivos Core y Switchs de distribución en la red de datos de la Universidad Nacional de Loja"**		
Inicio:	15:30	**Duración:**	16:30
Convocado por:	Ing. Jhon Calderón	**Fecha:**	14/12/2016

AGENDA

- Ostentación de los resultados del "Despliegue del Protocolo de Internet versión 6 (IPv6) para los dispositivos Core y Switchs de distribución en la red de datos de la Universidad Nacional de Loja", ante las partes interesadas.

OBSERVACIONES/RECOMENDACIONES

- Agregar esquema de direccionamiento IPv6 del Centro de Formación Zapotepamba y El Padmi.
- Realizar pruebas de configuración de IPv6 en el simulador de red GNS3.
- Validar la asignación de los parámetros de red IPv6 en los equipos finales, prestar especial atención en la asignación del DNS primario y secundario.

ASISTENTES:

Ing. Hernán Torres **COORDINADOR C.I.S.**	Ing. Milton Labanda **DIRECTOR U.T.I.**	Walter Camacho **TESISTA**
Ing. Rodrigo Japón **FUNCIONARIO U.T.I**	Ing. Juan Pablo Ramón **FUNCIONARIO U.T.I.**	Ing. Jhon Calderón **SUBDIRECTOR R.E.I**