UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

"METODOLOGÍA DE TRANSICIÓN DEL PROTOCOLO DE INTERNET VERSIÓN 4 A VERSIÓN 6 EN EL GOBIERNO PROVINCIAL DE IMBABURA"

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTOR: STALIN ANDRÉS HIDROBO MAFLA

DIRECTOR: ING. CARLOS ALBERTO VÁSQUEZ AYALA

IBARRA-ECUADOR

2016

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1.- IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DEL CONTACTO	
Cédula de Identidad	100344461-7
Apellidos y Nombres	Hidrobo Mafla Stalin Andrés
Dirección	Jorge Dávila Meza 4-32 y Av. Cristóbal de Troya
E-mail	sahidrobom@utn.edu.ec
Teléfono Fijo	062954199
Teléfono Móvil	0967580385
DATOS DE LA OBRA	
Título	"METODOLOGÍA DE TRANSICIÓN DEL PROTOCOLO DE INTERNET VERSIÓN 4 A VERSIÓN 6 EN EL GOBIERNO PROVINCIAL DE IMBABURA"
Autor	Hidrobo Mafla Stalin Andrés
Fecha	
Programa	Pregrado
Título por el que se aspira:	Ingeniería en Electrónica y Redes de Comunicación
Director	Ing. Carlos Alberto Vásquez Ayala

2.- AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, STALIN ANDRÉS HIDROBO MAFLA, con cédula de identidad Nro. 100344461-7, en calidad de autor y titular de los derechos patrimoniales del trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior artículo 144.

3.- CONSTANCIAS

El auto manifiesta que la obra objeto de la presente autorización es original y se la desarrolló sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad Técnica del Norte en caso de reclamación por parte de terceros.

Ibarra, al 1 día del mes de Marzo del 2016

…….

Stalin Andrés Hidrobo Mafla

100344461-7

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, STALIN ANDRÉS HIDROBO MAFLA, con cédula de identidad Nro. 100344461-7, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor del trabajo de grado denominado: "METODOLOGÁ DE TRANSICIÓN DEL PROTOCOLO DE INTERNET VERSIÓN 4 A VERSIÓN 6 EN EL GOBIERNO PROVINCIAL DE IMBABURA", que ha sido desarrollado para optar el título de Ingeniería en Electrónica y Redes de Comunicación, en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos concedidos anteriormente. En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

Ibarra, al 1 día del mes de Marzo del 2016

……

Stalin Andrés Hidrobo Mafla

100344461-7

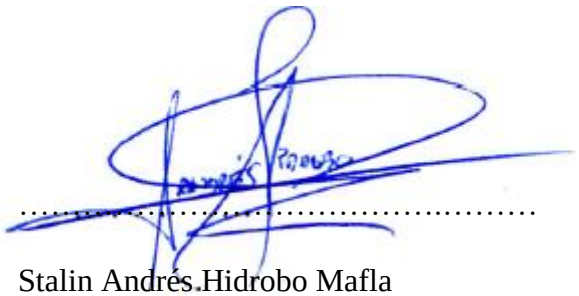
UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DECLARACIÓN

Yo, Stalin Andrés Hidrobo Mafla, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; y que éste no ha sido previamente presentado para ningún grado o calificación profesional.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las Leyes de Propiedad Intelectual, Reglamentos y Normatividad vigente de la Universidad Técnica del Norte



……

Stalin Andrés Hidrobo Mafla

100344461-7

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

Certifico que la Tesis “METODOLOGÍA DE TRANSICIÓN DEL PROTOCOLO DE INERNET VERSIÓN 4 A VERSIÓN 6 EN EL GOBIERNO PROVINCIAL DE IMBABURA” ha sido realizada en su totalidad por el señor: STALIN ANDRÉS HIDROBO MAFLA portador de la cédula de identidad numero:

100344461-7.

……

Ing. Carlos Vásquez.

Director de Tesis

AGRADECIMIENTO

Agradezco a Dios por protegerme durante todo mi camino brindándome salud, esperanza y fuerzas para superar obstáculos y dificultades a lo largo de mi vida.

A mi madre Esthela Mafla, por ser la mejor madre que Dios me ha regalado, por siempre darme tu amor incondicional, aunque haya cometido errores muchas veces tu siempre me diste tu apoyo y ayuda, siempre confiando en mí en momentos que ni siquiera yo creía en mí mismo. Gracias por todas las cosas que me has enseñado y por todos los sacrificios que hiciste por mí, eres una maravillosa mujer, por eso de esta manera hoy te lo agradezco desde el fondo de mi corazón

A mi padre Patricio Hidrobo, por haberme brindado tu sabiduría y compartido tus experiencias mediante consejos para prepararme a lo que la vida me depare sin rendirme ni desfallecer ante nada y siempre seguir adelante.

La amistad es uno de los regalos más valiosos con los que podemos contar, por eso agradezco a Sarita y Fernando, por su gran ayuda, tiempo y constancia en la elaboración de este proyecto de tesis.

A mi asesor Ing. Carlos Vásquez, que gracias a su ética profesional me ha guiado durante el desarrollo de esta tesis brindándome su tiempo, paciencia y conocimientos, preparándome para un futuro competitivo.

DEDICATORIA

A mi familia quienes por ellos soy lo que soy.

A mis padres por todo el esfuerzo que hicieron para educarme, por el apoyo y comprensión en los momentos difíciles, por las horas de consejos que me enseñaron el cómo afrontar la vida, me han dado todo lo que soy como persona, mis valores, principios, carácter, empeño, perseverancia, y coraje para conseguir mis objetivos y ayudarme con los recursos necesarios para estudiar. A mi hermano por estar siempre presente, y ser mi motivación e inspiración.

Stalin Andrés Hidrobo Mafla

CONTENIDO

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE II
CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE IV
DECLARACIÓN V
CERTIFICACIÓN VI
AGRADECIMIENTO VII
DEDICATORIA VIII
RESUMEN XXIII
ABSTRACT XXIV
PRESENTACIÓN XXV
CAPÍTULO 1 1
1. Antecedentes 1
1.1 Problema 1
1.2 Objetivos 1
1.2.1 Objetivo General 1
1.2.2 Objetivos Específicos 2
1.3 Alcance 2
1.4 Justificación 4
CAPITULO 2 6
2. Marco Teórico 6
2.1 Breve Historia Protocolo TCP/IP 6
2.2 Protocolo TCP/IP 7
2.2.1 Arquitectura de Protocolos TCP/IP 7
2.2.1.1 Capa de Aplicación 7
2.2.1.2 Capa de Transporte o extremo a extremo 7
2.2.1.3 Capa Internet 7
2.2.1.4 Capa de Acceso a la Red 8
2.3 Protocolo de Internet Versión 4 (IPv4) 8
2.3.1 Cabecera IPv4 9
2.3.2 Direccionamiento IPv4 13
2.3.2.1 Esquema de direcciones IPv4 15

2.3.2.2 Subredes IPv4 16
2.3.2.3 CIDR 16
2.3.2.4 Direcciones IPv4 privadas 17
2.4 Problemas con el Protocolo de Internet Versión 4 17
2.5 Historia del Protocolo de Internet Versión 6 19
2.6 Protocolo de Internet Versión 6 20
2.6.1 Introducción 20
2.6.2 Características de IPv6 21
2.6.2.1 Calidad de servicio (QoS) 21
2.6.2.2 Nodos vecinos 21
2.6.2.3 Capacidad de ampliación 22
2.6.3 Cabecera IPv6 22
2.6.3.1 Formato de la cabecera IPv6 22
2.6.3.2 Cabeceras de Extensión IPv6 23
2.6.3.2.1 Cabecera de Opciones Salto a Salto 25
2.6.3.2.2 Cabecera de Enrutamiento 25
2.6.3.2.3 Cabecera de Fragmentación 26
2.6.3.2.4 Cabecera de Opciones de Destino 27
2.6.3.2.5 Cabecera de Autenticación 27
2.6.3.2.6 Cabecera de seguridad del encapsulado de la carga útil 28
2.6.3.2.7 Orden de Cabeceras de Extensión en IPv6 30
2.6.4 Direccionamiento IPv6 31
2.6.4.1 Tipos de direcciones IPv6 31
2.6.4.1.1 Unicast. 31
2.6.4.1.2 Multicast. 34
2.6.4.1.3 Anycast. 35
2.6.4.2 Reglas de Utilización 35
2.6.4.3 Notación de Direcciones 36
2.6.4.3.1 Formato Hexadecimal 36
2.6.4.3.2 Formato Comprimido 37
2.6.4.3.3 Formato Compatible 39
2.6.4.4 Subredes IPv6 40
2.6.4.5 Plan de Direccionamiento 41
2.6.4.5.1 Obtención de un prefijo de sitio 41

2.7 Enrutamiento con IPv6 43
2.7.1 RIPng 43
2.7.2 OSPFv3 44
2.8 ICMPv6 46
2.8.1 Encapsulamiento de Mensajes ICMPv6 47
2.8.2 Tipos de Mensajes ICMPv6 47
2.9 Resolución de Nombres en IPv6 48
2.9.1 Resolución de dirección a nombres 49
2.10 Seguridad en IPv6 51
2.10.1 IPSec 51
2.10.1.1 Servicios de Seguridad 52
2.10.1.2 Autenticación de Encabezado IPSec (AH) 52
2.10.1.3 Carga de Seguridad Encapsulada IPSec (ESP) 52
2.11 IPv6 en el Mundo y Latinoamérica 53
2.12 IPv6 en Ecuador 56
2.12.1 Resumen del estado de la implementación de IPv6 en Ecuador: 56
2.13 Mecanismos de Transición de IPv4 a IPv6 58
2.13.1 Dual Stack o Doble Pila 58
2.13.2 Túneles 59
2.13.2.1 Tipos de Túneles 60
2.13.2.1.1 6to4 60
2.13.2.1.2 6OVER4 60
2.13.2.1.3 Teredo 60
2.13.2.1.4 Tunnel Broker 61
2.13.2.1.5 ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) 62
2.13.3 Mecanismos de Traducción 62
2.13.3.1 NAT-PT 63
2.13.3.2 SIIT 64
2.13.3.3 BIS 64
2.13.3.4 TRT 65
2.14 NAT64 65
2.14.1 Diferencias entre Stateless y Stateful NAT64 66
2.15 DNS64 67
CAPÍTULO 3 69

3. Situación Actual 69
3.1 Contexto de la Institución....69
3.1.1 Prefectura de Imbabura....69
3.1.1.1 Ubicación....69
3.1.1.2 Objetivos Estratégicos 70
3.1.1.3 Misión....70
3.1.1.4 Visión....70
3.1.2 Dirección de Tecnologías de la Información y Comunicaciones (TICs) 70
3.1.2.1 Objetivos....70
3.1.3 Topología Física de la Red....71
3.1.4 Cuarto de Equipos de Comunicación 73
3.1.4.1 Distribución de equipos de la Planta baja y Planta alta 2....73
3.1.4.2 Armario de Servidores....75
3.2 Red Interna de la Prefectura de Imbabura 77
3.2.1 Conexión a la Internet....77
3.2.2 Estructura Física 77
3.2.2.1 Cableado Estructurado....77
3.2.2.2 Backbone de Fibra Óptica 77
3.2.2.3 Equipos de Red....78
3.3 Análisis de Fichas Técnicas....78
3.4 Distribución de Direcciones IPv4 de la Prefectura de Imbabura....78
CAPÍTULO 4....81
4. Metodología de Transición de IPv4 a IPv6 en la Prefectura de Imbabura ...81
4.1 Implementación de la Metodología 81
4.1.1 Etapa de Información....81
4.1.1.1 Encuestas 81
4.1.1.2 Tabulación y Resultados obtenidos 82
4.1.2 Etapa de Elaboración del Plan de Transición 85
4.1.2.1 Manual de Petición de Recursos IPv6 a LACNIC 85
4.1.2.1.1 Para Un Cliente Nuevo 86
4.1.2.1.2 Firma de Contrato de Prestación de Servicios (CPS) 90
4.1.2.1.3 Proceso de Pago....90
4.1.2.1.4 Asignación del Recurso....90
4.1.2.2 Plan de Direccionamiento IPv6 92

4.1.2.3 Plan de Transición de acuerdo a los objetivos de la Prefectura de Imbabura 94
4.1.2.4 Selección del Mecanismo de Transición 95
4.1.2.4.1 Análisis comparativo entre Mecanismos de Transición 95
4.1.2.4.2 Mecanismo de Transición Seleccionado 97
4.1.3 Etapa de Implementación y Configuración de la Metodología 98
4.1.3.1 Configuración Router 881 (CNT) 98
4.1.3.2 Configuraciones en Firewall CISCO ASA5520 98
4.1.3.3 Configuraciones en Switch CISCO 4503 (CORE) 114
4.1.3.4 Configuración en Switch CISCO 2960 120
4.1.3.5 Configuración de Aplicaciones Seleccionadas 124
4.1.3.5.1 Servidor WEB 125
4.1.3.5.2 Servidor DNS 130
CAPÍTULO 5 141
5. Análisis de Factibilidad Técnica 141
5.1 Análisis de Factibilidad Técnica de la transición hacia el Protocolo de Internet Versión 6 141
5.1.1 Recurso Tecnológico 141
5.1.1.1 Hardware Necesario 141
5.1.1.2 Software Necesario 142
5.1.2 Recurso Humano 142
5.1.3 Evaluación Final 143
5.2 Pruebas de funcionamiento 143
5.2.1 DNS64, NAT64 y WEB 143
CONCLUSIONES 145
RECOMENDACIONES 147
GLOSARIO DE TÉRMINOS 148
BIBLIOGRAFÍA 150
ANEXO A. FICHAS TÉCNICAS DE EQUIPOS Y APLICACIONES 155
ANEXO B. FORMATO DE LA ENCUESTA 179
ANEXO C. TABULACIÓN DE ENCUESTAS 183
ANEXO D. INSTALACIÓN DE SOFTWARE 198
ANEXO E. MANUAL DE PROCEDIMIENTOS 241
ANEXO F. APLICACIONES ADICIONALES 246

INDICE DE TABLAS

Tabla 1. División de las Clases IPv4 15
Tabla 2. Intervalo de Clases IPv4 Disponibles 16
Tabla 3. Prefijos CIDR y su equivalente decimal 17
Tabla 4. Direcciones IPv4 privadas 17
Tabla 5. Orden de Cabeceras de Extensión IPv6 30
Tabla 6. Direcciones Asignadas Multicast 34
Tabla 7. Ejemplos de uso de formato hexadecimal con campos sucesivos de cero 37
Tabla 8. Ejemplos de uso de formato hexadecimal con campos con ceros al inicio 38
Tabla 9. Ejemplo de aplicación de ambos métodos de compresión 38
Tabla 10. Direcciones IPv6 y prefijos de red utilizando el valor de red con CIDR 40
Tabla 11. Representación de prefijos IPv4 privados a prefijos IPv6 42
Tabla 12. Cambios y Nuevas Características de RIPng 44
Tabla 13. Cambios y Nuevas Características de OSPFv3 45
Tabla 14. Tipos de mensaje ICMPv6 48
Tabla 15. Cuadro de diferencias Stateless y Stateful en NAT64 66
Tabla 16. Distribución de VLANS 79
Tabla 17. Direccionamiento IPv6 en base a VLANS 92
Tabla 18. Direccionamiento IPv4 e IPv6 94
Tabla 19. Análisis comparativo de los Mecanismos de Transición 96
Tabla 20. Requerimientos de Aplicaciones 142

INDICE DE FIGURAS

Figura 1. Comparación entre TCP/IP y OSI 8
Figura 2. Formato de Cabecera IPv4 9
Figura 3. Formato de direcciones IPv4 14
Figura 4. Dirección IPv4 de formato CIDR 14
Figura 5. Proyección de Fechas de Agotamiento de Direcciones IPv4 a nivel mundial 18
Figura 6. Formato de Cabecera IPv6 22
Figura 7. Arquitectura Cabeceras de Extensión IPv6 24
Figura 8. Formato de Cabecera Salto a Salto 25
Figura 9. Formato de Cabecera de enrutamiento 26
Figura 10. Formato Cabecera de Fragmentación 27
Figura 11. Formato Cabecera opciones de destino 27
Figura 12. Formato Cabecera de Autenticación 28
Figura 13.Encriptación en modo transporte 29
Figura 14. Encriptación en modo túnel 29
Figura 15. Formato Cabecera de seguridad del encapsulado de la carga útil 29
Figura 16. Ejemplo de formato de dirección global Unicast 32
Figura 17. Formato de direcciones de Enlace Local y Sitio Local 33
Figura 18. Formato de una dirección IPv6 compatible con IPv4 34
Figura 19. Partes de una dirección IPv6 36
Figura 20. Formato hexadecimal de dirección IPv6 37
Figura 21. Dirección IPv6 con una dirección IPv4 incrustada 39
Figura 22. Encapsulamiento Mensajes IPv6 47
Figura 23. Estructura del Registro DNS para IPv6 49
Figura 24. Ejemplo de PTR en IPv4 50
Figura 25. Ejemplo de PTR en IPv6 50
Figura 26. Cuadro estadístico de Transición a IPv6 en el mundo 55
Figura 27.Doble Pila o Dual Stack 59
Figura 28.Tunneling IPv6 59
Figura 29. Mecanismos de Traducción 62
Figura 30. NAT64 66
Figura 31. Esquema DNS64 y NAT64 67
Figura 32. Ubicación Prefectura de Imbabura 69

Figura 33. Topología Física de la Red 72
Figura 34. Distribución de Equipos Activos 73
Figura 35. Distribución de equipos Planta baja 74
Figura 36. Distribución de equipos Planta alta 2 75
Figura 37. Armario de Servidores 76
Figura 38. Portal IPv6 de LACNIC 86
Figura 39. Cómo obtener un bloque de direcciones IPv6 86
Figura 40. IPv6 para usuarios finales 87
Figura 41. Opción Formulario 87
Figura 42. Ventana para acceder a la cuenta 88
Figura 43. Ventana para crear Usuario Nuevo 88
Figura 44. Ingreso de datos de la Institución 89
Figura 45. Whois de LACNIC 91
Figura 46. Activación del Firewall 99
Figura 47. Carga de la imagen (IOS) del Firewall 100
Figura 48. Asignación de dirección IP al ASA, Acceso SSH y habilitación de la interfaz http 101
Figura 49. Descarga del ASDM (Interfaz Gráfica del ASA) 102
Figura 50. Launcher ASDM 102
Figura 51. Edición de Interfaces 103
Figura 52. Elección de la Interfaz a editarse 103
Figura 53. Configuración OUTSIDE IPv4 104
Figura 54. Configuración OUTSIDE IPv6 104
Figura 55. Configuración INSIDE IPv4 105
Figura 56. Configuración INSIDE IPv6 105
Figura 57. Interfaces definidas IPv4 e IPv6 106
Figura 58. Guardado de los cambios efectuados 106
Figura 59. Tráfico OUTSIDE IPv4 107
Figura 60. Tráfico INSIDE IPv4 107
Figura 61. Enrutamiento de cada VLAN IPv4 108
Figura 62. Enrutamiento de todas las VLANS IPv4 108
Figura 63. Tráfico en la red INSIDE IPv6 109
Figura 64. Tráfico en la red OUTSIDE IPv6 109
Figura 65. Enrutamiento de cada VLAN IPv6 110

Figura 66. Enrutamiento de todas las VLANS IPv6 110
Figura 67. Reglas de acceso para permitir el tráfico a la red INSIDE IPv4 111
Figura 68. Reglas para denegar el tráfico en el resto de redes IPv4 111
Figura 69. Reglas de acceso para permitir tráfico en la red INSIDE IPv6 112
Figura 70. Reglas para denegar el tráfico en el resto de redes IPv6 112
Figura 71. Reglas de acceso para permitir tráfico en la red OUTSIDE IPv4 113
Figura 72. Reglas para denegar tráfico en la red OUTSIDE IPv4 113
Figura 73. Reglas para denegar tráfico en la red OUTSIDE IPv6 114
Figura 74. Topología de la Red 114
Figura 75. Interfaz de VLAN en modo acceso 115
Figura 76. Creación de VLAN´s 116
Figura 77. Habilitación de vtp server 117
Figura 78. Estado de VLAN's 117
Figura 79. Puerto modo troncal 118
Figura 80.Habilitación de doble pila 119
Figura 81. Habilitación de IPv6 en los Switchs 119
Figura 82. Configuración Switch en modo trunk 121
Figura 83. Comando para verificar la ropagación de VLAN's 121
Figura 84. Habilitación del Switch en modo acceso 122
Figura 85. Habilitación de reenvio de paquetes en los Switchs 122
Figura 86. Direcciones IP para administrar el Switch 1 123
Figura 87. Direcciones IP para administrar el Switch 4 124
Figura 88. Pruebas de conectividad entre Switchs con los protocolos IPv4 e IPv6 124
Figura 89. Instalación de Web server 125
Figura 90. Comando para configuración de interfaces 126
Figura 91. Agregar los parámetros en IPv4 e IPv6 126
Figura 92. Comando para ingresar al fichero de red 127
Figura 93. Archivo Network 127
Figura 94. Reinicio de servicios 128
Figura 95. Direccionamiento de escucha por el puerto 80 128
Figura 96. Archivo del puerto 80 129
Figura 97. Reinicio del servicio http 129
Figura 98. Prueba de funcionamiento del servidor Web 130
Figura 99. Instalación de bind 130

Figura 100. Comando de Configuración de Interfaces 131
Figura 101.Configuración de Interfaces 131
Figura 102. Archivo de configuración named.conf 132
Figura 103. Reinicio de bind 133
Figura 104. Definición de zona primaria 133
Figura 105. Definición de zonas inversas IPv6 e IPv4 134
Figura 106. Archivo de zona directa 134
Figura 107. Archivo de zona inversa IPv4 135
Figura 108. Archivo de zona inversa IPv6 135
Figura 109. Diagnóstico de cada zona 136
Figura 110. Resolución de nombres AAAA 136
Figura 111. Resolución de zonas inversas 137
Figura 112. Página para descargar tayga 137
Figura 113.Instalación del paquete tayga 138
Figura 114. Comandos para crear la interfaz NAT64 y permisos de tráfico 139
Figura 115. Fichero tayga.conf 139
Figura 116. Ping en IPv6 140
Figura 129. Prueba de conectividad desde un usuario IPv4 144
Figura 130. Prueba de conectividad desde un usuario IPv6 144

ANEXO D

Figura D1 1. Página Oficial GNS3 198
Figura D1 2. Selección del S.O. 198
Figura D1 3. Descarga del Programa 199
Figura D1 4. Ubicación del archivo 199
Figura D1 5. GNS3 Setup 199
Figura D1 6. Aceptación de condiciones 200
Figura D1 7. Herramientas adicionales 200
Figura D1 8. Carpeta de destino 201
Figura D1 9. Progreso de Instalación 201
Figura D1 10. Icono GNS3 202
Figura D1 11. Proyecto Nuevo 202
Figura D1 12. Preferencias 203

Figura D1 13. Plantillas IOS router 203
Figura D1 14. Buscar el IOS 204
Figura D1 15. Selección del IOS 204
Figura D1 16. Imagen del IOS 205
Figura D1 17. Descripción del nombre 205
Figura D1 18. Selección de Memoria RAM 206
Figura D1 19. Elección de interfaces 206
Figura D1 20. Elección de WIC 207
Figura D1 21. Plantillas IOS router con el equipo nuevo agregado 207
Figura D1 22. Elección del equipo para trabajar 208

Figura D2 1. Primer paso para crear la máquina virtual 209
Figura D2 2. Elección de instalación personalizada 209
Figura D2 3. Versión de Workstation 210
Figura D2 4. Instalación manual 210
Figura D2 5. Elección de S.O. y Versión 211
Figura D2 6. Nombre y lugar de instalación del S.O. 211
Figura D2 7. Número de procesadores a utilizar 212
Figura D2 8. Memoria RAM a utilizar 212
Figura D2 9. Selección del tipo de red 213
Figura D2 10.Tipo de Kernel 213
Figura D2 11. Tipo de periférico que utiliza el disco duro 214
Figura D2 12. Creación de nuevo disco duro viertual 214
Figura D2 13. Capacidad del disco duro 215
Figura D2 14. Archivo de Inicio 215
Figura D2 15. Registro de lo escogido 216
Figura D2 16. Muestra de la máquina virtual creada 216
Figura D2 17. Carga del Archivo de imagen ISO 217
Figura D2 18. Pantalla Inicial de CentOS 217
Figura D2 19. Opción Disco encontrado 218
Figura D2 20. Inicio de Instalación de CentOS 218
Figura D2 21. Elección del Idioma del S.O. 219
Figura D2 22. Elección del Idioma del teclado 219
Figura D2 23. Almacenamiento básico 220

Figura D2 24. Opciones para el dispositivo de almacenamiento 220
Figura D2 25. Nombre del Host 221
Figura D2 26. Zona Horaria 221
Figura D2 27. Contraseña de root 222
Figura D2 28. Tipo de Instalación 222
Figura D2 29. Opci+on para escribir cambios al disco 223
Figura D2 30. Instalación predeterminada 223
Figura D2 31. Inicio de instalación 224
Figura D2 32. Paquetes de Instalación 224
Figura D2 33. Fin de instalación 225
Figura D2 34. Bienvenida a CentOS 225
Figura D2 35. Acuerdo de Licencia 226
Figura D2 36. Usuario para inicio de sesión 226
Figura D2 37. Fecha y Hora del Sistema 227
Figura D2 38. Inicio de Sesión 227

Figura D3 1. Inicio de ELASTIX 228
Figura D3 2. Elección de idioma 228
Figura D3 3. Idioma de teclado 229
Figura D3 4. Inicializar datos de instalación 229
Figura D3 5. Particionamiento para el servidor 230
Figura D3 6. Visualización de particiones 230
Figura D3 7. Configurar interfaz de red 231
Figura D3 8. Configuración de red para eth0 231
Figura D3 9. Configuración IPv4 para eth0 232
Figura D3 10. Configuración IPv6 para eth0 232
Figura D3 11. Configuración del nombre del host 233
Figura D3 12. Selección del uso horario 233
Figura D3 13. Contraseña de root 234
Figura D3 14. Instalación de paquetes 234
Figura D3 15. Inicio de servicio en modo consola 234
Figura D3 16. Contraseña de MySQL 235
Figura D3 17. Confirmación de contraseña de MySQL 235
Figura D3 18. Contraseña de admin 236

Figura D3 19. Confirmación de contraseña de admin 236
Figura D3 20. Consola del servidor en modo root 237
Figura D3 21. Herramienta de configuración de red 237
Figura D3 22. Selección de acción 238
Figura D3 23. Selección de dispositivo 238
Figura D3 24. Asignación de dirección IP del servidor 239
Figura D3 25. Guardar cambios 239
Figura D3 26. Reinicio de interfaces 240
Figura D3 27. Verificación de IP en la interfaz eth0 240

ANEXO F

Figura F1 1. Instalación de PostFix 246
Figura F1 2. Comando para configurar archivo de PostFix 247
Figura F1 3. Archivo de Configuración de PostFix 247
Figura F1 4. Inicio de Servicio PostFix al iniciar el Sistema Operativo 248
Figura F1 5. Reinicio del Servicio PostFix 249
Figura F1 6. Creación de carpeta Maildir 250
Figura F1 7. Creación de archivo para lectura de correos 250
Figura F1 8. Configuración de archivo para recibir correos 251
Figura F1 9. Creación de Usuario para prueba 251
Figura F1 10. Comando para instalar Telnet 252
Figura F1 11. Comando para instalación de Telnet 252
Figura F1 12. Ingreso al archivo de configuración de Telnet 253
Figura F1 13. Archivo de configuración de Telnet 253
Figura F1 14. Menú Sistema 254
Figura F1 15. Añadir el Puerto para Telnet 254
Figura F1 16. Puerto 23 de Telnet 255
Figura F1 17. Puerto Telnet añadido 255
Figura F1 18. Telnet al protocolo SMTP 256
Figura F1 19. Comprobación de Correo enviado 257
Figura F1 20. Pantalla de Inicio de Outlook 258
Figura F1 21. Configuración de Outlook 258

Figura F1 22. Opción configuración manual 259
Figura F1 23. Elección del Tipo de Servicio a configurar 259
Figura F1 24. Configuración de cuenta.....260
Figura F1 25. Prueba de conexión con Postfix 260
Figura F1 26. Finalización de configuración de correo 261

Figura F2 1. Instalación paquete FTP 262
Figura F2 2. Ingreso al archivo de Configuración FTP 262
Figura F2 3. Archivo de Configuración FTP 263

RESUMEN

El crecimiento de la Internet ocasiona que la cantidad de direcciones IP del protocolo IPv4, llegue a su límite o a una situación de una posible escasez. Por esta razón se impulsa a las Instituciones Públicas de nuestro país para que adopten el protocolo IPv6, ya que existe el acuerdo ministerial 007-2012, titulado "Medidas Sobre IPv6", para implementar políticas públicas e incorporar el nuevo protocolo, además de la coexistencia con el anterior sistema.

El proyecto que se presenta a continuación consiste en el desarrollo de una metodología que permita la transición del Protocolo de internet versión 4 a versión 6 para la Prefectura de Imbabura, para lo cual, inicialmente se realizó una investigación de los dos protocolos para compararlos, analizar sus ventajas y desventajas, con la finalidad de establecer una base para la futura implementación de una red integrada al protocolo IPv6.

Para cumplir con este objetivo se realizó un análisis comparativo entre los mecanismos existentes para ejecutar la transición de IPv4 a IPv6. Luego del análisis de la infraestructura de red de la Prefectura de Imbabura se logró identificar el método más idóneo en cuanto a robustez y adaptabilidad para establecer una comunicación entre los equipos y aplicaciones de la red.

Finalmente, luego de haber obtenido todos los datos previos, se inicia la configuración de equipos mediante una simulación de la red de la institución, además de dos aplicaciones para demostrar la funcionalidad de la coexistencia entre los protocolos IPv4 e IPv6 en la red de la Prefectura de Imbabura.

ABSTRACT

The rise in usage of the Internet has caused the numbers of IP addresses in IPv4 protocol to come close to its end and for this reason all Public Institutions in our country are adopting the IPv6 protocol. In Ecuador, there is the 007-2012 ministerial agreement, which is called “Measures about IPv6”, to implement public policies and incorporate the new protocol, keeping in mind the coexistence with the previous system.

The project consists of developing a methodology which allows the transition from IPv4 protocol to IPv6 protocol for the Imbabura Prefecture Network. Firstly, an investigation between the two protocols, IPv4 and IPv6, has been realized to compare them with each other and analyze their advantages and disadvantages, establishing a base to the future implementation of an integrated network.

To carry out this goal, a comparative analysis between the three transition mechanisms from IPv4 to IPv6 has been realized. After an analysis of the Imbabura Prefecture’s Network Infrastructure, the most suitable transition mechanism in sturdiness and adaptability was identified, to establish communication between network devices and network applications.

Finally, after obtaining the previous information, an equipment’s configuration has been started through a simulation of institution’s network and also two applications have been installed to show the coexistence between IPv4 and IPv6 protocols in the Imbabura Prefecture network.

PRESENTACIÓN

El proyecto de titulación “METODOLOGÍA DE TRANSICIÓN DEL PROTOCOLO DE INTERNET VERSIÓN 4 A VERSIÓN 6 EN EL GOBIERNO PROVINCIAL DE IMBABURA”, permitió establecer una base para la futura implementación de una red integrada a este protocolo en la institución. Se encuentra compuesto por los capítulos descritos a continuación.

Capítulo 1, en el cuál se presenta el modelo del anteproyecto aprobado.

Capítulo 2, donde se realizó un análisis del protocolo de internet 4 y 6 para realizar una comparación técnica de sus respectivos beneficios.

Capítulo 3, en el cual se analizó la Infraestructura de Red del Gobierno Provincial de Imbabura, luego se realizó las fichas técnicas de cada uno de los equipos, servicios y aplicaciones que conforman esta red, con lo cual se obtuvo un inventario de la información recolectada.

Capítulo 4, donde se ejecutó el análisis comparativo de los diferentes métodos para la transición de este protocolo, y se define cuál de ellos se deberá utilizar para garantizar la fluidez de la misma entre los dos protocolos. Además, se elaboró el manual de procedimientos para la transición.

Capítulo 5, en este capítulo se desarrolló el análisis de factibilidad de la transición hacia el Protocolo de Internet Versión 6 en el Gobierno Provincial de Imbabura, para la posterior implementación de la tecnología y la implementación de tres aplicaciones que soporten el protocolo.

CAPÍTULO 1

1. Antecedentes

En este capítulo se presenta el modelo de anteproyecto aprobado, el cual contiene la propuesta realizada para la implementación del plan de titulación.

1.1Problema

Con el transcurso de los años Internet ha tenido un gran crecimiento debido al avance de la tecnología, el desarrollo de las telecomunicaciones esto ha ocasionado una escasez de direcciones IPv4; razón por la cual se ha desarrollado el protocolo IPv6 para solventar este problema.

El Gobierno Provincial de Imbabura cuenta con una red basada en el Protocolo de Internet versión 4 pero debido al incremento del uso de nuevos portales para la adjudicación de contratos, administración y fiscalización de obras; además de la ampliación de su estructura física, ha visto necesario tener direcciones únicas para sus usuarios.

Al no tener una infraestructura común para estos protocolos la Institución está disminuyendo el abanico de prestaciones que podría brindar una transición de los protocolos IPv4 e IPv6, y de esta manera estaría atrasada en cuanto a las políticas del Gobierno Nacional para la implementación del Protocolo de Internet Versión 6 en las Instituciones públicas de nuestro país.

1.2 Objetivos

1.2.1 Objetivo General

Desarrollar una metodología que permita la transición de IPv4 a IPv6 en el Gobierno Provincial de Imbabura, mediante la utilización de diferentes mecanismos, con la finalidad de establecer una base para la implementación de una red integrada a este protocolo.

1.2.2 Objetivos Específicos

- Analizar los protocolos de Internet versión 4 y versión 6, para realizar una comparación técnica de los mismos.

- Describir la situación actual de la red del Gobierno Provincial de Imbabura, con la finalidad de tener una visualización clara de su estructura.

- Determinar la compatibilidad de los equipos, servicios y aplicaciones utilizados en el Gobierno Provincial de Imbabura, mediante la realización de fichas técnicas de cada uno de ellos

- Desarrollar el análisis comparativo de los mecanismos de transición entre las versiones de los protocolos mencionados.

- Elaborar un manual de procedimientos para la transición hacia el protocolo de internet versión 6.

- Indicar la factibilidad de una futura implementación de IPv6 en el Gobierno Provincial de Imbabura en base a este proyecto.

1.3 Alcance

Este proyecto está enfocado en el estudio del Protocolo de Internet versión 6 para el Gobierno Provincial de Imbabura, de tal manera que este pueda tener una metodología de transición con el protocolo de internet versión 4 utilizado actualmente en la Institución.

Como parte inicial en la elaboración del proyecto, se procederá a realizar una comparación entre los protocolos de internet en su versión 4 y versión 6, esto servirá como un informe detallado de los requerimientos técnicos y parámetros para la utilización de estas tecnologías, así como permitirá identificar las ventajas y desventajas que brindará la transición de este protocolo, en su posterior implementación.

Se procederá a definir la situación actual del entorno de la red del Gobierno Provincial de Imbabura para analizar la metodología de implementación del Protocolo de Internet versión 6. Mediante el desarrollo de fichas técnicas se identificará los equipos, servicios y aplicaciones compatibles con IPv6, así se podrá realizar un inventario de cada uno de los dispositivos de la red de la Institución.

Para la transición del Protocolo de Internet Versión 4 hacia Versión 6 existen diferentes métodos, los cuales se dividen en 3 grupos: método de doble pila que permite un soporte para los dos protocolos tanto en los hosts como en los routers, método de túneles, están basados en la encapsulación de paquetes IPv6 dentro de paquetes IPv4 para proporcionar un mecanismo para usar la infraestructura de la red IPv4 durante el tiempo que se implemente la red IPv6 y por último los métodos de traducción cuya solución se basa en asignar de manera temporal direcciones IPv4 a nodos IPv6, para que de esta manera todos los nodos logren acceder tanto a la red de IPv6 como a la de IPv4. Se escogerá uno de estos mecanismos de transición mediante un análisis comparativo de sus ventajas y desventajas al momento de una futura implementación. Además se planteará la utilización de NAT64 el cual permite que los hosts que solo tienen conectividad IPv4 puedan comunicarse con los hosts que solamente tienen conectividad IPv6 y DNS64 que realiza el mapeo de los nombres de dominio de direcciones IPv6, de esta manera si el host necesita un DNS y recibe como respuesta una dirección de 32 bits utilizará IPv4, y si recibe una de 128 bits utilizará IPv6.

Para el desarrollo de la metodología se empleará un manual de procedimientos que constará de las siguientes etapas: Realización de cuestionarios y entrevistas al personal del Departamento de Informática de la Institución para determinar los conocimientos y expectativas que poseen sobre esta nueva tecnología, además servirá para informar de forma breve el funcionamiento del protocolo y sus beneficios. Definición de un plan que vaya de acuerdo a la visión y objetivos del Gobierno Provincial de Imbabura. Estudio de la Intranet del Gobierno Provincial de Imbabura, para esto se tomará en cuenta: el número de PC’s que ocuparán IPv6 así como la cantidad de PC’s que usarán IPv4. Análisis del software que soporte la utilización del protocolo IPv6, el cual deberá ser empleado tanto en los clientes como en los servidores. Elaboración del plan de direccionamiento según

las políticas para la distribución y asignación de direcciones IPv6 que propone LACNIC. Elección del mecanismo de comunicación entre el protocolo IPv4 e IPv6.

Se realizará un análisis de factibilidad del proceso de transición, esto permitirá determinar el beneficio de la implementación a futuro de esta tecnología, además se implementará dos aplicaciones para demostrar la funcionalidad del protocolo en el Gobierno Provincial de Imbabura.

Para terminar el proyecto de titulación, se dará a conocer las conclusiones y recomendaciones obtenidas en el transcurso de la investigación y realización del trabajo.

1.4 Justificación

El crecimiento indetenible del Internet ocasiona que la cantidad de direcciones IP del protocolo IPv4, llegue a su límite o a una situación de una posible escasez. Por esta razón el Ministerio de Telecomunicaciones y de la Sociedad de Información MINTEL se encuentra impulsando la adopción del protocolo IPv6 en instituciones públicas de nuestro país, mediante el acuerdo ministerial 007-2012, titulado "Medidas Sobre IPv6", para implementar políticas públicas e incorporar el nuevo protocolo, además de la coexistencia con el anterior sistema.

El Gobierno Provincial de Imbabura al ser una entidad del Sector Público tiene un plazo de un año a partir de Junio de 2012, para comenzar con la implementación, de manera obligatoria, del protocolo IPv6 en sus sitios Web y plataformas de servicio.

Un diseño de una estructura de red que permita la transición de IPv4 hacia IPv6 en el Gobierno Provincial de Imbabura dará la solución del problema de agotamiento de direcciones, una mayor seguridad en la red y sus comunicaciones extremo a extremo.

La realización de este proyecto será una oportunidad para iniciar un análisis de la factibilidad de la implementación del protocolo IPv6 y la compatibilidad de los equipos existentes en la institución, además sentará las bases para la implementación de un modelo de red que utilice el Protocolo de Internet Versión 6.

En este capítulo se realiza un análisis del Protocolo de Internet en sus versiones 4 y 6 para realizar una comparación técnica de sus respectivos beneficios.

CAPITULO 2

2. Marco Teórico

En este capítulo se realiza un análisis del Protocolo de Internet en sus versiones 4 y 6 para realizar una comparación técnica de sus respectivos beneficios.

2.1 Breve Historia Protocolo TCP/IP

A inicios de los años 60, varios investigadores intentaban encontrar una forma de compartir recursos informáticos de una manera más eficiente. En 1961, Leonard Klienrock implementó la idea de que la comunicación entre ordenadores estuviese dividida en paquetes, cada paquete habría de contener la dirección de destino y lograría encontrar su camino a través de la red.

En 1969 la Agencia de Proyectos de Investigación Avanzada (Defense Advanced Research Projects Agency o DARPA) del Ejército de los EEUU desarrolló la ARPANET, cuya finalidad era resistir un ataque nuclear de la URSS, para lo que se pensó en una administración descentralizada. Así, si algunos ordenadores eran destruidos, la red seguiría funcionando. A pesar de que la red funcionaba bien, sufría de caídas habituales en el sistema. Esto desencadenó a que la expansión a largo plazo de esta red resultaría difícil y costosa. Por lo que se inició una búsqueda de un conjunto de protocolos más fiables, la cual finalizó, a mediados de los 70, con el desarrollo de TCP/IP.

En 1983, TCP/IP se integró en la versión 4.2 del sistema operativo UNIX de Berkeley y la integración en versiones comerciales de UNIX vino pronto. Así TCP/IP se convirtió en el estándar de Internet.

En la actualidad, TCP/IP es usado para varios propósitos. Por ejemplo, a menudo se diseñan *intranets* usando TCP/IP. En estos medios, TCP/IP brinda ventajas sobre otros protocolos. Una de sus ventajas es que trabaja sobre una gran variedad de hardware y sistemas operativos. (Ureña Poirier & Rodríguez Martín, 2010)

2.2 Protocolo TCP/IP

TCP / IP es un conjunto de reglas que define cómo dos equipos se dirigen y envían datos entre sí. Este conjunto de reglas se llama un protocolo. Múltiples protocolos que se agrupan juntos forman un conjunto de protocolos y trabajan juntos como una pila de protocolos.

TCP / IP es un conjunto fuerte, rápido y eficiente de protocolos. Esta pila de protocolos es el protocolo de facto de Internet. Como el intercambio de información a través de Internet se hace más generalizado, más individuos y empresas tendrán que entender TCP / IP.

2.2.1 Arquitectura de Protocolos TCP/IP

La Arquitectura TCP/IP, es un conjunto de protocolos, estos a su vez se dividen en cuatro capas, las cuales se describen a continuación:

2.2.1.1 Capa de Aplicación

Es aquella que permite la comunicación entre procesos de ordenadores separados.

2.2.1.2 Capa de Transporte o extremo a extremo

Brinda los datos de enrutamiento y ofrece mecanismos para conocer el estado de la transmisión.

2.2.1.3 Capa Internet

Permite seleccionar la mejor ruta y realizar la conmutación de paquetes. El protocolo más significativo de esta capa es el IP. Este protocolo proporciona los servicios básicos de transmisión de paquetes.

2.2.1.4 Capa de Acceso a la Red

Esta capa utiliza todos los aspectos que un paquete necesita para realizar un enlace físico real con los medios de la red. (Stallings, 2011)

En la Figura 1 se compara los modelos OSI y el modelo no oficial de los protocolos TCP/IP y se muestra como este abarca varias capas del modelo OSI.

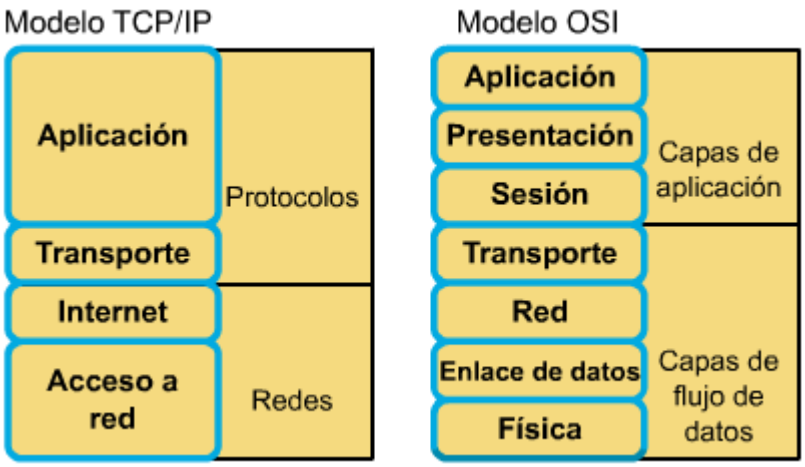


Figura 1. Comparación entre TCP/IP y OSI

Fuente: Recuperado de http://txdatos.files.wordpress.com/2011/02/13.png

2.3 Protocolo de Internet Versión 4 (IPv4)

IPv4 es el protocolo de nivel de red usado en Internet. Junto con otros protocolos auxiliares es responsable de transferir la información del usuario por la red. Este protocolo está definido en el RFC 791. (Alvarez, 2009)

IPv4 es un protocolo no orientado a conexión, no confiable. Entre sus funciones principales se pude mencionar:

- Establecer direccionamiento lógico de una red, para que los equipos puedan establecer el proceso de comunicación entre ellos.
- Entrega de datagramas a través de la red en la modalidad de mejor esfuerzo.
- Encapsulado y desencapsulado de datagramas.

IPv4 es un protocolo de “mejor esfuerzo” ya que no garantiza que un paquete que sea enviado realmente llegue a su destino, ni que los datagramas sean recibidos en el mismo orden en el cual fueron enviados.

2.3.1 Cabecera IPv4

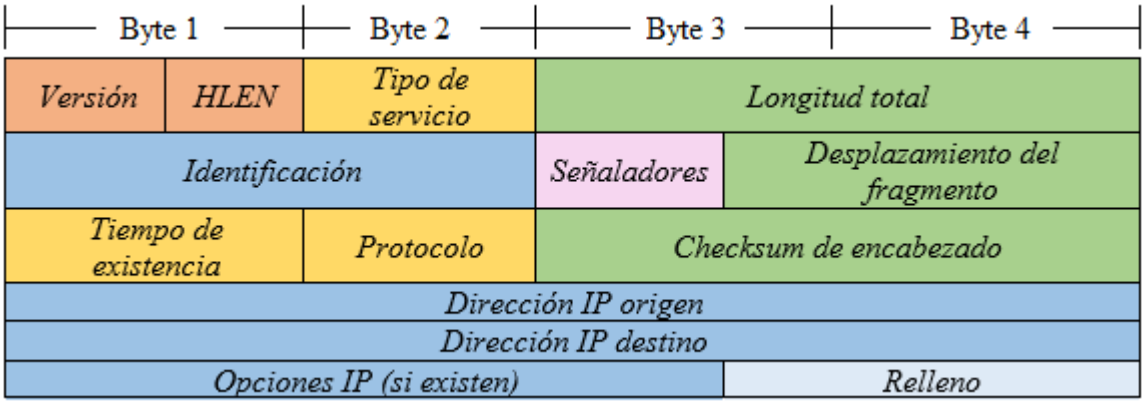


Figura 2. Formato de Cabecera IPv4

Fuente: Recuperado de http://tools.ietf.org/html/rfc791#page-11

La estructura de la cabecera IPv4 se muestra en la Figura 2, a continuación, se describe cada uno de sus campos.

Versión: 4 bits.

El campo versión indica el formato de la cabecera internet.

HLEN: 4 bits

El campo HLEN indica la longitud de la cabecera internet, en palabras de 32 bits sin incluir el campo de datos.

Tipo de Servicio: 8 bits

Indica los parámetros de calidad de servicio solicitada por el datagrama IP, los cuales son utilizados como una guía cuando se transmite un datagrama a través de una red en particular.

Varias redes ofrecen prioridad de servicio, generalmente aceptando solo el tráfico por encima de una cierta prioridad en el momento de sobrecarga.

Longitud Total: 16 bits

Contiene la longitud total del datagrama medida en octetos, incluyendo la cabecera internet y datos. El tamaño mínimo de los datagramas usados normalmente es de 576 octetos. Es recomendable que un host solamente envíe datagramas mayores a 576 octetos si tiene la seguridad que el host de destino se encuentre preparado para aceptar este tipo de datagramas más largos.

En caso de fragmentación este campo contendrá el tamaño del fragmento, no el del datagrama original.

Identificación: 16 bits

Es un valor único asignado al datagrama por el emisor que permite identificar a que datagrama pertenece el fragmento.

Señaladores: 3 bits

Especifican valores relativos a la fragmentación de paquetes. Contiene los valores (0, DF, MF)

- 0 – Reservado no se utiliza.
- DF – Dont_Fragment, si es 0 indica que se permite la fragmentación, si es 1 indica que no se permite.
- MF – More_Fragments, si es 0 indica que es el último fragmento del datagrama, si es 1 indica que hay más fragmentos.

Desplazamiento del Fragmento: 13 bits

Indica el desplazamiento medido en unidades de 8 bytes (64 bits). Se utiliza para facilitar el re ensamblaje del datagrama completo. Si es el primer o único fragmento el valor es 0.

Tiempo de Existencia: 8 bits

Indica el tiempo en segundos que un datagrama puede permanecer en la red. Si este campo contiene el valor 0, entonces el datagrama debe ser destruido, cada vez que algún nodo procesa este paquete disminuye su valor en 1 como mínimo.

Protocolo: 8 bits

Este campo indica el protocolo de alto nivel al que debe entregarse un paquete. Entre algunos de los valores que puede tomar este campo tenemos:

- 1: ICMP (Internet Control Message Protocol)
- 2: IGMP (Internet Group Management Protocol)
- 3: GGP (Gateway-to-Gateway)
- 4: IP (IP in IP (encapsulation)
- 5: ST (Stream)
- 6: TCP (Transmission Control Protocol)
- 7: CBT (Core Based Trees)
- 8: EGP (Exterior Gateway Protocol)
- 9: IGP (Interior Gateway Protocol)
- 10: BBN-RCC-MON (BBN RCC Monitoring)
- 17: UDP (User Datagram Protocol)
- 18: MUX (Multiplexing Protocol)
- 27: RDP (Reliable Data Protocol)
- 28: IRTP (Internet Reliable Transaction Protocol)
- 45: IDRP (Inter-Domain Routing Protocol)
- 46: RSVP (Reservation Protocol)

- 47: GRE (Generic Routing Encapsulation)
- 48: MHRP (Mobile Host Routing Protocol)
- 50: ESP (Encapsulating Security Payload)
- 51: AH (Authentication Header)
- 54: NARP (NBMA Address Resolution Protocol)
- 55: MOBILE (IP Mobility)
- 88: EIGRP (Enhanced Interior Gateway Routing Protocol)
- 89: OSPF (Open Shortest Path First)
- 94: IPIP (IP-within-IP Encapsulation Protocol)
- 95: MICP (Mobile Internetworking Control Protocol)
- 97: ETHERIP (Ethernet-within-IP Encapsulation)
- 98: ENCAP (Encapsulation Header)
- 103: PIM (Protocol Independent Multicast)
- 112: VRRP (Virtual Router Redundancy Protocol)
- 113: PGM (PGM Reliable Transport Protocol)
- 115: L2TP (Layer Two Tunneling Protocol)
- 118: STP (Schedule Transfer Protocol)
- 121: SMP (Simple Message Protocol)
- 131: PIPE (Private IP Encapsulation within IP)
- 132: SCTP (Stream Control Transmission Protocol)
- 133: FC (Fiber Channel)
- 137: MPLS-in-IP (Multiprotocol Label Switching in IP)
- 139: HIP (Host Identity Protocol)

Checksum de Encabezado: 16 bits

Este campo permite el control de la información incluida en la cabecera. Si el checksum de la cabecera no concuerda se descarta el datagrama. Se recalcula cada vez que cierto nodo cambia alguno de sus campos.

Dirección IP origen: 32 bits

Es la dirección IP del host que envía el datagrama.

Dirección IP destino: 32 bits

Es la dirección IP del host destino del datagrama.

Opciones IP: Variable

La utilización de este campo no es obligatoria. Las opciones pueden aparecer o no en los datagramas, pero cualquier nodo debe ser capaz de interpretarlas.

Relleno: Variable

Este campo es utilizado para asegurar que el tamaño de la cabecera IP sea un múltiplo de 32. El relleno es cero. (Defense Advanced Research Projects Agency, 1981)

2.3.2 Direccionamiento IPv4

Las redes IPv4 deben contar con:

- Un número de red exclusivo asignado por un ISP o, para las redes más antiguas, registrado por la IANA. Si se tiene previsto utilizar direcciones privadas, los números de red creados deben ser exclusivos para su organización.

- Direcciones IPv4 exclusivas para las interfaces de cada sistema en la red.

- Una máscara de red.

La dirección IPv4 es un número de 32 bits que identifica de forma exclusiva una interfaz de red en un sistema. Una dirección IPv4 se escribe en dígitos decimales, y se divide en cuatro campos de 8 bits separados por puntos. Cada campo de 8 bits representa un byte de la dirección IPv4. Este modo de representar los bytes de una dirección IPv4 se denomina normalmente formato de decimales con puntos.

La Figura 3, muestra los componentes de una dirección IPv4, 172.16.90.6

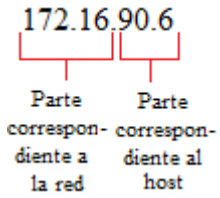


Figura 3. Formato de direcciones IPv4

Fuente: Recuperado de http://docs.oracle.com/cd/E19957-01/820-2981/ipplan-5/index.html

- ***172.16:*** Número de red IPv4 registrada. En la notación IPv4 basada en clases, este número también define la clase de red IP (la clase B en este ejemplo), que registra la IANA.

- ***90.6:*** Parte del host de la dirección IPv4. La parte del host identifica de forma exclusiva una interfaz en un sistema de una red. Para cada interfaz de una red local, la parte de la red de la dirección es la misma, pero la parte del host debe ser diferente.

Para crear una subred de una red IPv4 basada en clases, se debe definir una máscara de subred o máscara de red. La Figura 4 muestra la dirección de formato CIDR 192.168.10.1/24

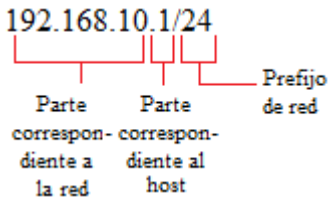


Figura 4. Dirección IPv4 de formato CIDR

Fuente: Recuperado de http://docs.oracle.com/cd/E19957-01/820-2981/ipplan-5/index.html

- ***192.168.10:*** Parte de la red, que se compone del número de red IPv4 que se recibe de un ISP.

- ***1:*** Parte del host, que se asigna a una interfaz de un sistema.

- ***/24:*** Prefijo de la red, que define cuántos bits de la dirección componen el número de red. El prefijo de la red también proporciona la máscara de subred para la dirección IP. Los prefijos de red también los asigna el ISP. (Oracle, 2010)

2.3.2.1 Esquema de direcciones IPv4

Esta sección describe las clases en las que se organizan las direcciones IPv4 estándar. Aunque la IANA ya no proporciona números de red basados en clases, estos números siguen utilizándose en muchas redes. Es posible que sea necesario administrar el espacio de dirección de un sitio con números de red basados en clases.

La Tabla 1 muestra la división de la dirección IPv4 estándar en espacios de direcciones de red y de host. Para cada clase, el rango especifica el intervalo de valores decimales del primer byte del número de red. La dirección de red indica el número de bytes de la dirección IPv4 que se dedican a la parte de red de la dirección. Cada byte se representa con *xxx*. La dirección de host indica el número de bytes que se dedican a la parte del host de la dirección. Por ejemplo, en una dirección de red de clase A, el primer byte está dedicado a la red y los tres últimos bytes al host.

Tabla 1. División de las Clases IPv4

Clase	Intervalo de bytes	Número de red	Dirección de host
A	0–127	xxx	xxx.xxx.xxx
B	128–191	xxx.xxx	xxx.xxx
C	192–223	xxx.xxx.xxx	xxx

Fuente: Recuperado de http://docs.oracle.com/cd/E19957-01/820-2981/ipplan-5/index.html

Los números del primer byte de la dirección IPv4 definen si la red es de clase A, B o C. Los tres bytes restantes comprenden el intervalo 0–255. Los números 0 y 255 están reservados. Se puede asignar los números del 1 al 254 a cada byte, dependiendo de la Clase que la IANA haya asignado a la red.

La Tabla 2 muestra qué bytes de la dirección IPv4 tiene asignados. La tabla también muestra el intervalo de números de cada byte que tiene a su disposición para asignarlos a los hosts. (Oracle, 2010)

Tabla 2. Intervalo de Clases IPv4 Disponibles

Clase de Red	Intervalo de bytes 1	Intervalo de bytes 2	Intervalo de bytes 3	Intervalo de bytes 4
A	0–127	1–254	1–254	1–254
B	128–191	Preasignado por la IANA	1–254	1–254
C	192–223	Preasignado por la IANA	Preasignado por la IANA	1–254

Fuente: Recuperado de http://docs.oracle.com/cd/E19957-01/820-2981/ipplan-5/index.html

2.3.2.2 Subredes IPv4

Las redes locales con varios hosts a veces se dividen en subredes. Si se divide el número de red IPv4 en subredes, se debe asignar un identificador de red a cada subred. Se puede alcanzar mayor eficacia del espacio de dirección IPv4 usando algunos de los bits de la parte de host de la dirección IPv4 como identificador de red. Cuando se utiliza como identificador de red, la parte especificada de la dirección pasa a ser el número de subred. Un número de subred se crea usando una máscara de red, que es una máscara de bits que selecciona las partes de red y subred de una dirección IPv4.

2.3.2.3 CIDR

Las clases de red que constituían IPv4 ya no se utilizan en Internet. En la actualidad, la IANA distribuye direcciones CIDR sin clase a sus registros de todo el mundo. Cualquier dirección IPv4 que se adquiera de un ISP tendrá el formato CIDR, como se muestra en la Figura 4.

El prefijo de red de la dirección CIDR indica la cantidad de direcciones IPv4 que se encuentran disponibles para los hosts de una red como se muestra en la Tabla 3. Estas direcciones se asignan a las interfaces de un host. Si un host tiene más de una interfaz física, se debe asignar una dirección de host para cada interfaz que se utilice. (Oracle, 2010). El prefijo de red de una dirección CIDR también define la longitud de la máscara de subred.

Tabla 3. Prefijos CIDR y su equivalente decimal

Prefijo de red CIDR	Direcciones IP disponibles	Equivalente de subred decimal con punto
/19	8,192	255.255.224.0
/20	4,096	255.255.240.0
/21	2,048	255.255.248.0
/22	1024	255.255.252.0
/23	512	255.255.254.0
/24	256	255.255.255.0
/25	128	255.255.255.128
/26	64	255.255.255.192
/27	32	255.255.255.224

Fuente: Recuperado de http://docs.oracle.com/cd/E19957-01/820-2981/ipplan-5/index.html

2.3.2.4 Direcciones IPv4 privadas

La IANA ha reservado tres bloques de direcciones IPv4 para que las compañías las utilicen en sus redes privadas. Estas direcciones están definidas en el RFC 1918, Address Allocation for Private Internets. Se puede utilizar este tipo de direcciones para los sistemas de las redes locales de una intranet corporativa, pero estas no son válidas cuando deban comunicarse fuera de la red local.

La Tabla 4 muestra los intervalos de direcciones IPv4 privadas y sus correspondientes máscaras de red. (Oracle, 2010)

Tabla 4. Direcciones IPv4 privadas

Intervalo de direcciones IPv4	Máscara de red
10.0.0.0 - 10.255.255.255	10.0.0.0
172.16.0.0 - 172.31.255.255	172.16.0.0
192.168.0.0 - 192.168.255.255	192.168.0.0

Fuente: Recuperado de http://docs.oracle.com/cd/E19957-01/820-2981/ipplan-5/index.html

2.4 Problemas con el Protocolo de Internet Versión 4

Las limitaciones de IPv4 fueron apareciendo con el crecimiento de las redes e Internet, entre las principales se puede mencionar:

- Gran dimensión de las tablas de enrutamiento en la red troncal de Internet, lo que hace que IPv4 sea ineficaz y perjudica considerablemente los tiempos de respuesta.

- Agotamiento de direcciones, derivada del crecimiento dela red Internet, “lo cual fue agravado además por la falta de coordinación en la delegación de direcciones durante los años 1980s, dejando incluso grandes espacios discontinuos. (Mandiola, 2012).

La escasez de direcciones no es igual en todos los puntos de la red; por ejemplo, es casi inapreciable por el momento en Norteamérica, pero en zonas como en Europa y Asia, la situación es crítica. Este problema es creciente, debido principalmente al tremendo avance de la telefonía móvil celular y la inminente aparición de la tercera generación de comunicaciones móviles o UMTS. Los móviles se convertirán en dispositivos siempre conectados a Internet y será necesario asignarlos una dirección IP fija y única. (Mandiola, 2012)

En la Figura 5 se puede observar las fechas aproximadas para el agotamiento de direcciones proyectada por el RIR.

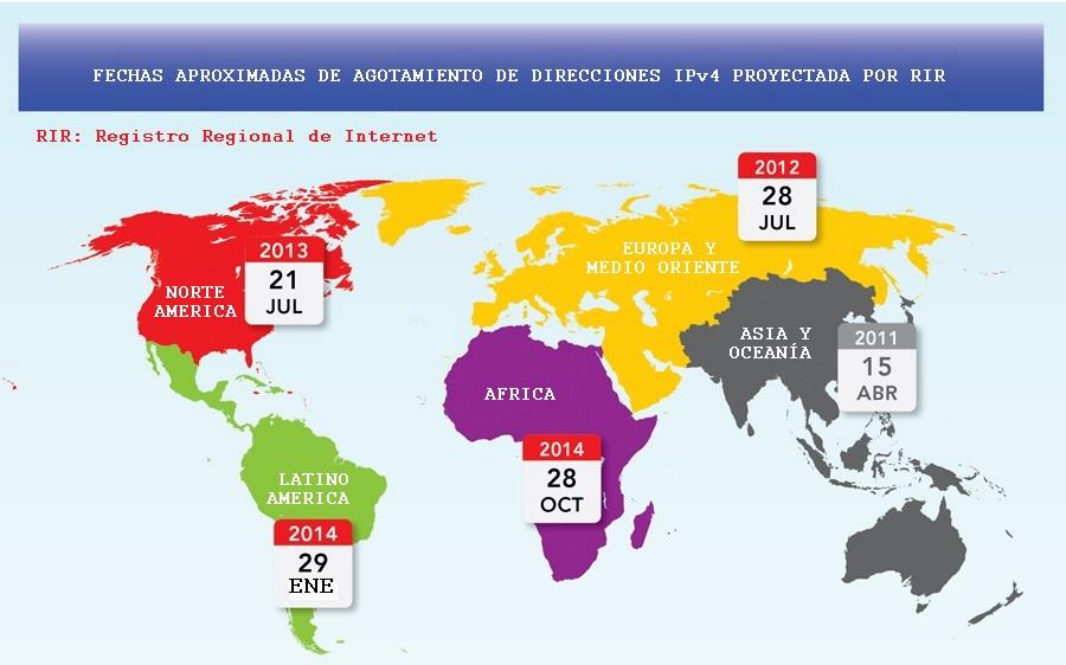


Figura 5. Proyección de Fechas de Agotamiento de Direcciones IPv4 a nivel mundial

Fuente: Recuperado de http://ipv6now.hk/en/WhatisIPv6.php

- IPv4 presenta otras dificultades entre las cuales se puede mencionar que no está preparado para soportar nuevos tipos de aplicaciones en tiempo real, ni mecanismos de seguridad avanzada sobre los datos transmitidos.

2.5 Historia del Protocolo de Internet Versión 6

A partir de la detección temprana de los problemas que presenta IPv4, el requerimiento de nuevas funcionalidades dado por el desarrollo de Internet y el avance tanto de aplicaciones como dispositivos que no fueron originalmente considerados, se acordó el desarrollo de un nuevo protocolo de direccionamiento.

Este nuevo protocolo no sólo debía dar la posibilidad de un mayor número de dispositivos conectados a la red global, sino que también se requería que solucionara las falencias detectadas en su predecesor y que diera lugar a los requerimientos de varias áreas de la industria que ahora estaban comprometidas en su utilización. (Gerometta, 2011)

Entre las fases más importantes en el desarrollo de IPv6 se puede mencionar:

- "En 1993 se publica el RFC 1550 con el propósito de reunir requerimientos y propuestas para el nuevo direccionamiento, por el momento denominado IPng.
- En 1995 se adopta la propuesta del proyecto SIPP que propone el mayor espacio de direccionamiento (RFC 1752).
- En 1995 se publican las especificaciones del ahora llamado IPv6 en el RFC 1883.
- En 1996 se inician las pruebas de IPv6 sobre Internet en el llamado 6bone. Cisco en este momento da soporte a IPv6 en un número limitado de plataformas de hardware.
- En 1997 se hacen los primeros avances en lo que hace a un formato de direcciones basado en la asignación a los ISPs.
- En 1998 se renuevan las especificaciones para IPv6 en el RFC 2460.
- En 1999 se comienza la asignación de prefijos IPv6 a los ISPs, al mismo tiempo que se forma el IPv6 Forum.

- En 2000/2001 los principales fabricantes incluyen IPv6 en sus principales líneas de productos.
- En 2001 Cisco hace disponible IPv6 de modo genérico en Cisco IOS release 12.2(1)T.
- En 2006 se concluye el período de pruebas sobre 6bone.” (Gerometta, 2011)
- “El 6 de Junio de 2012, The Internet Society (Asociación de internet) organizó el evento World IPv6 Launch Day (el día del lanzamiento mundial del sistema IPv6), para fomentar la transición al sistema IPv6.” (Edmond & Whitney, 2012)

Las más grandes compañías de internet como Google, Cisco, Microsoft, AT&T etc. han hecho que sus páginas de Internet sean accesibles a través de un sistema de direccionamiento IPv6 mediante el ajuste y apoyo de su sistema operativo al protocolo y así han posibilitado de forma permanentemente el sistema IPv6 en sus servicios.

Como pasa en cualquier periodo de transición aparecerán dificultades, pero la necesidad es la madre de los inventos y el sistema IPv6 es el futuro de internet. (Edmond & Whitney, 2012)

2.6 Protocolo de Internet Versión 6

2.6.1 Introducción

Cuando se utiliza Internet para cualquier actividad, como correo electrónico, navegación web, o cualquier aplicación o servicio, la comunicación entre los diferentes elementos de la red y nuestro computador o teléfono, utiliza un protocolo que denominamos Protocolo de Internet.

En los últimos años, desde que Internet tiene un uso comercial, la versión de este protocolo es IPv4.

Para que los dispositivos se conecten a la red, es necesaria una dirección IP. Cuando se diseñó IPv4, no se pensó que pudiera tener tanto éxito comercial, y dado que sólo dispone de 2^{32} direcciones, junto con el imparable crecimiento de usuarios y dispositivos, implica que en poco tiempo estas direcciones se agotarán.

Por este motivo, el organismo que se encarga de la estandarización de los protocolos de Internet (IETF), ha trabajado en los últimos años en una nueva versión del Protocolo de Internet, concretamente la versión 6, que posee direcciones con una longitud de 128 bits, es decir 2^{128} posibles direcciones (340.282.366.920.938.463.463.374.607.431.768.211.456).

Con una coexistencia ordenada entre IPv4 e IPv6 el despliegue se irá realizando gradualmente, ya que irá desplazándolo a medida que los dispositivos de cliente, equipos de red, aplicaciones, contenidos y servicios se vayan adaptando a la nueva versión del protocolo de Internet. (Gobierno de España, 2010)

2.6.2 Características de IPv6

IPv6 cuenta con las siguientes características:

2.6.2.1 Calidad de servicio (QoS)

IPv6 agrega en su cabecera un nuevo campo denominado etiqueta de flujo, el cual permite que los enrutadores sean identificados y estos a su vez proporcionen un control especial de los paquetes que pertenecen a un mismo flujo. La creación de este nuevo campo permite el desarrollo de nuevos modelos de clasificación de flujos de tráfico. Un flujo es un grupo de paquetes entre un origen y un destino. Dado que el tráfico está identificado en el encabezado IPv6, la compatibilidad con QoS se puede obtener de una forma más sencilla. (Gobierno de España: MIET, s.f.)

2.6.2.2 Nodos vecinos

El protocolo Descubrimiento de neighbors (vecinos) en IPv6 es semejante al protocolo ARP en IPv4, es el mecanismo por el cual un nodo nuevo que se incorpore a la red, descubre la presencia de otros nodos en su mismo enlace, además es capaz de localizar a routers y mantiene la información de conectividad a los vecinos activos. (Sandoval, 2008)

2.6.2.3 Capacidad de ampliación

El tamaño de direcciones cambia de 32 bits en IPv4 a 128 bits en IPv6, además se agregan encabezados de extensión a continuación del encabezado IPv6. El tamaño de los encabezados de extensión IPv6 sólo está limitado por el tamaño del paquete IPv6. (ORACLE, 2010)

2.6.3 Cabecera IPv6

2.6.3.1 Formato de la cabecera IPv6

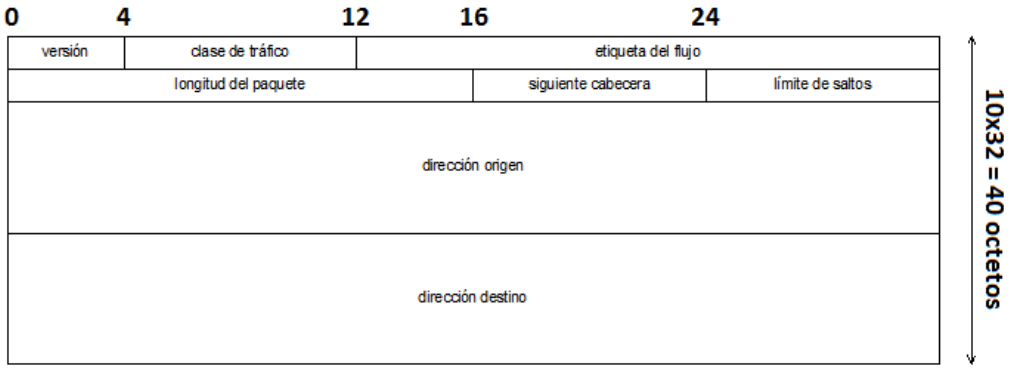


Figura 6. Formato de Cabecera IPv6

Fuente: Recuperado de http://www.ramonmillan.com/tutoriales/ipv6_parte1.php

La cabecera básica de IPv6, mostrada en la Figura 6, tiene una longitud fija de 40 octetos, consistiendo en los siguientes campos:

Versión (4 bits): Es el número de versión de IP, es decir, 6.

Clase de tráfico (8 bits): El valor de este campo especifica la clase de tráfico. Los valores de 0-7 están definidos para tráfico de datos con control de la congestión, y de 8-15 para tráfico de vídeo y audio sin control de la congestión.

Etiqueta del flujo (20 bits): Se crea para permitir tráficos con requisitos de tiempo real. Tiene una longitud de 20 bits. IPv6 define un flujo como una secuencia de paquetes enviados desde un origen a un destino específico. De este modo, la fuente asigna la misma

etiqueta a todos los paquetes que forman parte del mismo flujo. Su uso viene descrito en la RFC 1809.

Longitud del paquete (16 bits): Especifica el tamaño total del paquete, incluyendo la cabecera y los datos, en bytes. Es necesario porque también hay campos opcionales en la cabecera.

Siguiente cabecera (8 bits): Indica el tipo de cabecera que sigue a la cabecera fija de IPv6, por ejemplo, una cabecera TCP/UDP, ICMPv6 o una cabecera IPv6 opcional.

Límite de saltos (8 bits): Es el número de saltos máximo que le queda al paquete. El límite de saltos es establecido a un valor máximo por el origen y disminuye en 1 cada vez que un nodo encamina el paquete. Si el límite de saltos toma el valor 0, el paquete es descartado.

Dirección origen (128 bits): Es la dirección del origen del paquete.

Dirección destino (128 bits): Es la dirección del destino del paquete. (Palet, 2011)

2.6.3.2 Cabeceras de Extensión IPv6

En IPv6 la cabecera es de tamaño fijo, pero existen ocasiones en los que la cabecera estándar de IPv6 no es suficiente, en esos casos es necesario ampliar la cabecera con las denominadas (cabeceras de extensión de IPv6), las cuales son cabeceras opcionales que se codifican aparte.

Estas cabeceras están situadas entre la cabecera de IPv6 y las cabeceras de nivel superior utilizando el campo (siguiente cabecera) de la cabecera de IPv6 para indicar su existencia a los nodos.

Las cabeceras de extensión no son examinadas tampoco procesadas a lo largo de la ruta, salvo en el nodo de destino, al no ser procesadas por los nodos intermedios, los libera de la necesidad de procesar información que no es necesaria para los mismos, de esta manera optimizando el funcionamiento de routers y nodos intermedios.

La arquitectura general es la siguiente:

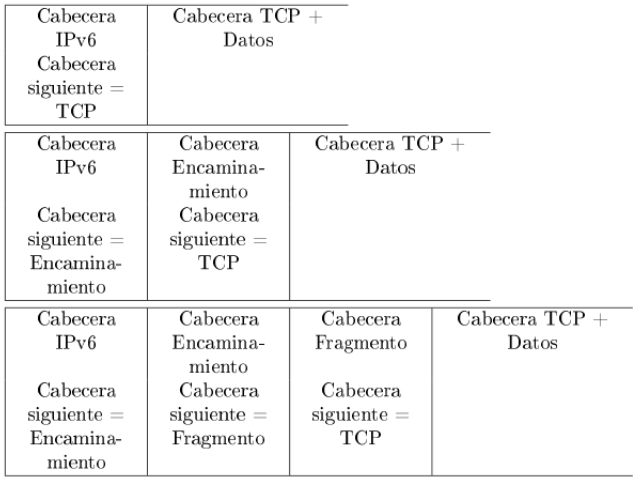


Figura 7. Arquitectura Cabeceras de Extensión IPv6

Fuente: Recuperado de http://eduangi.com/blog/2009/05/25/cabeceras-de-extension-de-ipv6/

Las cabeceras de extensión, a excepción de las (opciones de salto a salto) son procesadas por el nodo destino, hay que tener en cuenta que el nodo destino va a procesar las cabeceras de extensión en el orden estricto en el que hayan sido introducidas en el paquete, esto se conoce al leer la cabecera, la cual siempre tendrá un campo indicando la siguiente cabecera.

En el caso que el campo (cabecera siguiente) sea desconocido o tenga valor 0, el destinatario responderá al emisor con un mensaje ICMP de problema de parámetro, con un código ICMP 1 (encontrado tipo de cabecera siguiente desconocido) y el campo Puntero ICMP conteniendo el desplazamiento del valor desconocido dentro del paquete original.

El tamaño de las cabeceras de extensión para poder ser alineadas con la cabecera IPv6 deberá ser un múltiplo de 8 octetos.

Las cabeceras de extensión pueden ser del siguiente tipo:

- Opciones de salto a salto.
- Enrutamiento.
- Fragmentación.
- Opciones de destino.

- Autenticación.
- Seguridad del encapsulado de la carga útil. (Collado, 2009)

2.6.3.2.1 Cabecera de Opciones Salto a Salto

Se utiliza para llevar información opcional a los nodos que componen el camino y que se encuentran en cada salto, este tipo de cabecera se encuentra en aquellos paquetes de IPv6 que indican en el campo (cabecera siguiente) un 0.

El formato sería el que se muestra en la Figura 8:

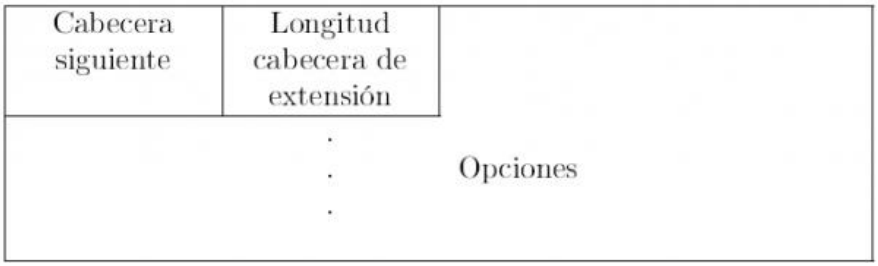


Figura 8. Formato de Cabecera Salto a Salto

Fuente: Recuperado de http://eduangi.com/blog/2009/05/26/cabecera-de-opciones-salto-a-salto/

- ***Cabecera siguiente (8 bits):*** Indica la siguiente cabecera.
- ***Longitud cabecera de extensión (8 bits):*** Longitud de la cabecera en octetos, no incluye el primer octeto.
- ***Opciones (Tamaño variable):*** Debe de tener un tamaño que permita la alineación del paquete, para ello se podrá utilizar Pad1 y PadN. (Collado, 2009)

2.6.3.2.2 Cabecera de Enrutamiento

Se utiliza en el enrutamiento de origen, contiene una lista de direcciones de todas o de algunas pasarelas a lo largo de la ruta deseada. Así, la dirección de destino contenida en la cabecera básica se modifica conforme el datagrama que se enruta de una puerta a la siguiente.

"Esta cabecera es muy útil ya que permite al origen establecer por dónde va a pasar la información que envía. (Lahera Pérez & González Rodríguez).

Su formato se muestra en la Figura 9.

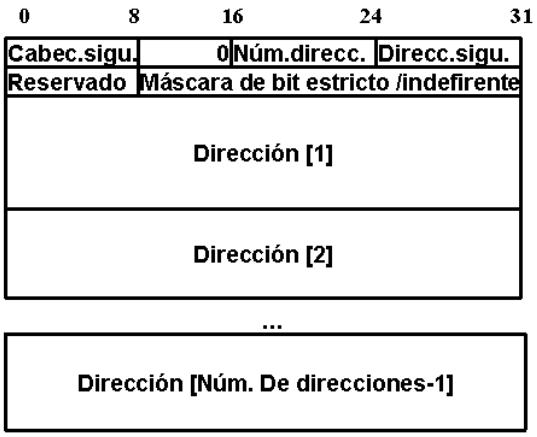


Figura 9. Formato de Cabecera de enrutamiento

Fuente: Manual Seminario IPv6. Visión general y comparativa con el actual IPv4

- ***Cabecera siguiente:*** Como todas las cabeceras indica cuál es la que prosigue.
- ***Tipo de enrutamiento:*** Se fija todo a 0.
- ***Número de direcciones:*** Es el número de direcciones a ser procesadas en la ruta, tiene un máximo de 20.
- ***Siguiente dirección:*** Indica la siguiente dirección a ser procesada.
- ***Reservado:*** Sin definir.
- ***Máscara:*** Indica saltos en el procesamiento secuencial de las direcciones, si la siguiente tiene el bit 1 en la máscara, hay procesamiento. 0 si es al contrario

2.6.3.2.3 Cabecera de Fragmentación

Se utiliza cuando los datos originales no caben en la unidad de transferencia máxima de cualquiera de las redes de la ruta. En estos casos el origen es el que fragmenta la información y los routers no intervienen en esta tarea. (Lahera Pérez & González Rodríguez).

Su formato se muestra en la Figura 10.

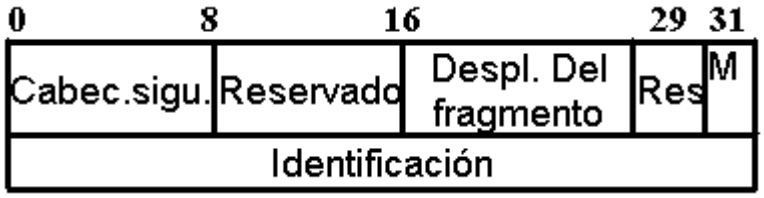


Figura 10. Formato Cabecera de Fragmentación

Fuente: Manual Seminario IPv6. Visión general y comparativa con el actual IPv4

- **Cabecera Siguiente**: Como todas las cabeceras indica cuál es la que prosigue.
- **Reservado**: Sin definir.
- **Desplazamiento del fragmento**: Indica la posición del contenido del datagrama en relación con el mensaje de datos de usuario inicial.
- **Flag M**: Indica si hay más fragmentos (1) o si no existen (0).
- **Identificador:** Ordena por número los fragmentos que corresponden al mismo mensaje.

2.6.3.2.4 Cabecera de Opciones de Destino

Sirve para llevar la información que solo será examinada por el destino deseado. (Lahera Pérez & González Rodríguez).

Su formato es igual al de la cabecera de salto a salto y se muestra en la Figura 11.

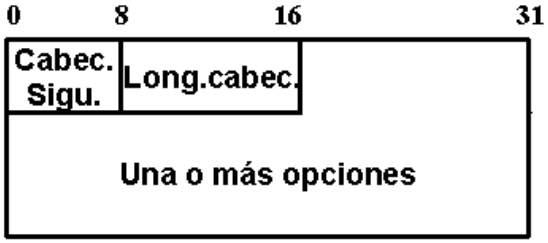


Figura 11. Formato Cabecera opciones de destino

Fuente: Manual Seminario IPv6. Visión general y comparativa con el actual IPv4

2.6.3.2.5 Cabecera de Autenticación

Define quien fue el que envió la información, es decir, la autenticidad del origen, así poder saber quién es el host sin cometer errores (Lahera Pérez & González Rodríguez)

Su formato se muestra en la Figura 12.

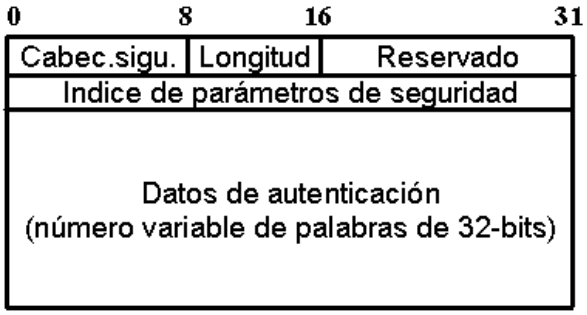


Figura 12. Formato Cabecera de Autenticación

Fuente: Manual Seminario IPv6. Visión general y comparativa con el actual IPv4

- **Cabecera Siguiente:** Como todas las cabeceras indica cuál es la que prosigue.
- **Longitud:** Indica la longitud del campo datos de autenticación en palabras de 32 bits.
- **Reservado:** Sin definir.
- **Índice de parámetros de seguridad:** Indica una asociación de seguridad.
- **Datos de autenticación:** Palabras de 32 bits que mediante la aplicación de un algoritmo nos ofrecen la autenticación.

Para realizar la autenticación se utiliza toda la trama y se quitan los campos que pueden variar, si se fragmenta la trama la autenticación se realizará extremo a extremo después del re-ensamblaje. Se aplica una clave de al menos 128 bits. (Lahera Pérez & González Rodríguez)

2.6.3.2.6 Cabecera de seguridad del encapsulado de la carga útil

Se presenta cuando los datos no se leen a su paso por la internet. El origen cifra los datos en dos modos:

- ***Modo Transporte:*** Se encripta una parte de la cabecera de seguridad del encapsulado de la carga útil además del segmento de transporte como se muestra en la Figura 13.

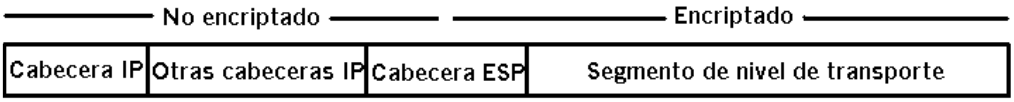


Figura 13.Encriptación en modo transporte

Fuente: Manual Seminario IPv6. Visión general y comparativa con el actual IPv4

- ***Modo Túnel:*** Como la cabecera IP ya tiene suficiente información para el encaminamiento, ésta se mantiene, pero se codifica todo el paquete IP y parte de la cabecera de seguridad como se muestra en la Figura 14. (Lahera Pérez & González Rodríguez).

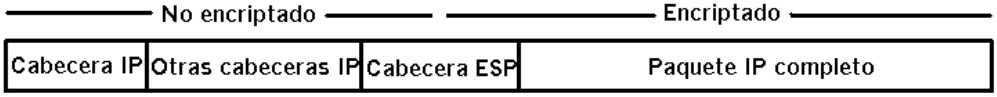


Figura 14. Encriptación en modo túnel

Fuente: Manual Seminario IPv6. Visión general y comparativa con el actual IPv4

El formato de la cabecera de seguridad del encapsulado de la carga útil se muestra en la Figura 15.

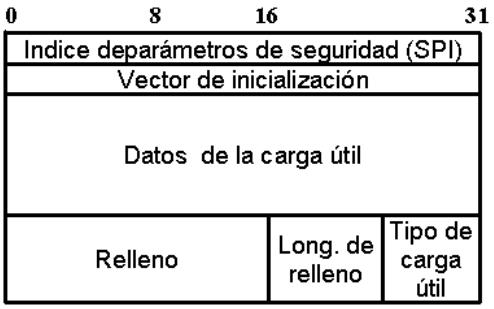


Figura 15. Formato Cabecera de seguridad del encapsulado de la carga útil

Fuente: Manual Seminario IPv6. Visión general y comparativa con el actual IPv4

- ***Índice de parámetros de seguridad:*** Asociación de seguridad.
- ***Vector de inicialización:*** Asociado al algoritmo DES-CBC de encriptación.
- ***Datos de carga útil:*** Datos que se van a encriptar.
- ***Relleno:*** Sin utilidad específica.
- ***Longitud de relleno***
- ***Tipo de carga útil:*** Protocolo de los datos de carga.

2.6.3.2.7 Orden de Cabeceras de Extensión en IPv6

Es importante tomar en cuenta el orden para las cabeceras de extensión y de las cabeceras de los paquetes, como se muestra en la Tabla 5.

Tabla 5. Orden de Cabeceras de Extensión IPv6

Cabecera de Extensión	Tipo	Tamaño	Descripción	RFC
Opciones salto a salto (*Hop-By-Hop Options*)	0	variable	Contiene datos que deben ser examinados por cada nodo a través de la ruta de envío de un paquete.	RFC 2460
Enrutamiento (*Routing*)	43	variable	Métodos para especificar la forma de rutear un datagrama. (Usado con IPv6 móvil)	RFC 2460, RFC 6275, RFC 5095
Cabecera de fragmentación (*Fragment*)	44	64 bits	Contiene parámetros para la fragmentación de los datagramas.	RFC 2460
Cabecera de autenticación (*Authentication Header (AH)*)	51	variable	Contiene información para verificar la autenticación de la mayor parte de los datos del paquete	RFC 4302
Encapsulado de seguridad de la carga útil (*Encapsulating Security Payload (ESP)*)	50	variable	Lleva la información cifrada para comunicación segura	RFC 4303
Opciones para el destino (*Destination Options*)	60	variable	Información que necesita ser examinada solamente por los nodos de destino del paquete.	RFC 2460
No Next Header	59	vacío	Indica que no hay más cabeceras	RFC 2460

Fuente: Recuperado de http://www.ictea.com/cs/knowledgebase.php?action=displayarticle&id=214

"Las cabeceras de extensión sólo aparecerán una vez excepto la (cabecera opciones de destino) que aparecerá justo antes de la (cabecera de enrutamiento) y antes de la (cabecera de capa superior).

También puede darse el caso debido a una tunelización o a un doble encapsulado que el protocolo de capa superior fuera IPv6, en ese caso se volvería a repetir el proceso completo." (Collado, 2009)

2.6.4 Direccionamiento IPv6

Los cambios dados por IPv6 no sólo se reflejan en la cantidad de direcciones, sino también incluyen nuevos tipos.

2.6.4.1 Tipos de direcciones IPv6

Una dirección IPv6 puede ser clasificada en tres tipos:

2.6.4.1.1 Unicast.

Se utiliza únicamente para identificar una interfaz de un nodo IPv6. Un paquete enviado a una dirección unicast es entregado a la interfaz identificada por esa dirección. A su vez este tipo de direcciones se subdividen en:

a. Direcciones Globales

Son las direcciones IPv6 utilizadas para el tráfico de IPv6 genéricos en el Internet de IPv6 y son similares a las direcciones unicast usadas para comunicarse a través de la Internet de IPv4. Representan la parte más importante de la arquitectura de direccionamiento de IPv6 y su estructura permite una agregación muy estricta de prefijos de enrutamiento para limitar el tamaño de la tabla de enrutamiento global de la Internet.

Cada Dirección global consta de tres partes:

- *Prefijo recibido del proveedor:* el prefijo asignado a una organización por un proveedor debe ser al menos de 48 bits (RFC 3177). El prefijo asignado a la organización es parte del prefijo del proveedor.
- *Sitio:* con un prefijo de 48 bits distribuido a una organización por medio de un proveedor, se abre la posibilidad para esa organización de tener 65,535 subredes (asignando un prefijo de 64 bits a cada una de las subredes). La organización puede usar los bits 49 a 64 (16 bits) del prefijo recibido para subredes.

- *Computadora:* utiliza cada Identificador de interfaz del nodo. Esta parte de la dirección IPv6, que representa los 64 bits de más bajo orden de la dirección, es llamada Identificador de Interfaz.

La Figura 16 muestra como ejemplo al prefijo 2001:0410:0110::/48 que es asignado por un proveedor a una organización. Dentro de la organización el prefijo 2001:0410:0110:0002::/64 es habilitado en una subred. Finalmente, un nodo en esta subred tiene la dirección 2001:0410:0110:0002:0200:CBCF:1234:4402. (Network Information Center México S.C., 2013)

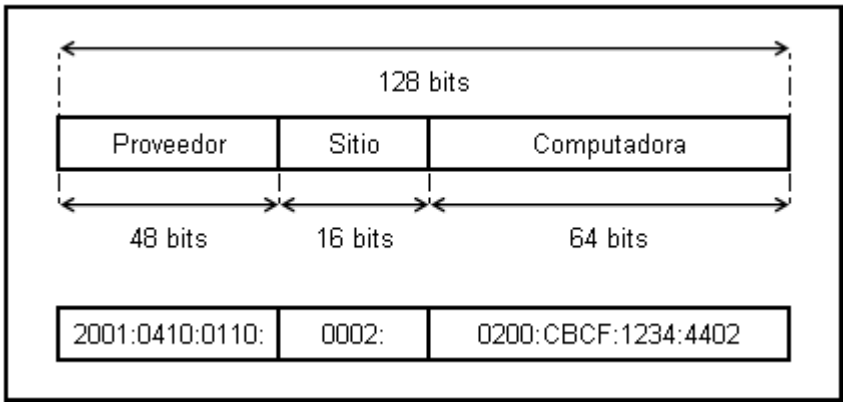


Figura 16. Ejemplo de formato de dirección global Unicast
Fuente: Recuperado de http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

b. Direcciones Link-Local

Se utilizan en enlaces sencillos, para mecanismos de autoconfiguración, descubrimiento de neighbors y en redes sin ruteadores. Es útil para crear redes temporales. Puede ser utilizada sin un prefijo global. Su formato se muestra en la Figura 17.

c. Direcciones Site-Local

Contiene información de subred dentro de la dirección. Son enrutadas dentro de un mismo sitio, pero los ruteadores no deben enviarlas fuera de éste. Además, es utilizada sin un prefijo global. Su formato se muestra en la Figura 17.

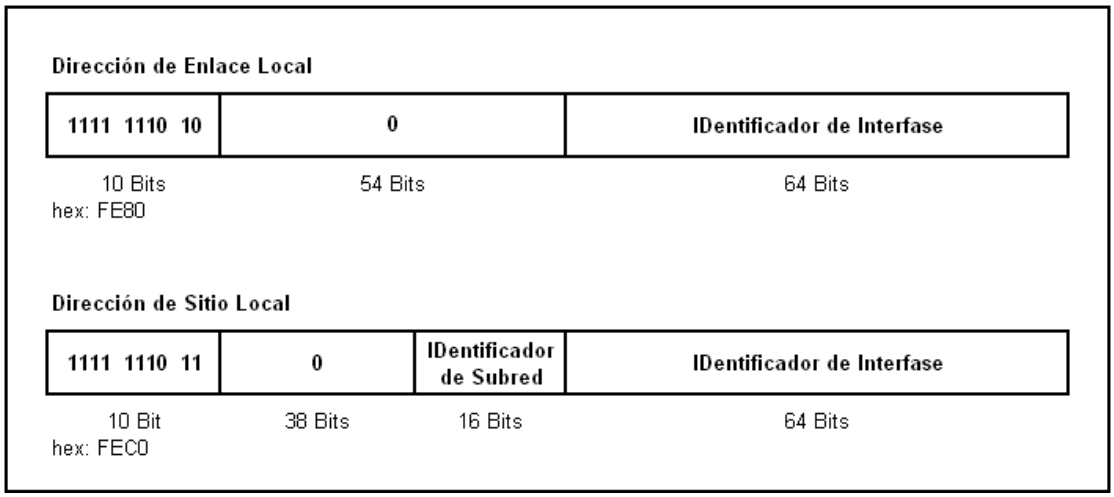


Figura 17. Formato de direcciones de Enlace Local y Sitio Local

Fuente: Recuperado de http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

El prefijo **FE80** identifica a una dirección de Enlace Local y el prefijo **FEC0** identifica a un Sitio local, ambos en hexadecimal.

d. Direcciones IPv6 especiales

Este tipo de direcciones se dividen en dos:

- ***Loopback.***

Al igual que en IPv4, cada dispositivo tiene una dirección loopback, que es usada por el nodo. En IPv6 se representa en el formato hexadecimal por el prefijo 0000:0000:0000:0000:0000:0000:0000:0001 y en el formato comprimido por ::1.

- ***Sin-Especificar.***

Es una dirección unicast sin asignar a alguna interfaz. Indica la ausencia de una dirección y es usada para propósitos especiales. Es representada en el formato hexadecimal con el prefijo 0000:0000:0000:0000:0000:0000:0000:0000 y con :: en el formato comprimido. (Network Information Center México S.C., 2013)

e. Direcciones Compatibles

Es utilizada por los mecanismos de transición en computadoras y routers para crear automáticamente túneles IPv4. De esa forma se entregan paquetes IPv6 sobre redes IPv4.

En la Figura 18 se muestra el formato descriptivo de una dirección IPv6 compatible con IPv4. En éste el prefijo se crea con el bit puesto a cero del de más alto nivel de los 96 bits, y los restantes 32 bits de menor nivel representan la dirección en formato decimal.

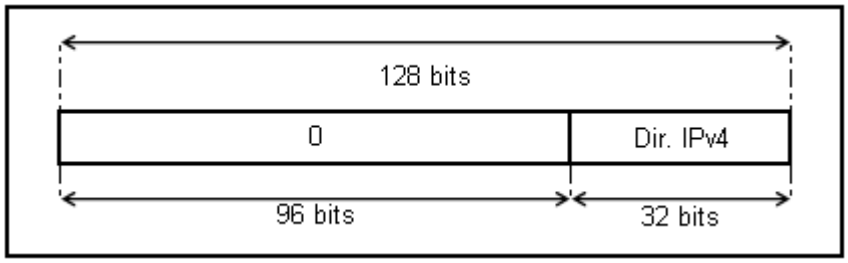


Figura 18. Formato de una dirección IPv6 compatible con IPv4
Fuente: Recuperado de http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

2.6.4.1.2 Multicast.

Se utiliza para identificar a un grupo de interfaces IPv6. Un paquete enviado a una dirección multicast es procesado por todos los miembros del grupo multicast. Este tipo de direcciones se subdividen en:

a. Direcciones Asignadas

Está definida y reservada por el RFC 2373 para la operación del protocolo IPv6. Dichas direcciones asignadas son usadas en el contexto de mecanismos específicos del protocolo. En la Tabla 6 se presentan las Direcciones Asignadas Multicast y su área de funcionamiento.

Tabla 6. Direcciones Asignadas Multicast

Dirección Multicast	Área de Funcionamiento	Significado	Descripción
FF01::1	Nodo	Todos los nodos	Todos los nodos en la interfaz local
FF01::2	Nodo	Todos los enrutadores	Todos los enrutadores en la interfaz local
FF02::1	Enlace Local	Todos los nodos	Todos los nodos en el enlace local
FF02::2	Enlace Local	Todos los enrutadores	Todos los enrutadores en el enlace local

FF05::2	Sitio	Todos los enrutadores	Todos los enrutadores en un sitio

Fuente: Recuperado de http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

b. Direcciones Nodo Solicitado

Es una dirección a la que se debe unir cada nodo por cada dirección unicast y anycast asignada. La dirección está formada tomando los 24 bits de bajo nivel de una dirección IPv6 (es la última parte del identificador de la computadora). La dirección se une con el prefijo FF02:0:0:0:0:1:FF00::/104, de esa manera el rango de direcciones Multicast de Nodo Solicitado va de FF02:0:0:0:0:1:FF00:0000 a FF02:0:0:0:0:1:FFFF:FFFF. (Network Information Center México S.C., 2013)

2.6.4.1.3 Anycast.

Se asigna a múltiples interfaces. Un paquete enviado a una dirección anycast es entregado a una de estas interfaces, usualmente la más cercana.

2.6.4.2 Reglas de Utilización

Las direcciones IPv6 son asignadas a interfaces, no a nodos, por lo que cada interfaz de un nodo necesita al menos una dirección unicast. A una sola interfaz se le pueden asignar múltiples direcciones IPv6 de cualquier tipo (unicast, anycast, multicast). Por lo cual un nodo puede ser identificado por la dirección de cualquiera de sus interfaces.

Existe la posibilidad de asignar una dirección unicast a múltiples interfaces para balanceo de cargas.

Una dirección típica de IPv6 consiste de tres partes como se muestra en la Figura 19.

a. El prefijo de enrutamiento global
b. El IDentificador de subred
c. El IDentificador de interfase

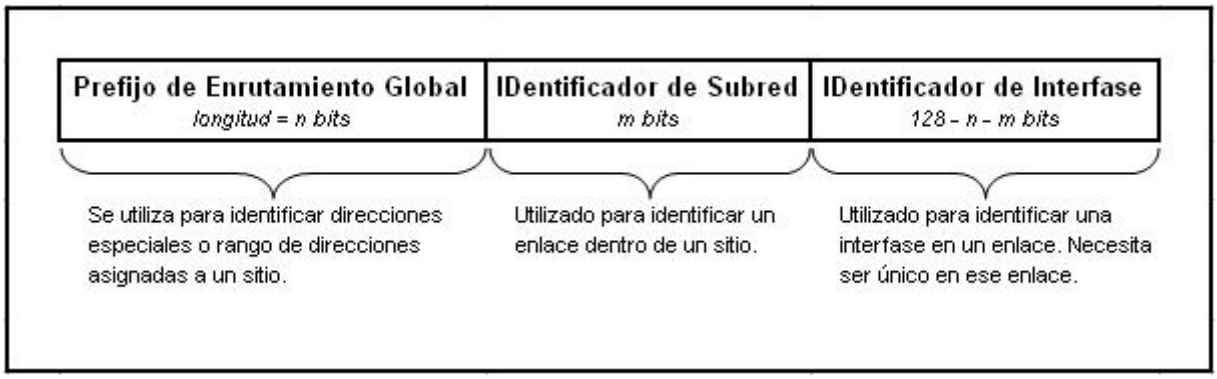


Figura 19. Partes de una dirección IPv6

Fuente: Recuperado de http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

2.6.4.3 Notación de Direcciones

Como lo define el RFC 2373 Arquitectura del Direccionamiento del Protocolo de Internet versión 6, existen tres formatos para representar direcciones IPv6.

- El primer formato es el método más largo. Este representa los 32 caracteres hexadecimales que forman la dirección. Es el más cercano a la forma en que la computadora procesa la dirección.

- Mediante una representación comprimida que se utiliza para simplificar la escritura de la dirección.

- El tercer método es el relacionado con los mecanismos de transición donde una dirección IPv4 está incluida dentro de una dirección IPv6. Este método es el menos importante de los tres, y sólo es útil si se utiliza algún mecanismo de transición como NAT-PT. (Network Information Center México S.C., 2013)

2.6.4.3.1 Formato Hexadecimal

Conocido también como formato completo y se compone de los ocho campos de 16 bits hexadecimales separados por dos puntos. Cada campo de 16 bits representa cuatro caracteres hexadecimales y los valores que puede tomar el campo de 16 bit van de 0x0000 a 0xFFFF. En la Figura 20 se presentan ejemplos de direcciones IPv6 en el formato hexadecimal.

Ejemplos de direcciones IPv6
0000:0000:0000:0000:0000:0000:0000:0000
0000:0000:0000:0000:0000:0000:0000:0001
2001:0410:0000:1234:FB00:1400:5000:45FF
3FFE:0B00:0C18:0001:0000:1234:AB34:0002
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

Figura 20. Formato hexadecimal de dirección IPv6

Fuente: Recuperado de http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

2.6.4.3.2 Formato Comprimido

En IPv6 es común que se presenten grandes cadenas de ceros dentro de las direcciones. Para simplificar su escritura es conveniente utilizar una sintaxis especial en donde se suprimen los valores consecutivos de ceros ante dos situaciones: campos sucesivos de ceros y campos con ceros al inicio.

- ***Campos sucesivos de ceros***

Para simplificar la longitud de una dirección IPv6, cuando se presentan de uno a múltiples campos de ceros, es legal representar estos como ceros ó :: (doble dos puntos). Sin embargo, es permitido usarlo una sola vez en la escritura de la dirección. En la Tabla 7, se presenta del lado izquierdo las direcciones en formato hexadecimal y del lado derecho se presenta la dirección en su formato comprimido.

Tabla 7. Ejemplos de uso de formato hexadecimal con campos sucesivos de cero

Formato Hexadecimal	**Formato comprimido utilizando ::**
0000:0000:0000:0000:0000:0000:0000:0000	::
0000:0000:0000:0000:0000:0000:0000:0001	::0001
2001:0410:0000:1234:FB00:1400:5000:45FF	2001:0410::1234:FB00:1400:5000:45FF
3FFE:0B00:0C18:0001:0000:1234:AB34:0002	3FFE:0B00:0C18:0001::1234:AB34:0002

Fuente: Recuperado de http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

- ***Campos con ceros al inicio***

El segundo método para comprimir direcciones se aplica a cada uno de los campos hexadecimales de 16 bits que tienen uno o más ceros al inicio. Esto significa que, si hay uno o más ceros al inicio de cada campo, estos pueden ser suprimidos para simplificar su longitud y facilitar su lectura y escritura. No obstante, si cada caracter del campo es cero al menos uno debe de ser mantenido. La Tabla 8 muestra del lado izquierdo las direcciones en su *Formato Hexadecimal* y del lado derecho están las direcciones en su *Formato comprimido* con los ceros suprimidos.

Tabla 8. Ejemplos de uso de formato hexadecimal con campos con ceros al inicio

Formato Preferido	Formato comprimido
0000:0000:0000:0000:0000:0000:**206.123.31.2**	0:0:0:0:0:0:206.123.31.2 o ::206.123.31.2
0000:0000:0000:0000:0000:0000:**ce7b:1f01**	0:0:0:0:0:0:ce7b:1f01 o ::ce7b:1f01
0000:0000:0000:0000:0000:**FFFF:206.123.31.2**	0:0:0:0:0:FFFF:206.123.31.2 o :: FFFF:206.123.31.2
0000:0000:0000:0000:0000:**FFFF:CE7B:1F01**	0:0:0:0:0:FFFF: ce7b:1f01 o ::FFFF: ce7b:1f01

Fuente: Recuperado de http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

- ***Combinación de ambos métodos de compresión***

Se pueden combinar la compresión de campos sucesivos de ceros con la compresión de campos con ceros al inicio para simplificar la longitud de la dirección IPv6. En la Tabla 9 se muestra un ejemplo de la aplicación con ambos métodos de compresión.

Tabla 9. Ejemplo de aplicación de ambos métodos de compresión

Formato Hexadecimal	Formato comprimido
0000:0000:0000:0000:0000:0000:0000:0000	::
0000:0000:0000:0000:0000:0000:0000:0001	::1
2001:0410:0000:1234:FB00:1400:5000:45FF	2001:410::1234:FB00:1400:5000:45FF
3FFE:0B00:0C18:0001:0000:1234:AB34:0002	3FFE:B00:C18:0001::1234:AB34:2
FE80:0000:0000:0000:0000:0000:0000:0009	FE80::9

Fuente: Recuperado de http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

2.6.4.3.3 Formato Compatible

Este tipo de representación es utilizado en una dirección IPv4 incrustada dentro de una dirección IPv6. La primera parte de la dirección IPv6 utiliza la representación hexadecimal y el otro segmento de IPv4 está en formato decimal. Esto representa específicamente una dirección usada por mecanismos de transición.

La dirección se divide en dos niveles, superior e inferior, y estos a su vez se subdividen. El nivel superior se fragmenta en seis campos con valores hexadecimales de 16 bits seguidos del nivel inferior compuesto de 4 campos con valores decimales de 8 bits. La Figura 21 muestra la distribución de la dirección IPv6 con una dirección IPv4 incrustada.

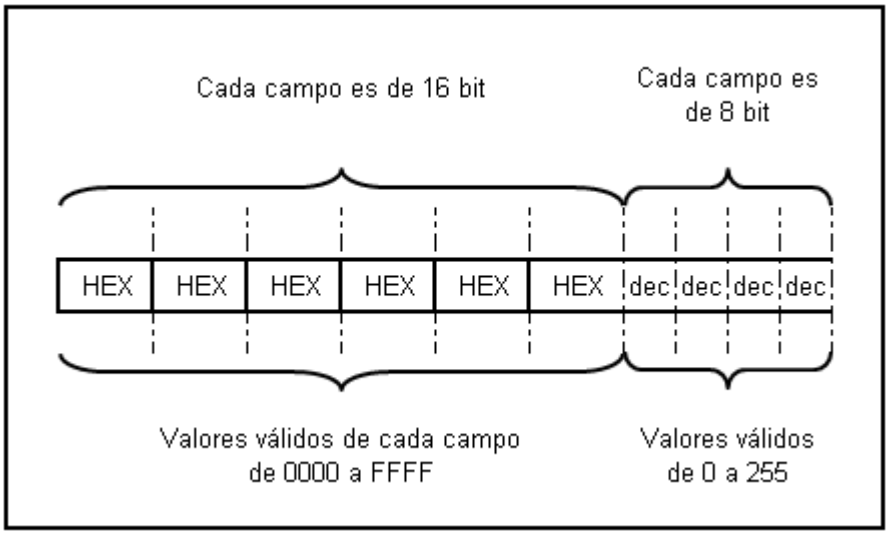


Figura 21. Dirección IPv6 con una dirección IPv4 incrustada

Fuente: Recuperado de http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

Existen dos tipos de direcciones IPv6 que tienen direcciones IPv4 incrustadas:

- ***Dirección IPv6 compatible con IPv4.***

Es utilizada para establecer un túnel automático que lleva paquetes IPv6 sobre redes IPv4. Esta dirección está vinculada con un mecanismo de transición del protocolo IPv6.

- ***Dirección IPv6 mapeada a IPv4.***

Se utiliza sólo en el ámbito local de nodos que tienen las direcciones IPv4 e IPv6. Los nodos usan direcciones IPv6 mapeadas a IPv4 de forma interna solamente. Estas direcciones no son conocidas afuera del nodo y no llegan al cable de comunicación como direcciones IPv6. (Network Information Center México S.C., 2013)

2.6.4.4 Subredes IPv6

En IPv6 la única forma de representar una máscara de red es mediante notación CIDR. Aunque las direcciones estén en formato hexadecimal, el valor de la máscara de red se mantiene como un valor decimal. La Tabla 10 muestra ejemplos de direcciones IPv6 y prefijos de red utilizando el valor de red en notación CIDR.

Tabla 10. Direcciones IPv6 y prefijos de red utilizando el valor de red con CIDR

Prefijo IPv6	**Descripción**
2001:410:0:1:0:0:0:45FF/128	Representa una subred con una sola dirección IPv6
2001:410:0:1::/64	El prefijo de red 2001:410:0:1::/64 puede manejar 2^{64} nodos. Esta es la longitud por defecto de un prefijo para una subred.
2001:410:0::/48	El prefijo de red 2001:410:0::/48 puede manejar 2^{16} prefijos de red de 64 bit. Esta es la longitud por defecto de un prefijo para un sitio.

Fuente: Recuperado de http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

Las partes más importantes a tomar en cuenta en las subredes IPv6 son las siguientes:

- El número de bits puestos a 1 en la máscara de red define la longitud del prefijo de red y la parte restante es para el direccionamiento del nodo. Esto es importante, ya que define cuándo los paquetes van a ser enviados al enrutador por defecto o a un nodo específico en la misma subred.

- Se suprime el concepto de dirección reservada en un rango de red. A diferencia de IPv4 donde se reservaba la primera y la última dirección de difusión de un rango, en IPv6 no existen estos conceptos.

- El número de bits para el direccionamiento del nodo dentro de un prefijo de sitio (48 bits) en IPv6 resulta ser tan grande que no es necesario hacer un plan de direccionamiento para un sitio utilizando diferentes valores de máscara de red. De tal manera que el cálculo de máscara de red para cada subred y el uso de VLSM no son requeridos. (Network Information Center México S.C., 2013)

2.6.4.5 Plan de Direccionamiento

Desarrollar un plan de direccionamiento es de gran importancia en la transición de IPv4 a IPv6, para lo cual es necesario realizar los siguientes pasos previos:

2.6.4.5.1 Obtención de un prefijo de sitio

Debe obtenerse un prefijo de sitio antes de configurar IPv6. El prefijo de sitio se utiliza en la derivación de direcciones IPv6 para todos los nodos de la implementación de IPv6.

Un ISP que admita IPv6 puede brindar a las empresas prefijos de sitio de IPv6 de 48 bits. Si el ISP sólo acepta IPv4, se puede buscar otro que sea compatible con IPv6 y mantener el ISP actual para IPv4.

a. Creación del esquema de numeración de IPv6

A menos que la red IPv6 que se proponga sea totalmente nueva, la topología de IPv4 ya configurada es utilizada como base para el esquema de numeración de IPv6.

b. Creación de un esquema de numeración para subredes

Se debe iniciar el esquema de numeración asignando las subredes IPv4 ya configuradas a subredes IPv6 equivalentes. Como ejemplo, supongamos que el prefijo de IPv6 2001:db8:3c4d/48 se ha asignado al sitio.

La tabla 11 muestra la asignación de prefijos de IPv4 privados a prefijos de IPv6.

Tabla 11. Representación de prefijos IPv4 privados a prefijos IPv6

Prefijo de subred IPv4	Prefijo de subred IPv6 equivalente
192.168.1.0/24	2001:db8:3c4d:1::/64
192.168.2.0/24	2001:db8:3c4d:2::/64
192.168.3.0/24	2001:db8:3c4d:3::/64
192.168.4.0/24	2001:db8:3c4d:4::/64

Fuente: Recuperado de http://docs.oracle.com/cd/E19957-01/820-2981/ipv6-planning-9/index.html

c. Creación de un plan de direcciones IPv6 para nodos

En la mayoría de los hosts, la configuración automática sin estado de direcciones IPv6 para sus interfaces es una estrategia válida. Cuando el host recibe el prefijo de sitio del enrutador más cercano, el protocolo ND (Neighbor Discovery) genera de forma automática direcciones IPv6 para cada interfaz del host.

Los servidores necesitan direcciones IPv6 estáticas. Si no se configura manualmente las direcciones IPv6 de un servidor, siempre que se reemplaza una tarjeta NIC del servidor se configura automáticamente una dirección IPv6. Al crear direcciones para servidores debe tenerse en cuenta lo siguiente:

- Proporcionar a los servidores ID´s de interfaz descriptivos y estables. Un método consiste en aplicar un sistema de numeración sucesiva a los ID de interfaz.

- Si no se cambia la numeración de la red IPv4, se debe utilizar como ID de interfaz las direcciones IPv4 ya creadas de los enrutadores y servidores. La dirección IPv4 puede convertirse a hexadecimal y aplicar el resultado como ID de interfaz.

Este solamente se utiliza si se es el propietario de la dirección IPv4 registrada, en lugar de haber obtenido la dirección de un ISP. Si se usa una dirección IPv4 brindada por un ISP, se crea una dependencia que puede causar problemas en caso de cambiar de ISP.

Anteriormente un diseñador de red debido al número limitado de direcciones IPv4, debía tener en cuenta si iba a utilizar direcciones registradas globales y direcciones privadas. El concepto de direcciones IPv4 globales y privadas no existe en cuanto a direcciones IPv6, por lo que se utiliza direcciones unicast globales, que incluyen el prefijo

de sitio, en todos los vínculos de la red, incluida la DMZ pública. (Oracle Corporation, 2010)

2.7 Enrutamiento con IPv6

IPv6 no cambió los fundamentos del enrutamiento del protocolo IP, el cual se basa en:

- La coincidencia del mayor prefijo.
- El uso de enrutamiento fuente.
- Re direcciona con ICMP.
- Utiliza los mismos protocolos de enrutamiento: RIP, OSPF, IS-IS y BGP.

No existen muchos cambios en el enrutamiento, por lo cual el cambio a IPv6 es transparente para el administrador de red. Únicamente se realizan modificaciones a la manera en que se maneja el enrutamiento para hacerlo más eficiente o para usar las características de IPv6.

2.7.1 RIPng

Es un protocolo para redes de tamaño pequeño a mediano. La versión mejorada para IPv6 conocida como RIP Siguiente Generación (RIPng, RIP next generation) (RFC 2080 y 2081) está basado en RIP versión 2 (RFC 1723) y hereda sus mismas características:

- Algoritmo vector-distancia Bellman-Ford.
- Actualizaciones cada 30 segundos.
- Tiempo de expiración de 180 segundos para rutas desconectadas.
- Métricas fijas.
- Diámetro de red de 15 saltos.
- Horizonte dividido y envenenamiento en reversa de trayectoria.
- Etiquetas de ruta.

La Tabla 12 muestra los cambios realizados al protocolo RIP:

Tabla 12. Cambios y Nuevas Características de RIPng

Características	Descripción
Rutas Anunciadas	RIPng anuncia rutas IPv6 compuestas de prefijos IPv6 con longitud y métrica.
Siguiente Salto	La dirección de Siguiente Salto es la dirección de enlace local IPv6 de la interfaz del ruteador que anuncia el prefijo.
Transporte de Protocolo IP	IPv6 es utilizado para llevar datagramas RIP usando UDP como protocolo de transporte.
Dirección IPv6 Fuente	La actualización RIP de la dirección fuente IPv6 es la dirección de enlace-local de la interfaz del ruteador fuente. Con excepción de cuando se contesta un Mensaje de Solicitud unicast desde un puerto distinto al puerto RIPng, en este caso, la dirección fuente es una dirección global válida).
Dirección IPv6 Destino	La dirección destino de la actualización RIP es FF02::9, que es la dirección multidifusión de todos los ruteadores RIP. Solamente los ruteadores RIPng atienden esta dirección multidifusión. Es una dirección multidifusión con alcance de enlace-local, la cual no es retransmitida a otros enlaces.
Límite de Salto = 255	Las actualizaciones RIP tienen el Límite de Salto de paquete IPv6 configurado en 255. Esto permite a los involucrados verificar si las actualizaciones vienen de ruteadores externos falsos.
Número de Puerto = 521	El puerto UDP es 521, en lugar de 520 para RIPv1 y 2.
RIPng versión = 1	El número de versión RIPng en el paquete RIP es 1, lo que representa que es la primera versión de RIPng. Se utiliza un puerto de transporte distinto. Los involucrados pueden diferenciar entre paquetes RIPv1, RIPv2 y RIPng.
Tabla de Enrutamiento	La tabla de enrutamiento de IPv6 es distinta de la tabla de enrutamiento de IPv4 para RIPv1 o RIPv 2. La ruta por omisión es anunciada como ::/0.
Autenticación	La autenticación RIPng se basa en la seguridad suministrada por IPSec.

Fuente: Recuperado de http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

2.7.2 OSPFv3

OSPFv3 (RFC 2740) es un protocolo de red independiente, parecido a IS-IS, por lo cual puede incluir rutas IPv6. OSPFv3 comparte los fundamentos de OSPFv2:

- Inundación (flooding).
- Elección de ruteador designado.

- Área de soporte.
- Cálculos de Djikstra para abrir la trayectoria más corta primero.
- Soporte de circuito en demanda.
- Áreas Stub y NSSA.
- Extensiones multidifusión (MOSPF).

La Tabla 13 muestra los cambios realizados al protocolo OSPFv3 (Network Information Center México S.C., 2013)

Tabla 13. Cambios y Nuevas Características de OSPFv3

Características	Descripción
LSAs de ruteador y red	No tienen semántica de direccionamiento y sólo llevan información de topología.
Nuevo LSA-con-Prefijo-Intra-Area	Este lleva direcciones y prefijos IPv6.
Direcciones en LSA	Son descritas como prefijo con una longitud de prefijo. La ruta por omisión es ::/0.
Identificación de Ruteador	ID del Ruteador es un valor de 32 bit sin importar si es dirección IPv4 o IPv6. Se usa en DR, BDR, LSAs, base de datos.
Alcance de la Inundación	Enlace, Área o AS.
Siguiente-Salto	La dirección de Siguiente-Salto es la dirección de enlace-local IPv6 de la interfase de ruteador que anuncia el prefijo.
Nuevo LSA de Enlace-Local	Lleva la dirección de enlace local de la interfaz de ruteador, los prefijos del enlace y las opciones.
Ejecución por cada enlace, en lugar de cada IP de subred	Interfaz OSPF que se puede conectar a un enlace en lugar de una subred IP. Están soportadas múltiples instancias en un enlace sencillo.
Usa IPv6 para el transporte de paquetes OSPF	Encabezado Siguiente = 89 para identificar un paquete IPv6 OSPFv3.
Paquetes OSPF con dirección IPv6 fuente	La dirección fuente del paquete OSPF es la dirección enlace-local de la interfaz del ruteador origen.
Paquetes OSPF con dirección IPv6 destino	Todos los ruteadores OSPF envían paquetes Hello y atienden a FF02::/5, que es la dirección multidifusión con enlace a todos los ruteadores OSPF.
Límite de Salto = 1 de paquetes OSPF	1 significa de enlace local.
OSPF versión = 3	Versiones previas son iguales a 1 o 2.

La Autenticación es realizada con IPSec	Se quitaron todos los datos de autenticación interna OSPF y ahora se provee seguridad con IPSec para proteger la integridad y ofrecer autenticación.

Fuente: Recuperado de http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

2.8 ICMPv6

Es un estándar definido en el documento RFC 4443, *"Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification"* [Especificación del Protocolo de control de mensajes de Internet (ICMP) para el Protocolo Internet versión 6 (IPv6)]. ICMPv6 es la implementación en IPv6 del protocolo ICMP originalmente diseñado para IPv4. Es utilizado por nodos IPv6 para reportar errores encontrados durante el procesamiento de paquetes, así como para realizar funciones relativas a niveles de interconexión de redes, tales como ping.

Este protocolo es uno de los pilares fundamentales de la arquitectura IPv6, sus mensajes y funcionalidad tienen que ser implementados en cada nodo. (Portal IPv6 Cuba, s.f.)

El protocolo ICMPv6 proporciona un espacio para los protocolos siguientes:

- ***Descubrimiento de escucha de multidifusión (MLD)***
  Consiste en una serie de tres mensajes ICMPv6, permite que los routers IPv6 aprendan direcciones multicast de los nodos que se encuentran en enlaces al que se encuentra unido el router, en resumen, es usado por hosts para reportar pertenencia a un grupo. (Tapia Cajas, 2014)

- ***Descubrimiento de vecinos (ND)***
  Son una serie de cinco mensajes ICMPv6 que gestionan la comunicación de un nodo a otro en un vínculo. Además, realiza la resolución de direcciones IPv6 y MAC, y mantiene información actualizada acerca del estado en que se encuentran los caminos hacia otros nodos. (Tapia Cajas, 2014)

2.8.1 Encapsulamiento de Mensajes ICMPv6

Los mensajes ICMPv6 se envían de manera automática cuando un paquete IPv6 no puede llegar a su destino.

Estos mensajes se encapsulan y envían como carga dentro de los paquetes IPv6, como se muestra en la Figura 22.

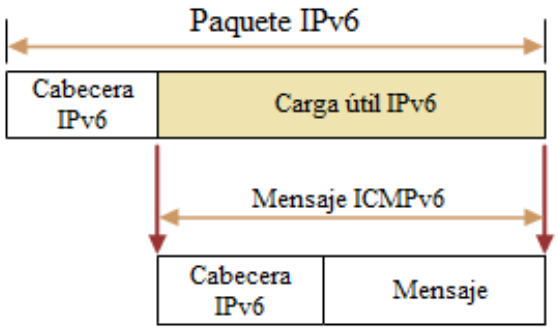


Figura 22. Encapsulamiento Mensajes IPv6

Fuente: Recuperado de http://msdn.microsoft.com/es-es/library/cc757063%28v=ws.10%29.aspx

2.8.2 Tipos de Mensajes ICMPv6

En el encabezado ICMPv6 se identifican diferentes tipos de mensajes ICMPv6. Estos se agrupan en dos tipos o clases:

- Mensajes de Error: 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.

- Mensajes de Información: Los valores de los mensajes informativos oscilan entre 128 y 255, de los cuales 130,131 y 132 están definidos para funciones multicast, y los códigos 133 hasta 137 son utilizados en el protocolo de ND.

En la Tabla 13 se muestran y describen los mensajes ICMPv6 que no están relacionados con MLD o ND. (Tapia Cajas, 2014)

Tabla 14. Tipos de mensaje ICMPv6

	Mensajes de Error ICMPv6	
Tipo	**Descripción y Códigos**	
1	**Destination Unreachable (Destino inaccesible):** informa al host remitente de que un paquete no se puede entregar.	
	Código	**Descripción**
	0	Sin ruta hacia el destino
	1	Comunicación prohibida administrativamente
	2	Sin asignar
	3	Dirección no alcanzable
	4	Puerto no alcanzable
2	**Packet Too Big (Paquete demasiado grande):** informa al host remitente de que el paquete es demasiado grande para el reenvío.	
3	**Time Exceeded (Tiempo agotado):** informa al host remitente de que el límite de saltos de un paquete IPv6 ha caducado.	
	Código	**Descripción**
	0	Límite de saltos excedido
	1	Tiempo de desfragmentación excedido
4	**Parameter Problem (Problemas de parámetros):** informa al host remitente que se produjo un error al procesar el encabezado IPv6 o un encabezado de extensión IPv6.	
	Código	**Descripción**
	0	Campo erróneo en cabecera
	1	Tipo de “cabecera siguiente” desconocida
	2	Opción IPv6 desconocida
	Mensajes Informativos ICMPv6	
Tipo	**Descripción**	
128	**Echo Request (Solicitud de eco)**: se utiliza para determinar si un nodo IPv6 está disponible en la red.	
129	**Echo Reply (Respuesta de eco)**: se emplea para responder al mensaje de solicitud de eco ICMPv6.	

Fuente: Librería MSDN

2.9 Resolución de Nombres en IPv6

IPv6 fue diseñado para trabajar con direcciones de 128 bits de los hosts de origen y destino, lo cual resulta difícil para los usuarios utilizar y recordar direcciones de 32 dígitos hexadecimales para intentar acceder a los recursos de la red. Para esto, se puede utilizar nombres únicos, que son más sencillos de recordar.

Al utilizar un nombre para una dirección IPv6, es necesario asegurarse de que este sea único y que pueda resolverse en la dirección IPv6 correcta.

La resolución de nombres de host permite asignar correctamente un nombre de host a una dirección IPv6. Un nombre de host es un alias que se da a un nodo IPv6 para identificarlo como host IPv6. El nombre de un host puede tener un máximo de 255 caracteres e incluir caracteres alfabéticos y numéricos, guiones y puntos. Además, es posible asignar varios nombres al mismo host.

Los nombres de dominio se resuelven enviando consultas de nombres DNS a un servidor DNS configurado, este servidor resuelve el nombre de dominio consultado en una dirección IPv6 y devuelve el resultado. (Nuñez Lara, 2009) (Microsoft, 2005)

2.9.1 Resolución de dirección a nombres

El RFC 1886 define un nuevo tipo de registro de recursos para DNS denominado "AAAA" el cual es utilizado para resolver el nombre de un dominio completo para una dirección IPv6.

Estos registros obtienen este nombre porque las direcciones IPv6 de 128 bits de longitud son cuatro veces más grandes que las direcciones de 32 bits que se usan en IPv4. Un registro DNS tiene la siguiente estructura: Nombre, Tipo de Registro y Dirección, donde el nombre es el nombre del dominio completo, el tipo de registro corresponde al registro que se está usando sea en IPv4 (A) o IPv6 (AAAA) y la dirección es la dirección que está asociada con el nombre.

La figura 23 muestra un ejemplo de la estructura de un registro DNS para IPv6.

Nombre	Tipo de registro	Dirección
host1.microsoft.com	AAAA	FEC0::1:2AA:FF:FE3F:2A1C

Figura 23. Estructura del Registro DNS para IPv6

Fuente: Nuñez, D. (2009). Estudio para la Migración de IPv4 a IPv6 para la Empresa Proveedora de Internet MILLTEC. S. A. Recuperado de http://bibdigital.epn.edu.ec/bitstream/15000/1871/1/CD-2447.pdf

En DNS la asignación de una dirección IP a un nombre a menudo se denomina mapeo reverso, el RFC 1886 describe el IP6.INT, un dominio creado para responder inversamente a consultas de direcciones IPv6; a este dominio también se lo denomina como puntero (PTR).

DNS usa siempre un nombre como una etiqueta, por lo que las direcciones IP se convierten en un pseudo nombre con un domino de nivel superior. En IPv4 el dominio de nivel superior es "in-addr.arpa" y la dirección está escrita en cuatro etiquetas en orden inverso; por ejemplo, si el mapeo inverso para la dirección 192.0.1.2 es host1.example.org entonces el registro DNS es como se describe en la figura 24:

Nombre	Tipo de registro	Valor
2.1.0.192.in-addr.arpa	PTR	host1.ejemplo.org

Figura 24. Ejemplo de PTR en IPv4

Fuente: Nuñez, D. (2009). Estudio para la Migración de IPv4 a IPv6 para la Empresa Proveedora de Internet MILLTEC. S. A. Recuperado de http://bibdigital.epn.edu.ec/bitstream/15000/1871/1/CD-2447.pdf

El nombre en la parte izquierda del registro se construye invirtiendo la dirección IPv4 y añadiendo puntos entre cada dígito decimal y además añadiendo el sufijo "in-addr.arpa". La parte derecha del registro es el nombre del host asociado con la dirección IP.

IPv6 usa el mismo registro PTR pero construye la parte izquierda del registro añadiendo puntos entre cada dígito hexadecimal de la dirección IPv6 totalmente ampliada y con un diferente y alto nivel de nombre de dominios ("ip6.arpa"). Por ejemplo, si el mapeo inverso para la dirección 3FFE:B00:0:1::1 es host2.ejemplo.org, entonces el registro DNS es como se describe en la figura 25:

Nombre	Tipo de registro	Valor
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.0.0.0.0.0.0.0.b.0.e.f.f.3.ip6.arpa	PTR	host2.ejemplo.org

Figura 25. Ejemplo de PTR en IPv6

Fuente: Nuñez, D. (2009). Estudio para la Migración de IPv4 a IPv6 para la Empresa Proveedora de Internet MILLTEC. S. A. Recuperado de http://bibdigital.epn.edu.ec/bitstream/15000/1871/1/CD-2447.pdf

En la parte izquierda del registro de la dirección IPv6 (3FFE:B00:0:1::1) es ampliada con todos los ceros, y luego es invertida y se insertan los puntos entre cada dígito hexadecimal. Si una persona tuviera que escribir manualmente dígitos, existe una posibilidad muy grande de cometer errores; por esta razón las herramientas de configuración e interfaces de usuario son necesarias para gestionar IPv6 en DNS.

El mapeo inverso (PTR) es usado con menor frecuencia que el mapeo normal (A ó AAAA).

Es principalmente utilizado en los servidores para obtener un nombre de una dirección IP que solicite iniciar una comunicación; esto ayuda en la recopilación de estadísticas, búsqueda de problemas y en la seguridad básica. (Nuñez Lara, 2009)

2.10 Seguridad en IPv6

2.10.1 IPSec

La seguridad dentro del protocolo IPv6 está basada en el protocolo IPSec. Utiliza servicios de seguridad cripotográfica, para proteger comunicaciones sobre la red del protocolo IP. Una implementación de IPv6 incluye inserciones de Encabezados de Autenticación (AH, Authentication Headers) y extensión de encabezados de Carga de Seguridad Encapsulada (ESP, Encapsulating Security Payload). El tener IPSec en cualquier nodo debe permitir sesiones de seguridad de extremo a extremo. IPSec puede ser usado en diferentes áreas como se indica a continuación. (Microsoft, s.f.)

- ***OSPFv3***

  Utiliza AH, la extensión de encabezados maneja ESP como un mecanismo de autenticación reemplazando la variedad de esquemas de autenticación y procedimientos definidos en OSPFv2.

- **Túneles**

  Los túneles IPSec pueden ser configurados entre ruteadores IPv6, en lugar de que cada computadora utilice IPSec.

- ***Administración de Red***

  IPSec se puede utilizar para garantizar el acceso del ruteador para la gestión de la red.

IPSec está definido en dos extensiones de encabezado separados de IPv6 que pueden ser puestas juntas dentro del mismo paquete IPv6. Las dos extensiones son Autenticación de Encabezado IPSec (AH) y extensión de encabezados de Carga de Seguridad Encapsulada (ESP). (Chamba, 2015)

2.10.1.1 Servicios de Seguridad

IPSec utiliza dos tipos de servicios de seguridad, los cuales se describen a continuación:

2.10.1.2 Autenticación de Encabezado IPSec (AH)

El primer encabezado provee integridad, autenticación del nodo fuente y protección contra repetición. AH protege la integridad de la mayoría de los campos de encabezado de IPv6, con excepción de aquellos que cambian sobre la trayectoria, tal como lo hacen el campo Límite de Salto. Además, autentica la fuente a través de un algoritmo basado en una firma.

IPSec es obligatorio para IPv6 tal como lo indica el RFC 2460, el cual indica que todas las comunicaciones IP extremo-a-extremo deben ser seguras si existe suficiente infraestructura para hacerlo en una gran escala.

2.10.1.3 Carga de Seguridad Encapsulada IPSec (ESP)

Es el segundo encabezado IPSec, éste provee confidencialidad, autenticación del nodo fuente, integridad interna del paquete y protección contra repetición. (Network Information Center México S.C., 2013)

2.11 IPv6 en el Mundo y Latinoamérica

El despliegue de IPv6 en el mundo, tiene lugar, sin cambios rápidos, pero dependiendo del punto de vista de la red se puede observar su desarrollo.

En cuanto a las redes académicas, en Japón, Europa y Norteamérica se ha producido un despliegue muy importante, debido a las grandes inversiones públicas para fomentar el mismo. En el caso europeo, la Comisión Europea ha cofinanciado, junto con el sector privado, un gran número de proyectos de investigación y desarrollo, que a su vez han posibilitado a la industria, la adquisición de conocimientos y la culminación del desarrollo y la estandarización de IPv6.

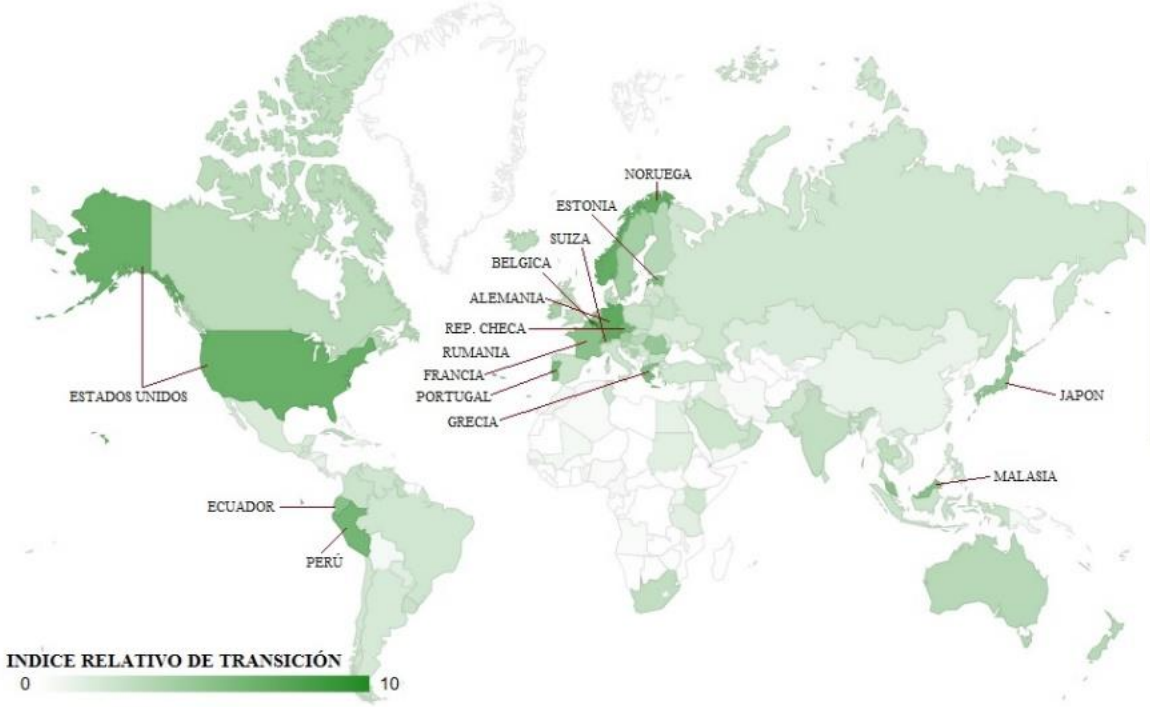
"Muchos países y regiones han adoptado políticas públicas, y recalcan que el despliegue de IPv6 no es caro si se planifica adecuadamente, es decir, con cierta anticipación, la cual depende del caso específico de cada red, y por tanto asegurándose que las adquisiciones de equipamiento, aplicaciones y servicios, tengan soporte de IPv6, de tal modo que no sea necesario realizar nuevas adquisiciones cuando se desee implementar IPv6.

Como consecuencia de este tipo de políticas públicas, en varios países y regiones de todo el mundo, hay fechas específicas para la activación obligatoria de IPv6 en las redes de la administración pública y otras redes relacionadas como educación, defensa, entre otras.

Desde el punto de vista de los grandes operadores de redes (carriers), que en su mayoría tienen redes intercontinentales, hace ya varios años han dado grandes pasos y tienen un soporte muy completo de IPv6.

La situación es muy diferente en la "última milla" ya que no han logrado explotar en su totalidad la implementación de IPv6, salvo excepciones notables sobre todo en Japón, algunos otros países asiáticos, y un reducido número de casos en Europa y Norteamérica." (Cicileo, y otros, 2009)

Combinando datos de Google y APNIC, es posible notar que las áreas con mayor visibilidad en cuanto a penetración de IPv6 son Bélgica, Suiza, Luxemburgo, Alemania, Estonia, Estados Unidos, Noruega, Francia, Alemania, República Checa, Rumania, Perú (principal representante de la región latinoamericana en la lista) y Ecuador, como se indica en la Figura 26. Resulta interesante, que áreas con trabajo estable en cuanto a IPv6, como Brasil y países asiáticos (entre los que destacan China y la India) aun no aparezcan en posiciones destacadas en la estadística. (Villa, 2015)



PAIS	DESPLIEGUE IPv6 (%)	USUARIOS (%)	INDICE RELATIVO DE TRANSICION (1-10)
Estados Unidos	34,76	14,1	6,8
Ecuador	34,59	3,87	5,3
Perú	31,91	11,6	6,2
Portugal	33,57	7,49	5,9
Noruega	39,18	9,68	6,9
Estonia	33,78	6,58	5,6
Alemania	39,35	13,8	7,1
Bélgica	49,49	32	10
Francia	30,45	5,46	5,2
Suiza	36,34	9,69	6,5
República Checa	32,72	8,87	6,3
Rumania	24,52	6,71	4,7
Grecia	29,65	7,32	5,4
Malasia	29,16	6,34	5,3
Japón	30,29	6,37	4,7

Figura 26. Cuadro estadístico de Transición a IPv6 en el mundo

Fuente: Recuperado de http://6lab.cisco.com/stats/index.php?option=all

"En el caso particular de la región de Latinoamérica y El Caribe, el mayor porcentaje de asignaciones IPv6 que ha realizado LACNIC han sido a Proveedores de Servicios de Internet (ISPs) y Registros Locales de Internet (LIRs); ubicándose en segundo lugar a nivel mundial en esta modalidad (después de Europa). En cuanto a asignaciones para organizaciones que no revenden servicios a terceros (conceptualizados como usuarios finales en este contexto), nuestra región únicamente supera a África. A pesar de estas cifras, LACNIC ostenta el mayor porcentaje de usuarios con bloques de direcciones IPv4 e IPv6.

El hecho de que la mayoría de quienes poseen prefijos IPv6 en Latinoamérica y el Caribe sean LIRs/ISPs hace presagiar que la región se encuentra actualmente en condiciones favorables para un crecimiento en el empleo de este protocolo. Brasil lidera ampliamente el total de asignaciones, seguidos a distancia por Argentina; mientras que Colombia, México y Chile les siguen los pasos, un poco más retirados." (Villa, 2015)

2.12 IPv6 en Ecuador

En la actualidad en Ecuador esta tecnología no se ha desarrollado en su totalidad, debido a la falta de información, conocimiento, o porque aún no es necesario que sea aplicada, pero esta tecnología avanza rápidamente y eventualmente se necesitará hacer uso de ella.

Las Instituciones de Educación Superior deben ser la base de información para que Ecuador adopte IPv6 como parte de su tecnología.

"IPv6 no resuelve todos los problemas de su antecesor, pero es la alternativa técnica y económica más adecuada a la realidad de nuestro país para afrontar el crecimiento futuro de la Internet. La transición a IPv6 en Ecuador se está iniciando y se requiere mayor difusión y capacitación, para esto es muy importante impulsar las actividades que podría ofrecer el IPv6TF-EC." (Mejía, 2012)

2.12.1 Resumen del estado de la implementación de IPv6 en Ecuador:

Bloques IPv6 asignados y utilizados (al 20 de agosto de 2012):

- 31 bloques IPv6 asignados/distribuidos por LACNIC a organizaciones ecuatorianas
- 19 bloques utilizados (vistos en el Internet Global)
- 16 organizaciones diferentes utilizan prefijos IPv6

Oferta de servicios son soporte de IPv6:

- El punto de intercambio de tráfico local de Internet (NAP.EC) tiene IPv6 nativo habilitado.
- Proveedores (ISP) que pueden proveer tránsito IPv6 nativo: 4
- Proveedores (ISP) que proveen servicio HOME con soporte IPv6 nativo: 0

El dominio .EC tiene servidores con IPv6 habilitado (uno de estos servidores está alojado en NAP.EC) y al adquirir un dominio es posible delegar la autoridad a servidores DNS con dirección IPv4 o IPv6 (glue A y AAAA). Una estadística de los dominios .EC con "glue AAAA" (delegados a servidores con dirección IPv6) es la siguiente (al 23 de agosto de 2012):

- Dominios de entidades sin fines de lucro (org.ec):1
- Dominios de entidades gubernamentales (gob.ec): 2
- Dominios de entidades educativas (edu.ec): 3
- Dominios de segundo nivel directo (.ec): 2

Páginas locales que se pueden acceder sobre IPv6:

- www.aeprovi.org.ec
- www.ipv6tf.ec
- www.cedia.org.ec
- www.mintel.gob.ec
- www.conatel.gob.ec
- www.nic.ec
- Páginas de algunas universidades ecuatorianas (Mejía, 2012)

2.13 Mecanismos de Transición de IPv4 a IPv6

Debido a que el protocolo más utilizado en la actualidad en Internet es el IPv4, no es posible su sustitución, es decir, no se puede apagar la red, ni siquiera por unos instantes y cambiar a IPv6. (Gobierno de España . Ministerio de Industria, Energía y Turismo., s.f.)

Una de las principales razones para el diseño de IPv6, fue que pudiera realizarse una transición suave hacia la nueva versión del protocolo IP, sin que fuera necesario pasar de una versión a otra en forma abrupta. (Guillermo, s.f.)

Se están desarrollando mecanismos que facilitan la realización y entendimiento de la transición de IPv4 a IPv6. Entre dichos mecanismos que permitirán esta convivencia y la migración progresiva tanto de las redes como de los equipos de usuario se pueden destacar los siguientes: (Boronat Seguí & Montagud Climent, 2013)

- Dual Stack o Doble Pila
- Túneles
- Mecanismos de Traducción

2.13.1 Dual Stack o Doble Pila

La doble pila hace referencia a una solución de nivel IP con doble pila de protocolos (RFC 4213: Mecanismos básicos de transición para hosts y ruteadores de IPv6), incluyendo de forma simultánea, tanto la pila de protocolos de IPv4 como la de IPv6 en cada dispositivo conectado a la red. Por tanto, cada dispositivo tendrá dos direcciones IP, una IPv4 y otra IPv6. Esto permite a los dispositivos establecer sesiones utilizando cualquiera de los dos protocolos según sus necesidades. Se trata de una solución fácil de implementar y ampliamente soportada, lo cual facilita el despliegue de IPv6. (Boronat Seguí & Montagud Climent, 2013)

De esta forma, cuando se establece una conexión hacia un destino sólo IPv4, se utilizará la conectividad IPv4 y si el destino es una dirección IPv6, se utilizará la red IPv6. En caso que el destino tenga los dos protocolos, normalmente se preferirá intentar

conectar primero por IPv6 y en segunda instancia por IPv4, como se muestra en la Figura 27. (Guillermo, s.f.)

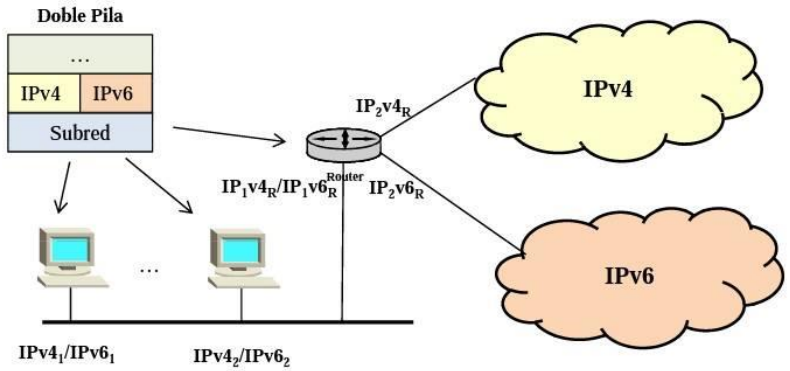


Figura 27.Doble Pila o Dual Stack

Fuente: Boronat, F. (2013). Direccionamiento e Interconexión de Redes basada en TCP/IP (IPV4/IPV6, DHCP, NAT, Encaminamiento RIP y OSPF)

2.13.2 Túneles

Esta técnica permite interconectar las nubes IPv6 a través de un servicio IPv4 nativo por medio de un túnel. Los paquetes IPv6 son encapsulados por un router de extremo antes de ser transportado a través de la red IPv4, siendo desencapsulados en el extremo de la red IPv6 receptora, como se muestra en la Figura 28.

Se trata de una medida temporal, ya que, en el futuro, IPv4 irá desapareciendo paulatinamente y todos los dispositivos implementarán IPv6 de forma nativa.

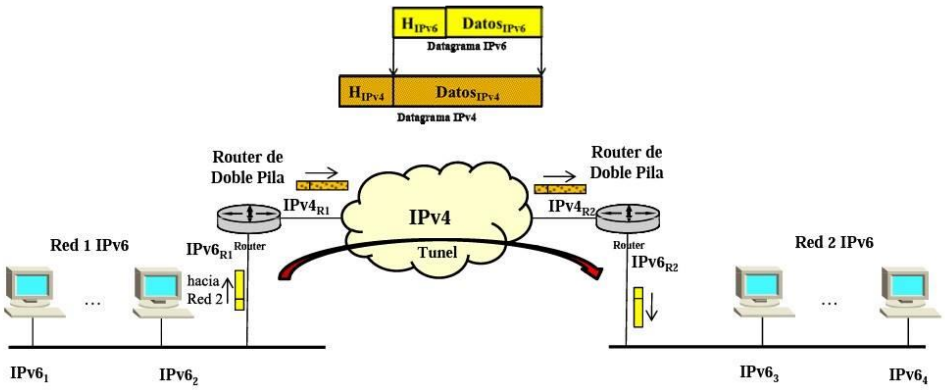


Figura 28.Tunneling IPv6

Fuente: Boronat, F. (2013). Direccionamiento e Interconexión de Redes basada en TCP/IP (IPV4/IPV6, DHCP, NAT, Encaminamiento RIP y OSPF)

2.13.2.1 Tipos de Túneles

Se pueden encontrar diferentes tipos de túneles:

2.13.2.1.1 6to4

6to4 es un mecanismo de túnel utilizado para transferir paquetes del Protocolo de Internet Versión 6 encapsulados dentro de paquetes IPv4, para atravesar redes solo IPv4.

6to4 es una técnica de creación de túneles automáticos que proporciona comunicación entre islas IPv6 de manera transparente al usuario IPv6. 6to4 ofrece conectividad unicast entre sites IPv6 a través de una red IPv4, utilizando a ésta última como conexión punto a punto entre los dos routers que forman el túnel (routers dual-stack en la frontera entre sites IPv4 e IPv6). (Sánchez, 2014)

El mecanismo 6to4 se creó para apoyar la coexistencia de las dos versiones durante la transición a IPv6, que se espera llevará años.

2.13.2.1.2 6OVER4

6OVER4 es similar a 6to4 con la diferencia de que se utiliza en los dispositivos finales. Es un proceso simple y de fácil configuración. Los dispositivos finales deben soportar IPv4 e IPv6.

6OVER4 también es conocido como el tunneling multicast IPv4, es una tecnología de túneles automáticos ya sea de equipo a equipo, de equipo a router o de router a equipo, que provee conectividad unicast y multicast IPv6 entre nodos IPv6 a través de una intranet IPv4. Esta técnica se encuentra definida en el (RFC 2529: Transmisión de dominios IPv6 sobre IPv4 sin túneles explícitos). (Ahuatzin Sánchez, 2005)

2.13.2.1.3 Teredo

Los túneles Teredo encapsulan datagramas IPv6 en segmentos UDP sobre IPv4 y trabajan de manera similar a los mecanismos anteriores, con la ventaja de que pueden

atravesar redes que estén utilizando NAT (como los routers domésticos). Existen nodos denominados Teredo relays, que tienen acceso a la red IPv6, reciben los datagramas IPv4 por su conexión a la red IPv4, los desencapsulan y reenvían por la red IPv6. (Boronat Seguí & Montagud Climent, 2013)

Teredo se compone de tres elementos: un servidor Teredo, un retransmisor Teredo y un cliente Teredo.

El servidor provee la dirección IPv4 al cliente; una vez que el cliente aprende la dirección IPv4, automáticamente construirá la dirección IPv6 del servidor donde la dirección de IPv4 está incrustada. El retransmisor ayuda a los clientes a conectarse a hosts de solo IPv6. Las comunicaciones de hosts solo IPv6 en el "backbone" no están soportadas de forma inmediata.

En lugar de eso, el servidor Teredo mediará entre los clientes Teredo y los retransmisores Teredo y seleccionará el apropiado, el cual es seleccionado por la distancia entre el cliente y el retransmisor, así como el número de clientes a los cuales les provee servicio el retransmisor.

El cliente Teredo es un nodo que reside detrás de un NAT y que desea tener conectividad IPv6. Para la configuración de la dirección, el cliente obtiene el prefijo del servidor; especialmente, se requiere que el cliente tenga una dirección IPv4 antes del proceso de calificación con el fin de mantener el mapeo de dirección y número de puerto asociado con el puerto de servicio Teredo. (Network Information Center México S.C., 2013)

2.13.2.1.4 Tunnel Broker

Consiste en un túnel IPv6 dentro de la red IPv4, creado en el propio computador o red hasta el proveedor que va a brindar la conectividad IPv6. El procedimiento consiste en registrarse en un proveedor de acceso Tunnel Broker y descargar un software o script de configuración que permita establecer este túnel.

La conexión del túnel se realiza a través de una solicitud en el servidor web del proveedor que ofrece este servicio, es indicado para redes pequeñas o para un host único independiente. (Alonso, 2008)

2.13.2.1.5 ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

Permite conectar dispositivos con doble pila a través de redes IPv4. Los dispositivos con doble pila utilizan ISATAP para encapsular datagramas IPv6 en datagramas IPv4, utilizando la red IPv4 como un nivel de enlace o subred subyacente para IPv6. A diferencia de 6to4, ISATAP utiliza IPv4 como un nivel de enlace de una red de acceso múltiple sin broadcast, por lo que no requiere que la red IPv4 subyacente soporte multicast. ISATAP está implementado en los últimos sistemas operativos de Microsoft, incluso para dispositivos móviles, así como en algunas versiones de Cisco IOS[1]. (Boronat Seguí & Montagud Climent, 2013)

2.13.3 Mecanismos de Traducción

Consiste en utilizar un dispositivo en la red que convierta los paquetes de IPv4 a IPv6 y viceversa. Ese dispositivo tiene que ser capaz de realizar la traducción en los dos sentidos deco el fin de permitir la comunicación, como se muestra en la Figura 29. (Cicileo, Portal IPv6, 2012)

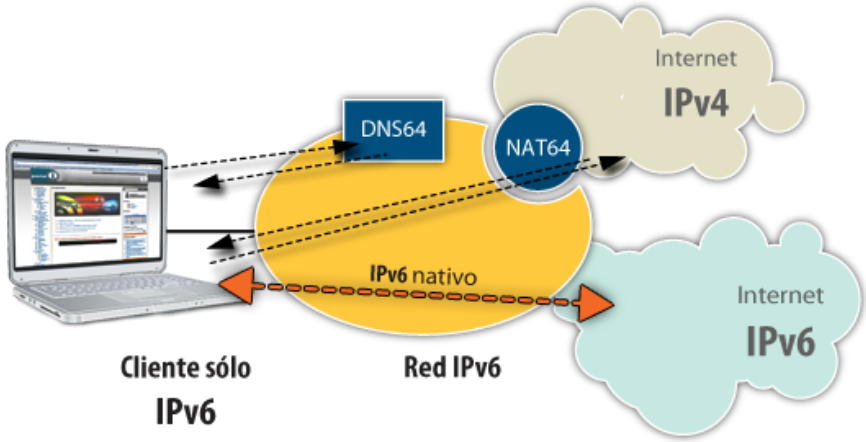


Figura 29. Mecanismos de Traducción

Fuente: Recuperado de http://www2.lacnic.net/newportalipv6/wp-content/uploads/2013/06/mec_red_sp.png

[1] IOS: sistema operativo de los dispositivos de Cisco, es un paquete de funciones de enrutamiento, conmutación, que se integra estrechamente con un sistema operativo multitarea.

La traducción será necesaria, cuando un dispositivo que sólo soporta IPv4 intente comunicarse con otro dispositivo que sólo soporte IPv6, es considerada una estrategia a corto plazo pero que permite coexistir a los dos protocolos para facilitar su transición a la red IPv6.

Las aplicaciones que utilizan protocolos que incluyen información IP en la porción de datos (como FTP o SIP) requieren la implementación de gateways de capa de aplicación para soportar la traducción. (Gerometta, Mis Libros de Networking, 2015)

Hay varias tecnologías disponibles para realizar estas traducciones tales como:

- NAT-PT: Network Address Translation – Protocol Translation
- SIIT: Stateless IP/ICMP Translation
- BIS: Bump In the Stack
- TRT: Transport Relay Translator

2.13.3.1 NAT-PT

Es un mecanismo de traducción IPv6-IPv4, que fue diseñado para permitir que los dispositivos que soportan solo IPv6 se comuniquen con los dispositivos que sólo soporten IPv4 y viceversa.

El funcionamiento del mecanismo NAT-PT consiste en:

a. Las direcciones IPv6 a IPv4 definen direcciones falsas IPv6 empleando una dirección IPv4 de destino y anteponiendo el prefijo NAT. Para poder establecer comunicaciones de datos se debe configurar en el NAT-PT con un prefijo de 96 bits. En consecuencia, el NAT-PT examina los paquetes para identificar direcciones falsas, y finalmente traduciendo el paquete a IPv4.

b. Las direcciones IPv4 a IPv6 funcionan como un NAT bidireccional, donde la traducción es semejante al inciso a), generando un paquete IPv6 con dirección origen, mientras que la dirección falsa IPv6 contiene internamente una

dirección IPv4 de tal manera se inicia la comunicación. (Coellar Solórzano & Cedeño Mendoza, 2013)

Una de las propuestas iniciales de mecanismos de traducción fue NAT-PT (RFC 2766), que al día de hoy ha sido desaconsejado debido a sus fallas (RFC 4966) y ha sido reclasificado como "histórico" por la IETF. (Cicileo, Portal IPv6, 2012)

2.13.3.2 SIIT

La traducción IP/ICMP sin estado (asíncrona) es un algoritmo que traduce entre encabezados de paquetes IPv4 e IPv6 (incluyendo los encabezados ICMP), puede usarse como la parte de una solución que permite hosts IPv6 qué no tiene una dirección IPv4 permanentemente asignada, se comuniquen con hosts solo IPv4. Es decir, permite a PCs que poseen IPv6 comunicarse con PCs que tienen IPv4.

Con la aplicación de un traductor de protocolo, es posible adaptar la nueva red solo IPv6 internamente y tener clientes IPv6 que accedan mediante la Internet IPv4 normal o cualquier otro nodo IPv4. (Sánchez Pinos, 2006)

2.13.3.3 BIS

El mecanismo BIS (Bump in the Stack) permite a hosts que utilizan Dual Stack comunicarse con hosts IPv6 utilizando aplicaciones IPv4. Puede resultar muy útil para aquellas aplicaciones que no han migrado a IPv6 para así establecer comunicación entre hosts IPv6. En consecuencia, cuando las aplicaciones IPv4 buscan comunicarse con aplicaciones IPv6, éste realiza el mapeo entre una dirección IPv6 y una dirección IPv4.

Se encarga de traducir aplicaciones IPV4 y redes situadas por debajo de IPV6, es decir el controlador de interfaz de red. Básicamente el diseño del stack consta de una pila dual stack, en el cual añade tres módulos, un traductor, un nombre de la extensión de la resolución y la dirección de un mapeado.

Admite que los hosts se conviertan en traductores autónomos, para lo cual ya no es necesario un traductor externo. Está ubicado en el área de seguridad del protocolo de

internet (IP), y posteriormente es el encargado de verificar los datos que pasan entre TCP/IPv4 y una interface de red, además de traducirlos a IPv6 y viceversa.

Permite la comunicación de hosts IPv4 a IPv6, pero no existe comunicación IPv6 a IPv4. Es imposible enviar o recibir algún paquete IPv4 para la red, por lo que, si una aplicación IPv4 pretende comunicarse con otra aplicación IPv4 a través del BIS, se produce un error si no hay mecanismos de traducción adicionales en algún lugar de la ruta de comunicación. (Coellar Solórzano & Cedeño Mendoza, 2013)

2.13.3.4 TRT

El mecanismo TRT (Traducción en capa de Transporte) especificado por el RFC3142, establece que los hosts IPv6 intercambien el tráfico TCP o UDP con hosts IPv4. Es decir, que permite comunicarse directamente entre aplicaciones IPv6 e IPv4. Actúa a nivel de la capa de transporte, y a diferencia del BIS, actúa como una pasarela entre ambos protocolos, estableciendo una conexión para IPv6 y otra para IPv4 permitiendo el reenvío de paquetes entre ambas direcciones.

Ninguna modificación de los hosts es necesaria, el sistema TRT puede ser muy fácil de instalar en las redes con capacidades de IPv6. El mecanismo TRT es traducido y ejecutado en un nodo dual stack para así establecer la comunicación con un host o con el servidor. (Coellar Solórzano & Cedeño Mendoza, 2013)

2.14 NAT64

NAT64 es un mecanismo que permite a hosts con conectividad solo IPv6 comunicarse con hosts con conectividad solo IPv4.

La estructura para el NAT64 está definida en el RFC 6144, allí se define el marco para la traducción IPv4/IPv6. Dicha estructura debe tener los siguientes componentes:

- Traducción de direcciones
- Traducción de IP y ICMP
- Mantenimiento de estado de traducción

- DNS64
- ALG para protocolos de capa de aplicación

Un traductor de IP/ICMP tiene dos modos posibles de operación: stateles y stateful (RFC 6144). De esta forma NAT64 puede implementarse en modo stateless (RFC 6145) o modo stateful (RFC 6146).

Para lograr este objetivo se debe contar con un equipo de red que sea capaz de realizar una traslación de protocolos IPv4 a IPv6 y viceversa como se muestra en la Figura 30. Entre otras cosas, en este mapeo se debe incluir el mapeo de las direcciones de capa de red de los dos protocolos.

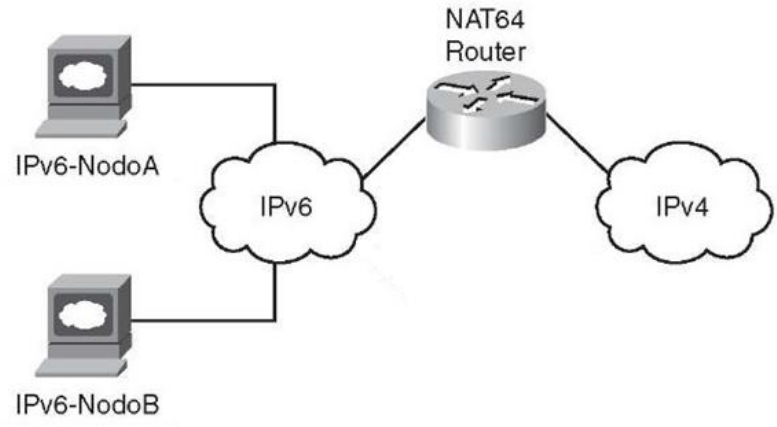


Figura 30. NAT64

Fuente: Recuperado de http://what-when-how.com/wp-content/uploads/2011/09/tmp1929_thumb.jpg

Del lado de la red solo IPv6, las direcciones IPv4 se mapean dentro de un prefijo IPv6 el cual debe tener suficientes bits de host para mapear todo el espacio IPv4. Normalmente se utiliza el prefijo 64::ff9b/96. (Universidad de la República de Uruguay, 2014)

2.14.1 Diferencias entre Stateless y Stateful NAT64

Tabla 15. Cuadro de diferencias Stateless y Stateful en NAT64

Stateless	Stateful
Traducción 1:1 (utiliza una dirección IPv4 por cada host IPv6)	Traducción 1:N
Los sistemas IPv6 deben tener direcciones IPv4-traducibles. No preserva las direcciones IPv4	Los sistemas IPv6 pueden usar cualquier tipo de direcciones IPv6. Mantiene las direcciones IPv4.

El flujo no crea estado en el traductor, se aplica algoritmo a los encabezados.	Cada flujo crea un estado en el traductor, basado en el número de traducciones.
Asegura transparencia de direcciones de extremo a extremo y escalabilidad.	Usa sobrecarga de direcciones, debido a que carece de transparencia de extremo a extremo.

Fuente: Recuperado de http://prueba.rau.edu.uy/index.php/introduccion/84-nat64

2.15 DNS64

Para que los hosts solo IPv6, puedan comunicarse con los hosts solo IPv4 hace falta un componente adicional que hace la traducción a nivel de DNS. Este es el rol del DNS64, el cual se encarga de recibir las consultas DNS de los hosts solo IPv6 y modificar las respuestas de tal manera de incluir registros AAAA que mapean las direcciones IPv4 dentro del prefijo NAT64 (RFC 6147[2]).

Ambos mecanismos permiten a un cliente IPv6 iniciar una comunicación con un servidor solo IPv4. También permiten la comunicación peer-to-peer entre un nodo IPv4 y uno IPv6, donde la comunicación puede haber sido inicializada por un extremo que usa NAT o técnicas de comunicaciones peer-to-peer, como se muestra en la Figura 31.

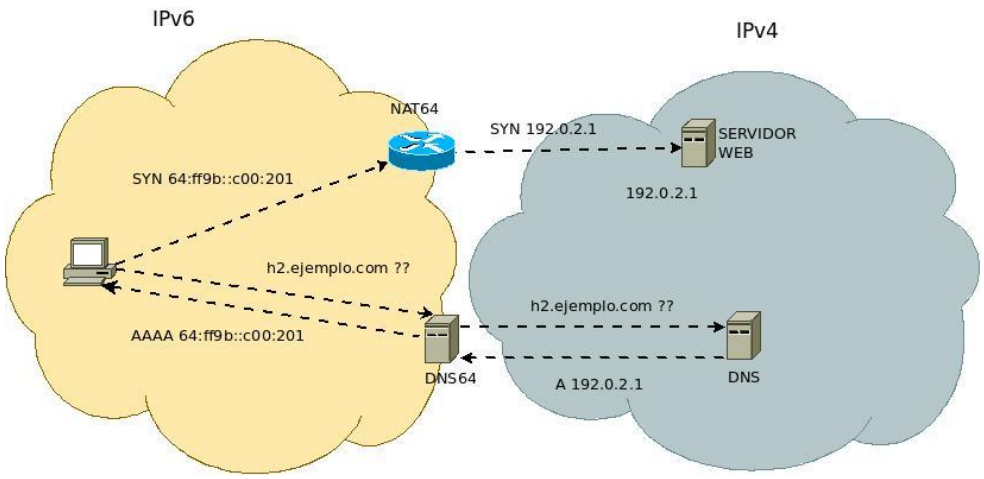


Figura 31. Esquema DNS64 y NAT64

Fuente: Recuperado de http://prueba.rau.edu.uy/index.php/joomlaspanishorg/proyecto-ipv6/mecanismos-de-transicion/60-dns64

[2] RFC 6147: DNS64. Extensiones DNS para la traducción de direcciones de red de clientes IPv6 a servidores IPv4

Para permitir a un nodo IPv6 que inicia una comunicación con un nodo IPv4, hacer consultas al DNS acerca del nodo IPv4 con el cual se quiere comunicar, se usa el DNS64. El DNS64 se utiliza para resumir los registros AAAA a partir de los registros A. La dirección IPv6 contenida en el registro AAAA contiene un prefijo Pref64::/n. El NAT64 debe procesar solamente paquetes entrantes que contenga una dirección destino que pertenezcan al pool de direcciones IPv4 asignadas al NAT64. (Universidad de la República de Uruguay, 2014)

Capítulo 3

3. Situación Actual

En este capítulo se analiza la Infraestructura de Red del Gobierno Provincial de Imbabura, luego se realizarán las fichas técnicas de cada uno de los equipos, servicios y aplicaciones que conforman esta red para finalizar realizando un inventario de la información recolectada.

3.1 Contexto de la Institución

3.1.1 Prefectura de Imbabura

3.1.1.1 Ubicación

La Prefectura de Imbabura se encuentra ubicada en la ciudad Ibarra, entre las calles Simón Bolívar y Miguel Oviedo, tal como se muestra en la Figura 32.

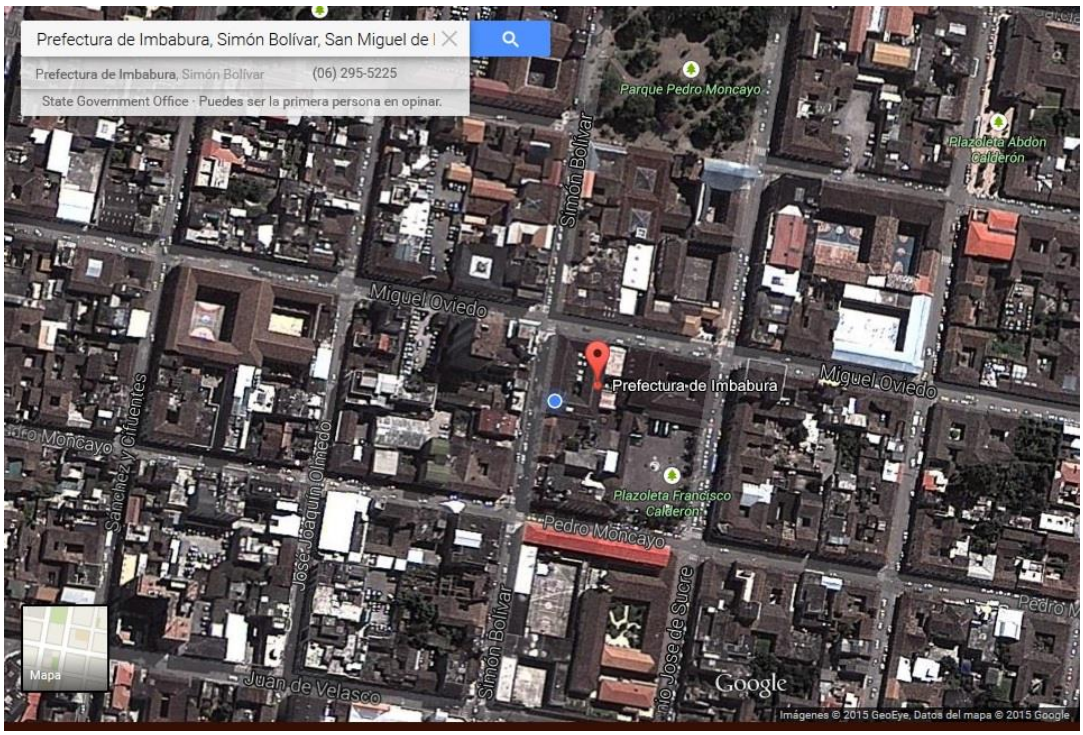


Figura 32. Ubicación Prefectura de Imbabura

Fuente: Recuperado de https://www.google.com.ec/maps/place/Prefectura+de+Imbabura/@0.3497107,-78.1174803,381m/data=!3m1!1e3!4m2!3m1!1s0x8e2a3cb64702d561:0xfb2189edff787e1b?hl=es-419

3.1.1.2 Objetivos Estratégicos

- "Fomentar el desarrollo económico provincial
- Consolidar el sistema de transporte y movilidad provincial
- Implementar el sistema de gestión ambiental provincial con enfoque intercultural y visión de cuenca hidrográfica
- Diseñar políticas, planes y programas, tendientes a fortalecer la inclusión social, el desarrollo cultural que permitan hacer de Imbabura una provincia equitativa, solidaria e intercultural.
- Generar mecanismos de articulación y lineamientos para la coordinación endógena institucional e interinstitucional.
- Tecnificar los procesos de administración y gestión institucional." (Prefectura de Imbabura, 2015)

3.1.1.3 Misión

"La Prefectura de Imbabura se consolida como una institución de derecho público, autónoma, descentralizada, transparente, eficiente, equitativa, incluyente y solidaria; líder del desarrollo económico, social y ambiental provincial." (Prefectura de Imbabura, 2015)

3.1.1.4 Visión

"La Prefectura de Imbabura es la institución encargada de coordinar, planificar, ejecutar y evaluar el Plan de Desarrollo Provincial Participativo; fortaleciendo la productividad, la vialidad, el manejo adecuado de sus recursos naturales y promoviendo la participación ciudadana; a fin de mejorar la calidad de vida de sus habitantes." (Prefectura de Imbabura, 2015)

3.1.2 Dirección de Tecnologías de la Información y Comunicaciones (TICs)

3.1.2.1 Objetivos

- Garantizar el buen funcionamiento de toda la red informática.

- Mantener y evaluar de manera continua los procesos que se operan en las unidades administrativas, financieras y operacionales de la Prefectura de Imbabura.

- Ofrecer asesoría y asistencia técnica en el área de redes y sistemas de información.

- Gestionar las mejoras tecnológicas para el buen funcionamiento de los recursos computacionales con que cuenta la Institución.

3.1.3 Topología Física de la Red

La Prefectura de Imbabura cuenta con un cuarto de equipos de comunicación ubicado en la planta alta 1 del edificio principal, al cual está conectado las diferentes dependencias y pisos del ya mencionado edificio principal. La Figura 33 indica la Topología Física de la Red.

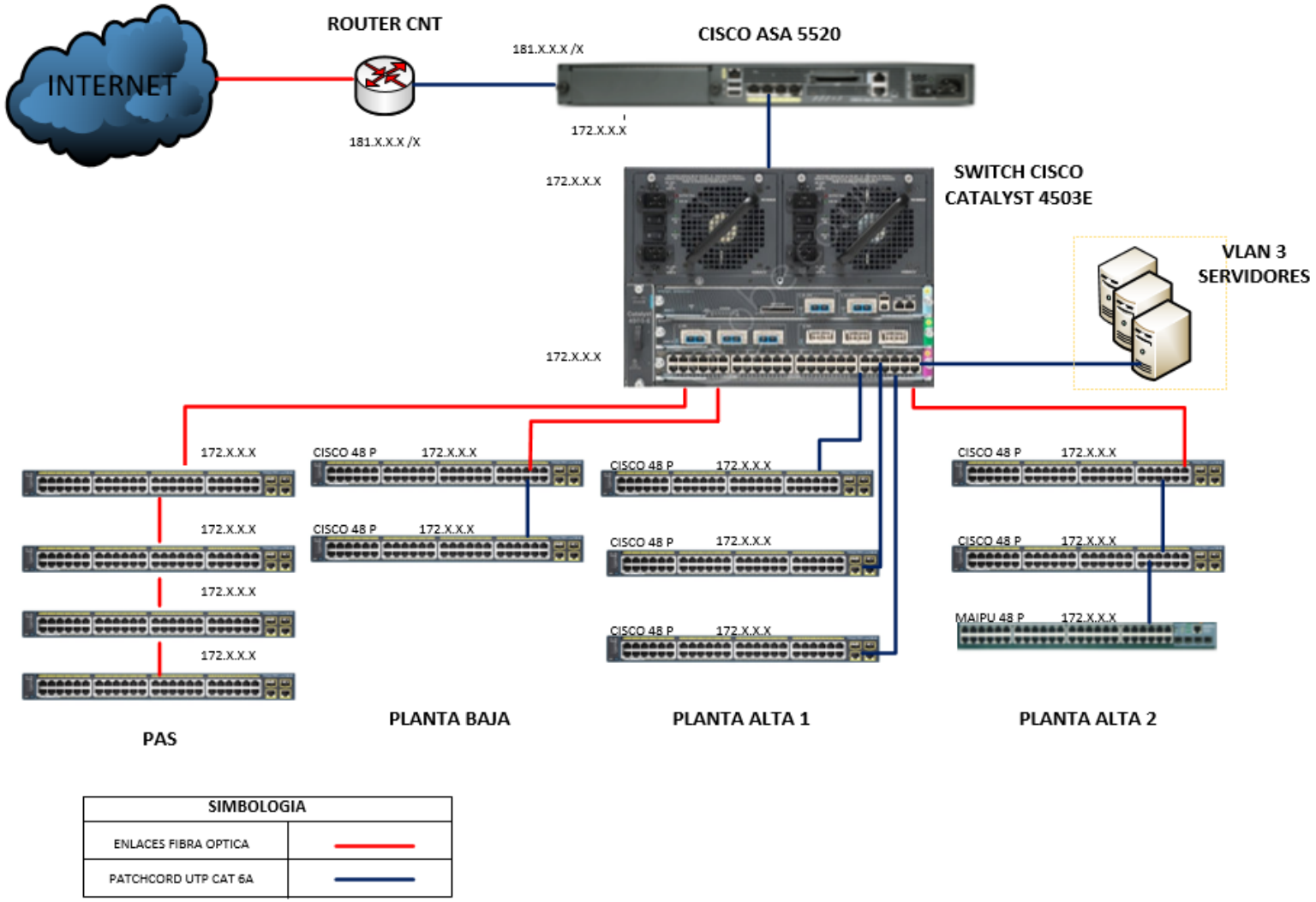


Figura 33. Topología Física de la Red

Fuente: Prefectura de Imbabura

3.1.4 Cuarto de Equipos de Comunicación

El Cuarto de Equipos de comunicación está ubicado en la Dirección de Tecnologías de la Información del edificio principal, éste cuenta con los siguientes elementos, como se muestra en la Figura 34.

- CISCO ASA 5520
- Switch CISCO 4503E (CORE)
- 3 Switch CISCO Catalyst 2960S
- Switch CISCO Catalyst 2960X
- Armario de Servidores

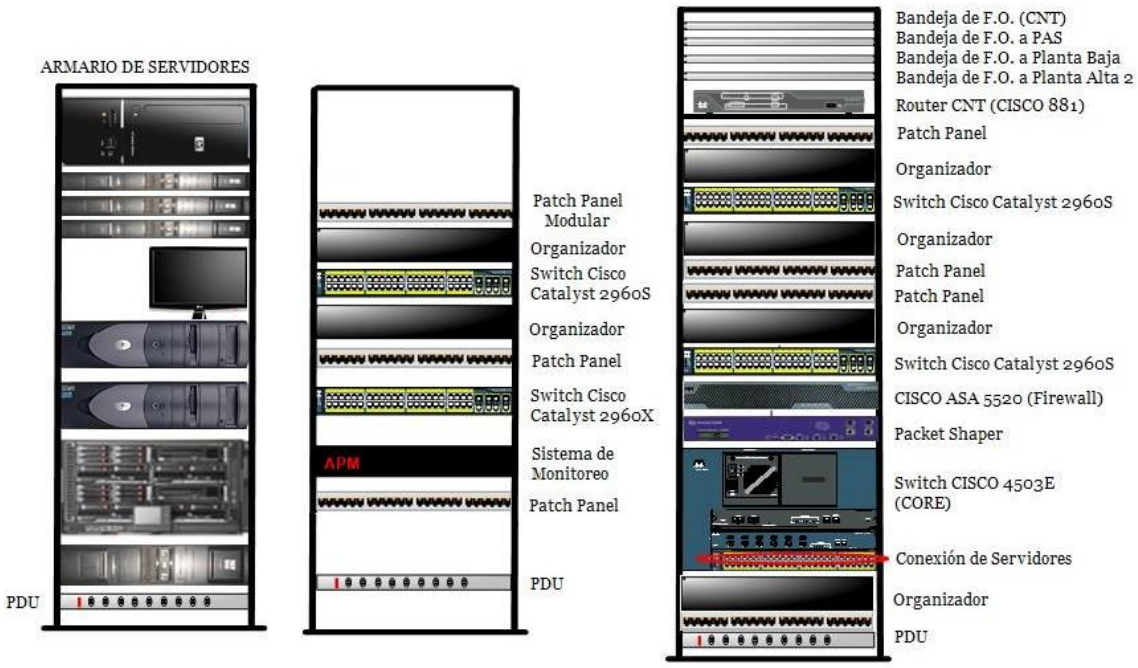


Figura 34. Distribución de Equipos Activos

Fuente: Prefectura de Imbabura

3.1.4.1 Distribución de equipos de la Planta baja y Planta alta 2

Estos equipos permiten la interconexión con el cuarto de comunicación principal, y cuenta con:

- 4 Switch CISCO 2960S
- Switch MAIPU MyPower S3152

Las figuras 35 y 36 indican la distribución de equipos de Planta baja y Planta alta 2 respectivamente.

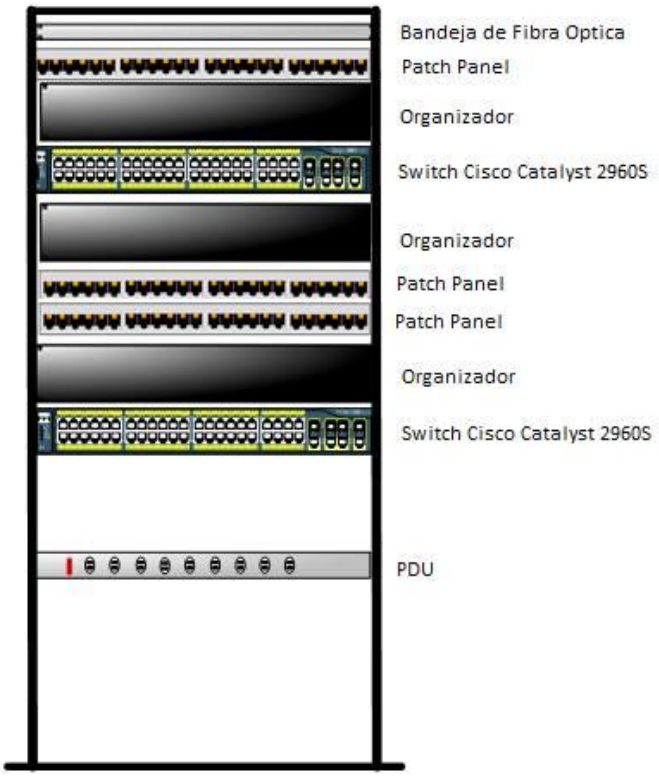


Figura 35. Distribución de equipos Planta baja

Fuente: Prefectura de Imbabura

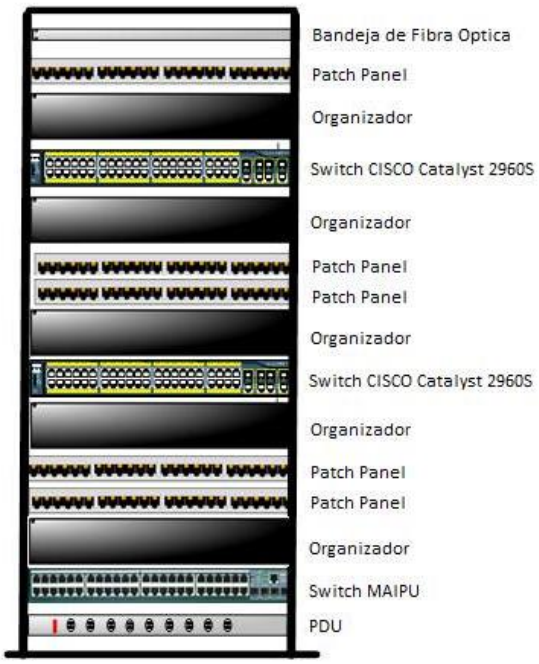


Figura 36. Distribución de equipos Planta alta 2

Fuente: Prefectura de Imbabura

3.1.4.2 Armario de Servidores

El cuarto de comunicaciones alberga varios servidores, los cuales se listan a continuación:

- Servidor de Telefonía IP
- Servidor de Streaming de Video
- Servidor Sistema Financiero Contable
- Servidor Geolocalización
- Servidor Ambiente de Desarrollo
- Servidor de Relojes Biométricos
- Servidor de Cámaras
- Servidor DNS
- Servidor Proxy
- Servidor Cloud
- Servidor de Gestión Documental
- Servidor de Desarrollo de Software

- Servidor de Licenciamiento
- Servidor de Archivos
- Servidor Web

Para este proyecto se realizará la coexistencia del Servidor Web y Servidor DNS. Estos se encuentran alojados en distintos equipos, los cuales se muestran en las Fichas Técnicas del Anexo A. El Servidor Blade Alberga la mayoría de Servidores, este cuenta con una distribución de 12 cuchillas divididas en 3 partes:

- 2 Servidores HP Proliant BL460c Generación 7
- 1 Servidor HP Proliant BL460c Generación 8

Dentro del Armario de servidores se ubica un dispositivo para almacenamiento y además varios equipos que se utilizan como servidores, que de igual manera se muestran en al Anexo A.

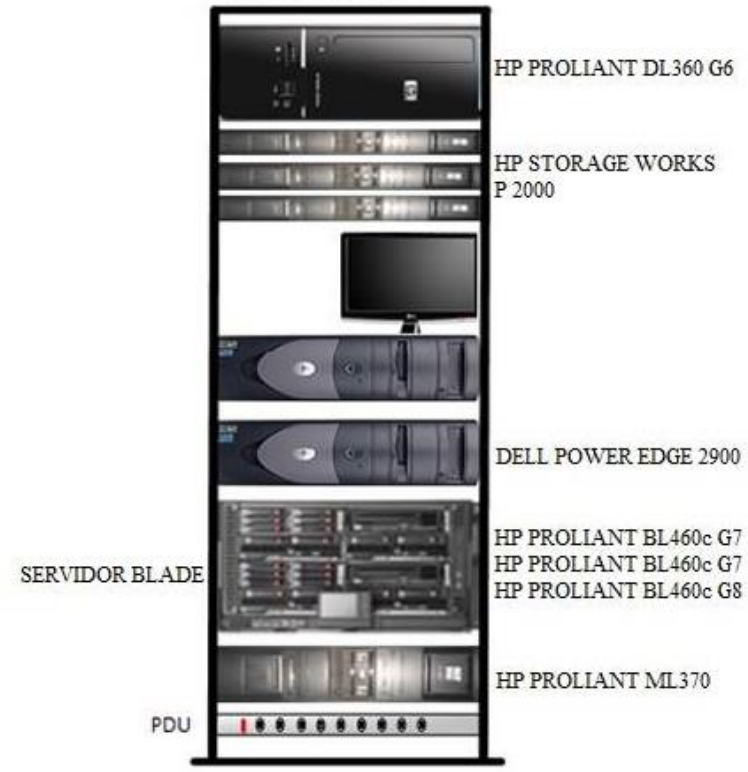


Figura 37. Armario de Servidores

Fuente: Prefectura de Imbabura

3.2 Red Interna de la Prefectura de Imbabura

3.2.1 Conexión a la Internet

La Red de la Prefectura de Imbabura se encuentra conectada hacia Internet mediante el proveedor de servicios CNT el cual brinda un ancho de banda de 30 [Mbps], con el límite de que la Red Inalámbrica del Edificio Principal es de 3 [Mbps].

3.2.2 Estructura Física

3.2.2.1 Cableado Estructurado

Desde el cuarto de comunicaciones, parte la interconexión de los enlaces de Fibra Óptica entre pisos y también el enlace con las oficinas del PAS (Patronato de Acción Social), y a su vez, todas las instalaciones de cableado estructurado horizontal de las áreas cercanas a éste.

El cable instalado en cada uno de los puntos de datos es de cobre, tipo UTP cat6A marca HUBBELL, y cumple con parámetros y todas las características TIA/EIA 568-B.2-1, todo con su respectivo sistema de etiquetado.

El sistema de ductería se encuentra instalado sobre el cielo falso de cada una de las oficinas de edificio, con un fin estético para la ubicación de puntos.

3.2.2.2 Backbone de Fibra Óptica

El Sistema de Cableado de Fibra Óptica corresponde a un mismo fabricante, la Fibra Óptica instalada entre pisos del edificio es de tipo OM3 con una velocidad de transmisión de 10Gbps, además posee protección para defensa contra roedores.

La conexión entre el edificio de la Prefectura de Imbabura y el Patronato (PAS), se encuentra vía subterránea, con sus respectivas normas y estándares.

3.2.2.3 Equipos de Red

El proveedor de servicios se conecta a la red a través de un Router CISCO 881 el cual se enlaza a un Switch CISCO ASA 5520 el cual cumple las funciones de Firewall, a continuación, se conecta el Switch de CORE, este equipo tiene características y funciones de Capa 3, y es el encargado de recibir todos los enlaces de Conexión de Fibra Óptica Entre Edificios y entre pisos del mismo edificio donde está ubicado.

Los Switchs CISCO 2960, tienen características y funciones de capa 2, son administrables y permiten la interconexión de todos los usuarios a la Red de la Prefectura de Imbabura, que actualmente son alrededor de 250, los cuales utilizan diferentes tipos de aplicaciones y servicios.

Las Características y Especificaciones, se muestran en el Anexo A, de las Fichas Técnicas de los Equipos.

3.3 Análisis de Fichas Técnicas

Después de haber analizado las características y especificaciones de los equipos en las fichas técnicas se puede observar, que todos los equipos de red son compatibles con IPv6, por tal razón se determina que la infraestructura de red no presentará inconvenientes para una futura implementación.

Es importante señalar que cada uno de los equipos brinda distintas funcionalidades de IPv6, por lo tanto, facilitarán la coexistencia entre protocolos.

3.4 Distribución de Direcciones IPv4 de la Prefectura de Imbabura

La red se encuentra conectada mediante IPv4 con la dirección pública X.X.X.X/X la cual permite un direccionamiento IP privado dividido en 24 VLANs con dirección 172.X.X.X /X, el cual esta mostrado en la tabla 16

Tabla 16. Distribución de VLANS

NOMBRE VLAN	ID VLAN	RED	GATEWAY	INTERVALOS	BROADCAST
ADMIN_EQUIPOS	2	172.X.X.X/X	172.X.X.X	172.X.X.X – 172.X.X.X	172.X.X.X
SERVIDORES	3	172.X.X.X/X	172.X.X.X	172.X.X.X– 172.X.X.X	172.X.X.X
GESTION_TECNOLOGICA	4	172.X.X.X/X	172.X.X.X	172.X.X.X – 172.X.X.X	172.X.X.X
PREFECTURA	5	172.X.X.X/X	172.X.X.X	172.X.X.X – 172.X.X.X	172.X.X.X
PROCURADURIA	6	172.X.X.X/X	172.X.X.X	172.X.X.X – 172.X.X.X	172.X.X.X
PLANIFICACION	7	172.X.X.X/X	172.X.X.X	172.X.X.X – 172.X.X.X	172.X.X.X
GESTION_TECNICA	8	172.X.X.X/X	172.X.X.X	172.X.X.X – 172.X.X.X	172.X.X.X
RELACIONES_PUBLICAS	9	172.X.X.X/X	172.X.X.X	172.X.X.X – 172.X.X.X	172.X.X.X
ADMIN_GENERAL	10	172.X.X.X/X	172.X.X.X	172.X.X.X – 172.X.X.X	172.X.X.X
INFRAESTRUCT_FISICA	11	172.X.X.X/X	172.X.X.X	172.X.X.X – 172.X.X.X	172.X.X.X
DESARROLLO_ECONOM	12	172.X.X.X/X	172.X.X.X	172.X.X.X – 172.X.X.X	172.X.X.X
PAS	13	172.X.X.X/X	172.X.X.X	172.X.X.X – 172.X.X.X	172.X.X.X
WIFI	20	172.X.X.X/X	172.X.X.X	172.X.X.X - 172.X.X.X	172.X.X.X
WIFI_EXTERNA	15	172.X.X.X/X	172.X.X.X	172.X.X.X - 172.X.X.X	172.X.X.X
BODEGA	16	172.X.X.X/X	172.X.X.X	172.X.X.X – 172.X.X.X	172.X.X.X
FAUSTO-GIS	17	172..X.X/X	172.X.X.X	172.X.X.X – 172.X.X.X	172.X.X.X
FISCALIZACION	18	172.X.X.X/X	172.X.X.X	172.X.X.X – 172.X.X.X	172.X.X.X
CONTRATACIÓN PÚBLICA	19	172.X.X.X/X	172.X.X.X	172.X.X.X – 172.X.X.X	172.X.X.X
INVITADOS	30	172.X.X.X/X	172.X.X.X	172.X.X.X – 172.X.X.X	172.X.X.X
RELOJES_BIOM	31	172.X.X.X/X	172.X.X.X	172.X.X.X - 172.X.X.X	172.X.X.X

CAMARAS	32	172.X.X.X/X	172.X.X.X	172.X.X.X - 172.X.X.X	172.X.X.X
TELEFONIA	40	172.X.X.X/X	172.X.X.X	172.X.X.X – 172.X.X.X	172.X.X.X
MUTUALISTA	50	172.X.X.X/X	172.X.X.X	172.X.X.X – 172.X.X.X	172.X.X.X
ENLACE_EQUIPOS	101	172.X.X.X/X	172.X.X.X	172.X.X.X - 172.X.X.X	172.X.X.X

Fuente: Prefectura de Imbabura

Capítulo 4

4. Metodología de Transición de IPv4 a IPv6 en la Prefectura de Imbabura

En éste capítulo se realizará el análisis comparativo de los diferentes métodos para la transición de este protocolo, y se definirá cuál de ellos se deberá utilizar para garantizar la robustez y adaptabilidad de la red. Además, se elaborará el Manual de procedimientos para la transición.

4.1 Implementación de la Metodología

4.1.1 Etapa de Información

Esta etapa se ha dividido en dos fases, la realización de encuestas acerca del protocolo IPv6, y la tabulación de los datos obtenidos. Con esto se aporta para que los encargados de la administración y soporte de la Dirección de Tecnologías de la Información de la Prefectura de Imbabura, estén informados acerca de la adopción a futuro de este protocolo.

Las encuestas irán dirigidas a todo el personal de TIC's, ya que tienen mayor conocimiento dentro del área de sistemas y redes de comunicación, el total de personal dentro de este departamento es de Nueve personas.

4.1.1.1 Encuestas

El objetivo de las encuestas, es saber qué conocimiento e interés posee el grupo sobre el protocolo IPv6.

La encuesta está dividida en cuatro partes y cada una de ellas se refiere a un tema en específico:

- Parte I: Conocimientos Generales de IPv6
- Parte II: Distribución de Información del Protocolo
- Parte III: Uso de Redes Nuevas
- Parte IV: Factor de Desventajas del Protocolo

El Departamento de Tecnología de la Prefectura de Imbabura, consta de 9 personas, de los cuales se encuestó a Seis, todos de género masculino.

En el Anexo B, se adjunta el formato de la encuesta revisada por el Director del Departamento de Tecnologías de la Información y Comunicación, y las encuestas realizadas.

4.1.1.2 Tabulación y Resultados obtenidos

A continuación, se muestran los resultados obtenidos de las encuestas realizadas. Para llevar a cabo un análisis de forma eficiente, se creó un archivo en Microsoft Excel, en donde se realizó la recolección de todos los datos obtenidos para posteriormente ser analizados mediante tablas y gráficas, lo cual se muestra en el anexo C

Al analizar a los encuestados se puede observar que la mayoría oscila entre los 30 y 45 años, todos ellos cuentan con un título de Tercer Nivel relacionado con software o tecnología, lo que resulta beneficioso para el estudio del proyecto ya que la mayoría tiene noción sobre el tema de las preguntas realizadas.

- ❖ PARTE I: Conocimientos Generales de IPv6

En la primera parte de la encuesta realizada, se puede observar que en general la mayoría del personal conoce acerca del protocolo IPv6, pero no a profundidad y también se sienten optimistas acerca de conocer más sobre el mismo, es necesario sugerir una capacitación previa con relación al tema para que el personal adquiera conocimiento sobre esta tecnología para su uso futuro.

Dentro de esta encuesta se realizó las siguientes preguntas de los cuales se obtuvo los resultados mencionados a continuación:

Se preguntó al personal que Señale el nivel de conocimiento que tiene acerca de IPv6, y se obtuvo como resultado que el 16.7% conoce bien IPv6 o lo ha utilizado, mientras que el 83.3% conoce poco acerca de IPv6.

En cuanto al conocimiento acerca del contenido que existe actualmente en IPv6, se pudo observar que el 33.3% ha escuchado algo, pero no concreto, mientras que el 66.7% conoce algo acerca del contenido existente en IPv6.

De la misma manera se preguntó el Cómo se enteraron de que es IPv6, y los resultados dieron a conocer que, el 50% se enteró por medio de cursos o fuentes oficiales, y el otro 50% por medio de la red de Internet.

La consideración del uso de IPv6 como prioridad para el usuario dio a conocer que el 33.3% si lo considera, pero no les preocupa, el 50% si lo considera y siempre están pendientes del tema, el 16.7% optó por otra opción y supo manifestar que considera debería abrirse más espacio o velocidad en una red.

- PARTE II: Distribución de Información del Protocolo

La parte dos, permitió observar que la mayoría de encuestados considera que la implementación de este protocolo es importante, pero en una medida de largo plazo, ya que según su opinión no existe la información o recursos necesarios para realizar la transición, además es posible resaltar que en su totalidad los usuarios desean probar el funcionamiento del protocolo de internet versión 6. Nuevamente se presenta la necesidad de obtener mayor conocimiento sobre hardware, software y sitios de Internet que permitan la utilización del protocolo IPv6.

La consideración del uso de IPv6 como prioridad para las comunicaciones a nivel Global obtuvo como respuesta del 50% si lo considera, pero a largo plazo, el 33.3% lo considera como prioridad, y el 16.7% considera que se debe buscar una solución ahora.

En cuanto a la necesidad de adoptar el Protocolo IPv6, el 16.7% considera que después de un año sería necesario y el 83.3% considera la necesidad a corto plazo (menos de un año).

En relación a la navegación en IPv6, al 16.7% No le gustaría y al 83.3% Si le gustaría ser pionero en dicha navegación.

Acerca del Hardware y Software está preparado para IPv6, el 33.3% no lo tiene, pero podría tenerlo a largo plazo, mientras que el 66.7% si lo tiene, pero necesitaría de unos cuantos cambios.

- PARTE III: Uso de Redes Nuevas

La Parte III, permite identificar que los encuestados tienen apreciaciones distintas hacia el protocolo, entre las cuales se presentan la falta de acceso a los servicios ya que para la mayoría es una tecnología nueva y complicada, se pudo observar el interés de adquirir conocimiento sobre la forma de conectividad del protocolo IPv6. Luego de esta etapa de preguntas, es necesario realizar sugerencias para que el personal inicie un período de información sobre el tema analizado.

Indicando si se ha accedido por algún medio a la red IPv6, el 66.7% de los encuestados no ha accedido a la red IPv6, mientras que el 16.7% lo ha hecho en el trabajo y el 16.7% en algún sitio en internet que ya cuenta con este servicio.

Preguntando la razón por la que le atrae o no un servicio de conectividad IPv6, el 20% manifiesta que es complicado, otro 20% dice que puede ser inseguro, y el 60% brinda diferentes opiniones al respecto tales como: una percepción de que el protocolo brindará una velocidad mayor en el momento de la conectividad, falta de interés al no existir muchas instituciones públicas conectadas, o una atracción por conocer mucho más de esta tecnología.

- PARTE IV: Factor de Desventajas del Protocolo

En esta parte de la encuesta, se puede observar que las principales dificultades que presenta el Protocolo IPv6 se basan en la falta de interés por parte de las instituciones públicas y sectores productivos del país, además se percibe que existe una falta de regulación para su implementación, a pesar de que en el año 2012 se estableció un acuerdo ministerial que impulsa la adopción del protocolo, aun así, no se ha difundido de manera extensa para una implementación de la tecnología

La falta de promoción y capacitaciones sobre la tecnología permite que la mayoría de usuarios piense que no existe mucha disponibilidad de servicios brindados con este protocolo, a pesar de que la Academia ha hecho grandes avances con el soporte de esta tecnología, la mayoría de personas no están familiarizadas con estos progresos.

4.1.2 Etapa de Elaboración del Plan de Transición

4.1.2.1 Manual de Petición de Recursos IPv6 a LACNIC

El proveedor de servicios de internet CNT al cual se encuentra conectada la red de datos la Prefectura de Imbabura, actualmente no brinda el servicio compartido de IPv4 a IPv6 por lo q se hizo necesario investigar cómo obtener un recurso de direcciones para una futura implementación del protocolo. Para esto existe la organización LACNIC que permite obtener un registro y asignación de direcciones IPv6 para organizaciones y usuarios finales ubicadas en América Latina y Caribe

LACNIC contribuye al desarrollo de internet en la región mediante una política activa de cooperación. Para solicitar un bloque IPv6 como Usuario Final, LACNIC ofrece una asignación de direcciones IPv6, para poder encontrar sus políticas y formularios, es necesario entrar a su página oficial.

A pesar de que hoy en día no se exige la aplicación de este protocolo, ni en el mercado corporativo, residencial y mucho menos en el estatal, es necesario mantenerse preparado para una futura migración. El siguiente manual tiene como objetivo brindar información sobre los pasos a seguir para la obtención de un bloque de direcciones IPv6.

4.1.2.1.1 Para Un Cliente Nuevo

- Ingresar al portal IPv6 de LACNIC a la dirección http://portalipv6.lacnic.net/, como se muestra en la Figura 38

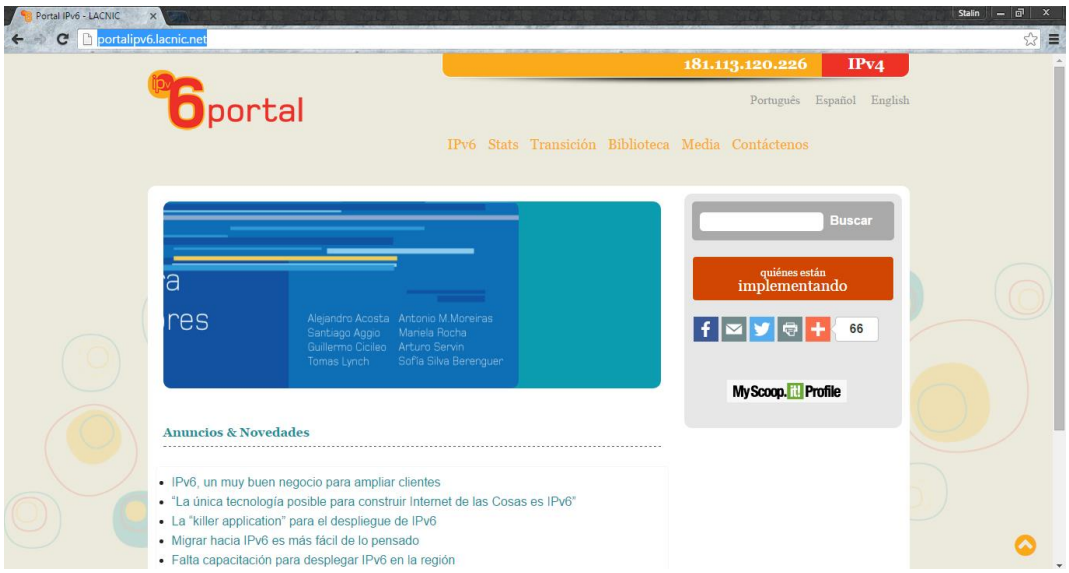


Figura 38. Portal IPv6 de LACNIC

Fuente: Recuperado de http://portalipv6.lacnic.net/

- Hacer click en la pestaña IPv6 y escoger la opción ¿Cómo obtener un bloque de direcciones IPv6?, mostrado en la Figura 39.

Figura 39. Cómo obtener un bloque de direcciones IPv6

Fuente: Recuperado de http://portalipv6.lacnic.net/

- En la ventana que se indica en la Figura 40 elegir la opción IPv6 para usuarios finales.

Figura 40. IPv6 para usuarios finales

Fuente: Recuperado de http://portalipv6.lacnic.net/

- Hacer click en la opción Formulario, mostrado en la Figura 41.

Figura 41. Opción Formulario

Fuente: Recuperado de http://portalipv6.lacnic.net/

- En el caso de tener una cuenta de usuario, ingresar los datos pertinentes, caso contrario hacer click en lacnic.net/newid, para crear una cuenta nueva. Como se muestra en la Figura 42.

Figura 42. Ventana para acceder a la cuenta

Fuente: Recuperado de http://portalipv6.lacnic.net/

- En la ventana mostrada en la Figura 43, llenar los datos solicitados por LACNIC para crear la cuenta

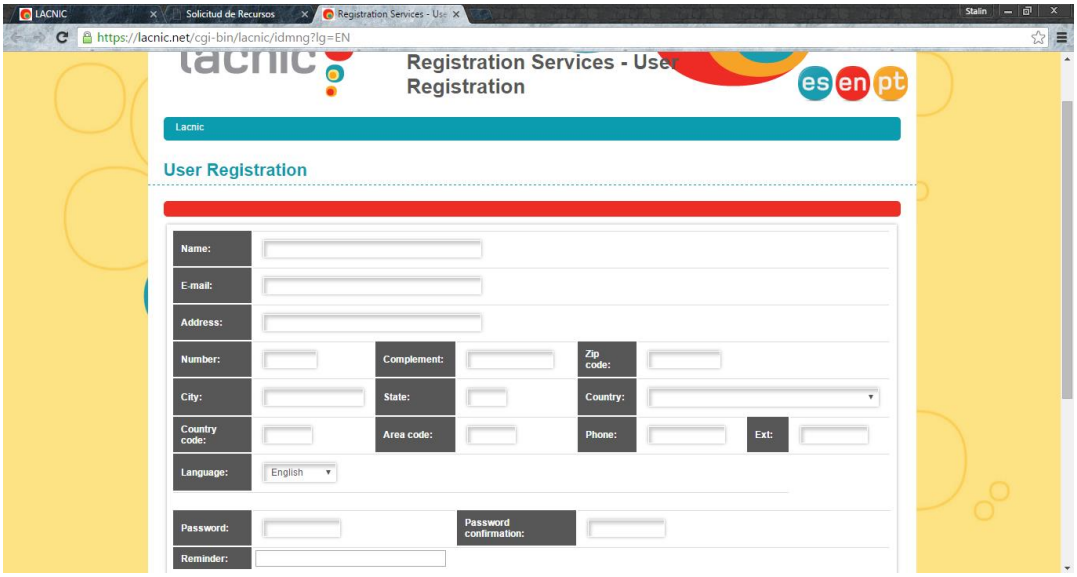


Figura 43. Ventana para crear Usuario Nuevo

Fuente: Recuperado de http://portalipv6.lacnic.net/

- Verificar en el correo electrónico un mensaje en donde se encuentran las instrucciones para ingresar al sistema. Una vez dentro del sistema de LACNIC, se debe ingresar los datos de la Institución que requiera de los recursos IPv6, este formulario se muestra en la Figura 44.

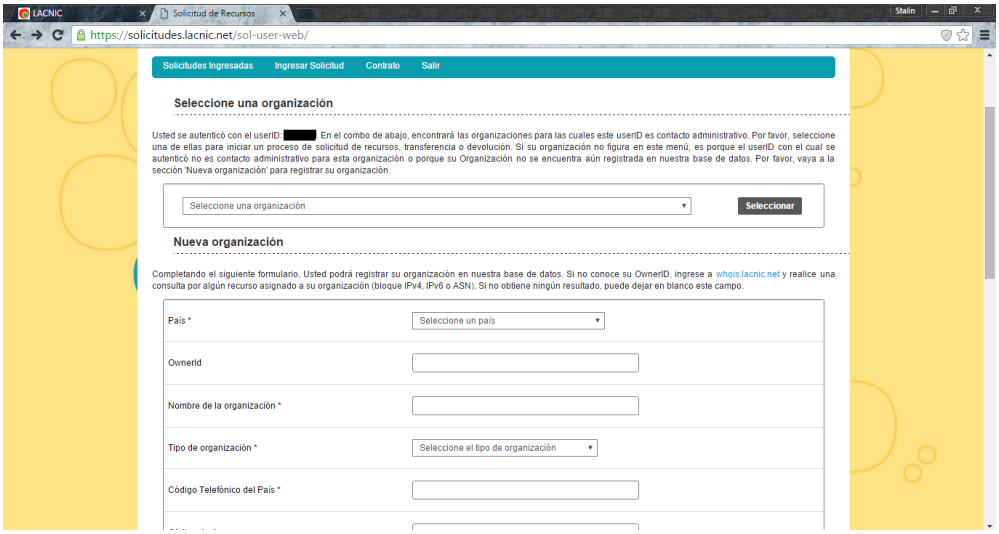


Figura 44. Ingreso de datos de la Institución

Fuente: Recuperado de http://portalipv6.lacnic.net/

- Una vez completada la información se debe realizar el envío de la solicitud de recursos y esperar a que LACNIC envíe su respuesta.

- LACNIC se contactará para dar seguimiento a su requerimiento. La respuesta contendrá el estatus de su solicitud: “Información Completa o Se Requiere de Información Adicional”

- El proceso no dará paso a la siguiente etapa mientras no se envíe toda la información necesaria para procesar la solicitud.

- Una vez que se tenga la información necesaria, se recibirá un mensaje con el resultado de la evaluación:

  - ❖ Solicitud Aprobada: El solicitante recibe el aviso de que la solicitud fue aprobada, y las instrucciones pasa seguir con el proceso.
  - ❖ Solicitud Rechazada: El solicitante recibe el aviso de que su solicitud fue rechazada, con la información de los requerimientos que no fueron cubiertos para ser apto para la asignación de recursos.
  - ❖ Solicitud vencida: Las solicitudes de recursos tienen una vigencia de 3 meses, en caso de que en este tiempo siga pendiente se procederá a su

cancelación. Una vez que cuente con la información o requerimientos se podrá acceder a una nueva solicitud.

4.1.2.1.2 Firma de Contrato de Prestación de Servicios (CPS)

- Una vez aprobada la solicitud, se procede a elaborar el CPS, para el cual se solicitará enviar la documentación requerida para firmar el contrato.

- Lista toda la documentación, se hará llegar el Contrato en formato PDF para proceder a la respectiva revisión, impresión y firmas.

4.1.2.1.3 Proceso de Pago

- Con el Contrato firmado, verificado y aprobado por el área legal, se hará llegar el Contrato Administrativo y de Pago de la Organización, además el recibo de pago con la cantidad a cancelar.

4.1.2.1.4 Asignación del Recurso

- Finalmente, una vez que la institución bancaria haya reportado su depósito, se le hará llegar a los contactos administrativo y de pago de la organización una notificación de la liberación del recibo, y la confirmación de generación de la factura electrónica, para así ser consultada en el sistema de LACNIC, y se realizará la asignación automática de los recursos aprobados en la solicitud, y desde ese momento se puede comenzar a hacer uso de dichos recursos ya asignados.

- Podrá verificar la asignación en WHOIS de LACNIC, mostrado en la Figura 45. (IAR México, 2010)

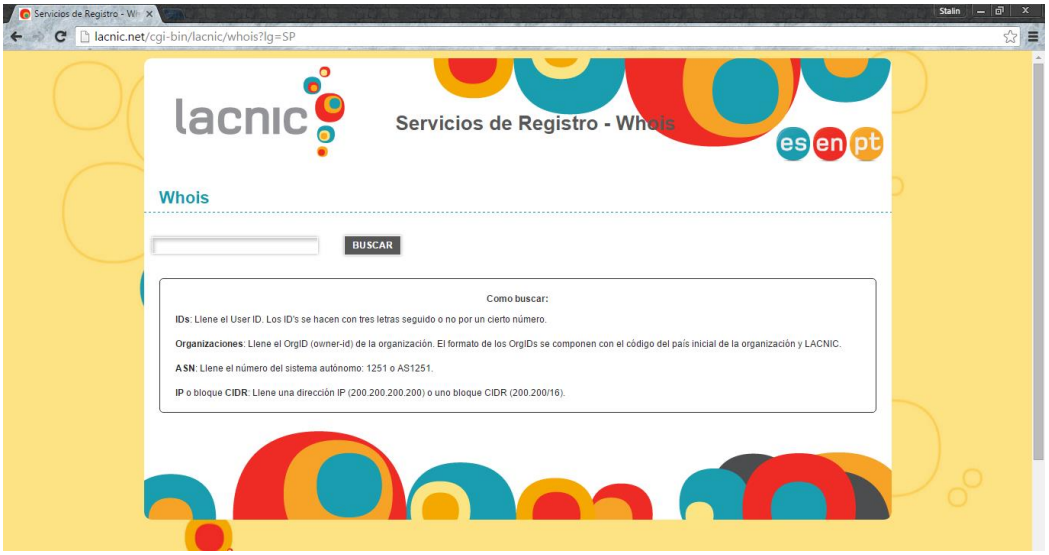


Figura 45. Whois de LACNIC

Fuente: Recuperado de http://lacnic.net/cgi-bin/lacnic/whois?lg=SP

4.1.2.2 Plan de Direccionamiento IPv6

En la Tabla 17 se describe el direccionamiento IPv6 en base a las VLAN's reales de la Prefectura de Imbabura.

Tabla 17. Direccionamiento IPv6 en base a VLANS

NOMBRE	VLAN	GATEWAY IPv4DIR IPv4	DIR IPv6	GATEWAY VLAN IPv6
ADMIN_EQUIPOS	2	192.16.2.1	2001:DB8:3000:2::/64	2001:DB8:3000:2::1/64
SERVIDORES	3	192.16.3.1	2001:DB8:3000:3::/64	2001:DB8:3000:3::1/64
GESTION_TECNOLOGICA	4	192.16.4.1	2001:DB8:3000:4::/64	2001:DB8:3000:4::1/64
PREFECTURA	5	192.16.5.1/64	2001:DB8:3000:5::/64	2001:DB8:3000:5::/64
PROCURADURIA	6	192.16.6.1/64	2001:DB8:3000:6::/64	2001:DB8:3000:6::/64
PLANIFICACION	7	192.16.7.1/64	2001:DB8:3000:7::/64	2001:DB8:3000:7::/64
GESTION_TECNICA	8	192.16.8.1/64	2001:DB8:3000:8::/64	2001:DB8:3000:8::/64
RELACIONES_PUBLICAS	9	192.16.9.1/64	2001:DB8:3000:9::/64	2001:DB8:3000:9::/64
ADMIN_GENERAL	10	192.16.10.1/64	2001:DB8:3000:A::/64	2001:DB8:3000:A::/64
INFRAESTRUCT_FISICA	11	192.16.11.1/64	2001:DB8:3000:B::/64	2001:DB8:3000:B::/64
DESARROLLO_ECONOM	12	192.16.12.1/64	2001:DB8:3000:C::/64	2001:DB8:3000:C::/64
PAS	13	192.16.13.1/64	2001:DB8:3000:D::/64	2001:DB8:3000:D::/64
WIFI	20	192.16.14.1/64	2001:DB8:3000:E::/64	2001:DB8:3000:E::/64
WIFI_EXTERNA	15	192.16.15.1/64	2001:DB8:3000:F::/64	2001:DB8:3000:F::/64
BODEGA	16	192.16.16.1/64	2001:DB8:3000:10::/64	2001:DB8:3000:10::/64
FAUSTO-GIS	17	192.16.17.1/64	2001:DB8:3000:11::/64	2001:DB8:3000:11::/64
FISCALIZACION	18	192.16.18.1/64	2001:DB8:3000:12::/64	2001:DB8:3000:12::/64

CONTRATACIÓN PÚBLICA	19	192.16.19.1/64	2001:DB8:3000:13::/64	2001:DB8:3000:13::/64
INVITADOS	30	192.16.30.1/64	2001:DB8:3000:1E::/64	2001:DB8:3000:1E::/64
RELOJES_BIOM	31	192.16.31.1/64	2001:DB8:3000:1F::/64	2001:DB8:3000:1F::/64
CAMARAS	32	192.16.32.1/64	2001:DB8:3000:20::/64	2001:DB8:3000:20::/64
TELEFONIA	40	192.16.40.1/64	2001:DB8:3000:28::/64	2001:DB8:3000:28::/64
MUTUALISTA	50	192.16.50.1/64	2001:DB8:3000:32::/64	2001:DB8:3000:32::/64
ENLACE_EQUIPOS	101	192.16.101.1/64	2001:DB8:3000:65::/64	2001:DB8:3000:65::/64

Fuente: Prefectura de Imbabura

La Tabla 18 muestra el direccionamiento para la WAN y LAN de la Prefectura de Imbabura.

Tabla 18. Direccionamiento IPv4 e IPv6

NOMBRE	DIR IPv4	DIR IPv6
OUTSIDE (WAN) ASA	192.168.0.150/24	2001:DB8:3000::150/64
INSIDE (LAN) ASA	192.16.2.2	2001:DB8:3000:2::2/64
IP PUBLICA CNT	192.168.0.225/24	2001:DB8:3000::225/64
CORE	192.16.2.1/24	2001:DB8:3000:2::1/64
Red Local Sumarizada	192.16.0.0/16	

Fuente: Prefectura de Imbabura

4.1.2.3 Plan de Transición de acuerdo a los objetivos de la Prefectura de Imbabura

Es conveniente que las instituciones públicas comiencen a prepararse, ya que, es posible empezar a adoptar esta tecnología, de tal manera, tomando en cuenta el objetivo institucional de "Tecnificar los procesos de administración y Gestión Institucional" se ha determinado seguir los siguientes pasos que pueden guiar a realizar la transición.

- Hoy en día existen proveedores de servicios de internet que ofrecen conectividad IPv6. Se debe consultar al ISP sobre cómo va a brindar el servicio, sea compartiendo protocolos o solo acceso IPv6.

- Controlar los equipos IPv4, específicamente los Switchs, servidores, PCs y dispositivos móviles de usuarios, para determinar los que admiten IPv6.

- Realizar una auditoría de los Servicios y Aplicaciones para identificar los que están habilitados el protocolo IPv6.

Para hacer uso de la información investigada, hay que identificar las partes de red de la institución que deberán cambiarse para adoptar IPv6, y para implementar esta tecnología es necesario tomar en consideración la probabilidad de necesitar recursos especializados en IPv6.

- Utilizar Dual Stack (Doble Pila), para coexistir entre protocolos IPv4 e IPv6 en la red, ya que éstos pueden ser ejecutado en paralelo e independientemente, sin necesidad de túneles ni servicios de traducción, y así salir de forma gradual de IPv4.

- Es necesario utilizar servicios de traducción para brindar la conectividad a los usuarios IPv6 que necesitan tener acceso a servicios y aplicaciones en IPv4. Este proceso se consigue llevar a cabo con el levantamiento de NAT64 y DNS64.

- Supervisar el proceso y efectos de la transición de IPv6 mediante pruebas (en redes simuladas) que representen el funcionamiento de los dispositivos que conforman la red sobre el protocolo de internet versión 6 en la institución con la finalidad de observar ventajas y desventajas del proceso.

4.1.2.4 Selección del Mecanismo de Transición

4.1.2.4.1 Análisis comparativo entre Mecanismos de Transición

Tomando en cuenta las características de la red de la Prefectura de Imbabura, donde se plantea las metodologías de transición para su posterior implementación, y luego de haber analizado los dispositivos de red y servidores, se hace necesario utilizar una comparación técnica para escoger el método que mejor se adapte a la institución. En la tabla 19, se realiza una descripción de cada uno de los mecanismos de transición tomando en cuenta su forma de operación, configuración, ventajas y desventajas.

Tabla 19. Análisis comparativo de los Mecanismos de Transición

METODOS	Dual Stack	Túneles	Traducción
Forma de Operación	Utiliza de forma simultánea IPv4 e IPv6 en cada nodo de la red, lo que permite que los dos protocolos puedan interactuar entre sí de manera transparente.	Envía paquetes IPv6 dentro de paquetes IPv4 y viceversa, para transportarlos sobre el enrutamiento IPv4.	Traduce cabeceras IPv4 en cabeceras IPv6 y viceversa, realiza conversiones de direcciones o actúa en el intercambio de trafico TCP a UDP.
Configuración	Router, Switchs y host se configuran para admitir ambos protocolos. Cada uno de los nodos posee los dos stacks de protocolos.	Son configurados de forma automática, ya que los extremos del túnel están determinados por las direcciones IPv4 encapsuladas dentro de direcciones IPv6	Requiere tener habilitados los mecanismos de traducción IPv4 e IPv6 en los routers de las dos redes.
Ventajas	Administración conjunta de ambos Protocolos de internet.	Permite transmitir paquetes IPv6 mediante la infraestructura IPv4, sin necesidad de cambios a los mecanismos de enrutamiento.	Opera de distintas formas, traduciendo cabeceras IPv4 en cabeceras IPv6 y viceversa
Desventajas	Requiere que todo el equipamiento soporte los dos protocolos.	El uso de túneles genera retardo en una transmisión de datos.	No es una técnica deseable a largo plazo.

Fuente: Recuperado de http://dspace.utpl.edu.ec/bitstream/123456789/12614/1/Soto_Velasco_Gissella_Patricia.pdf , http://www.cu.ipv6tf.org/transicionipv6.htm

4.1.2.4.2 Mecanismo de Transición Seleccionado

La transición de IPv4 a IPv6 no es una tarea sencilla, por lo que debe realizarse de una manera progresiva mientras sea posible la coexistencia entre los dos protocolos, teniendo en cuenta que los servicios que la institución presta no deben afectarse.

Luego de haber estudiado cada uno de los métodos y el análisis efectuado a la infraestructura de la red de la Prefectura de Imbabura, se pudo determinar que esta tiene compatibilidad con el protocolo IPv6, por lo que se escogió el método de coexistencia que se adapta de mejor manera a esta situación.

Por lo tanto, se utilizará el mecanismo de Dual Stack ya que este al ser una metodología de transición que trabaja sobre una red nativa IPv6, garantiza la conectividad de los dos protocolos desde el Firewall ASA hacia el Switch de CORE el cual realiza la distribución a cada uno de los Switchs de acceso para llegar a los host alojados en la red interna de la Prefectura de Imbabura, este método es adecuado debido a que todos los dispositivos de red son compatibles con el Protocolo IPv6.

Para el manejo de aplicaciones se vio la necesidad de utilizar métodos de traducción como son el NAT64 y DNS64, ya que estos no trabajan en una red basada en ipv4, sino en una red basada en ipv6, permitiendo la interconexión mediante el envío de paquetes IPv6 dentro de la red IPv4.

Debido a que no todas las aplicaciones de la red soportan el manejo de IPv6, se desarrolla la simulación de las aplicaciones DHCP, WEB y DNS, con la finalidad de probar el funcionamiento de los traductores de red, estos servicios fueron sugeridos por el administrador de la red.

Por tal razón se realizará el uso de estas metodologías para la simulación de la transición, tomando en cuenta que el proyecto al ser implementado no afecte a la estructura de red.

4.1.3 Etapa de Implementación y Configuración de la Metodología

Tomando en cuenta que la topología de la red de la Prefectura de Imbabura tiene un modelo jerárquico, las configuraciones han sido realizadas de manera descendente, partiendo desde el Nivel de acceso, que en el caso de esta red está formado por el Switch de CORE y el Switch ASA (Firewall), atravesando por los Switchs de distribución los cuales están representados por los Switch 2960 de cada planta del edificio, llegando así a los servicios y aplicaciones que brinda la Institución.

4.1.3.1 Configuración Router 881 (CNT)

En este equipo de red no se puede realizar ninguna configuración, debido a que el proveedor de Internet no permite la manipulación del mismo, este router solamente cuenta con servicio sobre IPv4, ya que en la actualidad el proveedor de servicios CNT no ofrece la utilización compartida de IPv4 e IPv6

4.1.3.2 Configuraciones en Firewall CISCO ASA5520

La configuración del Firewall está basada en el control del tráfico de red y enrutamiento, es decir, se establecen las reglas que permiten o deniegan la comunicación entre las zonas INSIDE y OUTSIDE.

A continuación, hacer doble click sobre el dispositivo ASA para abrir la consola de comandos. Para configurar el ASA a través de la consola de comandos se debe seguir los siguientes pasos:

- Se puede activar el Firewall (ASA) mediante el comando, como se muestra en la Figura 46.

ciscoasa# activation-key 0x4a3ec071 0x0d86fbf6 0x7cb1bc48 0x8b48b8b0 0xf317c0b

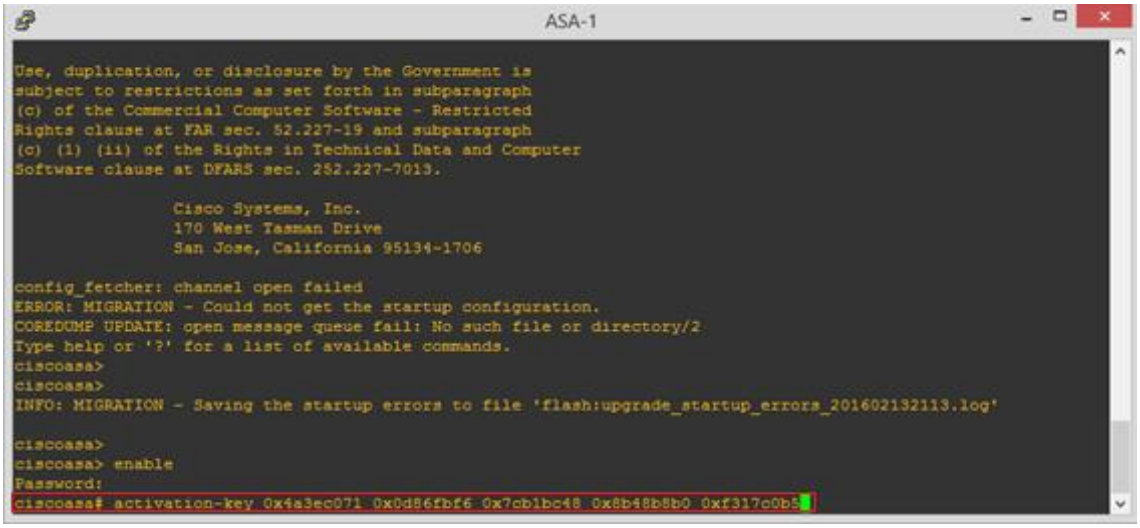


Figura 46. Activación del Firewall

Fuente: GNS3

- Luego se debe reiniciar el Firewall para seguir con las configuraciones con el comando:

ciscoasa# reboot.

- Para cargar la imagen del programa ASDM del firewall se utiliza el siguiente comando, lo cual se indica en la Figura 47.

ciscoasa# copy tftp flash:asdm-641.bin
Address or name of remote host [ ]? <direccion IP>
Source filename [ ]? Asdm-641.bin
Destination filename [asdm-641.bin]? <Enter>

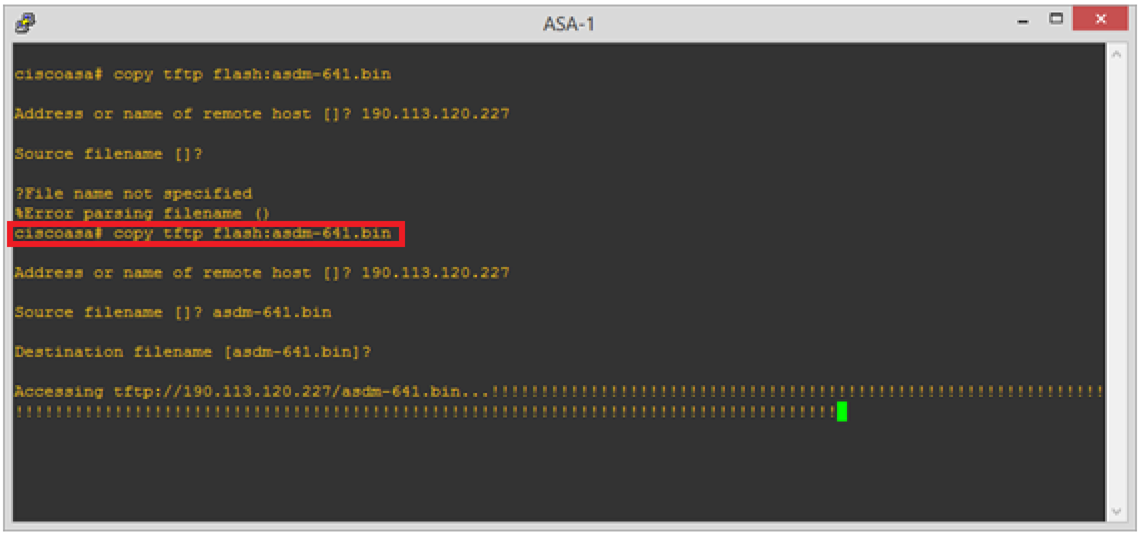


Figura 47. Carga de la imagen (IOS) del Firewall

Fuente: GNS3

- Una vez que se termina el proceso anterior se procede a asignar una dirección IP al firewall ASA, para esto se debe utilizar los comandos:

ciscoasa# configure terminal
ciscoasa(config)# int gigabitEthernet 0
ciscoasa(config-if)# ip address 192.168.0.150 255.255.255.0
ciscoasa(config-if)# security-level 90
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# no shutdown

- Comandos para habilitar el acceso SSH, este se realiza para tener acceso al Switch con seguridad ya que las contraseñas para la autenticación están encriptadas.

ciscoasa(config-if)# enable password cisco
ciscoasa(config)# aaa authentication ssh console LOCAL
ciscoasa(config)# crypto key generate rsa modulus 1024
ciscoasa(config)# ssh 192.168.0.0 255.255.255.0 management

- Comandos para habilitar la interfaz http (web)

ciscoasa(config)# asdm image flash:asdm-641.bin
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.0.0 255.255.255.0 management

- Definir el usuario y contraseña, sin olvidar asignar el nivel 15 de privilegios para este usuario, como se observa en la Figura 48.

ciscoasa(config)# username cisco password cisco privilege 15

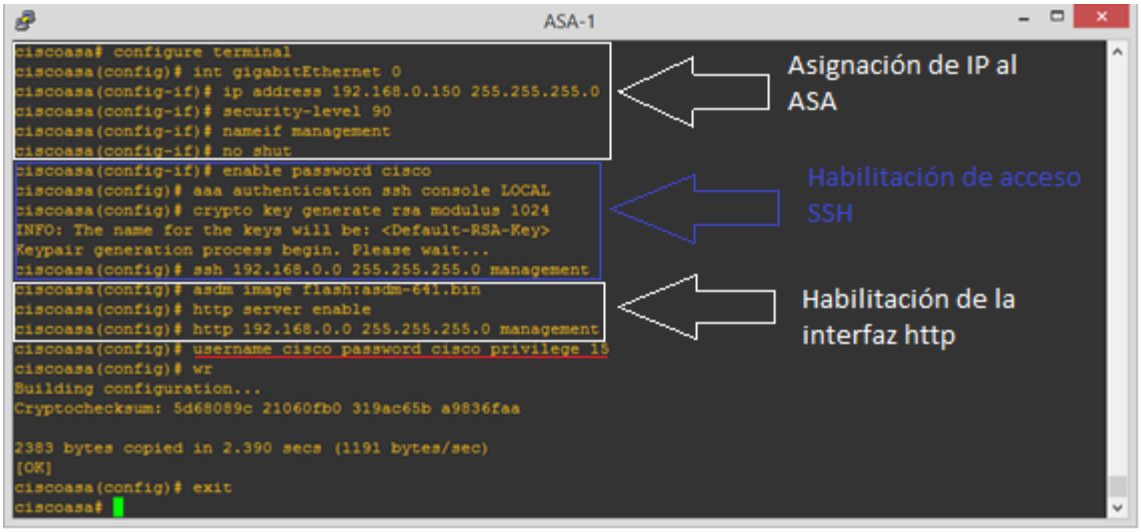


Figura 48. Asignación de dirección IP al ASA, Acceso SSH y habilitación de la interfaz http
Fuente: GNS3

Para descargar el programa para entrar a la interfaz gráfica del ASA 5520

- Abrir el navegador y en la barra de dirección poner https:// <dirección asignada al ASA>
- Pulsar “Install ASDM Launcher and RUN ASDM”. Se instala y ejecuta el ASDM, como se muestra en la Figura 49.

Figura 49. Descarga del ASDM (Interfaz Gráfica del ASA)

Fuente: CISCO ASA

Una vez completado todos estos pasos se puede administrar el ASA de Cisco mediante la interfaz gráfica, mostrada en la Figura 50.

- Ingresar al ASDM, para ello se debe poner un nombre de usuario y contraseña.

Figura 50. Launcher ASDM

Fuente: ASDM

- En el botón Configuración se encuentran las interfaces.
- Para empezar a definir cada interfaz que se va a utilizar INSIDE (LAN) y OUTSIDE (WAN) con el botón Edit. Este se indica en la Figura 51.

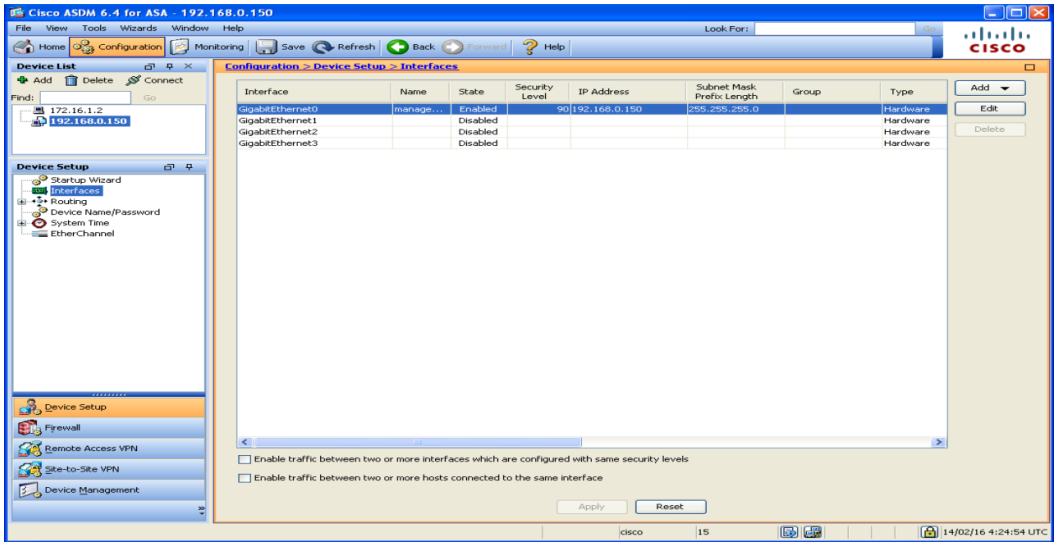


Figura 51. Edición de Interfaces

Fuente: ASDM

- Elegir la interfaz que se va a editar, como se muestra en la Figura 52, en este caso OUTSIDE.

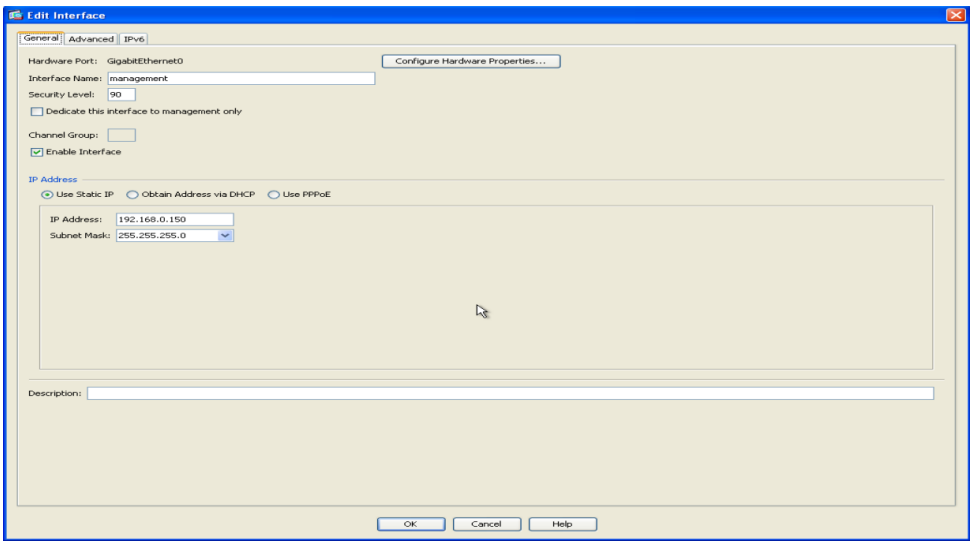


Figura 52. Elección de la Interfaz a editarse

Fuente: ASDM

- Configuración OUTSIDE IPv4

Llenar y cambiar los datos de la interfaz, como se indica en la Figura 53.

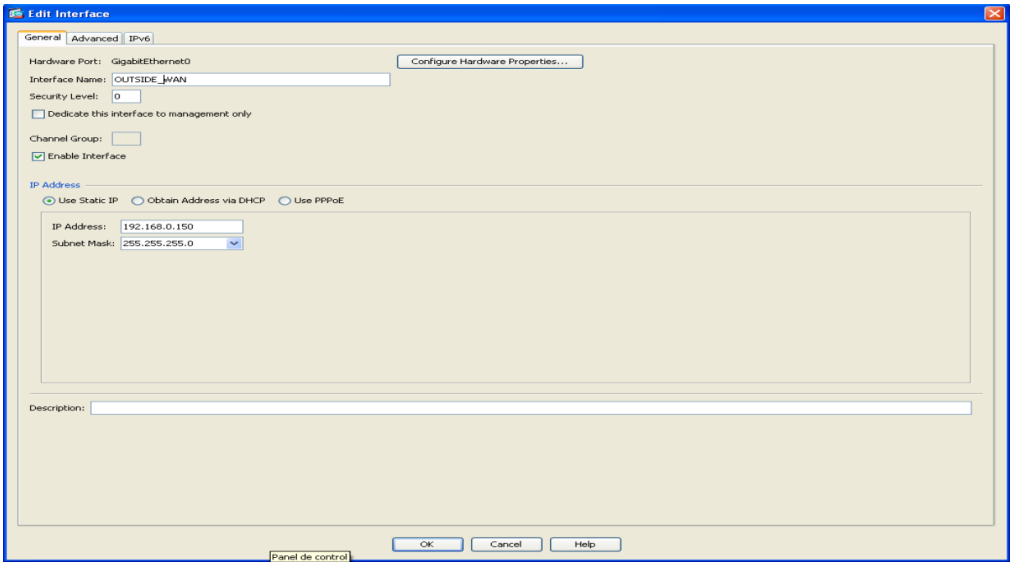


Figura 53. Configuración OUTSIDE IPv4

Fuente: ASDM

- Configuración OUTSIDE IPv6

En la pestaña IPv6 se puede encontrar opciones para configurar el Protocolo IPv6, esto se indica en la Figura 54.

Mediante el botón Add, se puede añadir la dirección IPv6 para la interfaz.

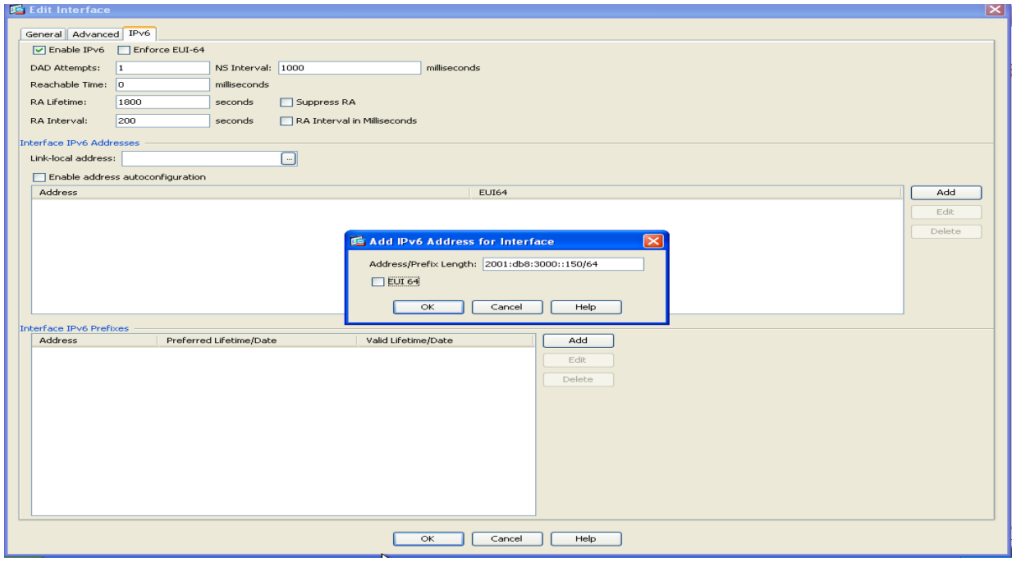


Figura 54. Configuración OUTSIDE IPv6

Fuente: ASDM

- Configuración INSIDE IPv4

Llenar y cambiar los datos de la interfaz, como se muestra en la Figura 55.

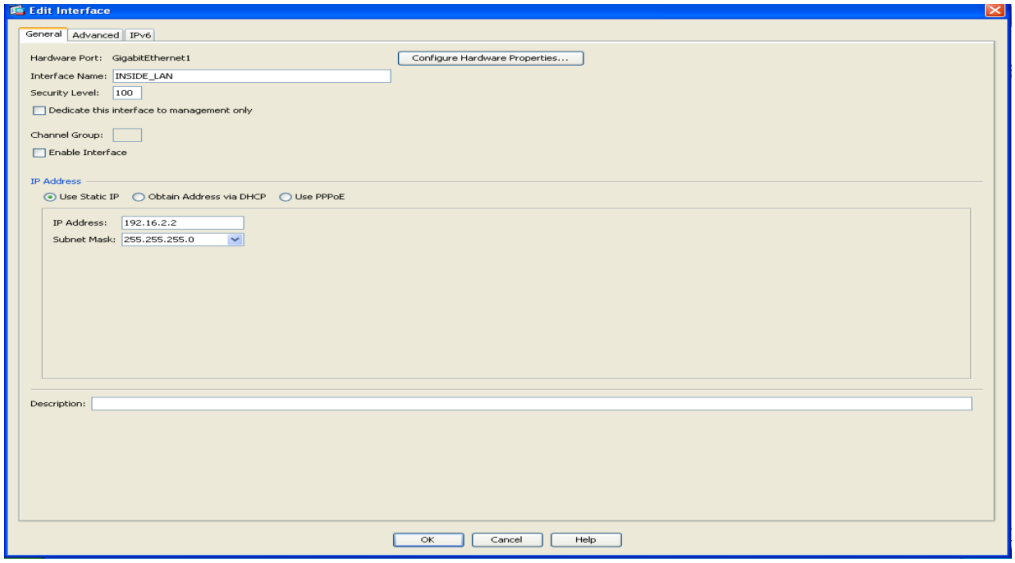


Figura 55. Configuración INSIDE IPv4

Fuente: ASDM

- Configuración INSIDE IPv6

En la pestaña IPv6 se puede encontrar opciones para configurar el Protocolo IPv6. Mediante el botón Add, se puede añadir la dirección IPv6 para la interfaz, lo cual se indica en la Figura 56.

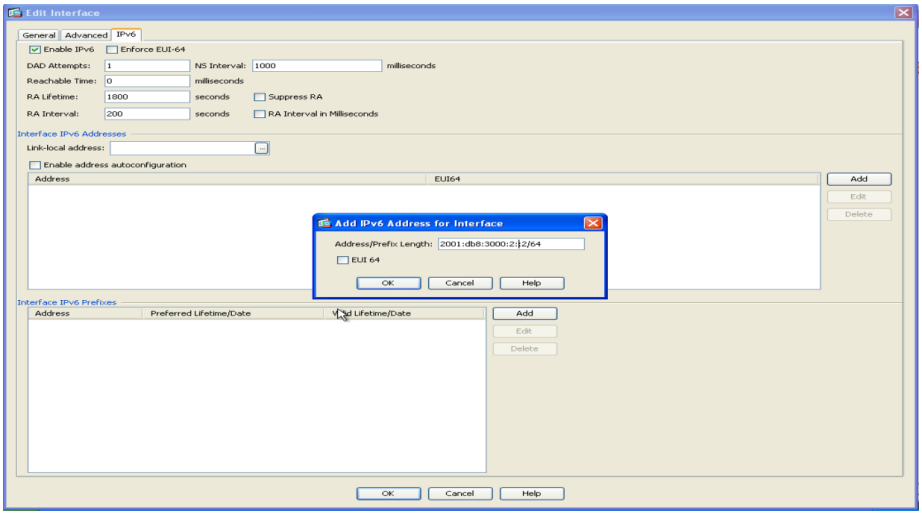


Figura 56. Configuración INSIDE IPv6

Fuente: ASDM

- Interfaces definidas en IPv4 e IPv6

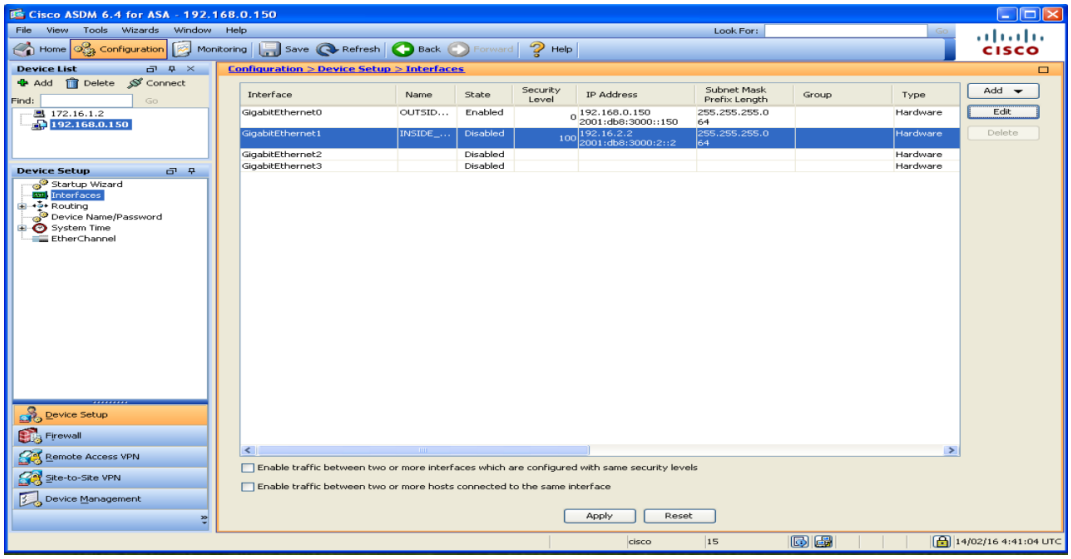


Figura 57. Interfaces definidas IPv4 e IPv6

Fuente: ASDM

- Aplicar los cambios realizados con el boton Apply
- Guardar los cambios con el botón Save, como se muestra en la Figura 58.

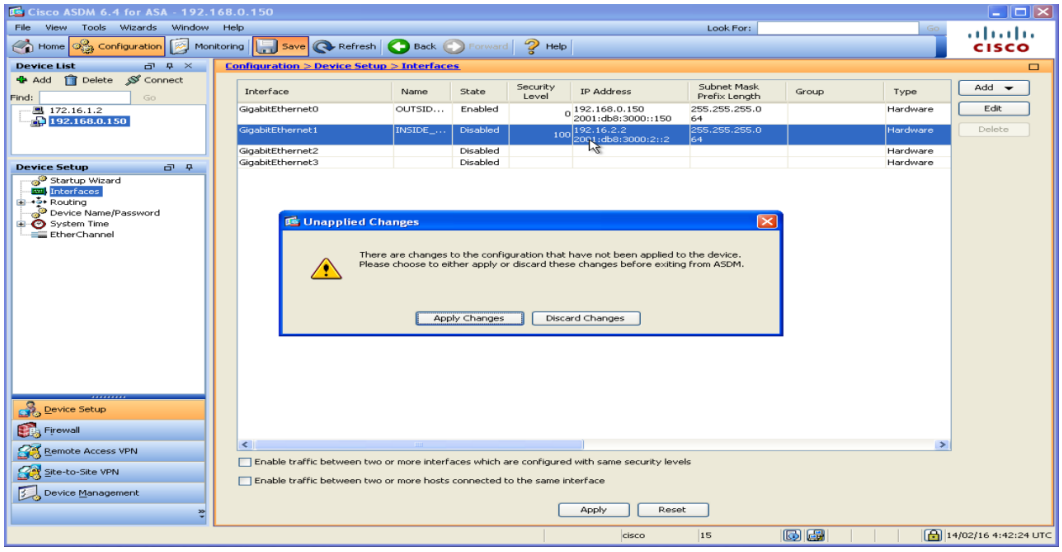


Figura 58. Guardado de los cambios efectuados

Fuente: ASDM

- En el botón Configuración, Routing, Static Routes, añadimos el enrutamiento de acuerdo a la conveniencia.
- Permitir el trafico en la red OUTSIDE IPv4, como se indica en la Figura 59.

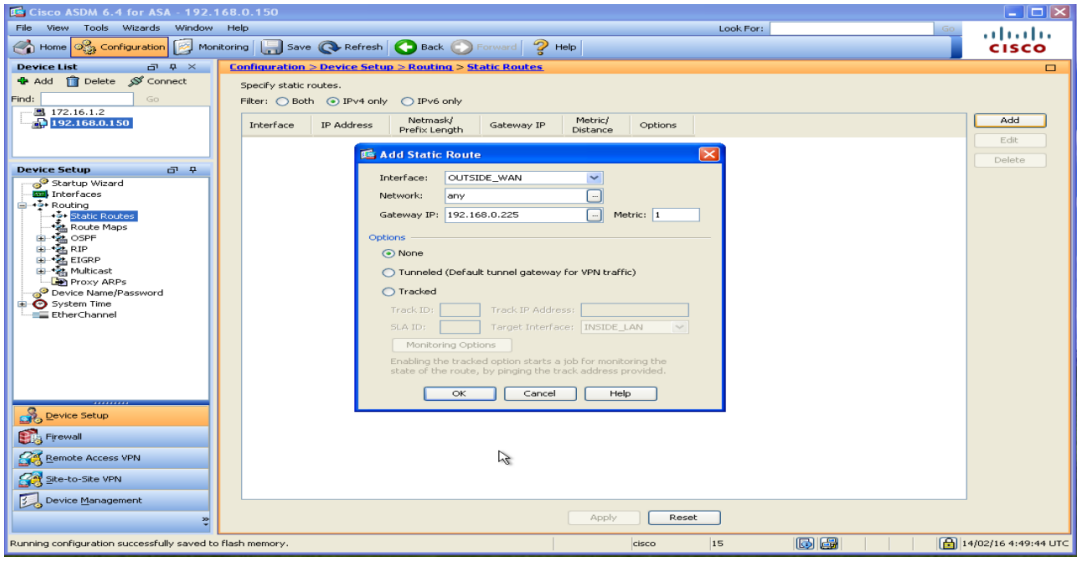


Figura 59. Tráfico OUTSIDE IPv4

Fuente: ASDM

- Permitir trafico en la red INSIDE IPv4, mostrado en la Figura 60.

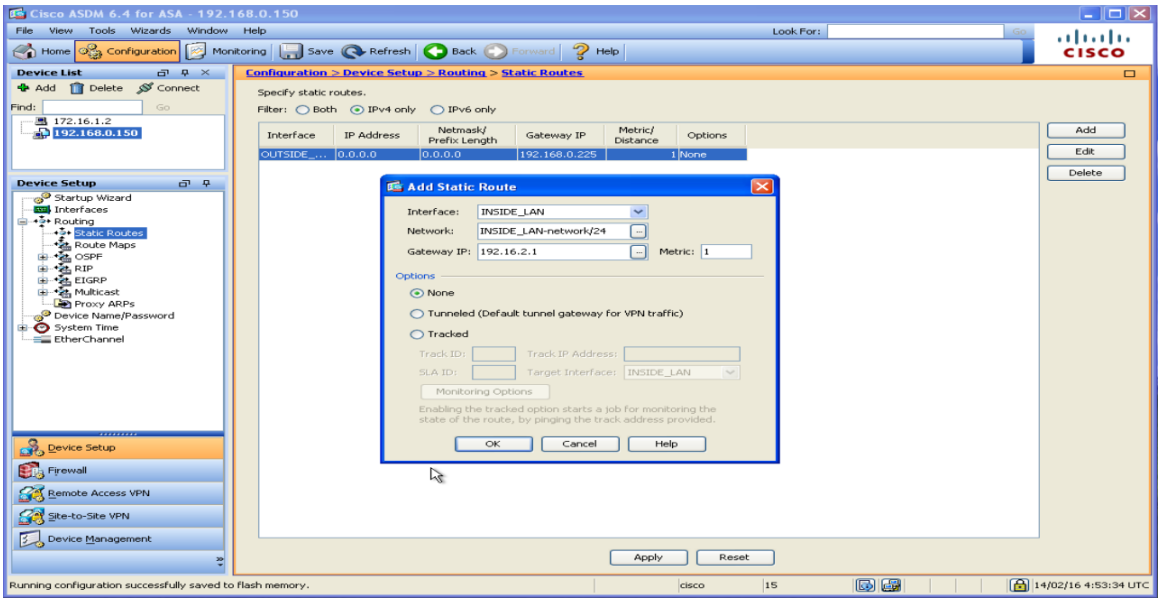


Figura 60. Tráfico INSIDE IPv4

Fuente: ASDM

- En la Figura 61 se muestra el enrutamiento de cada VLAN IPv4

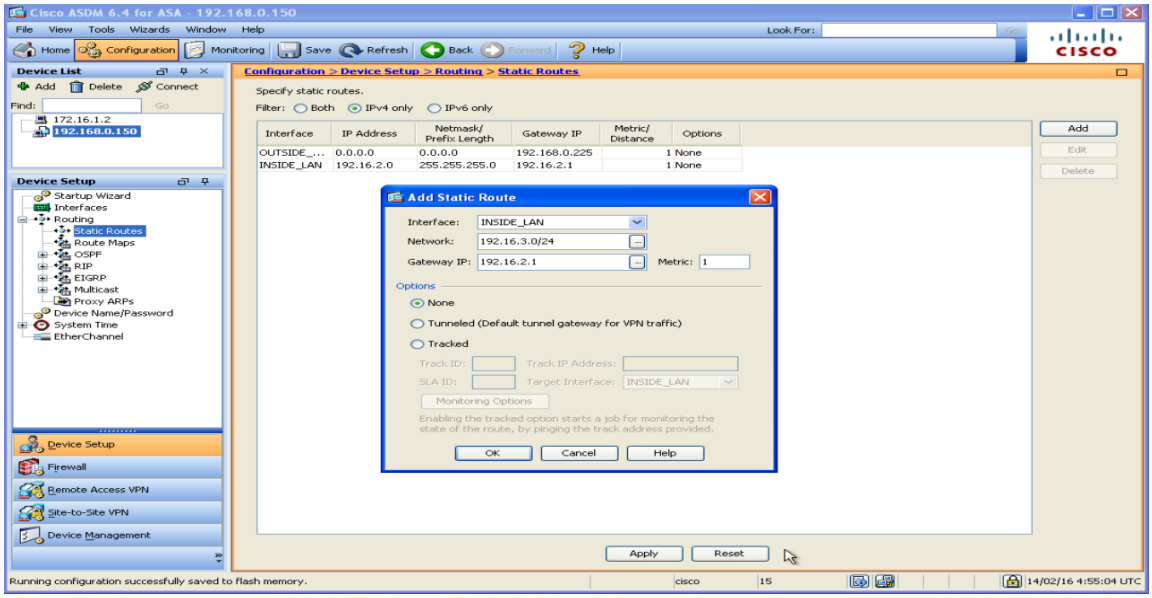


Figura 61. Enrutamiento de cada VLAN IPv4

Fuente: ASDM

- En la Figura 62 se indica el enrutamiento de todas las VLANS IPv4

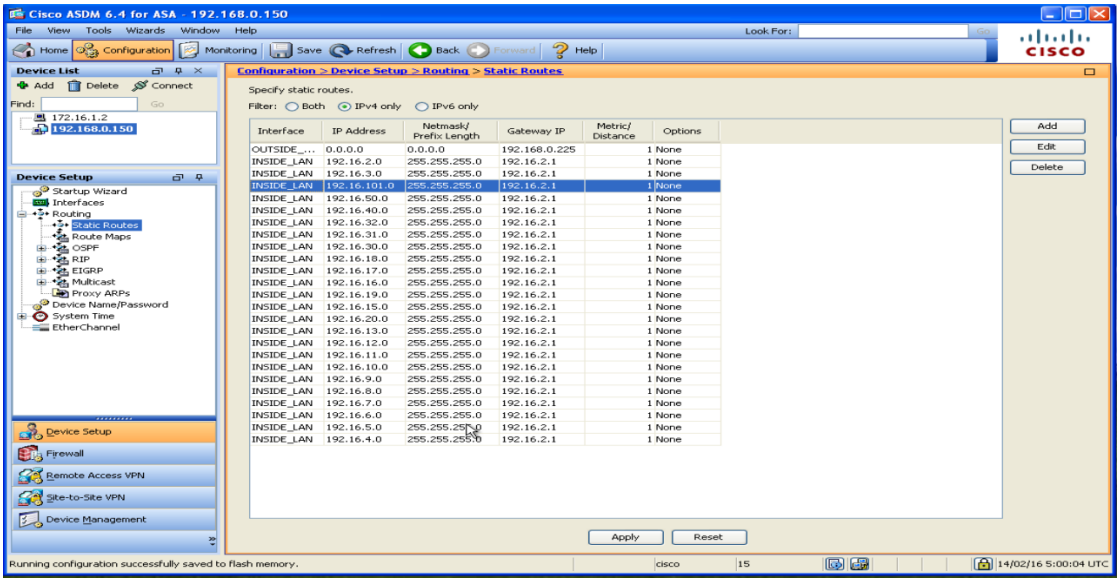


Figura 62. Enrutamiento de todas las VLANS IPv4

Fuente: ASDM

- La figura 63 muestra la forma de permitir tráfico en la red INSIDE IPv6

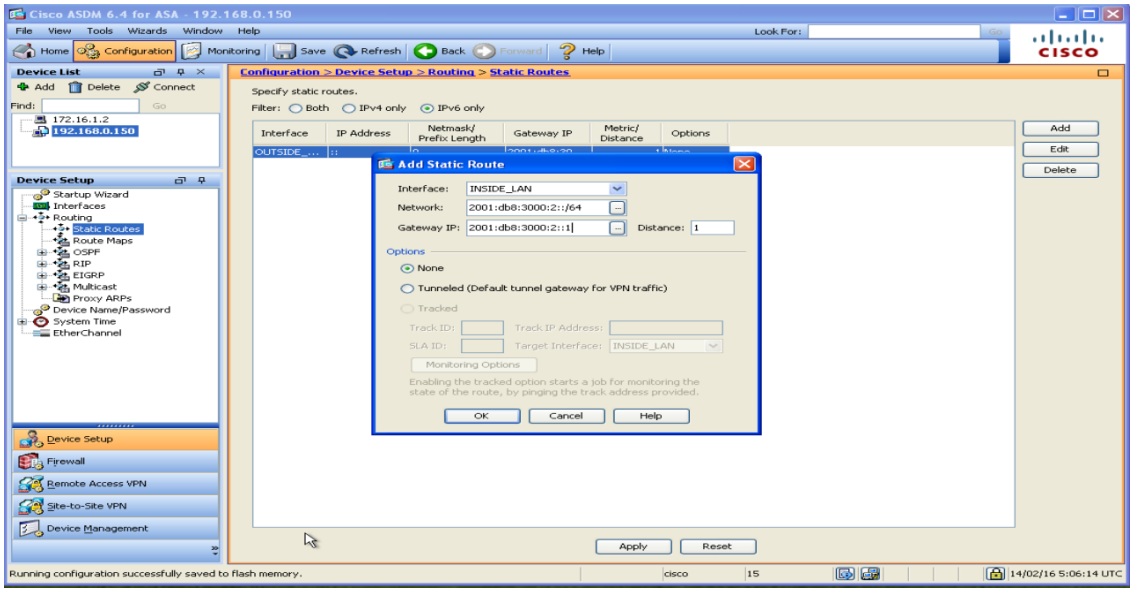


Figura 63. Tráfico en la red INSIDE IPv6

Fuente: ASDM

- La figura 64, muestra como permitir tráfico en la red OUTSIDE IPv6

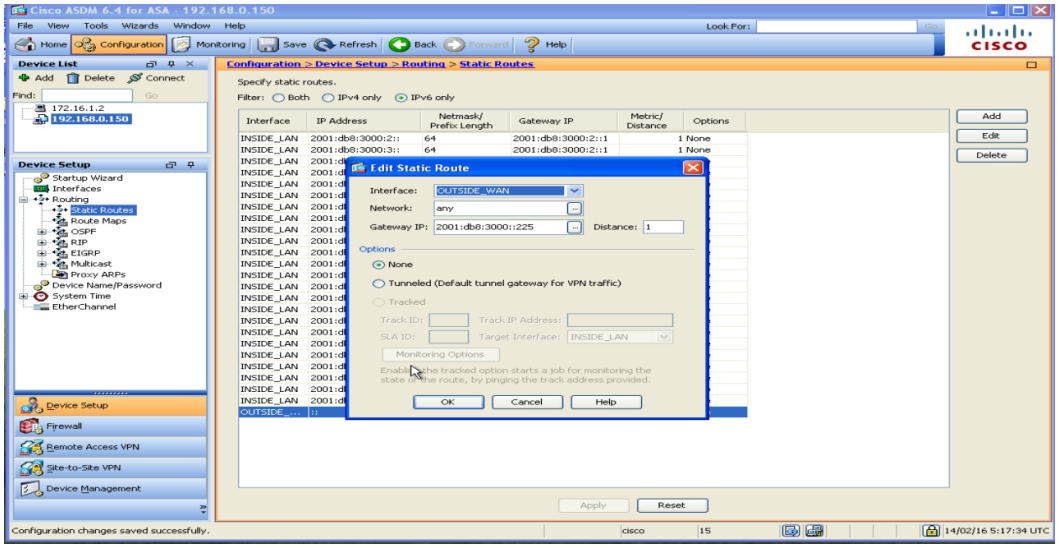


Figura 64. Tráfico en la red OUTSIDE IPv6

Fuente: ASDM

- El enrutamiento de cada VLAN IPv6 se muestra en la Figura 65.

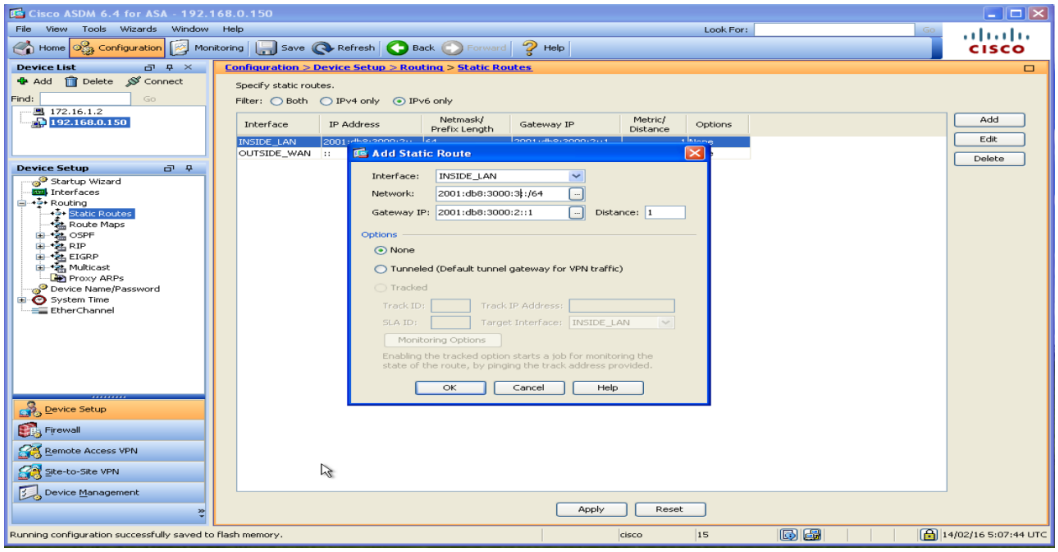


Figura 65. Enrutamiento de cada VLAN IPv6

Fuente: ASDM

- El enrutamiento de todas las VLANS IPv6, esta indicaco en la Figura 66

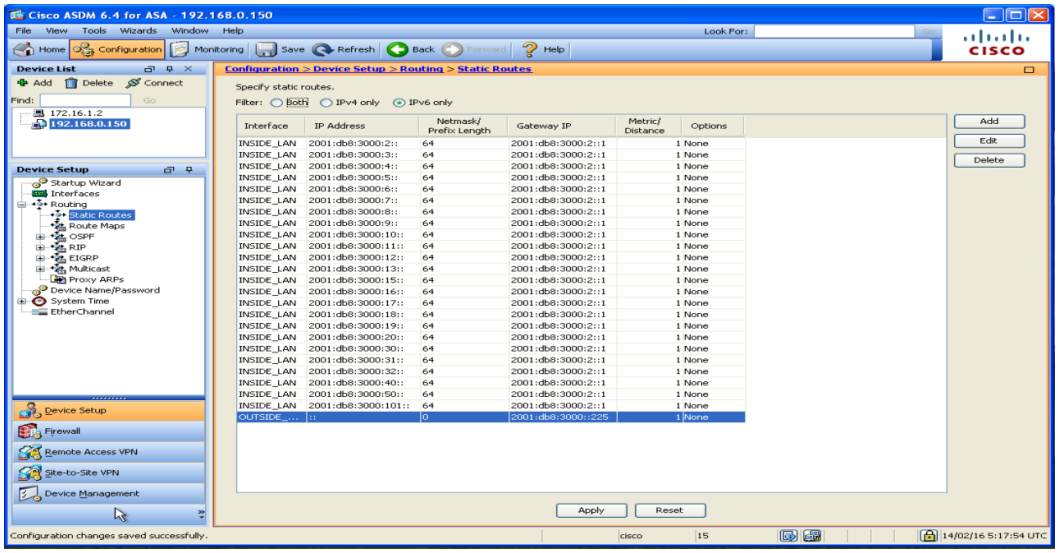


Figura 66. Enrutamiento de todas las VLANS IPv6

Fuente: ASDM

- En el botón de Configuración, Firewall, Access Rules, añadir reglas de acceso para permitir trafico a la red local IPv4 (INSIDE), tal como se indica en la Figura 67.

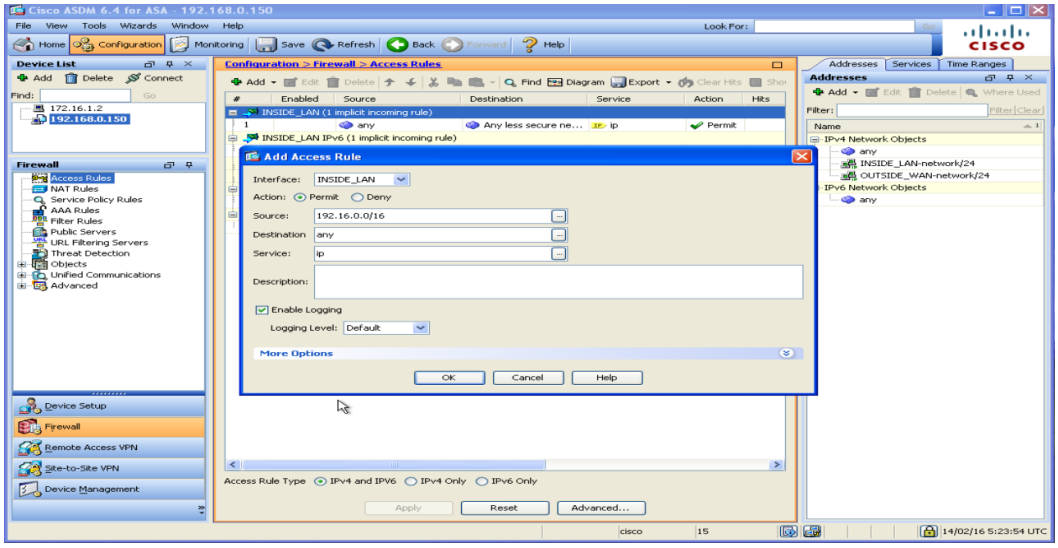


Figura 67. Reglas de acceso para permitir el tráfico a la red INSIDE IPv4

Fuente: ASDM

- La regla implicita para denegar el trafico en el resto de las otras redes IPv4, se indica en la Figura 68.

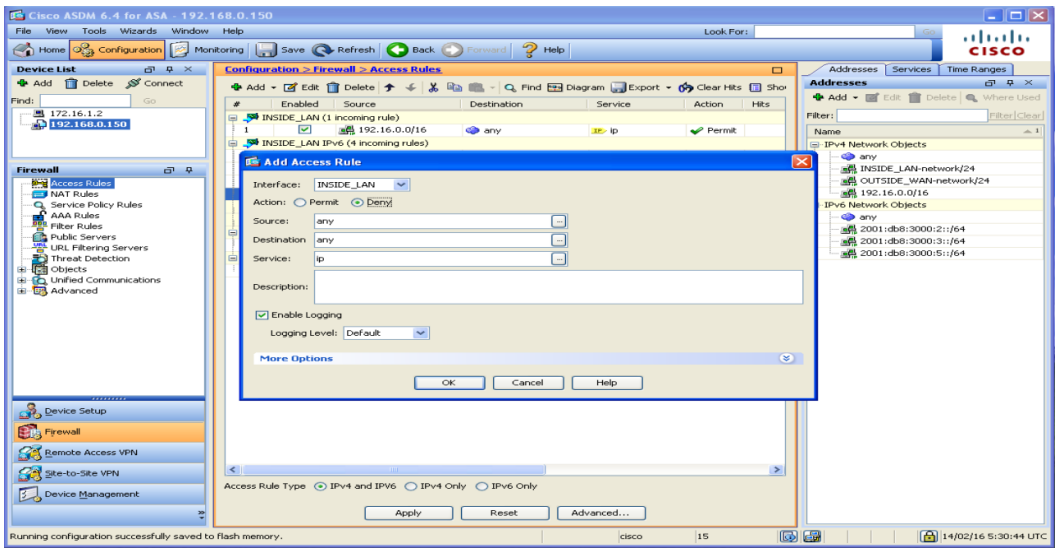


Figura 68. Reglas para denegar el tráfico en el resto de redes IPv4

Fuente: ASDM

- La Figura 69, muestra las reglas de acceso para permitir trafico en la red local IPv6 (INSIDE)

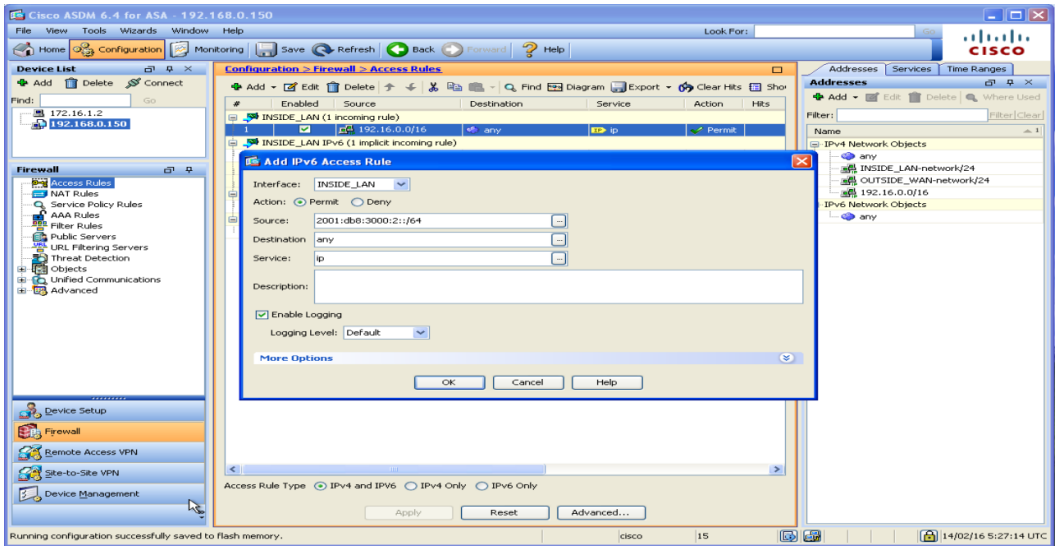


Figura 69. Reglas de acceso para permitir tráfico en la red INSIDE IPv6

Fuente: ASDM

- La figura 70, indica la regla implicita para denegar el trafico en el resto de las otras redes IPv6.

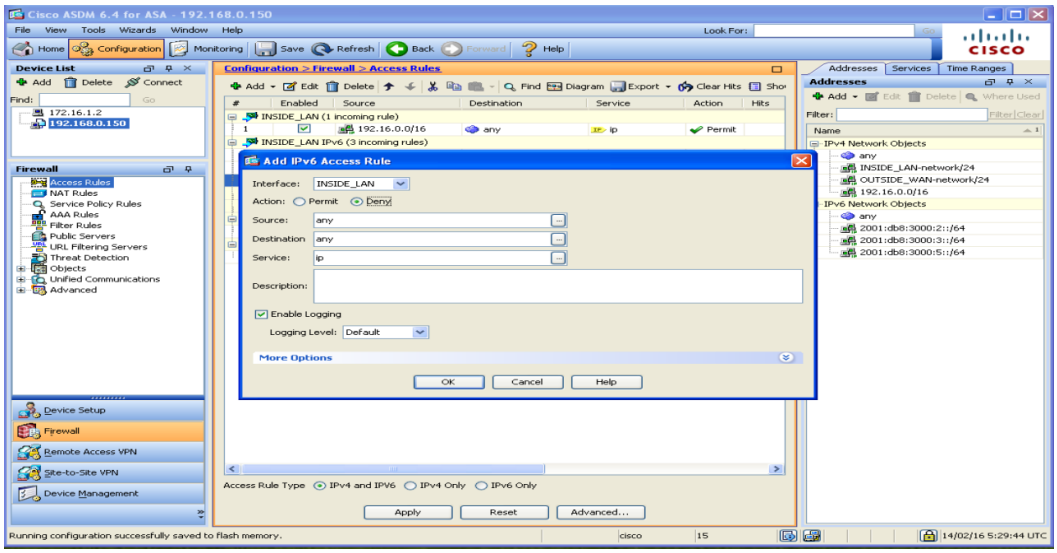


Figura 70. Reglas para denegar el tráfico en el resto de redes IPv6

Fuente: ASDM

- Las reglas de acceso para permitir el trafico de la red OUTSIDE IPv4, estan mostradas en la Figura 71.

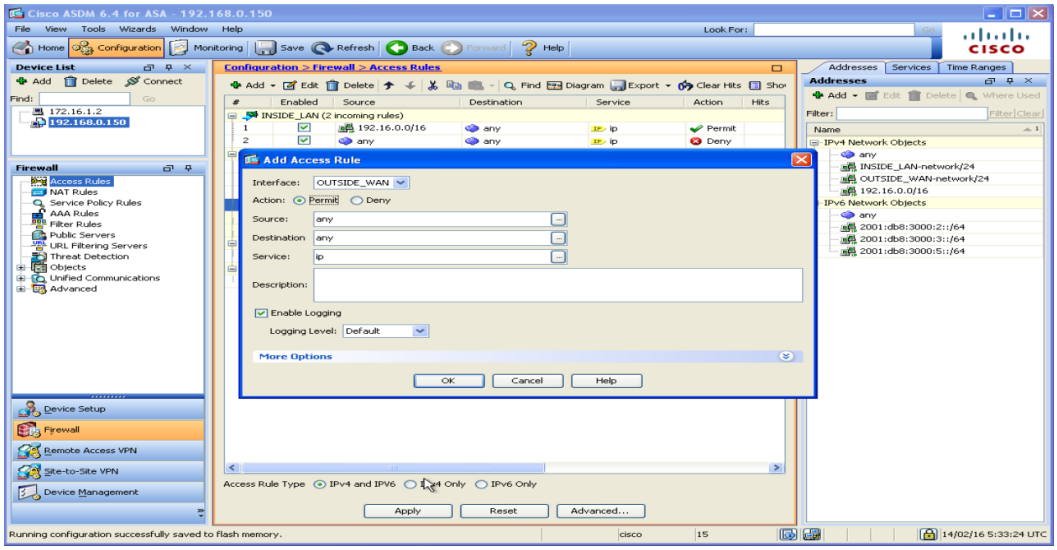


Figura 71. Reglas de acceso para permitir tráfico en la red OUTSIDE IPv4

Fuente: ASDM

- Las reglas para denegar el trafico de la red OUTSIDE IPv4, se muestran en la Figura 72.

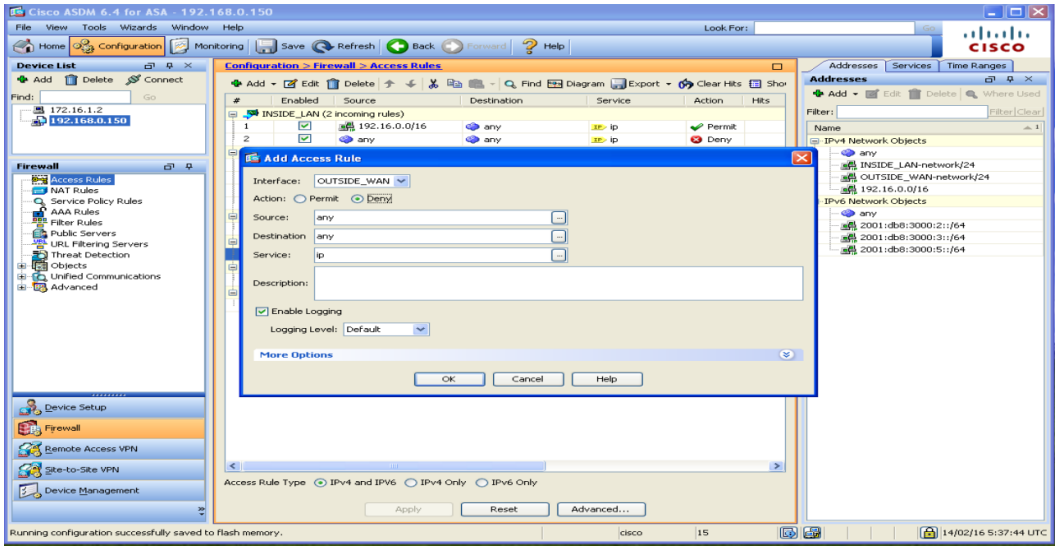


Figura 72. Reglas para denegar tráfico en la red OUTSIDE IPv4

Fuente: ASDM

- La Figura 73, indica como denegar el trafico en la red OUTSIDE IPv6

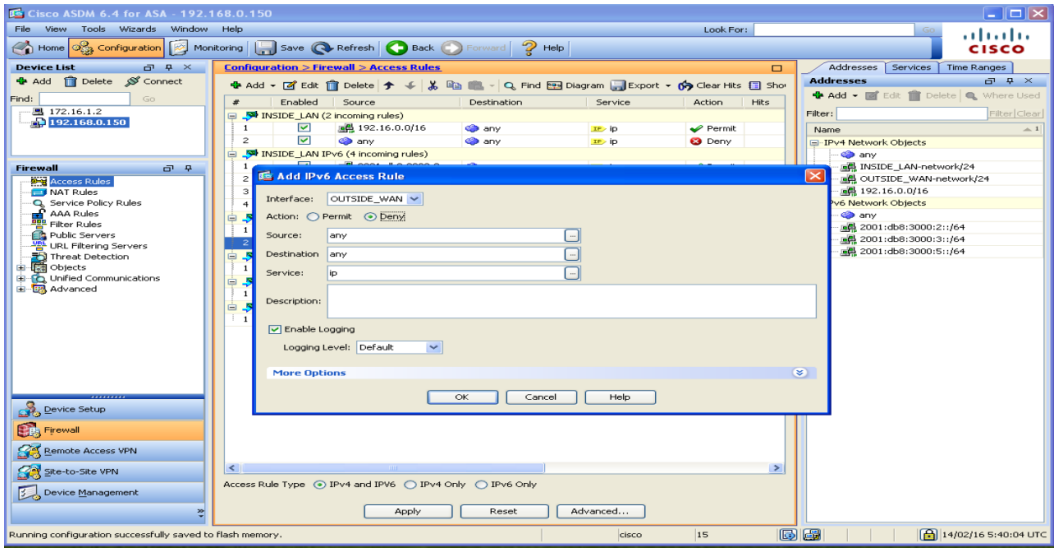


Figura 73. Reglas para denegar tráfico en la red OUTSIDE IPv6

Fuente: ASDM

4.1.3.3 Configuraciones en Switch CISCO 4503 (CORE)

La configuración de las VLANS de la red local y la comunicación de ellas hacia el ASA 5520 se realizan en el Switch CORE, se mostrará la configuración de una de ellas, pero el proceso es el mismo para cada una de las VLANS.

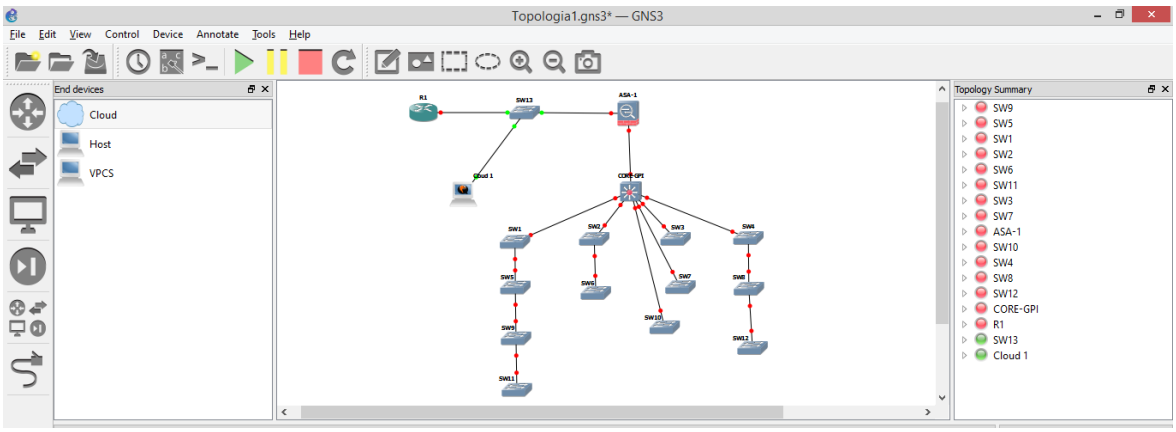


Figura 74. Topología de la Red

Fuente: GNS3

Hacer doble click sobre el Switch de CORE que se muestra en la Figura 74, para abrir la consola de configuración.

Dentro de la consola para colocar en modo acceso al puerto o interfaz de la VLAN se deben escribir los siguientes comandos, como se muestra en la Figura 75.

CORE-GPI#configure terminal
CORE-GPI(config)# interface fastEthernet 0/0
CORE-GPI(config-if)# switchport mode access
CORE-GPI(config-if)# switchport access vlan 2
CORE-GPI(config-if)# no shutdown

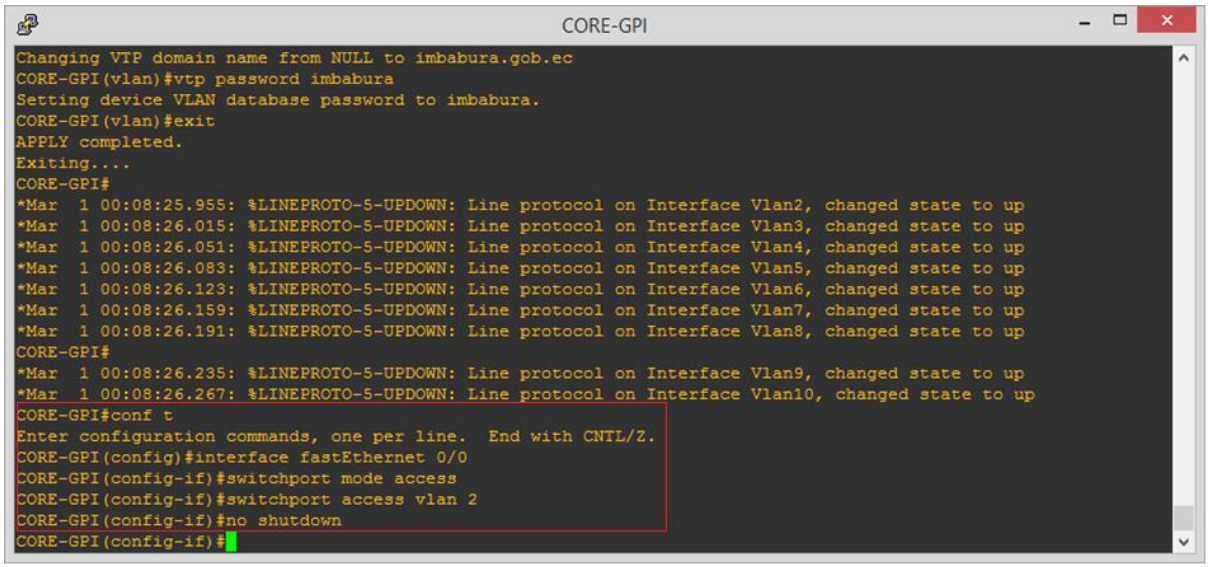


Figura 75. Interfaz de VLAN en modo acceso
Fuente: GNS3

Para crear una VLAN se debe introducir las siguientes líneas de comandos, lo cual se muestra en la Figura 76.

CORE-GPI# vlan database
CORE-GPI(vlan)# vlan <número de la vlan> name <nombre de la vlan>

Esto se debe hacer para cada VLAN q se necesite de acuerdo al direccionamiento que se tenga.

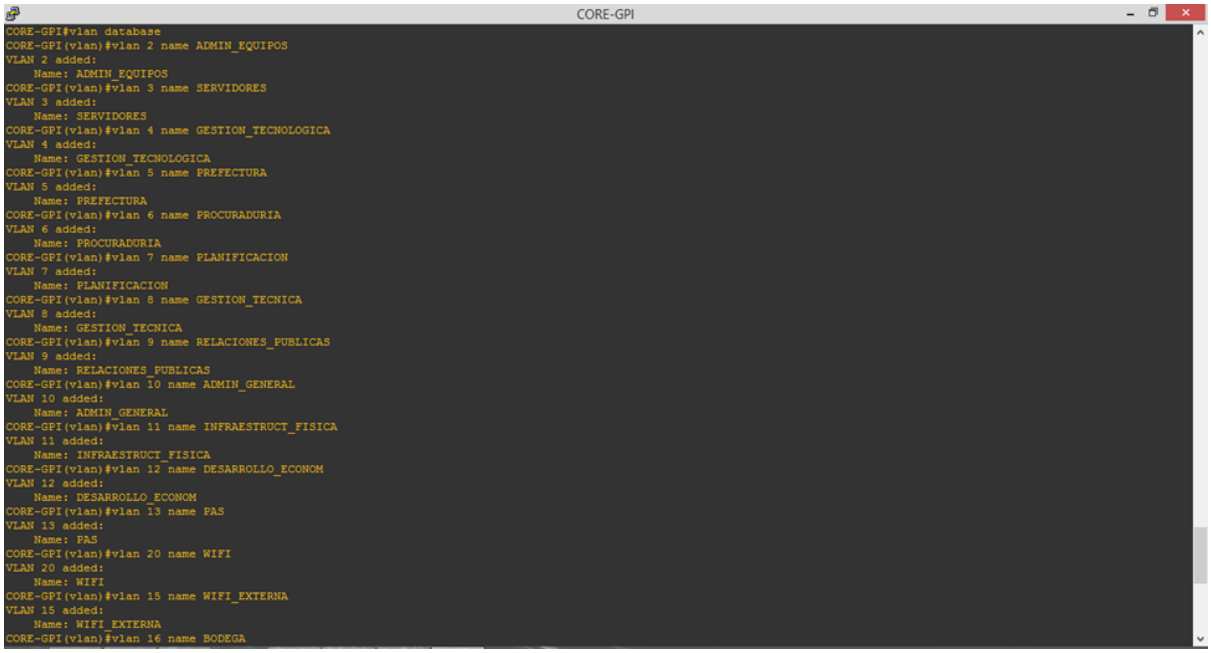


Figura 76. Creación de VLAN´s

Fuente: GNS3

Para que las VLAN's se propaguen por el resto de la red es necesario habilitar vtp server, como se muestra en la Figura 77, ya que esto reduce la necesidad de configurar la misma VLAN en todos los Switchs. Con los siguientes comandos se habilita VTP.

CORE-GPI(vlan)# vtp server

CORE-GPI(vlan)# vtp domain <nombre de dominio>

CORE-GPI(vlan)# vtp password <asignar una contraseña>

CORE-GPI(vlan)# exit

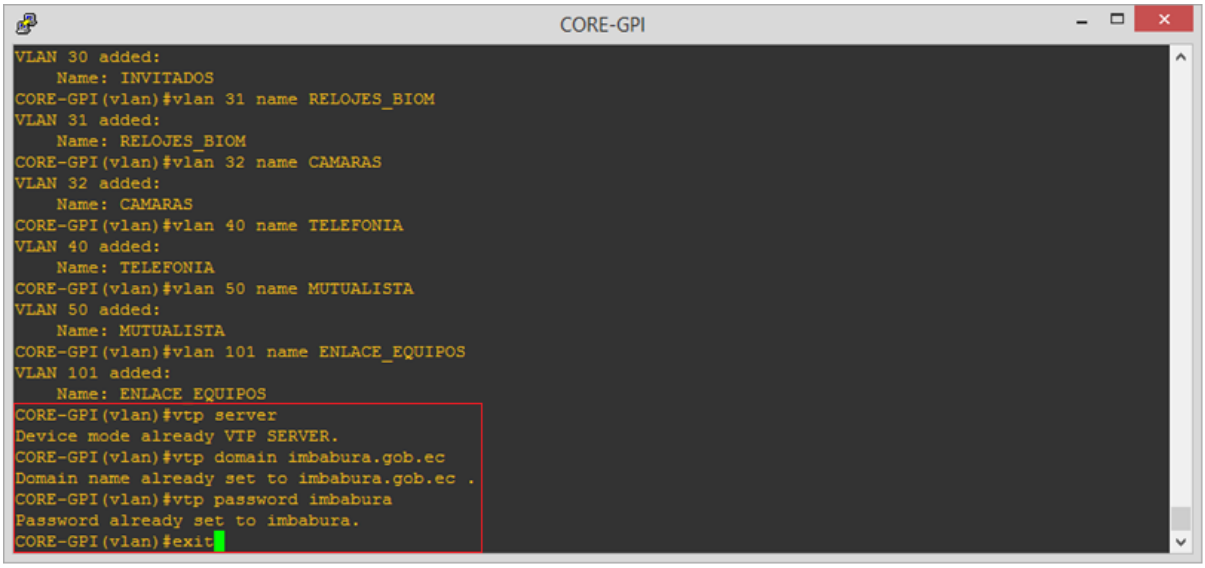


Figura 77. Habilitación de vtp server

Fuente: GNS3

En la Figura 78, se observa el comando para la verificación el estado de las VLAN's.

CORE-GPI# show vlan-switch

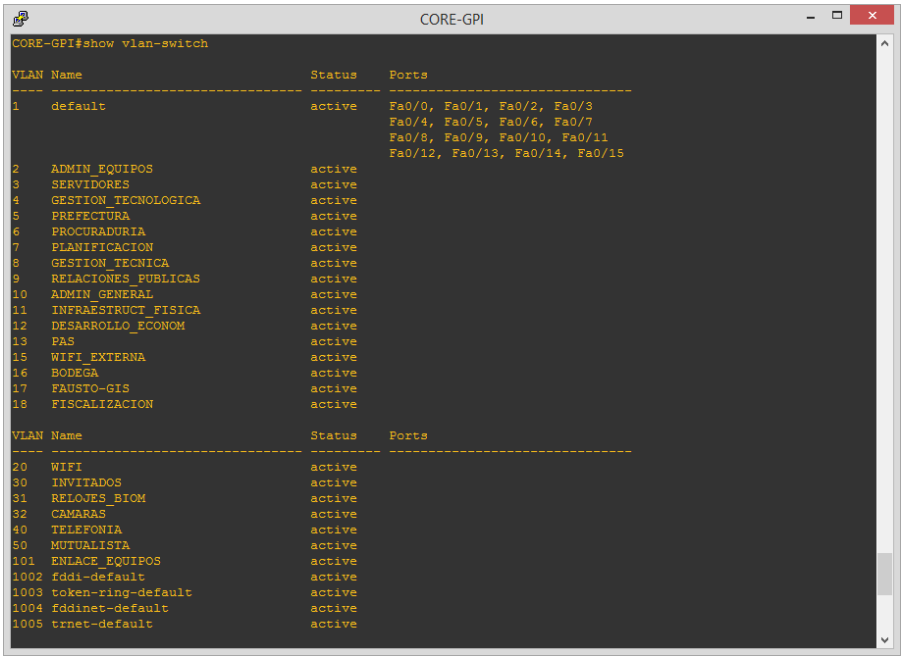


Figura 78. Estado de VLAN's

Fuente: GNS3

Para que los dispositivos de la red que se encuentren conectados en diferentes Switchs se puedan comunicar donde existan VLANS's, se debe configurar Trunk ya que es un enlace entre dos Switchs en el cual se canaliza el tráfico que pertenece a las VLAN's.

El puerto Trunk debe ser configurado en los dos extremos del enlace, en este caso, en los Switchs que están conectados directamente al Switch de CORE mediante los comandos, lo cual se indica en la Figura 79.

CORE-GPI# configure terminal
CORE-GPI(config)# interface fastEthernet 0/3
CORE-GPI(config-if)# switchport mode trunk
CORE-GPI(config-if)# exit

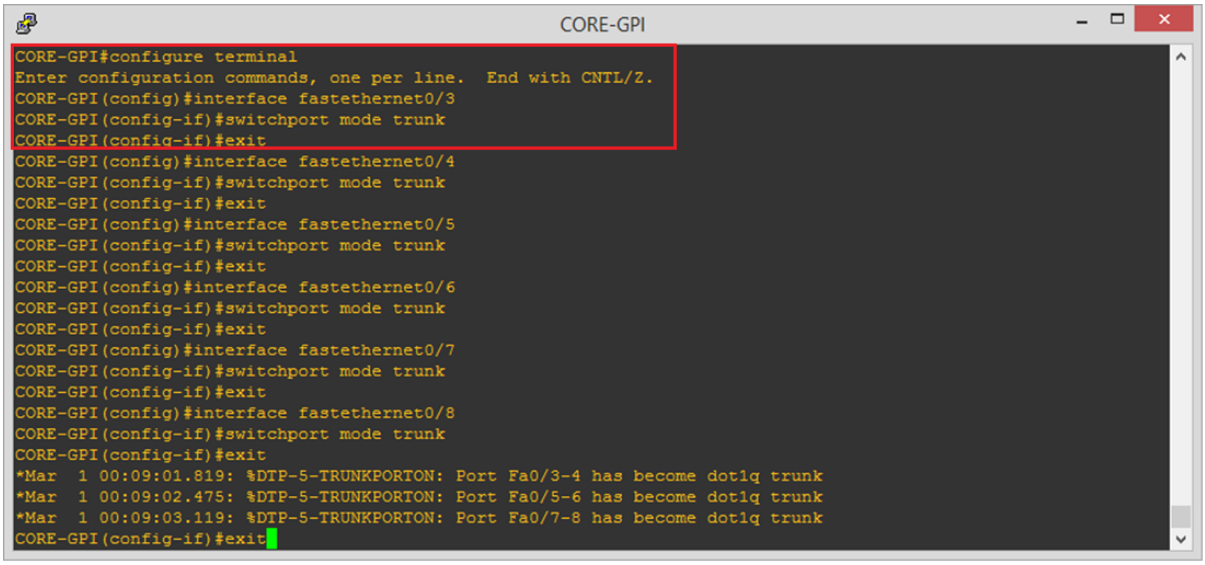


Figura 79. Puerto modo troncal

Fuente: GNS3

En la Figura 80 se muestran los comandos que se debe configurar en el equipo para que tenga los dos protocolos de internet.

CORE-GPI# configure terminal
CORE-GPI(config)# interface vlan <número de la vlan>
CORE-GPI(config-if)# ip address <direccion IP> <mascara de subred>
CORE-GPI(config-if)# ipv6 address <direccion IPv6>/<prefijo>
CORE-GPI(config-if)# ipv6 enable

CORE-GPI(config-if)# no shutdown

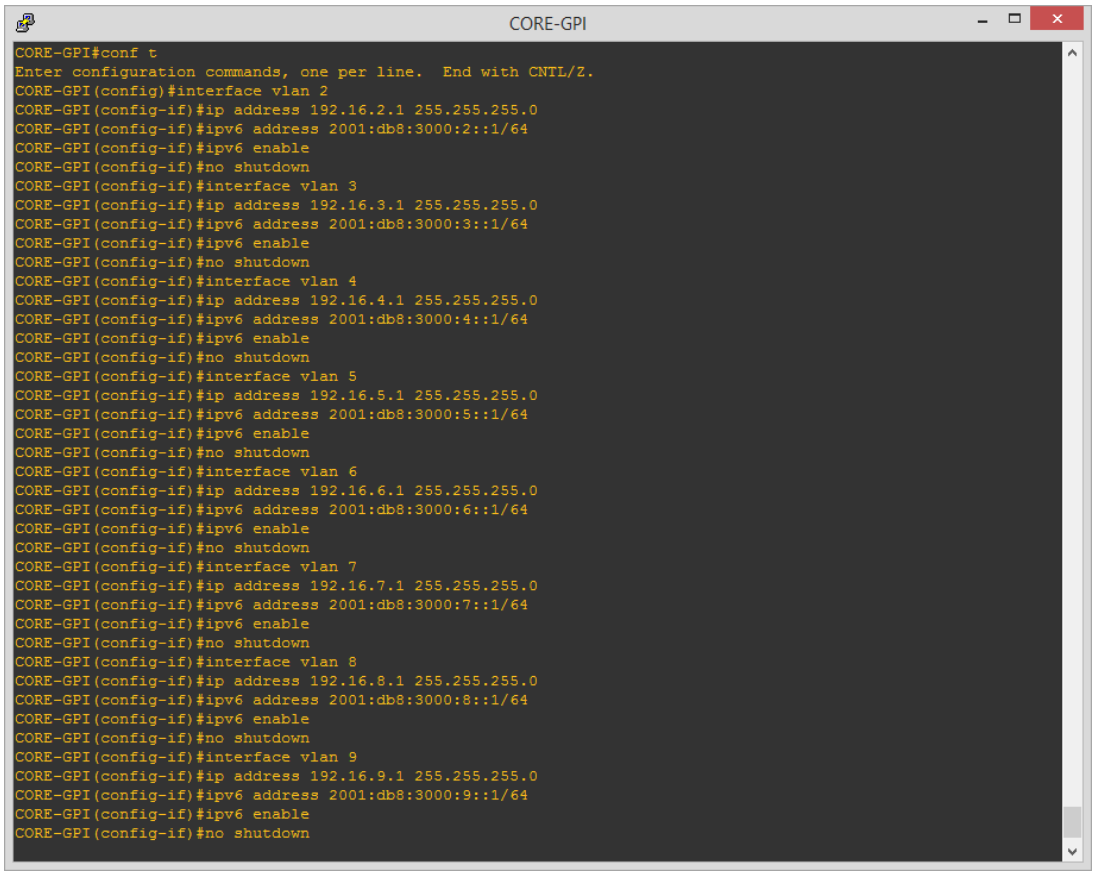


Figura 80.Habilitación de doble pila

Fuente: GNS3

Para habilitar IPv6 se utiliza los siguientes comandos, mostrados en la Figura 81.

SW1# configure terminal

SW1(config)# IPv6 unicast-routing

Esto se debe realizar en cada Switch de la Red

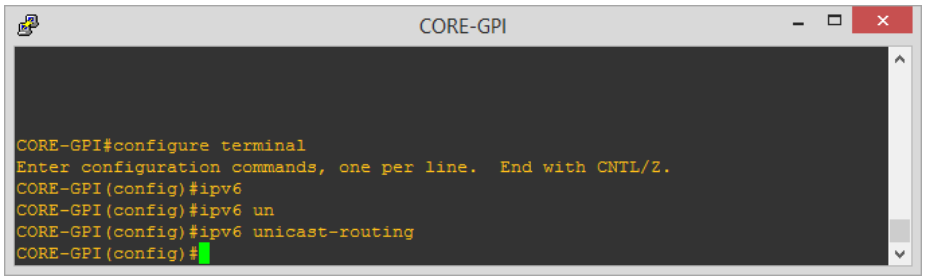


Figura 81. Habilitación de IPv6 en los Switchs

Fuente: GNS3

4.1.3.4 Configuración en Switch CISCO 2960

En una red conmutada, las VLAN separan a los dispositivos en diferentes dominios de colisión y subredes de Capa 3. Los dispositivos dentro de una VLAN pueden comunicarse entre sí sin necesidad de ruteo.

El diseño de la topología segmenta la red según el grupo o la función a la que corresponde el dispositivo. Por ejemplo, la VLAN del departamento de Tecnologías de la Información sólo tendrá dispositivos asociados con el departamento de Tecnología, mientras que en el departamento de Fiscalización la VLAN sólo tendrá dispositivos relacionados con Fiscalización. Si se habilita el ruteo, los dispositivos de cada VLAN pueden comunicarse entre sí, sin necesidad de que estén todos en el mismo dominio de transmisión.

Dicho así, para que se propaguen las VLANs previamente configuradas en el Swiths de CORE se debe habilitar en cada Switch de la topología el cliente VTP y el puerto en modo troncal mediante los siguientes comandos para así recibir las actualizaciones de las VLANs.

```
SW2# configure terminal
SW2(config)# interface fastEthernet 0/0
SW2(config-if)# switch mode trunk
SW2(config-if)# exit
```

Si existen más interfaces conectadas, se deben habilitar de acuerdo al requerimiento de la topología como se muestra en la Figura 82.

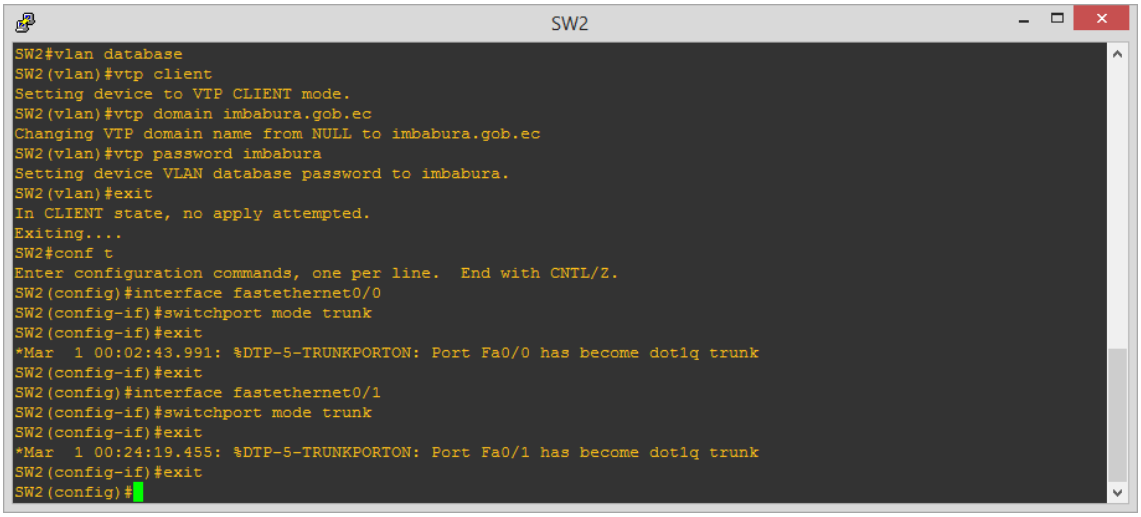


Figura 82. Configuración Switch en modo trunk

Fuente: GNS3

Verificar que las VLAN's estén propagadas mediante el comando, como se muestra en la Figura 83.

SW2# show vlan-switch → comando para simulación

SW2# show vlan → comando switch 2960

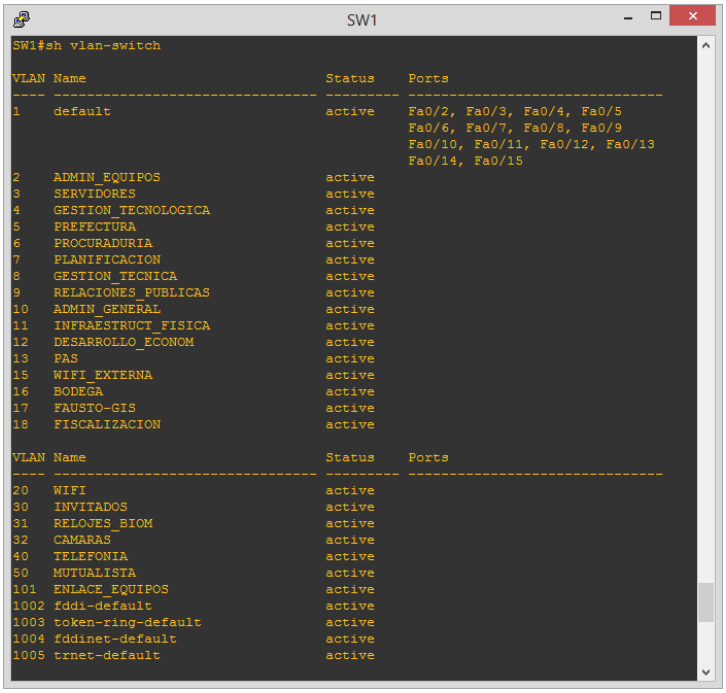


Figura 83. Comando para verificar la ropagación de VLAN's

Fuente: GNS3

Para habilitar un puerto del Switch en modo acceso para dar conectividad a la VLAN pertinente, se debe digitar los siguientes comandos, los cuales se muestran en la Figura 84.

SW1# configure terminal
SW1(config)# interface fastEthernet 0/2
SW1(config-if)# switchport mode Access
SW1(config-if)# switchport access vlan 2
SW1(config-if)# no shutdown
SW1(config-if)# exit

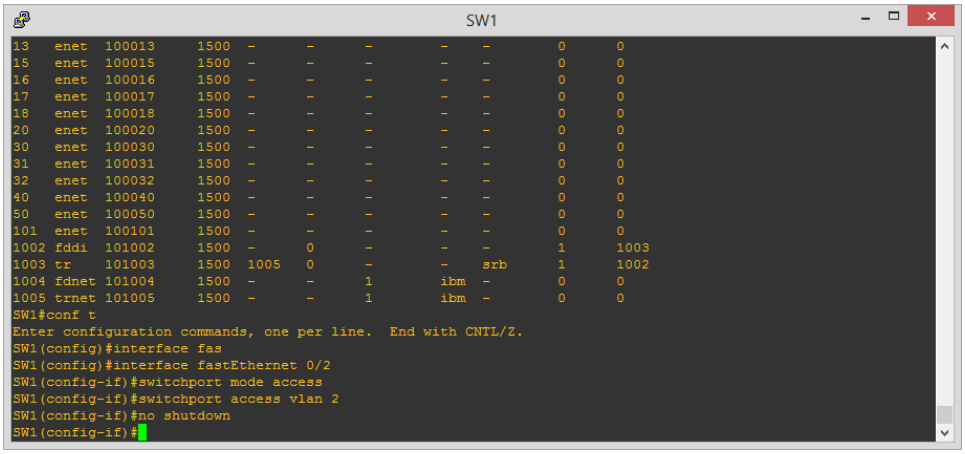


Figura 84. Habilitación del Switch en modo acceso

Fuente: GNS3

En el caso de los Switchs se debe digitar el comando ipv6 unicast-routing, para la habilitación del reenvio de paquetes IPv6, como se indica en la Figura 85.

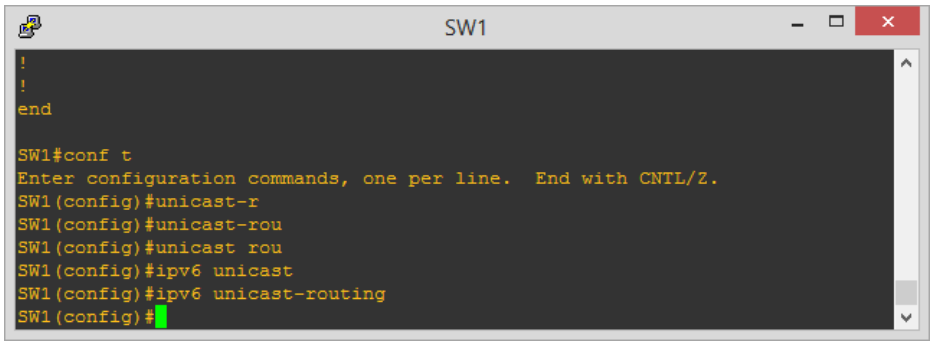


Figura 85. Habilitación de reenvio de paquetes en los Switchs

Fuente: GNS3

Agregar una dirección IP en sus versiones IPv4 e IPv6 para administrar el Switch 1, como indica la Figura 86.

SW1# configure terminal
SW1(config)# ipv6 unicast-routing
SW1(config)# interface vlan 2
SW1(config-if)# ip address <dir IPv4> <máscara>
SW1(config-if)# ipv6 address <dir IPv6> <prefijo>
SW1(config-if)# ipv6 enable
SW1(config-if)# no shutdown
SW1(config-if)#exit

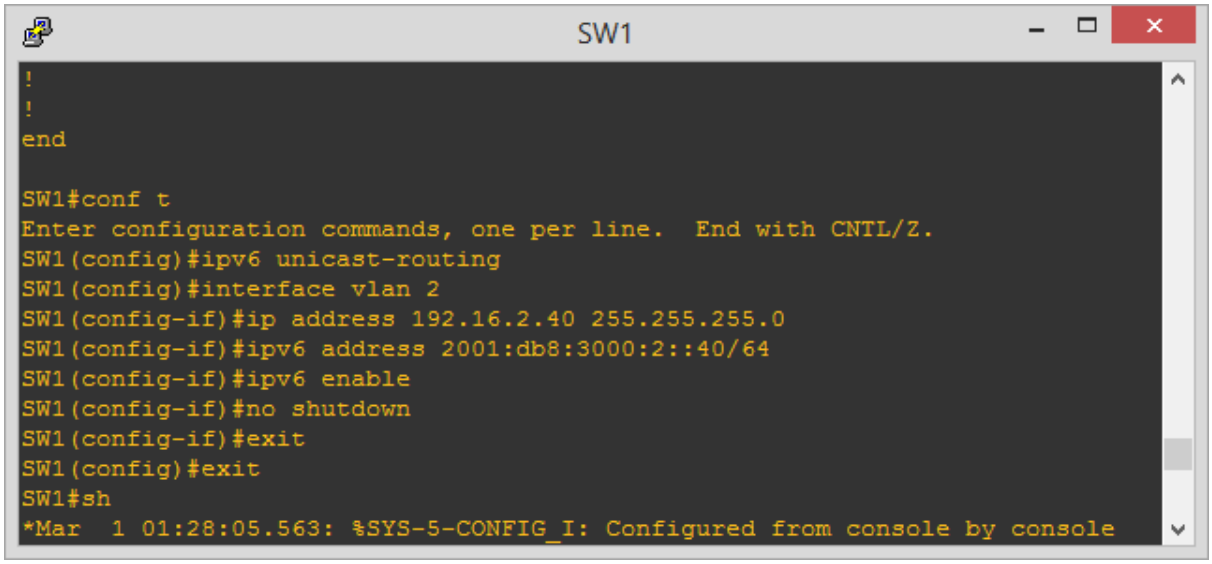


Figura 86. Direcciones IP para administrar el Switch 1

Fuente: GNS3

Agregar una dirección IP en sus versiones IPv4 e IPv6 para administrar el Switch 1, como se muestra en la Figura 87.

SW1# configure terminal
SW1(config)# ipv6 unicast-routing
SW1(config)# interface vlan 2
SW1(config-if)# ip address <dir IPv4> <máscara>
SW1(config-if)# ipv6 address <dir IPv6> <prefijo>
SW1(config-if)# ipv6 enable

SW1(config-if)# no shutdown

SW1(config-if)#exit

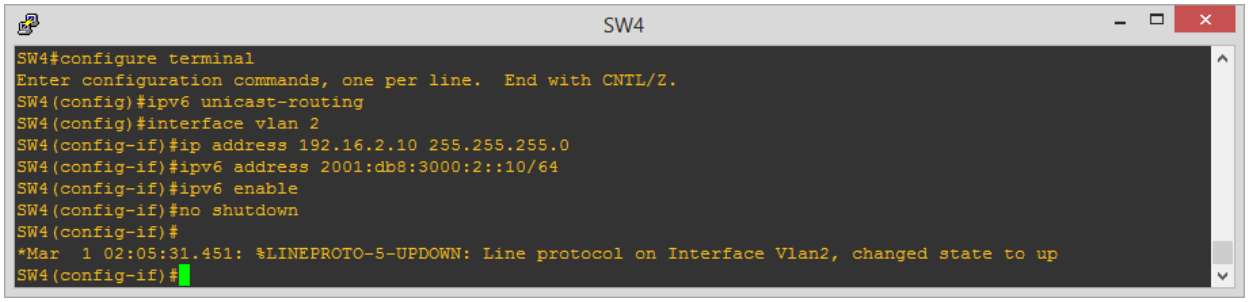


Figura 87. Direcciones IP para administrar el Switch 4

Fuente: GNS3

En la Figura 88 se muestra la prueba de conectividad en IPv4 e IPv6, para esto se debe utilizar los siguientes comandos

SW4# ping <dir IPv4 del SW1>

SW4# ping ipv6 <IPv6 del SW1>

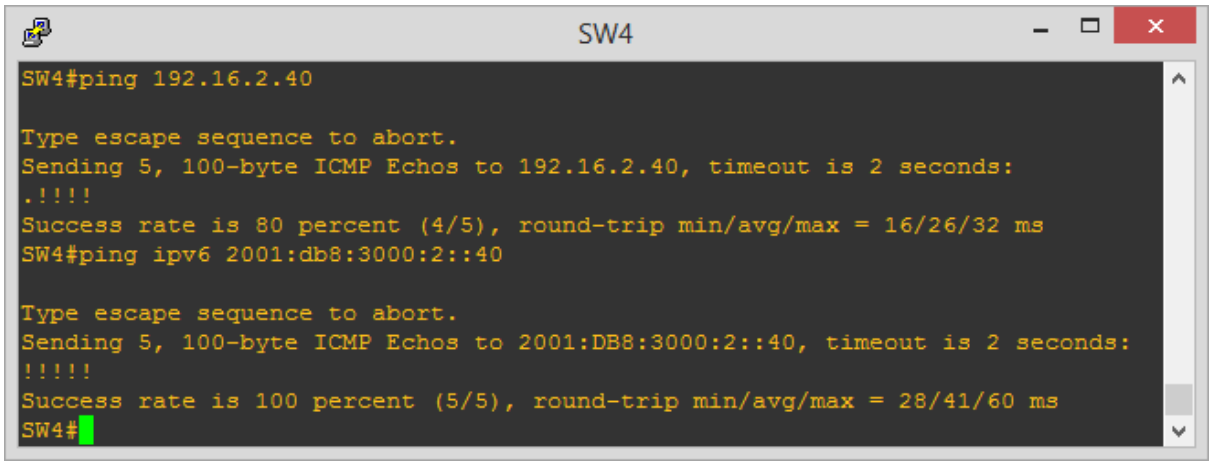


Figura 88. Pruebas de conectividad entre Switchs con los protocolos IPv4 e IPv6

Fuente: GNS3

4.1.3.5 Configuración de Aplicaciones Seleccionadas

Los servicios y aplicaciones se van a levantar sobre la plataforma de software libre CentOS 6.4, con la finalidad de solventar la funcionalidad de la red en doble pila. El Sistema Operativo debe estar previamente instalado (la instalación CentOS se encuentra

en el Anexo D). El desarrollo de las aplicaciones sirve como base demostrativa en el desarrollo del proceso de transición de los protocolos de internet IPv4 e IPv6.

4.1.3.5.1 Servidor WEB

En el levantamiento del Servidor WEB se establecerá que los servicios funcionen con los dos protocolos de internet (IPv4 / IPv6), inicialmente se debe instalar el paquete de Web server utilizando el comando, como se muestra en la Figura 89.

:

yum -y group install “Web server”

Figura 89. Instalación de Web server

Fuente: CentOS

El Servidor debe estar configurado en la interfaz tanto en IPv4 como en IPv6, con esto podrá recibir peticiones de los usuarios de ambos protocolos. Se debe ingresar con el siguiente comando al fichero de configuración de interfaces. El cual se muestra en la Figura 90.

vi/etc/sysconfig/network-scripts/ifcfg-eth0

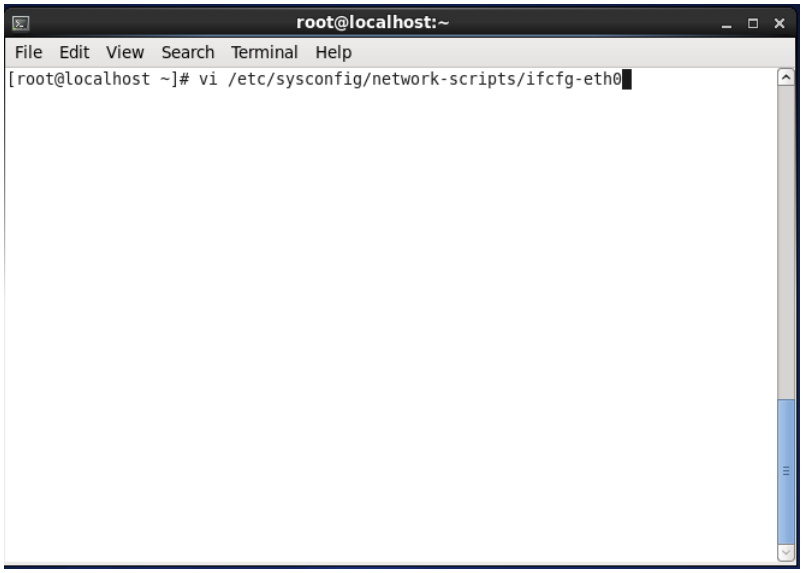


Figura 90. Comando para configuración de interfaces

Fuente: CentOS

Dentro del fichero agregar y editar las líneas con los parámetros correspondientes tanto en IPv4 como en IPv6, como se muestra en la Figura 91.

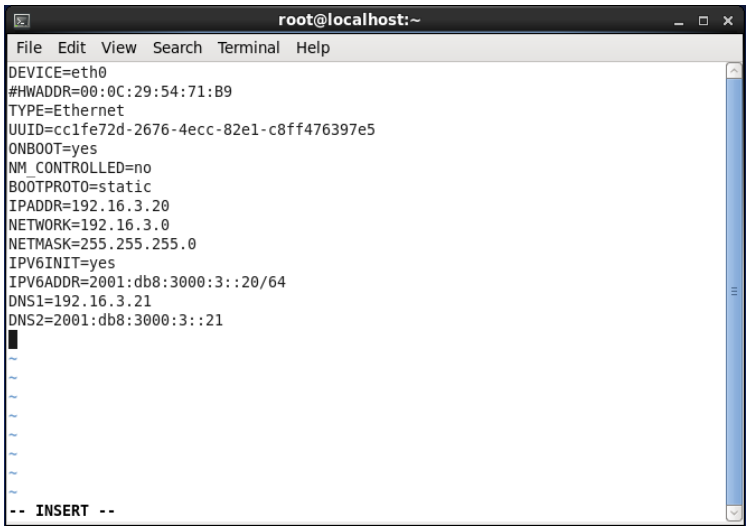


Figura 91. Agregar los parámetros en IPv4 e IPv6

Fuente: CentOS

Otro de los ficheros a editar para que el servidor trabaje en ambos protocolos de internet es el archivo de red que se encuentra en vi/etc/sysconfig/network como se muestra en la Figura 92.

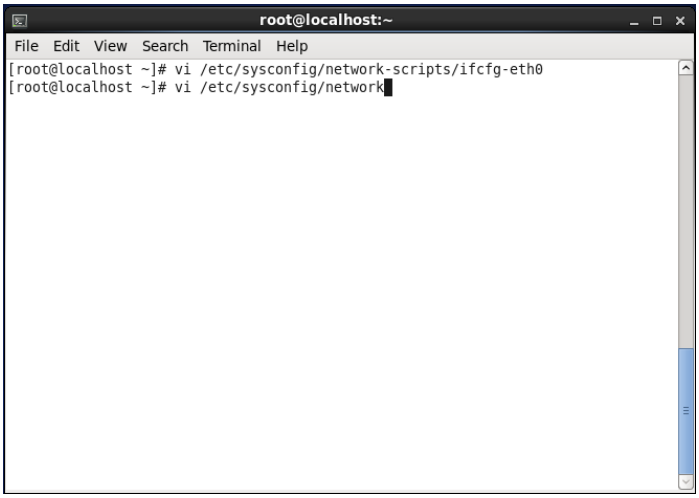


Figura 92. Comando para ingresar al fichero de red

Fuente: CentOS

Las líneas que se añaden sirven para que el equipo servidor trabaje sobre IPv6 y para que sea estable al no auto-configurarse en el Protocolo de Internet versión 6, como se indica en la Figura 93.

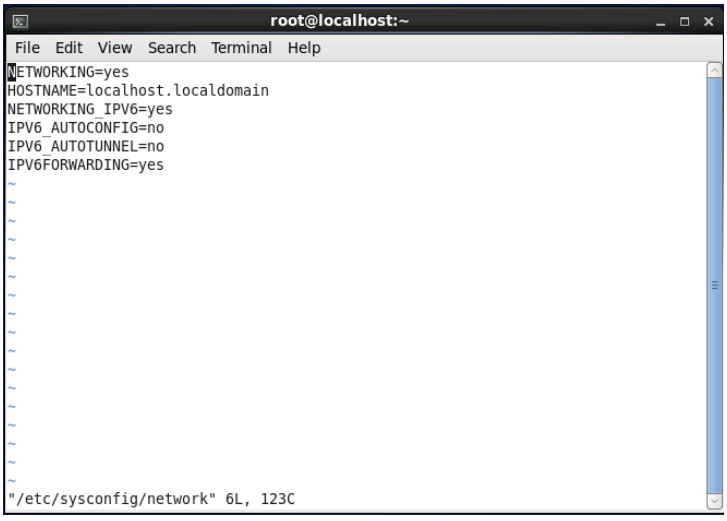


Figura 93. Archivo Network

Fuente: CentOS

Se debe reiniciar el servicio para que surtan efecto los cambios realizados en los ficheros mediante el comando, lo cual se muestra en la Figura 94.

#service network restart

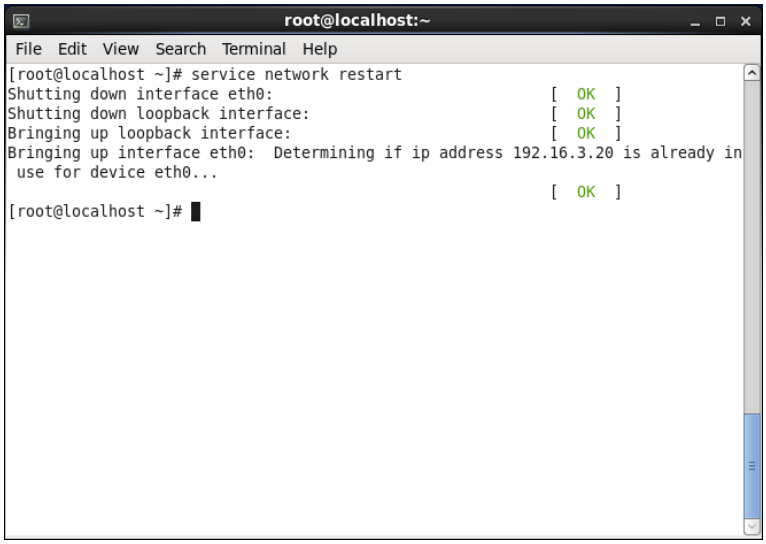


Figura 94. Reinicio de servicios

Fuente: CentOS

Para el direccionamiento del servidor web para que se escuche por el puerto 80, digitar el siguiente comando, como se muestra en la Figura 95.

vi /etc/httpd/conf/httpd.conf

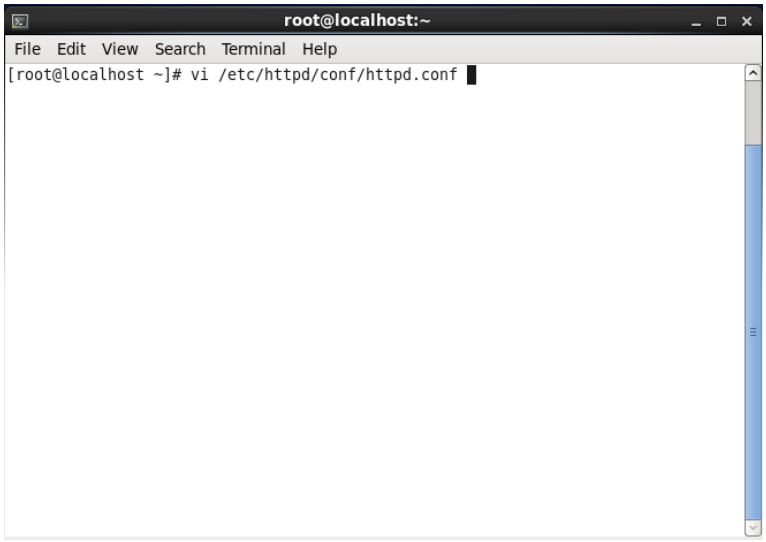


Figura 95. Direccionamiento de escucha por el puerto 80

Fuente: CentOS

Dentro del fichero, editar la línea 136 y cambiar por Listen *:80, con el fin de que todas las peticiones que se realicen en el servidor web sean escuchadas por este puerto, esto se indica en la Figura 96.

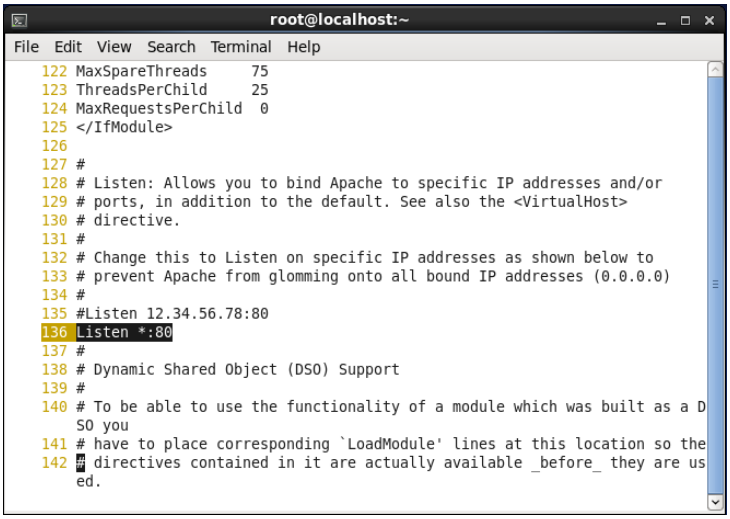


Figura 96. Archivo del puerto 80

Fuente: CentOS

Reiniciar el servicio http para que los cambios realizados hagan efecto con el comando service httpd restart, tal como se muestra en la Figura 97.

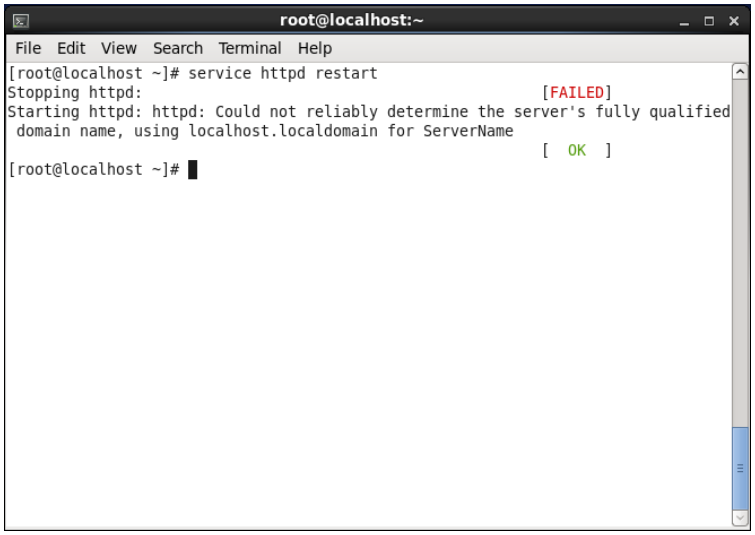


Figura 97. Reinicio del servicio http

Fuente: CentOS

Al finalizar el anterior proceso se puede observar que ingresando las direcciones tanto en IPv4 como IPv6 en el navegador se verifica el funcionamiento del servidor web, esto se muestra en la Figura 98.

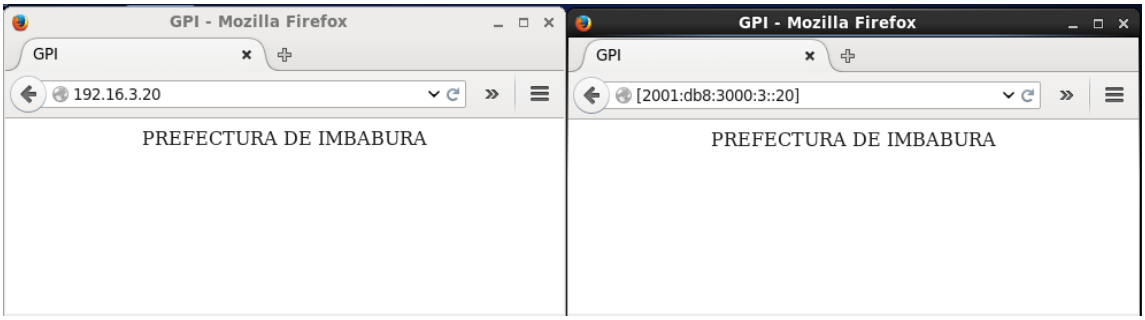


Figura 98. Prueba de funcionamiento del servidor Web

Fuente: CentOS

4.1.3.5.2 Servidor DNS

Para el funcionamiento del DNS64 es necesario instalar uno de los paquetes desarrollado para el servidor de nombre de dominios, en CentOS este paquete se llama bind y se instala mediante el comando, como se indica en la Figura 99.

#yum install bind* -y

Figura 99. Instalación de bind

Fuente: CentOS

Las configuraciones de interfaces del servidor DNS64 se realiza digitando el siguiente comando #vi /etc/sysconfig/network-scripts/ifcfg-eth1, como indica la Figura 100.

Figura 100. Comando de Configuración de Interfaces

Fuente: CentOS

Dentro del script agregar las direcciones de red correspondientes, tanto IPv4 como IPv6, como indica la Figura 101.

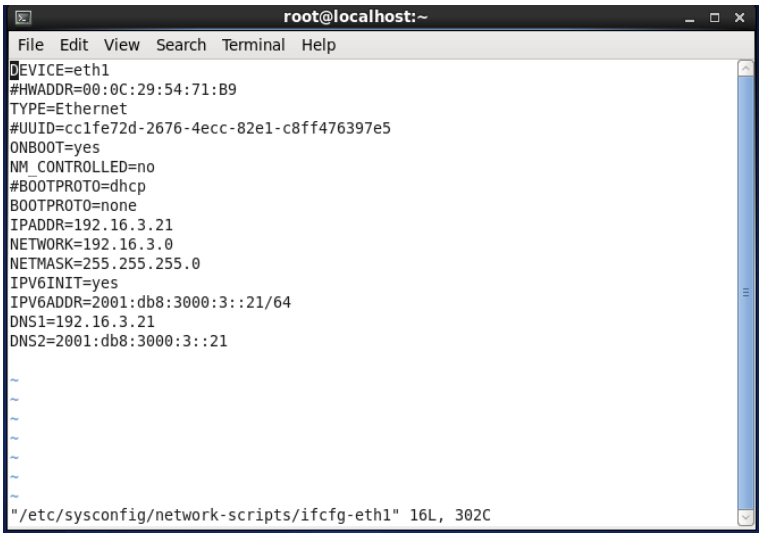


Figura 101.Configuración de Interfaces

Fuente: CentOS

El siguiente paso para iniciar la configuración del servidor DNS64 se debe editar el fichero named.conf, mediante el comando:

#vi /etc/named.conf

En el archivo de configuración modificar la línea 12 cambiando de {::1;} a {any;} para que resuelva a todos los usuarios que se encuentran con IPv6.

Agregar las líneas 19, 20 y 21 de los reenviadores (forwarders) a internet, estos sirven para enviar consultas de nombres DNS externos a los usuarios locales dentro del dominio de la red.

Se edita la línea 24 reemplazando el contenido por {any;} para que el servidor escuche consultas desde cualquier servidor IP.

Las líneas 25, 26 y 27 indican aquellas consultas DNS de los usuarios que solo tienen registro A y no AAAA, para estos se entregan a los clientes añadiendo 2001:db8:3000:3::21/96, como se muestra en el figura 102.

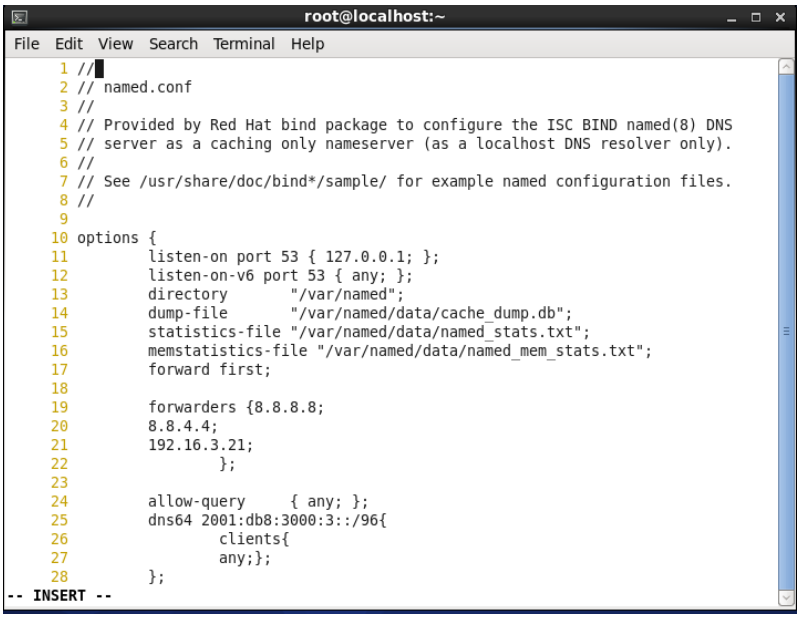


Figura 102. Archivo de configuración named.conf

Fuente: CentOS

Luego de cambiar y agregar contenido en el archivo, se debe reiniciar bind mediante el comando que se muestra en la Figura 103.

#service named restart

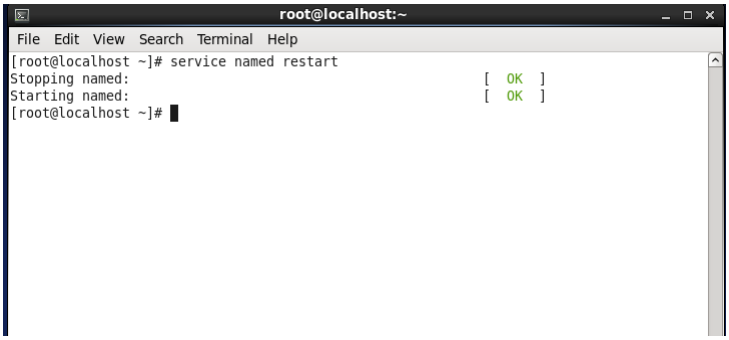


Figura 103. Reinicio de bind

Fuente: CentOS

- CREACIÓN DE ZONAS DNS64

La primera zona que se debe definir es la zona directa, en el fichero de configuración named.conf, las 4 líneas editadas se describen como, esto se muestra en la Figura 104.

- La primera línea es el nombre de la zona
- La segunda línea indica el tipo de zona master o directa
- La tercera línea muestra el lugar donde está el archivo de configuración de la zona directa
- La cuarta línea indica que no recibe actualizaciones de otros DNS

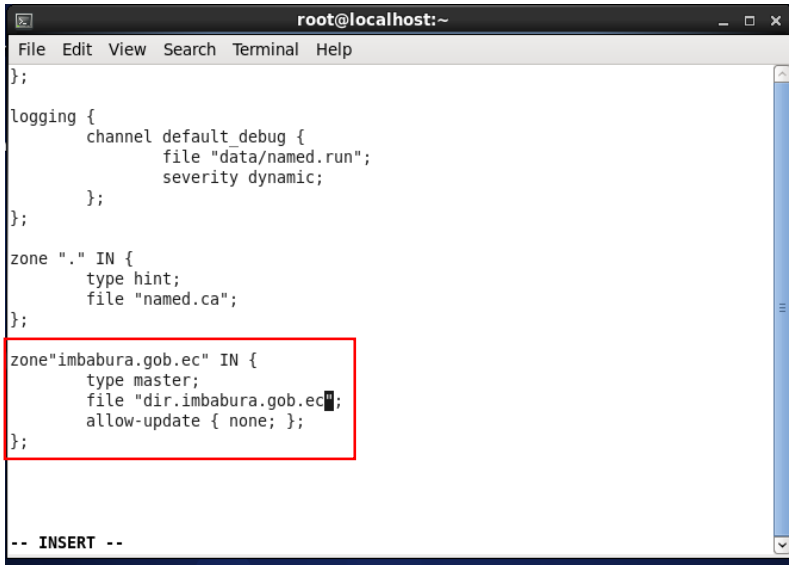


Figura 104. Definición de zona primaria

Fuente: CentOS

En la Figura 105, se muestra la definición de las zonas inversas en IPv6 e IPv4

La zona inversa IPv6 se definen nibbles

La zona inversa IPv4 se definen números decimales

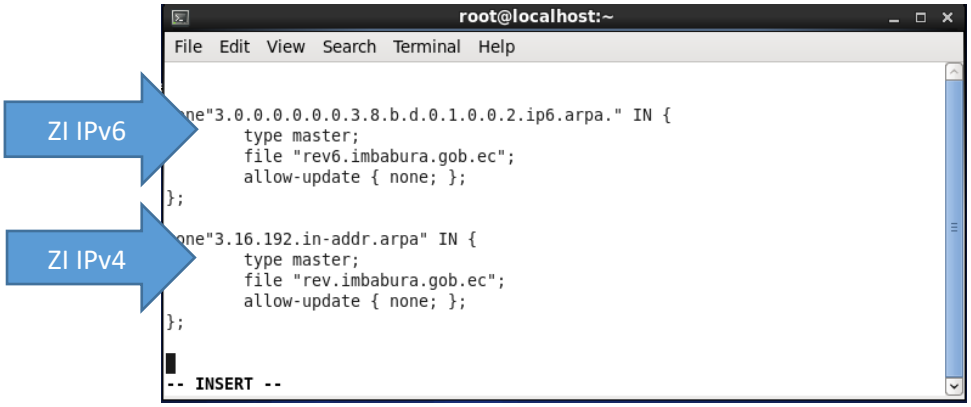


Figura 105. Definición de zonas inversas IPv6 e IPv4

Fuente: CentOS

Crear los archivos de cada una de las zonas

- Empezando por modificar la zona directa, con el comando:

#vi /var/named/dir.imbabura.gob.ec, y cambiar las líneas como se muestra en la Figura 106.

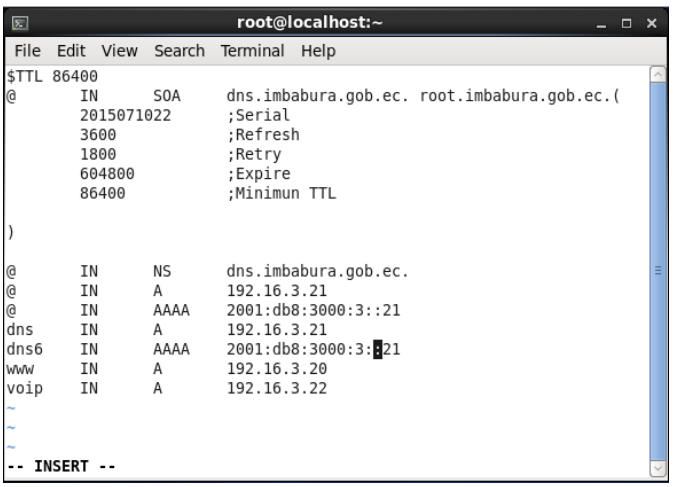


Figura 106. Archivo de zona directa

Fuente: CentOS

- Como segundo paso modificar la zona inversa IPv4 con el comando:

#vi /var/named/rev.imbabura.gob.ec, y cambiar las líneas como se muestra en la Figura 107.

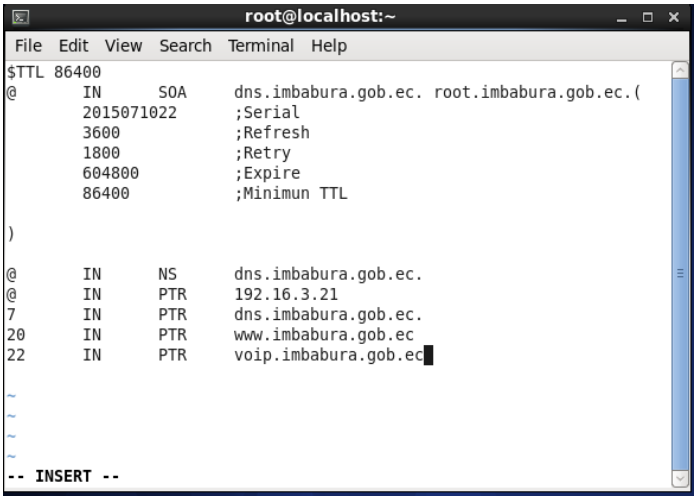


Figura 107. Archivo de zona inversa IPv4

Fuente: CentOS

- Como tercer paso modificar la zona inversa IPv6 con el comando:

#vi /var/named/rev6.imbabura.gob.ec, y cambiar las líneas como se muestra en la Figura 108.

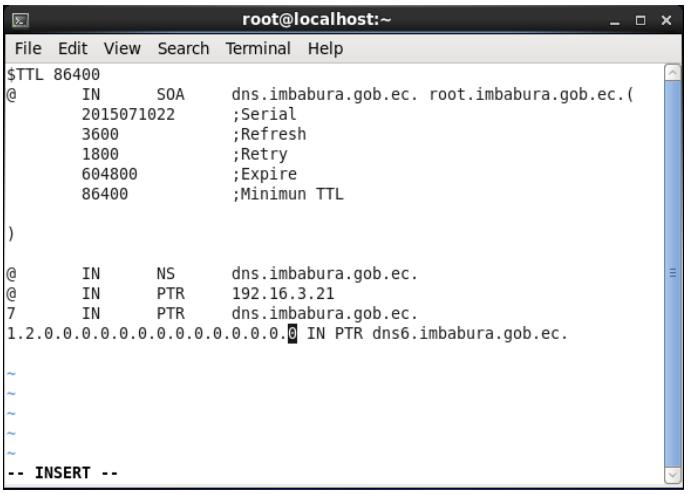


Figura 108. Archivo de zona inversa IPv6

Fuente: CentOS

Con el comando #dig dns.imbabura.gob.ec, se puede ver diagnósticos por zonas, esto se muestra en la Figura 109.

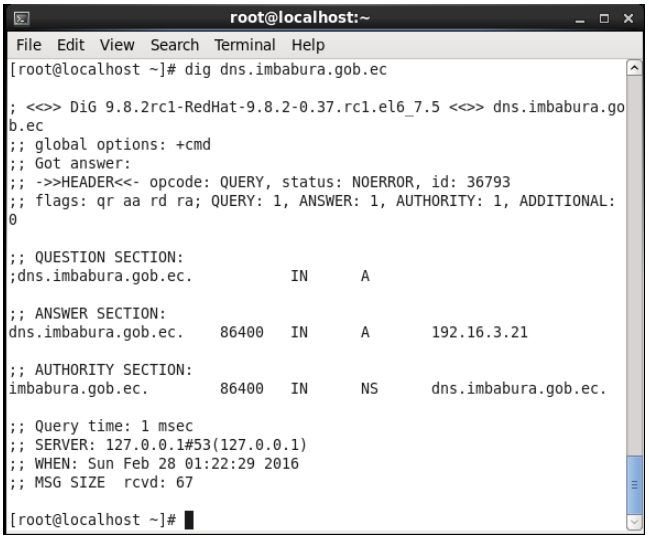


Figura 109. Diagnóstico de cada zona

Fuente: CentOS

Revisar que la resolución de nombres con registros AAAA si se está realizando, con el comando, como se indica en la Figura 110.

#dig dns.imbabura.gob.ec aaaa

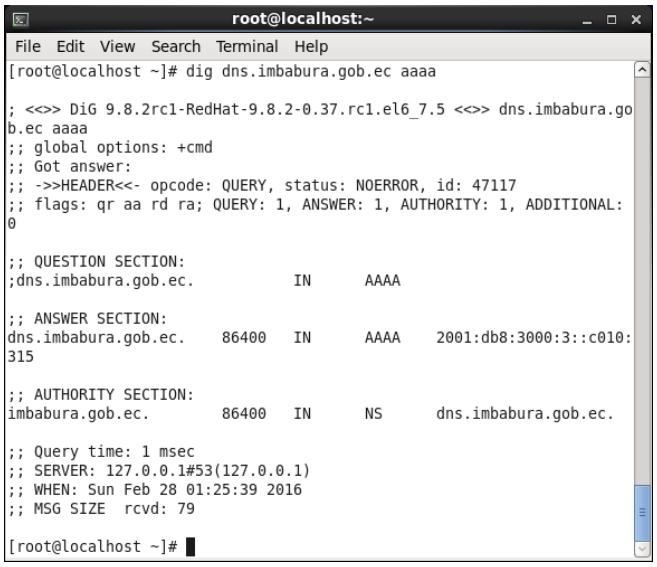


Figura 110. Resolución de nombres AAAA

Fuente: CentOS

Mostrar la resolución de zonas inversas, con el comando, como se muestra en la Figura 111.

#dig -x 2001:db8:3000:3::21

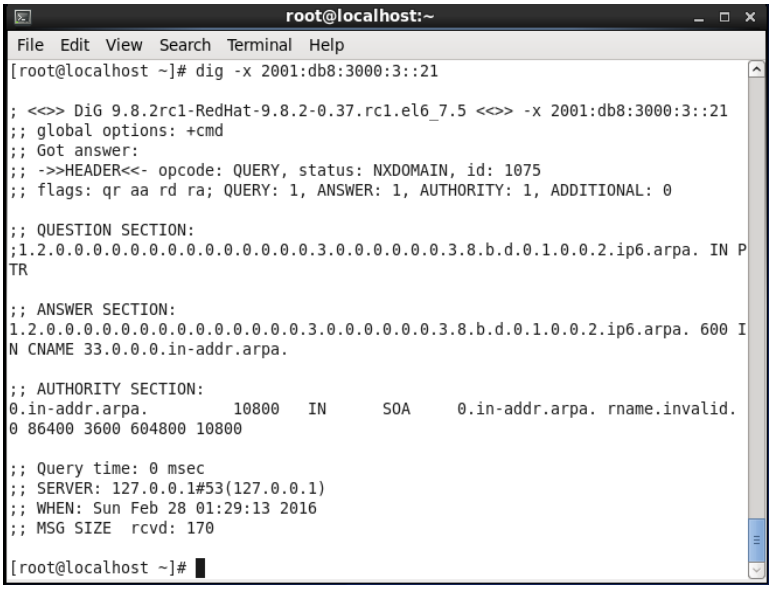


Figura 111. Resolución de zonas inversas

Fuente: CentOS

Para el funcionamiento del NAT64 es necesario instalar uno de los paquetes desarrollado para la traducción de direcciones de red, en CentOS este paquete se llama tayga, es necesario entrar al siguiente link y descargar desde el enlace FTP, como se muestra en la Figura 112.

http://rpm.pbone.net/index.php3/stat/4/idpl/30376782/dir/opensuse/com/tayga-0.9.2-6.51.x86_64.rpm.html

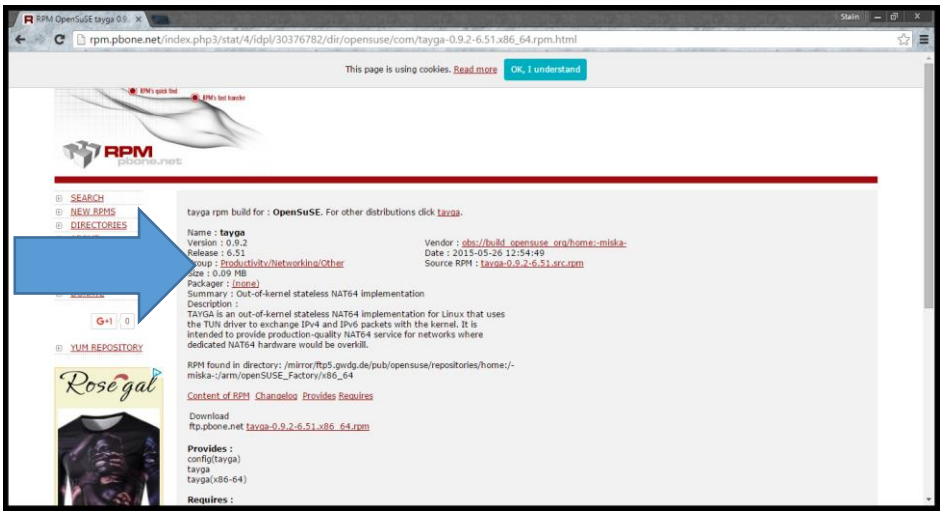


Figura 112. Página para descargar tayga

Fuente: RPM OpenSuSE

En la consola, entrar a la carpeta Download e instalar el paquete tayga, como se indica en la Figura 113.

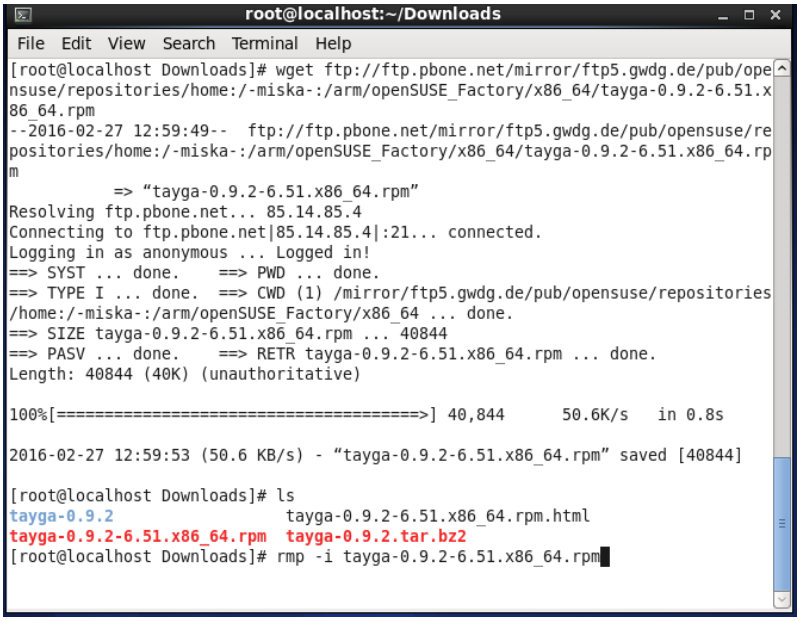


Figura 113.Instalación del paquete tayga

Fuente: CentOS

Estos comandos crean la interfaz nat64 con las direcciones IP, (192.16.3.21) IPv4 y (2001:db8:3000:3::21) IPv6, además las rutas y la habilitación de los reenviadores (forwarders) seteados en 1

- Si se setea en 1 se activan los reenviadores
- Si se setea en 0 se deshabilitan los reenviadores

También se agrega las reglas de nat y se da permisos de tráfico en el firewall del servidor, como se muestra en la Figura 114.

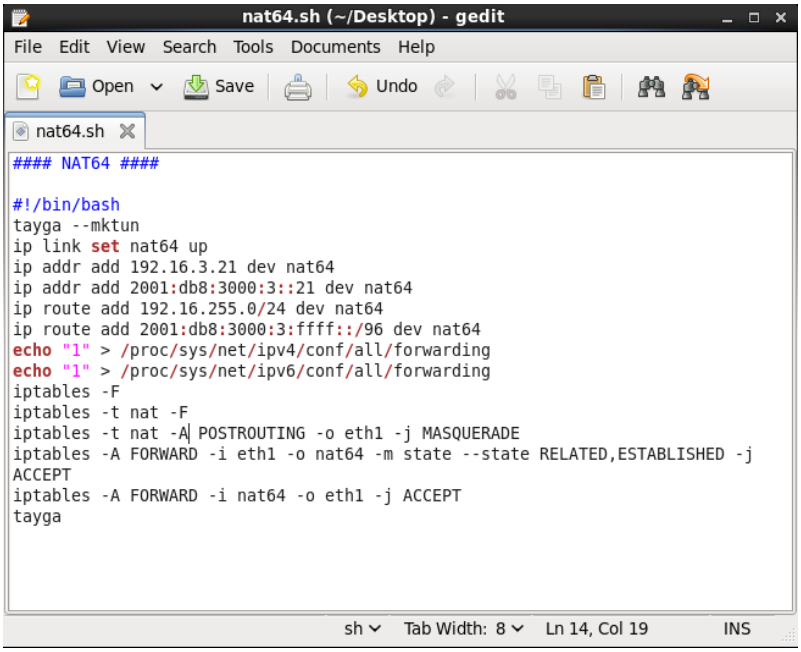


Figura 114. Comandos para crear la interfaz NAT64 y permisos de tráfico

Fuente: CentOS

Configurar el fichero tayga.conf, y asignar los valores de NAT y rangos con los que va a traducir las direcciones de IPv4 a IPv6, como indica la Figura 115.

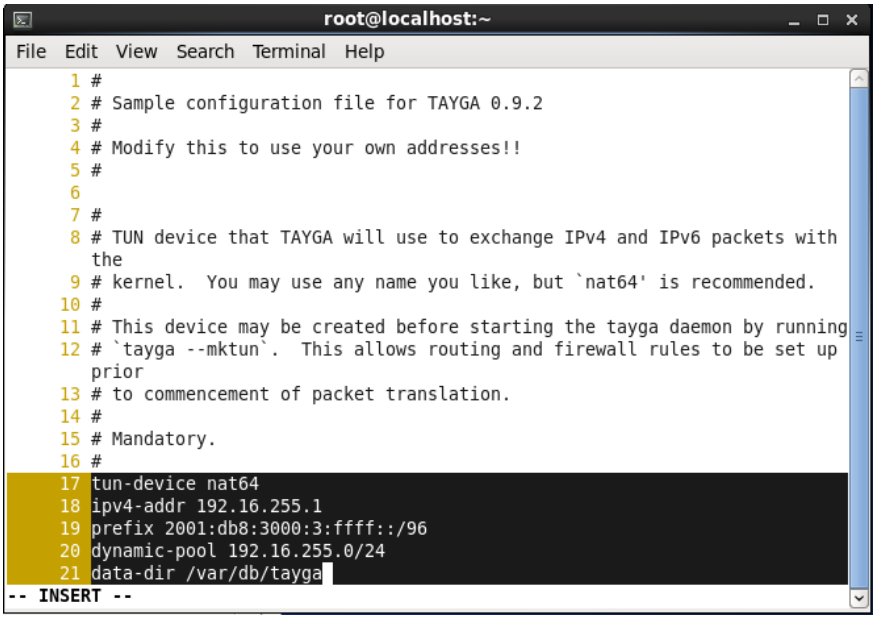


Figura 115. Fichero tayga.conf

Fuente: CentOS

Para saber si la traducción de IPs se ha realizado con éxito, hacer ping a la interfaz en IPv6, con su respectiva extensión de IPv4. Como muestra la Figura 116.

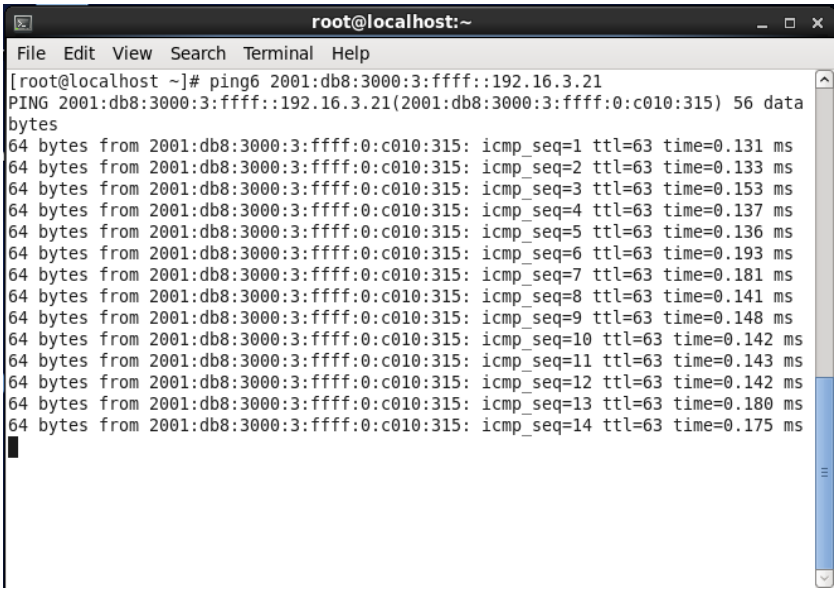


Figura 116. Ping en IPv6

Fuente: CentOS

Capítulo 5

5. Análisis de Factibilidad Técnica

En este capítulo se desarrollará el análisis de factibilidad de la transición hacia el Protocolo de Internet Versión 6 en el Gobierno Provincial de Imbabura, para la posterior implementación de la tecnología y la implementación de dos aplicaciones que soporten el protocolo.

5.1 Análisis de Factibilidad Técnica de la transición hacia el Protocolo de Internet Versión 6

Para determinar si el proyecto es factible técnicamente, se debe realizar una serie de evaluaciones las cuales permitan establecer si el hardware, software y recurso humano con el que cuenta la Dirección de Tecnologías de Información de la Prefectura de Imbabura, posee las capacidades técnicas necesarias para garantizar una futura transición del protocolo IPv4 a IPv6.

5.1.1 Recurso Tecnológico

El recurso tecnológico se valorará en términos generales tomando en cuenta el hardware y software utilizado para la transición de los protocolos mencionados.

5.1.1.1 Hardware Necesario

Luego de haber identificado los métodos de transición adecuados para la infraestructura de red, se pudo determinar que los dispositivos son compatibles con IPv6, tal como se indica en el Anexo A de las fichas técnicas, esto facilitaría una futura implementación de la tecnología.

5.1.1.2 Software Necesario

Para demostrar que la transición entre IPv4 e IPv6 es viable en la Prefectura de Imbabura, se utilizó el siguiente software, el cual cuenta con licensiamiento libre:

- CentOS
- WebServer
- PostFix
- FTP
- Elastix

En la Tabla 20 se señalan los requerimientos de cada una de las aplicaciones que fueron utilizadas para las pruebas de funcionamiento de la coexistencia de protocolos.

Tabla 20. Requerimientos de Aplicaciones

Aplicación	**Procesador**	**Memoria RAM**	**Disco**
CentOS	1 GHz (mínimo) 1,5 GHz (óptimo)	1GB	20GB (mínimo) 40GB (óptimo)
Web	700 MHz	64 MB	50 MB
FTP	450 MHz	256 MB	15 MB
SMTP	1 GHz	2 a 4 GB	170 GB
Elastix	600 MHz	512 MB	40 GB

Fuente: Recuperado de http://elastixtech.com/elastix-requisitos-para-usarlo/

Para este proyecto se escogio utilizar Software Libre en este caso el Sistema Operativo CentOS que es la mejor alternativa en cuanto a seguridad para el manejo de servidores, además la Prefectura de Imbabura utiliza este sistema en la mayoría de sus aplicaciones instaladas.

5.1.2 Recurso Humano

En cuanto al personal que maneja la red, la Dirección de TIC’s de la Prefectura de Imbabura esta estructurada de manera jeraquica como se muestra a continuación.

- Director del Departamento: Es el jefe de la Dirección de Tecnologías de la Información, bajo su jurisdicción está el manejo de las areas de infraestructura y de software.

- Jefe de Operaciones: Es la persona encargada de ver el estado de la red, y asegurar su disponibilidad, mantenimiento y rendimiento, tiene bajo su dirigencia dos Ingenieros en Infraestructura.

- Ingeniero de Infraestructura: Se encarga del correcto funcionamiento del Cuarto de Comunicaciones.

Luego de haber descrito la estructura administrativa y en base a las encuestas realizadas al personal lo cual se muestra en el Anexo B se puede determinar que es necesario que exista mayor conocimiento en cuanto al Protocolo IPv6, para lo cual se sugirió al Director de TIC's que en el momento que se decida realizar la transición se realice una capacitación para que todo el personal este al tanto sobre el manejo y beneficios de la utilización de esta tecnología.

5.1.3 Evaluación Final

Al culminar el estudio de factibilidad técnica se establece que la Prefectura de Imbabura podrá realizar una transición de protocolos de internet siempre y cuando cuente con la asignación de recursos IPv6 necesarios.

5.2 Pruebas de funcionamiento

5.2.1 DNS64, NAT64 y WEB

En la Figura 129, se muestra la prueba de conectividad desde un usuario IPv4 al servidor WEB.

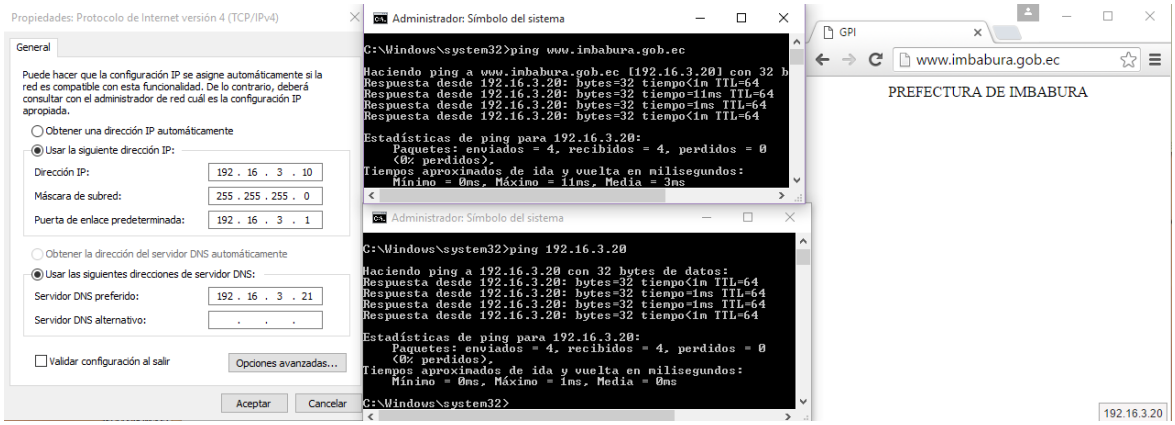


Figura 117. Prueba de conectividad desde un usuario IPv4

Fuente: Aplicaciones de Windows

En la Figura 130 mostrada a continuación, se indica la prueba de conectividad desde un usuario IPv6 hacia el servidor WEB.

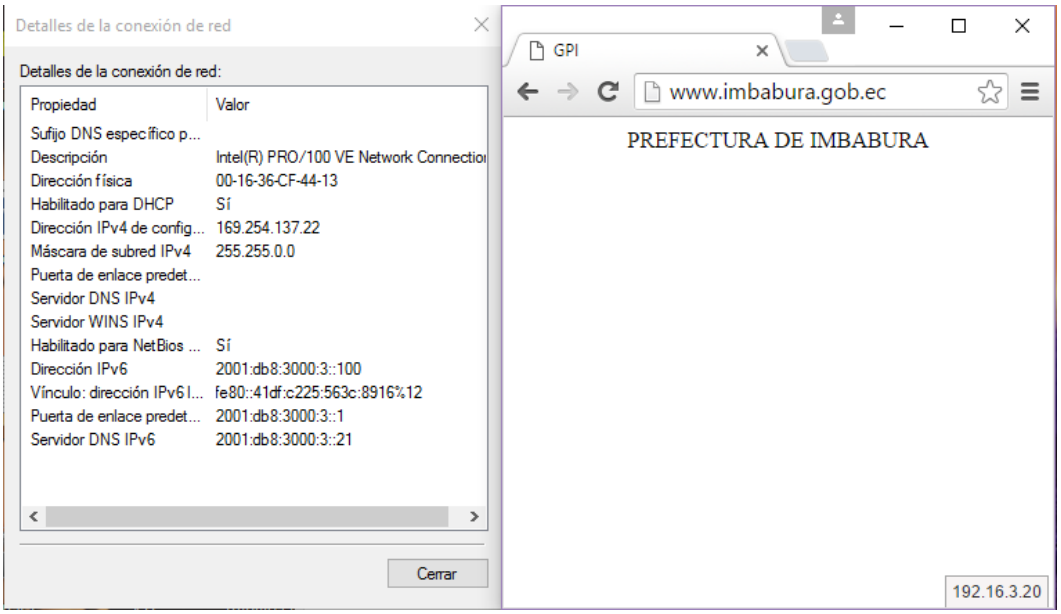


Figura 118. Prueba de conectividad desde un usuario IPv6

Fuente: Aplicaciones de Windows

CONCLUSIONES

- Una de las principales razones de la creación del protocolo IPv6, fue la escasez de direcciones disponibles IPv4, es decir que la capacidad de asignación de direcciones se extiende a un rango mucho mayor, en comparación con el Protocolo de Internet versión 4, dando una solución a la necesidad de conectar una gran cantidad de dispositivos a la red.

- Cada día es más importante que las instituciones tanto públicas como privadas conozcan sobre el protocolo IPv6, para que puedan planificar su uso en la infraestructura de red, de tal manera que en el momento que sea necesaria una transición completa, estas redes puedan adaptarse de manera efectiva al protocolo.

- Luego de haber realizado el análisis de la red de datos de la Prefectura de Imbabura se pudo observar que todos los equipos que funcionan en la red son compatibles con el protocolo IPv6, con la realización de las encuestas se pudo determinar que a pesar del interés sobre la adopción de este protocolo la mayoría de personal principalmente de la Dirección de TIC’s no conocen a profundidad sobre el tema y les gustaría recibir capacitaciones sobre el mismo.

- Al realizar un análisis comparativo de los métodos de transición se pudo determinar que utilizar el método de doble pila era el más idóneo para los equipos de red de la Prefectura de Imbabura, ya que permite que cada uno de los protocolos trabajen de manera independiente, y a la vez todos los usuarios puedan acceder de manera continua a la red, sin causar interrupciones o caídas.

- En cuanto a la implementación de aplicaciones se determinó el uso de mecanismos de traducción DNS64 y NAT64, siendo así, los usuarios que se encuentren solo en IPv6 deberán acceder a los diferentes servicios que aun trabajen específicamente en IPv4, lo cual garantiza una coexistencia de los protocolos.

- Se realizó un plan de direccionamiento basado en la distribución existente en IPv4, se utilizó direcciones de acuerdo al RFC 4291, dejando así un modelo a seguir para al momento de realizar la implementación en la Prefectura de Imbabura.

- Se utilizó el software GNS3 para la simulación, permitiendo la comprobación del funcionamiento del mecanismo de transición planteado, para esto se configuro de manera jerárquica cada uno de los dispositivos de red partiendo desde el Firewall Cisco ASA, pasando por el Switch de CORE y los Switch de acceso que permiten llegar al usuario final.

- El análisis de factibilidad mostró que la implementación en un futuro de este proyecto es de suma importancia ya que permitirá que la Prefectura de Imbabura este a la vanguardia de la tecnología, pero para realizar este proceso se debe capacitar a cada miembro del personal para que conozcan más sobre la utilización de este protocolo.

RECOMENDACIONES

- Se sugiere que el personal del Departamento de Tecnologías de Información realice diversas capacitaciones sobre el protocolo IPv6 para que puedan estar informados sobre las ventajas que este proporciona.

- El proveedor de servicios de la Prefectura de Imbabura informo que no pueden asignar un recurso de IPv6 para la institución, por tanto, para una futura implementación se deberá solicitar directamente LACNIC, tal como se indica en el manual de petición de recursos IPv6.

- Es importante identificar qué servicios trabajaran con cada protocolo, ya que no todas las versiones de los sistemas soportan IPv6, por lo que se debe tomar mucha atención al momento de realizar las fichas técnicas tanto de los equipos como de los servidores.

- Es necesario crear un plan de transición para poder en forma ordenada realizar cada uno de los pasos para que la institución pueda adoptar de a poco este protocolo. Por lo que toda la documentación de configuraciones de este proyecto se entregó al Director de TIC's

- En la implementación de IPv6 se podrá hacer uso de los mismos equipos utilizados para IPv4. Por tal motivo se recomienda el uso del método transición de doble pila ya que este permite una coexistencia entre ambos protocolos.

- Las configuraciones para los Switch de acceso y distribución, así como de los equipos involucrados en el mecanismo de transición deben realizarse solo por personal autorizado y con los conocimientos apropiados para la manipulación de las aplicaciones que hacen posible todo el proceso de traducción entre IPv6 e IPv4.

GLOSARIO DE TÉRMINOS

6

6bone
: red IPv6 de carácter experimental creada para ayudar a los vendedores y usuarios a participar en la evolución y transición a IPv6, 24

A

ARPANET
: Advanced Research Projects Agency Network, Red de la Agencia de Proyectos de Investigación Avanzada, 7

B

Berkeley
: Universidad de California en Berkeley, 7

C

Carriers
: Empresa de Telecomunicaciones que habilitan el tráfico de datos a otras empresas proveedoras de servicios de red., 67

Checksum
: Suma de control, es una función que tiene como propósito principal detectar cambios accidentales en una secuencia de datos para proteger la integridad de los mismos., 15

CIDR
: Classless Inter-Domain Routing, Enrutamiento entre dominios sin clases, consiste en la capacidad de que un enrutador utilice protocolos que no consideran las clases como los límites naturales de las subredes., 18

Cisco
: es una empresa global con sede en San José, (California, Estados Unidos), principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones., 24

I

IANA
: Internet Assigned Numbers Authority, Autoridad de Asignación de Números de Internet, entidad que supervisa la asignación global de Dirección IP, la asignación de Números de Sistemas Autónomos, la gestión de la zona radicular en el Domain Name System (DNS), los tipos de medios, y otros símbolos y números relacionados con el Protocolo de Internet., 16

IPng
: IP next generation, nombre con el cual se nombró a la versión 6 del protocolo de Internet, es una red basada en la transmisión de paquetes capáz de proveer servicios integrados, y capáz de explotar al máximo el Ancho de Banda del canal haciendo uso de las tecnologías de calidad de serviciode tal modo que el transporte sea totalmente independiente a la infraestructura de red utilizada., 24

ISP
: Service Provider, Proveedor de Servicios de Internet, 16

M

Multicast
: es un método de envío de paquetes a nivel IP que solo serán recibidos por un determinado grupo de hosts., 76

Q

QoS
: Quality of Service, Calidad de Servicio, es un conjunto de tecnologías que garantiza la transmisión de cierta cantidad de información en un tiempo determinado a uno o varios dispositivos., 26

R

RFC
: Request for Comments, serie de publicaciones del IETF que describen diversos aspectos del funcionamiento de Internet, redes de computadoras, protocolos, procedimientos, etc., 10

RIR

Regional Internet registry, Registro Regional de Internet, 22

S

SIPP
Simple Internet Protocol Plus, está diseñada para ser un paso de evolución de IPv4., 24

T

TCP/IP
Transmission Control Protocol, Protocolo de Control de Transmisión / Internet Protocolo, Protocolo de Internet, 7

U

Ultima milla
Es el tramo final de una línea de comunicación, ya sea telefónica o un cable óptico, que llega al usuario final., 67

UMTS
Universal Mobile Telecommunications System, Sistema Universal de Telecomunicaciones Móviles, 22

Unicast
Es el envío de información desde un único emisor a un único receptor. Este método envía por separado el tráfico de datos a cada equipo que los haya solicitado, a su vez esto provoca inundación (flooding) en la red por la cantidad de tráfico que se genera., 76

UNIX
Sistema operativo multiplataforma, multitarea y multiusuario desarrollado originalmente por empleados de Bell de AT&T., 7

URSS
Unión de Repúblicas Socialistas Soviéticas, 7

BIBLIOGRAFÍA

Defense Advanced Research Projects Agency. (Septiembre de 1981). *Internet Protocol*. Obtenido de IETF: http://tools.ietf.org/html/rfc791

Ahuatzin Sánchez, G. (Enero de 2005). *Desarrollo de un esquema de traducción de direcciones IPv6-IPv4-IPv6.* Obtenido de http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/ahuatzin_s_gl/capitulo2.pdf

Alonso, J. (2008). *LACNIC*. Obtenido de Coexistencia y Transición: http://www.labs.lacnic.net/site/sites/default/files/ES-Transicion.pdf

Alvarez, E. (2009). *Introducción a IP version 4.* Obtenido de Notas de clase IPv4: http://www-2.dc.uba.ar/materias/tc/downloads/apuntes/ipv4.pdf

Blank, A. G. (20 de Febrero de 2006). TCP/IP Foundations. San Francisco, Estados Unidos. Obtenido de http://www.eblib.com

Boronat Seguí, F., & Montagud Climent, M. (2013). *Direccionamiento e Interconexión de Redes basada en TCP/IP (IPV4/IPV6, DHCP, NAT, Encaminamiento RIP y OSPF).* Valencia: Editorial de la Universidad Politécnica de Valencia.

CCM. (Febrero de 2016). *OpenDNS*. Obtenido de http://es.ccm.net/faq/410-opendns-un-dns-rapido-y-util

Chamba, D. F. (2015). *Universidad Regional Autónoma de los Andes Uniandes.* Obtenido de http://www.dspace.uniandes.edu.ec/bitstream/123456789/333/1/TUAIS014-2015.pdf

Cicileo, G. (2012). *Portal IPv6*. Obtenido de Mecanismos de Transición: http://portalipv6.lacnic.net/mecanismos-de-transicion/

Cicileo, G., Gagliano, R., O'Flaherty, C., Olvera Morales, C., Palet Martínez, J., Rocha, M., & Vives Martínez, Á. (2009). *IPv6 para Todos: Guía de uso y aplicación para diversos entornos.* Buenos Aires: Internet Society. Capítulo Argentina.

CISCO. (2013). *Catalyst 4500 Series Switches.* Obtenido de http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-series-switches/data_sheet_c78-530856.pdf

CISCO. (Mayo de 2013). *Catalyst 4503-E.* Obtenido de http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1982.pdf

CISCO. (19 de Febrero de 2013). *CISCO ASA 5520.* Obtenido de http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1932.pdf

CISCO. (2014). *Cisco 880 Series Integrated Services Routers.* Obtenido de http://www.cisco.com/c/en/us/products/collateral/routers/887-integrated-services-router-isr/data_sheet_c78_459542.pdf

CISCO. (2015). *Cisco Line Cards.* Obtenido de http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/catalyst-4500-series-line-cards/product_data_sheet0900aecd802109ea.pdf

CISCO. (2016). *Cisco Catalyst 2960-X Series Switches.* Obtenido de http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/data_sheet_c78-728232.pdf

CISCO. (s.f.). *Cisco Catalyst 2960 Series Switches.* Obtenido de http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-series-switches/product_data_sheet0900aecd80322c0c.html

Coellar Solórzano, J., & Cedeño Mendoza, J. (2013). *Propuesta para la Transición de IPv4 a IPv6 en el Ecuador a través de la Supertel.* Guayaquil: Universidad Católica de Santiago de Guayaquil.

Collado, E. (25 de Mayo de 2009). *IPv6*. Obtenido de http://eduangi.com/blog/2009/05/25/cabeceras-de-extension-de-ipv6/

Definición de UNIX. (2010). Obtenido de ALEGSA: http://www.alegsa.com.ar/Dic/unix.php

DELL. (Mayo de 2006). *Servidor DELL PowerEdge 2900.* Obtenido de http://www.dell.com/downloads/emea/products/pedge/es/PE2900_Spec_Sheet_Quad.pdf

Edmond, K., & Whitney, T. (8 de Julio de 2012). *La Historia de IPv6*. Obtenido de The Prisma - The Multicultural Newspaper: http://www.theprisma.co.uk/es/2012/07/08/la-historia-de-ipv6/

Gerometta, O. (19 de Noviembre de 2011). *IPv6 - Algo de Historia*. Obtenido de Mis Libros de Networking: http://librosnetworking.blogspot.com/2011/11/ipv6-algo-de-historia.html

Gerometta, O. (4 de Enero de 2015). *Mis Libros de Networking*. Obtenido de es considerada una estrategia de corto plazo pero que permite la coexistencia de ambas redes para facilitar una transición hacia la red IPv6.

Gobierno de España . Ministerio de Industria, Energía y Turismo. (s.f.). *IP.v6 Protocolo de Internet Versión 6*. Obtenido de http://www.ipv6.es/es-ES/transicion/quees/Paginas/Transicion.aspx

Gobierno de España. (2010). *IP.v6 Protocolo de Internet Versión 6*. Obtenido de ¿Qué es IPv6?: http://www.ipv6.es/es-ES/introduccion/Paginas/QueesIPv6.aspx

Gobierno de España: MIET. (s.f.). *Protocolo de Internet Versión 6*. Obtenido de http://www.ipv6.es/es-ES/Faqs/Paginas/tecnicas.aspx#14

Guillermo, C. (s.f.). *IPv6 Portal*. Obtenido de http://portalipv6.lacnic.net/mecanismos-de-transicion/

Hewlett Packard Enterprise. (25 de Noviembre de 2015). *HPE MSA P2000 G3 MSAS.* Obtenido de http://www8.hp.com/h20195/v2/GetPDF.aspx/c04168365.pdf

Hewlett Packard Enterprise. (22 de Enero de 2016). *HPE BladeSystem c3000 Enclosure.* Obtenido de http://www8.hp.com/h20195/v2/GetPDF.aspx/c04128340.pdf

HP. (Marzo de 2003). *Servidor Proliant ML370 G3.* Obtenido de http://h10032.www1.hp.com/ctg/Manual/c00690216.pdf

HP. (14 de Octubre de 2011). *HP Proliant DL360 G6.* Obtenido de http://www.nts.nl/site/html/modules/pdf/Server/HP%20Proliant%20DL360G6.pdf

HP. (1 de Marzo de 2013). *HP Proliant BL460c G7 Server Blade.* Obtenido de http://www8.hp.com/h20195/v2/GetPDF.aspx/c04128282.pdf

HP. (Agosto de 2013). *HP Proliant BL460c G8.* Obtenido de http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA3-9690ENW.pdf

IAR México. (2010). *Internet Addresses & Resources Mexico*. Obtenido de http://www.iar.mx/jsf/static_content/services/resources_request/portable_ip_asn_wish/requestProcess.jsf

IPv6 en Colombia. (s.f.). Obtenido de http://www.encuestafacil.com/RespWeb/Cuestionarios.aspx?EID=1219099&MSJ=NO#Inicio

IPv6 Task Force. (2004). *IPv6 Task Force México*. Obtenido de http://www.ipv6tf.mx/formSurvey.php

Lahera Pérez, J. A., & González Rodríguez, C. (s.f.). *IPv6. Visión general y comparativa con el actual IPv4.* Barcelona: Universidad Politécnica de Catalunya.

MAIPU. (s.f.). *MyPower S3100 Series Switch.* Obtenido de http://www.intelek.cz/db/repository.nsf/v/FBB689D5416D4292C125774400257B9C/$file/Datasheet_Maipu_Switch_S3100_Series.pdf

Mandiola, R. (11 de Febrero de 2012). *Limitaciones de IPv4*. Obtenido de Protocolo de Internet Versión 6: http://protocolointernetversion6ipv6.blogspot.com/2012/02/limitaciones-de-ipv4.html

Mejía, F. (20 de Agosto de 2012). *IPv6 Task Force Ecuador*. Obtenido de http://www.ipv6tf.ec/index.php?option=com_content&view=article&id=104:ipv6-en-ecuador&catid=41:general&Itemid=107

Microsoft. (Enero de 2005). *Developer Network*. Obtenido de Características de IPv6: http://msdn.microsoft.com/es-es/library/cc780593%28v=ws.10%29.aspx

Microsoft. (s.f.). *TechNet*. Obtenido de https://technet.microsoft.com/en-us/library/bb531150.aspx

Millán Tejedor, R. J. (2001). *El Protocolo IPv6 (I)*. Obtenido de www.ramonmillan.com/tutoriales/ipv6_parte1.php

MSDN Library. (Enero de 2005). *Protocolo de mensajes de control de Internet para IPv6 (ICMPv6)*. Obtenido de http://msdn.microsoft.com/es-es/library/cc757063%28v=ws.10%29.aspx

Network Information Center México S.C. (Mayo de 2013). *IPv6Mx*. Obtenido de Fundamentos de IPv6: http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

Network Informations Center México S.C. (s.f.). *Fundamentos de IPv4*. Obtenido de IPv6Mx: http://www.ipv6.mx/index.php/informacion/fundamentos/ipv4

Nuñez Lara, D. F. (Agosto de 2009). *Escuela Politécnica Nacional.* Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/1871/1/CD-2447.pdf

Oracle. (2010). *Cómo diseñar un esquema de direcciones IPv4*. Obtenido de http://docs.oracle.com/cd/E19957-01/820-2981/ipplan-5/index.html

ORACLE. (2010). *Guía de administración del sistema: servicios IP*. Obtenido de Características principales de IPv6: https://docs.oracle.com/cd/E24842_01/html/820-2981/ipv6-overview-8.html

Oracle Corporation. (2010). *Preparación de un plan de direcciones IPv6*. Obtenido de http://docs.oracle.com/cd/E19957-01/820-2981/ipv6-planning-9/index.html

Palet, J. (Marzo de 2011). *Tutorial de IPv6.* Obtenido de http://long.ccaba.upc.es/long/050Dissemination_Activities/jordi_palet_tutorialipv6introduccion.pdf

Portal IPv6 Cuba. (s.f.). *Introduccion a IPv6*. Obtenido de http://www.cu.ipv6tf.org/icmpipv6.htm

Prefectura de Imbabura. (2015). *Prefectura de Imbabura*. Obtenido de http://www.imbabura.gob.ec/

Sánchez Pinos, D. (2006). *Herramientas de Transición a IPv6*. Obtenido de http://dspace.ups.edu.ec/bitstream/123456789/205/3/Capitulo%202.pdf

Sánchez, J. (11 de Marzo de 2014). *Networking and Internet Technologies.* Obtenido de 6to4: Tráfico IPv6 a través de una red IPv4: http://blogs.salleurl.edu/networking-and-internet-technologies/6to4-tunneling/

Sandoval, P. (Noviembre de 2008). *REDES: Protocolo IPv6*. Obtenido de http://redes-ipv6.blogspot.com/2008/11/protocolo-de-descubrimiento-de-vecino_14.html

Stallings, W. (2011). *Comunicaciones y Redes de Computadores.* Prentice Hall.

Tapia Cajas, M. A. (Agisto de 2014). *Escuela Politécnica Nacional.* Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/8364/3/CD-5728.pdf

THE APACHE SOFTWARE FOUNDATION. (2016). Obtenido de http://www.apache.org/

Universidad de la República de Uruguay. (2014). *RAU2*. Obtenido de http://prueba.rau.edu.uy/index.php/introduccion/84-nat64

Universidad de la República de Uruguay. (2014). *RAU2*. Obtenido de http://prueba.rau.edu.uy/index.php/joomlaspanishorg/proyecto-ipv6/mecanismos-de-transicion/60-dns64

Anexo A. Fichas Técnicas de Equipos y Aplicaciones

Anexo B. Formato de la Encuesta

IPv6 en la Prefectura de Imbabura

Cargo: _____ Edad: _____

Fecha: _____

Instrucciones

Esta encuesta está realizada para conocer el interés sobre el nuevo estándar IPv6.

La encuesta no le llevará más de [5] minutos.

Gracias por su colaboración.

Parte I: Conocimientos Generales de IPv6.

1) _____ **Señale el nivel de conocimiento que tiene acerca de IPv6.**
   a. Conozco bien IPv6 o lo he utilizado.
   b. Conozco poco acerca de IPv6.
   c. He escuchado el término, pero no sé lo que significa.
   d. No tengo ningún conocimiento acerca de IPv6.

2) _____ **¿Conoce el contenido que existe actualmente en IPv6?**
   a. No tengo ningún conocimiento acerca del contenido de IPv6.
   b. He escuchado algo, pero no concreto.
   c. Conozco algo acerca del contenido existente en IPv6.
   d. Conozco el contenido existente en IPv6.
   e. Conozco y he utilizado el contenido de IPv6.

3) _____ **¿Cómo se enteró de qué es IPv6?**
   a. No lo conozco.
   b. Por medio de un amigo.
   c. Por medio de cursos, fuentes oficiales.
   d. Por medio de la red de internet.
   e. Otro, por favor especifique _____
      _____

4) _____ **¿Considera el uso de IPv6 como prioridad para usted como usuario?**

a. No lo considero importante.
b. No, pero podría llegar a serlo.
c. Sí, pero no me preocupa.
d. Sí, estoy pendiente siempre del tema.
e. Sí, estoy buscando siempre una solución.
f. Otro, por favor especifique _____
_____

Parte II: Distribución de información del Protocolo.

1) _____ **¿Considera el uso de IPv6 como prioridad para las comunicaciones a nivel Global?**

a. No lo considero importante.
b. No, pero puede llegar a ser importante.
c. Sí, pero a largo plazo.
d. Sí, es una prioridad.
e. Sí, se debe buscar una solución ahora.

2) _____ **¿Considera necesario la adopción de IPv6?**

a. No, de ninguna manera.
b. No, pero después de unos años sí.
c. Sí, a corto plazo (menos de un año)
d. Sí, de inmediato.

3) _____ **¿Le gustaría ser pionero en la navegación IPv6?**

a. No me gustaría.
b. No, pero siento curiosidades.
c. Sí, pero no me parece muy prioritario.
d. Sí me gustaría serlo.

4) _____ **¿Tiene su Hardware y Software preparado para IPv6?**

a. No, para nada.

b. No, pero podría a largo plazo tenerlo.
c. Sí, pero tendría que realizar unos pequeños cambios.
d. Sí, tengo todo lo necesario.

Parte III: Uso de Redes Nuevas

1) _____ **Indique si ha accedido por alguno de los siguientes medios a la red IPv6**
   a. No he accedido.
   b. En el trabajo, o donde algún amigo
   c. Por túneles de acceso gratuito.
   d. Desde algún sitio en internet.
   e. Desde mi propia conexión a IPv6

2) _____ **¿Por qué razón o razones no le atrae un servicio de conectividad IPv6?**
   a. Es innecesario.
   b. Es aburrido.
   c. Es complicado.
   d. Es inseguro.
   e. Otro, por favor especifique _____
   _____

Parte IV: Factor de Desventajas del Protocolo

1) _____ **¿IPv6 no está estandarizado y aun no es una tecnología madura?**
   a. SI
   b. NO

2) _____ **¿Falta de regulación para la adopción de IPv6?**
   a. SI
   b. NO

3) _____ **¿El retorno de inversión es elevado, en el caso de implementar?**
   a. SI

b. NO

4) _____ **¿IPv4 es suficiente, IPv6 no brinda el soporte adecuado?**

a. SI

b. NO

5) _____ **¿Falta de aplicaciones con soporte para IPv6?**

a. SI

b. NO

6) _____ **¿Falta de disponibilidad de servicios IPv6?**

a. SI

b. NO

7) _____ **¿Escasez de promoción del protocolo IPv6?**

a. SI

b. NO

8) _____ **¿Falta de capacitación acerca de IPv6?**

a. SI

b. NO

9) _____ **¿Falta de interés por parte de Organismos públicos, privados, la Industria, las Instituciones educativas y diferentes Sectores Productivos del país?**

a. SI

b. NO

Anexo C. Tabulación de Encuestas

Anexo D. Instalación de Software

D1. INSTALACION DE GNS3

- Ingresar a la página oficial de GNS3, y clic en download.

  http:// www.gns3.com

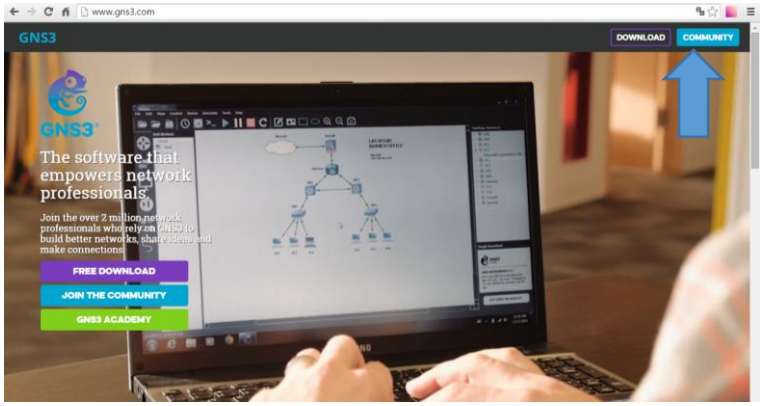


Figura D1 1. Página Oficial GNS3

Fuente: www.gns3.com

- Seleccionar el Sistema Operativo para el cual se requiere instalar GNS3. En este caso seleccionaremos para Windows.

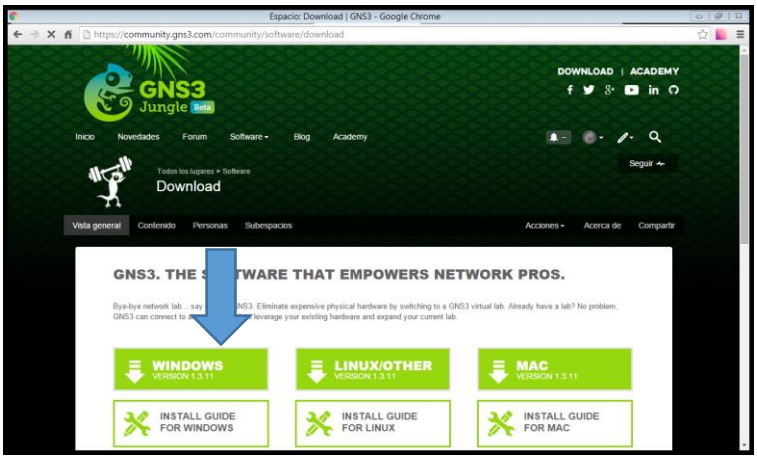


Figura D1 2. Selección del S.O.

Fuente: www.gns3.com

- Luego esperar a que se realice la descarga del programa

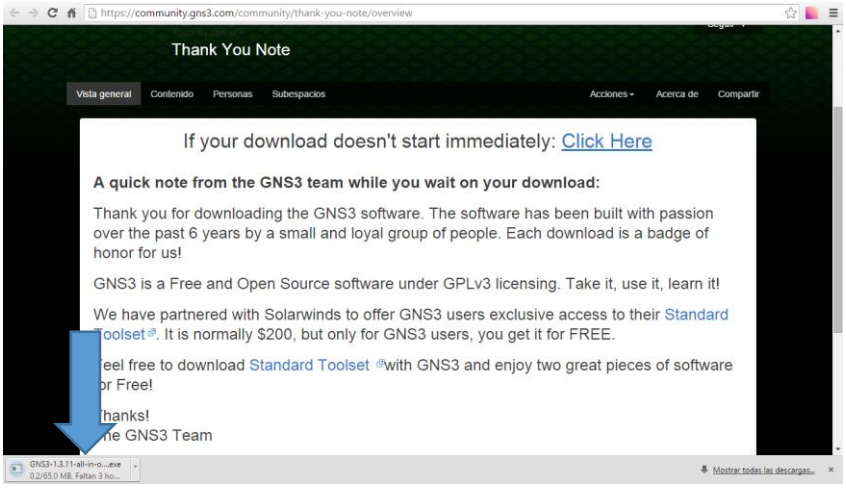


Figura D1 3. Descarga del Programa

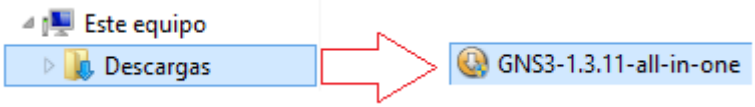


Figura D1 4. Ubicación del archivo

Fuente: Equipo de Windows

- En la ventana, dar click en siguiente para continuar con la instalación.

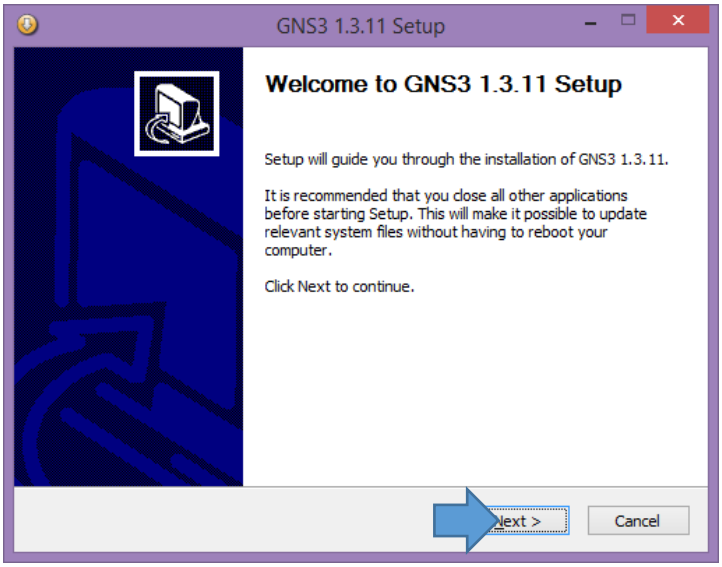


Figura D1 5. GNS3 Setup

Fuente: GNS3

- Esta ventana es la de aceptación de las condiciones de uso de GNS3, dar click en I Agree para continuar.

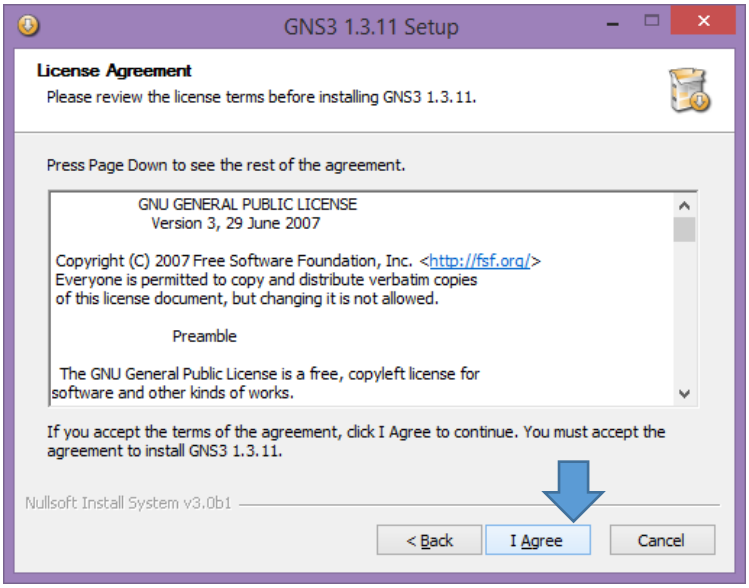


Figura D1 6. Aceptación de condiciones

Fuente: GNS3

- Elegir que herramientas se desea instalar junto a GNS3, todas son de gran ayuda para una experiencia completa en el uso de este software. Click en siguiente para continuar.

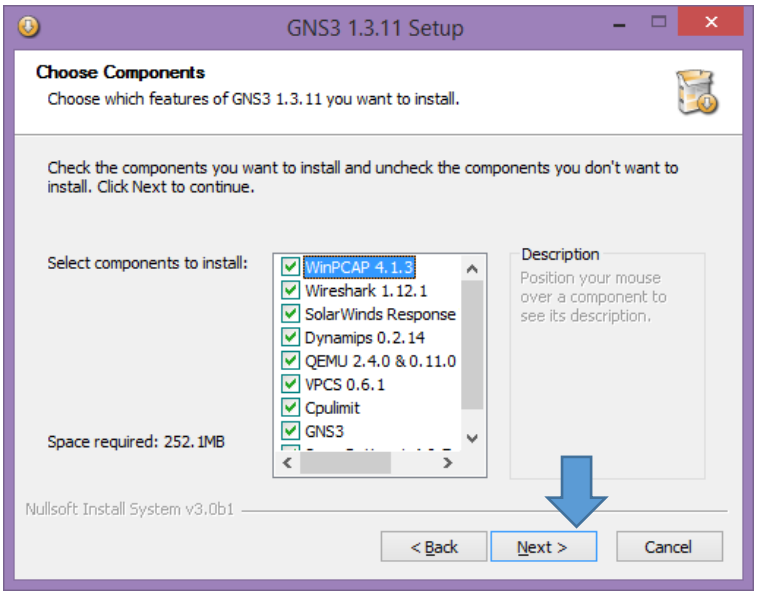


Figura D1 7. Herramientas adicionales

Fuente: GNS3

- Seleccionar la ubicación donde se quiere instalar el programa, click en Install.

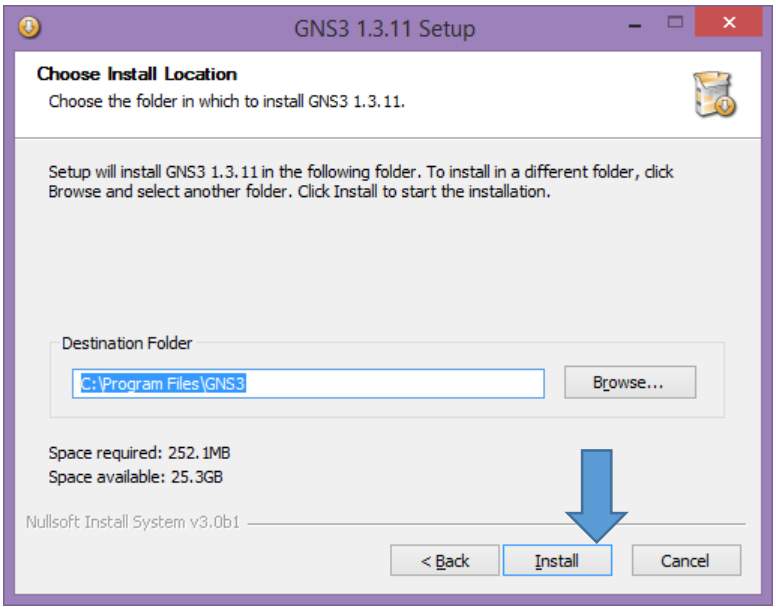


Figura D1 8. Carpeta de destino

Fuente: GNS3

- Esperar a que instale y seguir los pasos en el transcurso, por último, finalizar.

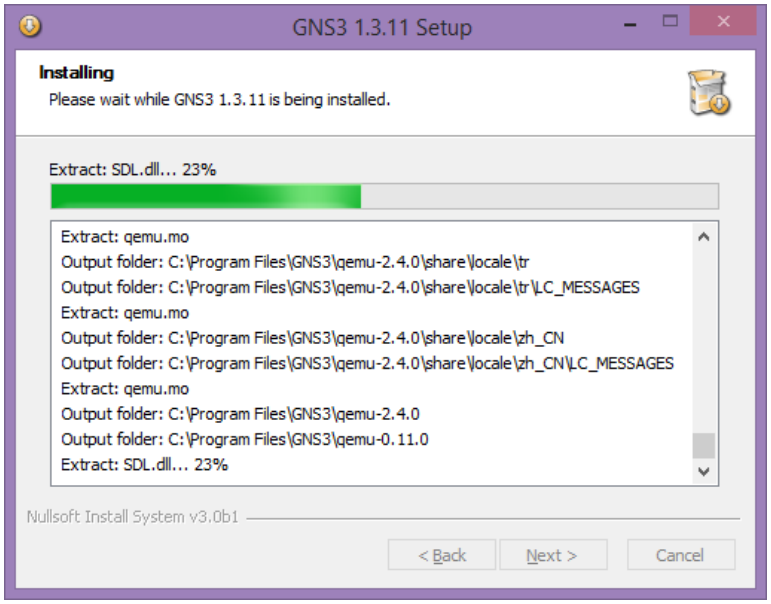


Figura D1 9. Progreso de Instalación

Fuente: GNS3

- Buscar el icono de GNS3 para iniciar del programa.

Figura D1 10. Icono GNS3

Fuente: Equipo Windows

- En la siguiente ventana empezar dando un nombre al Proyecto que se va a iniciar y así empieza a disfrutar de GNS3.

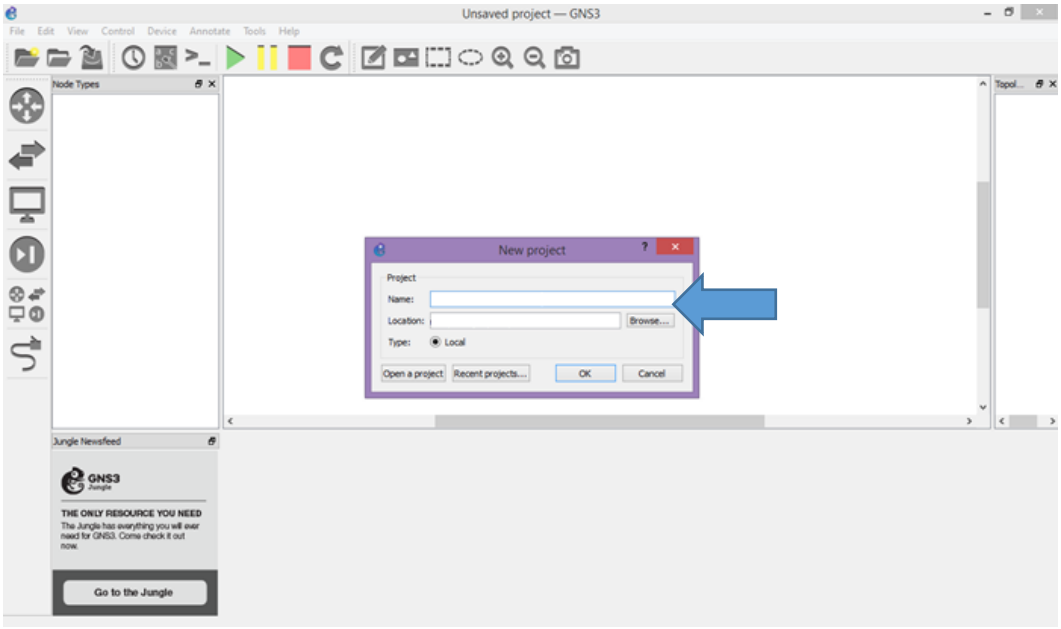


Figura D1 11. Proyecto Nuevo

Fuente: GNS3

- Para cargar el IOS de un router nos dirigimos a Edit ➔ Preferences

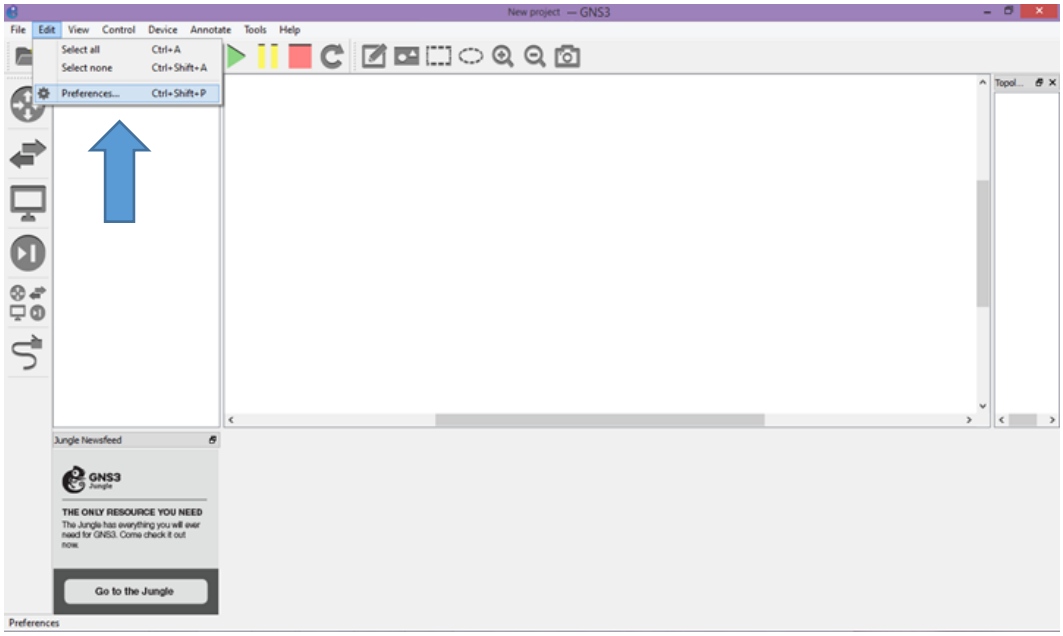


Figura D1 12. Preferencias

Fuente: GNS3

- En la siguiente ventana se elige Dynamips ➔ IOS routers ➔ New

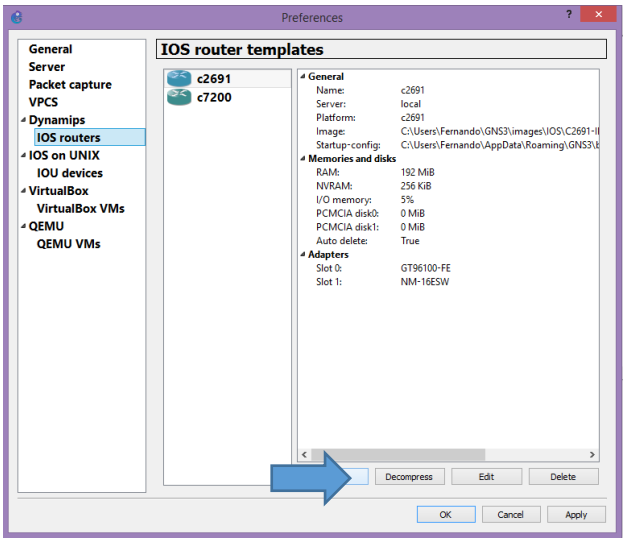


Figura D1 13. Plantillas IOS router

Fuente: GNS3

- Para seleccionar del IOS del router o dispositivo se da Click en Browse

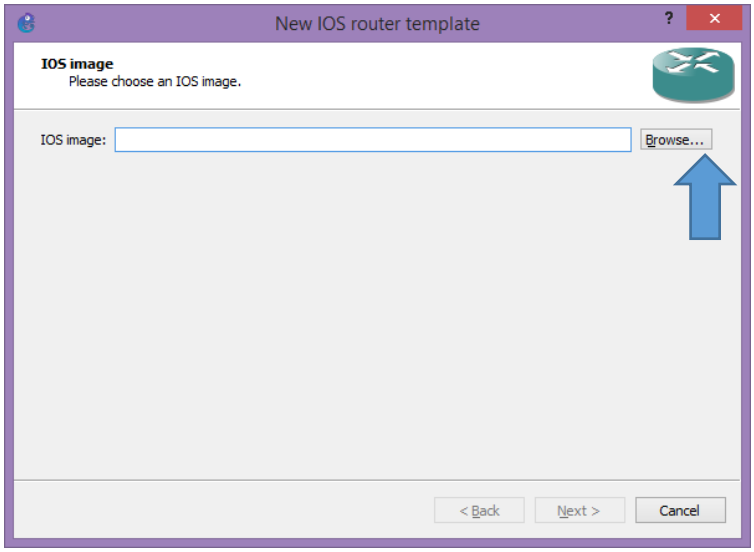


Figura D1 14. Buscar el IOS

Fuente: GNS3

- Seleccionar el IOS que se desee utilizar, click en abrir.

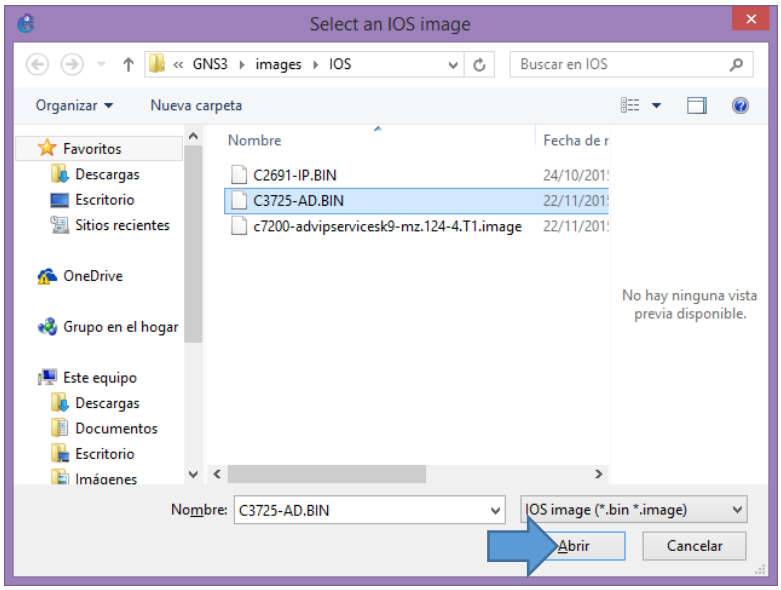


Figura D1 15. Selección del IOS

Fuente: GNS3

- Luego de haber seleccionado el IOS, dar click en siguiente.

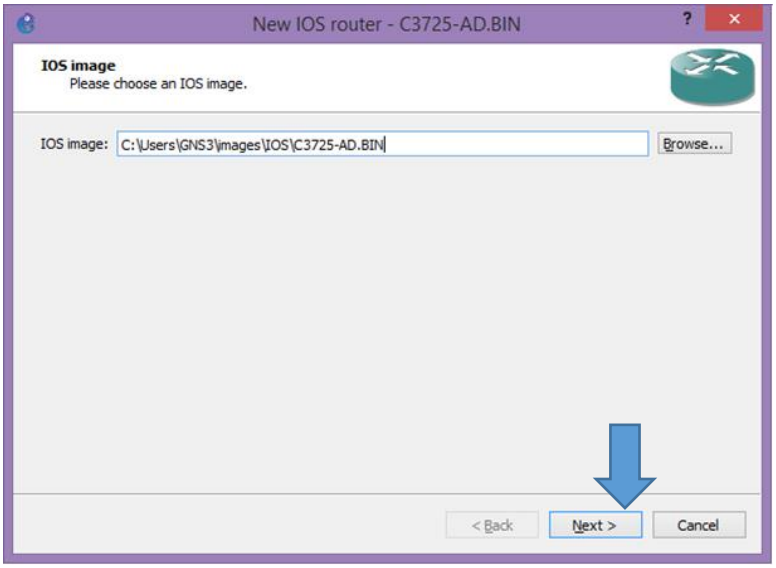


Figura D1 16. Imagen del IOS

Fuente: GNS3

- Escribir la descripción del nombre, click en siguiente.

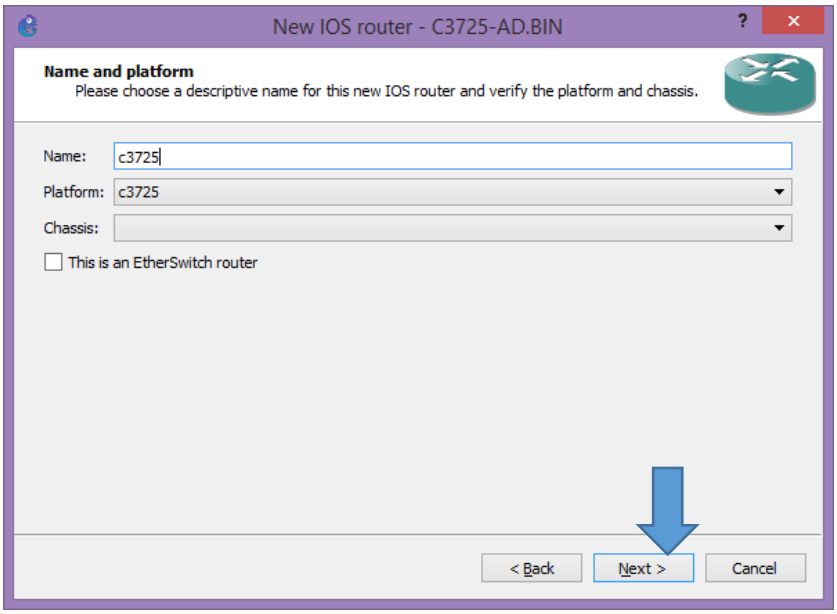


Figura D1 17. Descripción del nombre

Fuente: GNS3

- Seleccionar la memoria RAM que utilizará el equipo, click en siguiente.

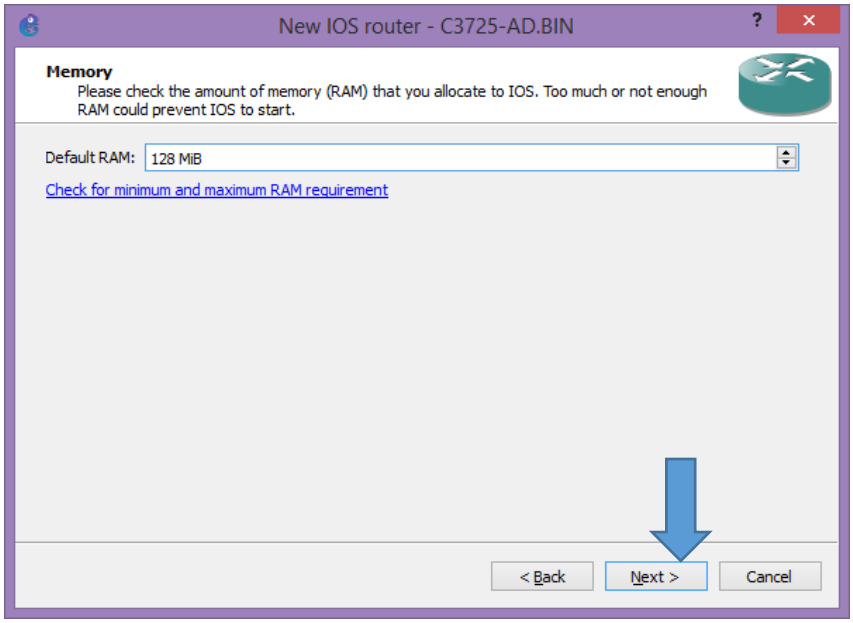


Figura D1 18. Selección de Memoria RAM

Fuente: GNS3

- Elegir las interfaces con las que dispone el equipo, click en siguiente.

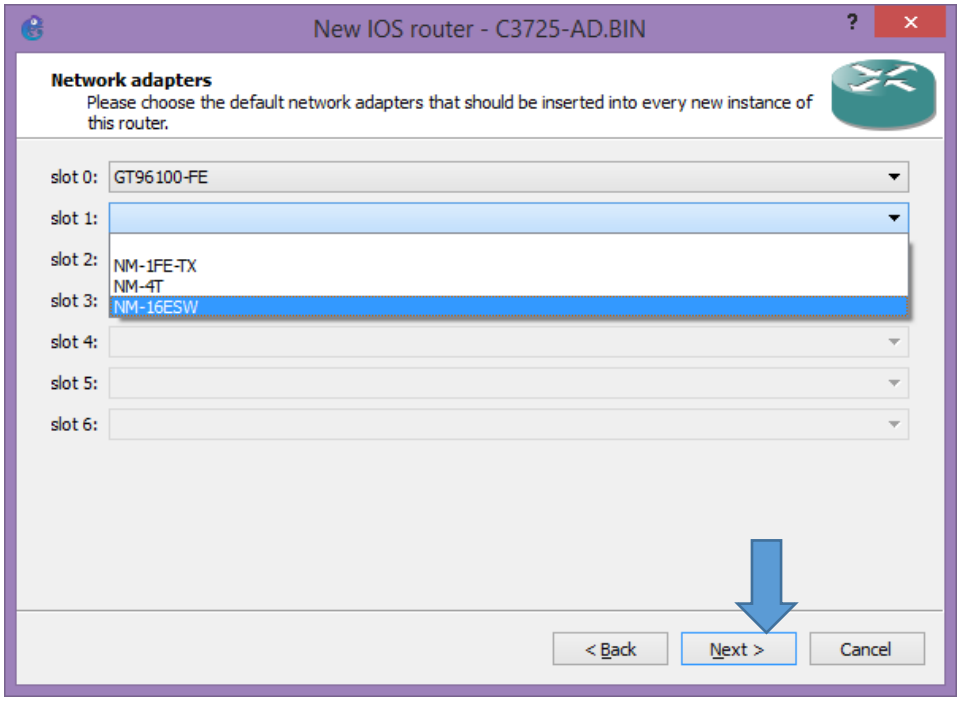


Figura D1 19. Elección de interfaces

Fuente: GNS3

- La elección del módulo WIC es opcional, depende del usuario si desea utilizar o no. Click en siguiente.

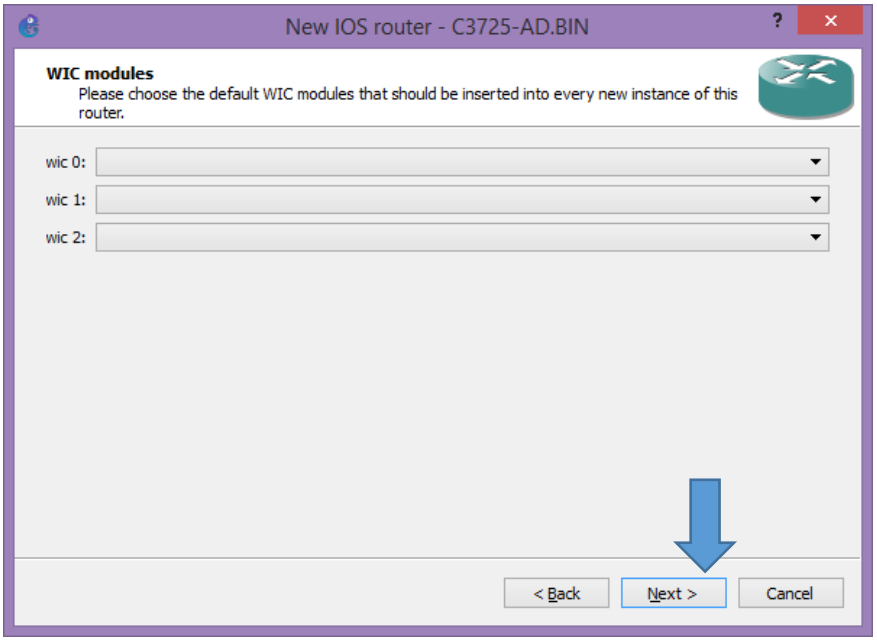


Figura D1 20. Elección de WIC

Fuente: GNS3

- En la siguiente ventana dar click en finalizar, y se puede observar al router o equipo agregado, dar click en aplicar ➔ ok.

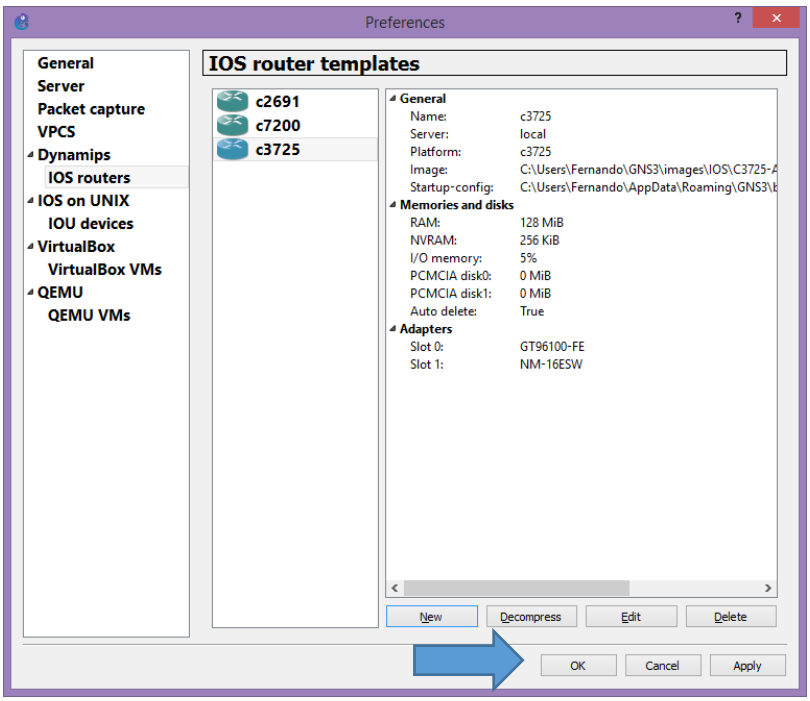


Figura D1 21. Plantillas IOS router con el equipo nuevo agregado

Fuente: GNS3

- Para trabajar con el dispositivo añadido, dirigirse a la barra lateral y selecionar buscar Routers, escoger el equipo y ubicarlo en el área de trabajo.

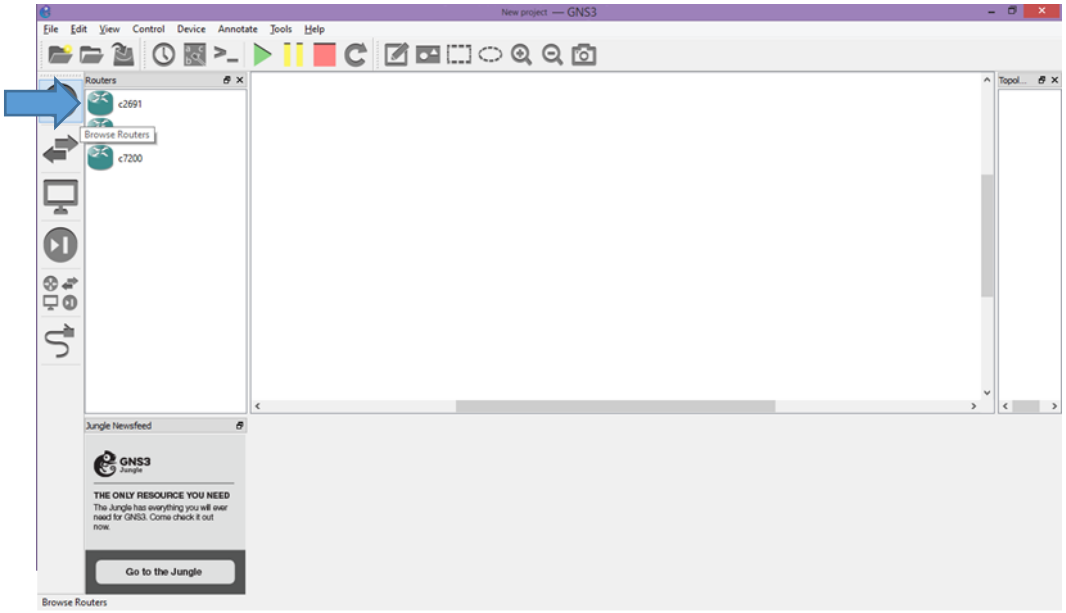


Figura D1 22. Elección del equipo para trabajar

Fuente: GNS3

D2. INSTALACIÓN DE CENTOS EN LA MÁQUINA VIRTUAL

- Como primer paso se debe crear una nueva máquina virtual

- Haciendo click en File (Archivo) y luego en New Virtual Machine (Nueva Máquina Virtual)

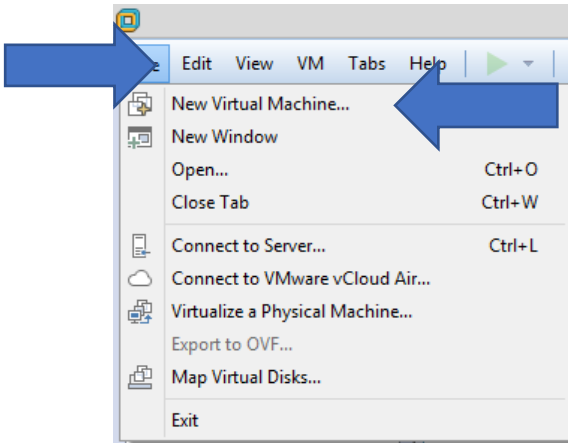


Figura D2 1. Primer paso para crear la máquina virtual

Fuente: VMware

- En la ventana siguiente hacer click en Custom para elegir una instalación personalizada, y luego Next (siguiente)

Figura D2 2. Elección de instalación personalizada

Fuente: VMware

- Escoger la versión de Workstation que se quiere instalar, por lo general se lo deja por defecto, click en siguiente.

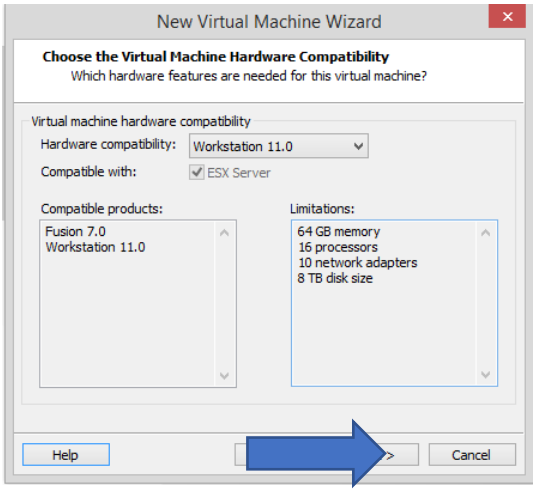


Figura D2 3. Versión de Workstation

Fuente: VMware

- Elegir la última opción para instalar manualmente, click en siguiente.

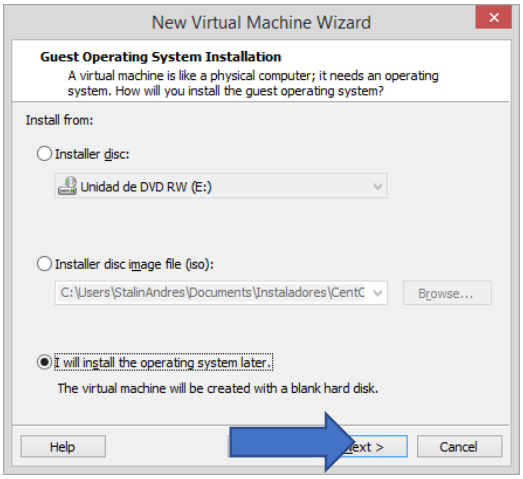


Figura D2 4. Instalación manual

Fuente: VMware

- Elegir el Sistema Operativo y su Versión, click en siguiente.

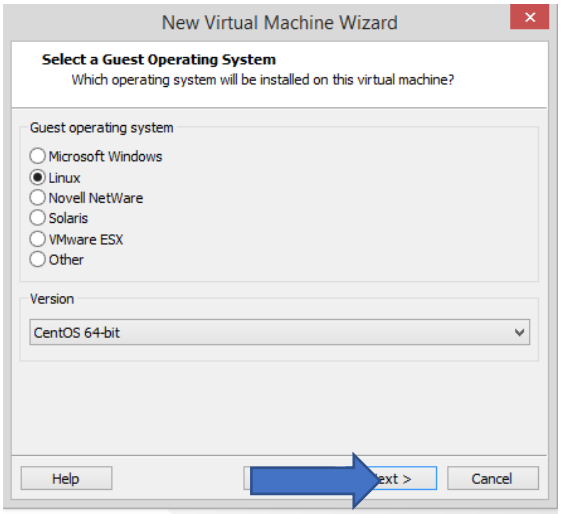


Figura D2 5. Elección de S.O. y Versión

Fuente: VMware

- Agregar el nombre y el lugar para que se instale el Sistema Operativo Virtual, click en siguiente.

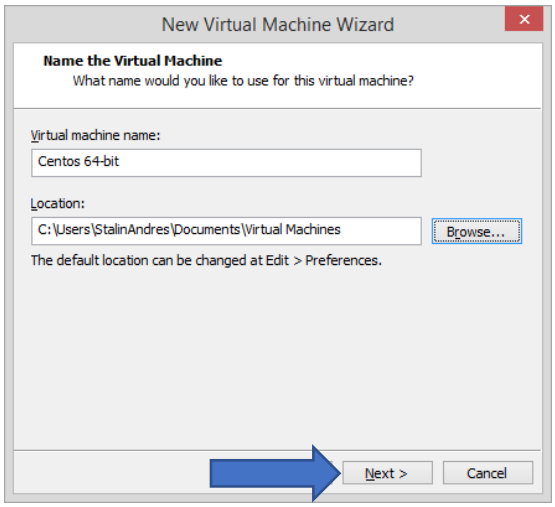


Figura D2 6. Nombre y lugar de instalación del S.O.

Fuente: VMware

- Elegir el número de procesadores a utilizar, por lo general se mantienen las opciones dadas por defecto, click en siguiente.

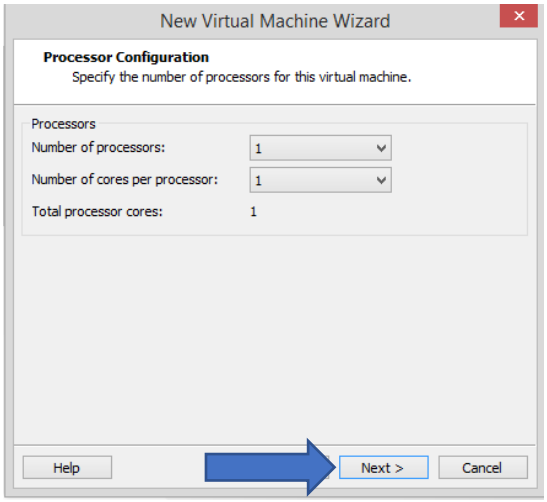


Figura D2 7. Número de procesadores a utilizar

Fuente: VMware

- Dependiendo de la capacidad de memoria RAM que disponga la máquina real seleccionar la cantidad de memoria RAM a utilizar en la máquina virtual, click en siguiente.

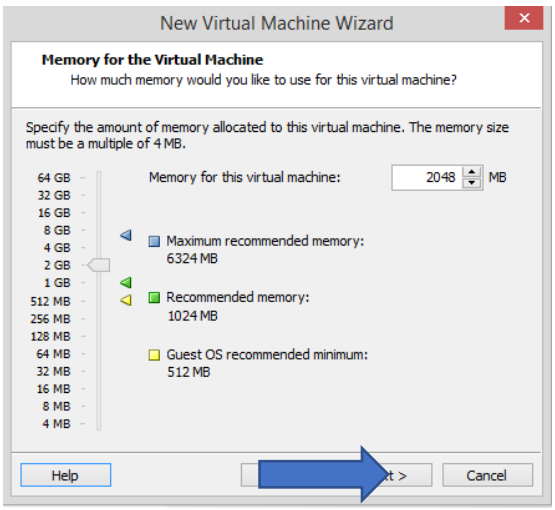


Figura D2 8. Memoria RAM a utilizar

Fuente: VMware

- Escoger el tipo de red “Bridged networking”, para utilizar las interfaces reales, click en siguiente.

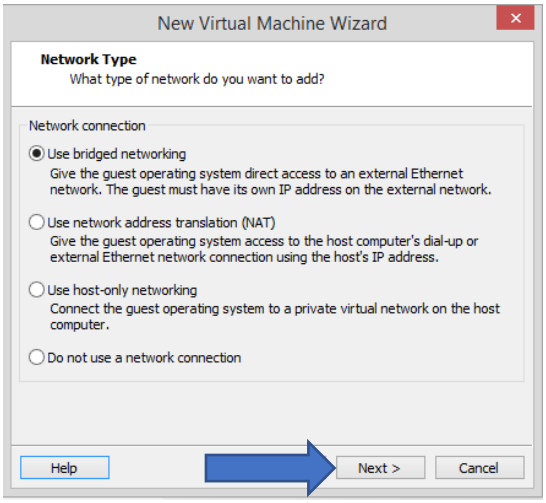


Figura D2 9. Selección del tipo de red

Fuente: VMware

- En el tipo de kernel del sistema operativo, se recomienda dejarlo por defecto, click en siguiente.

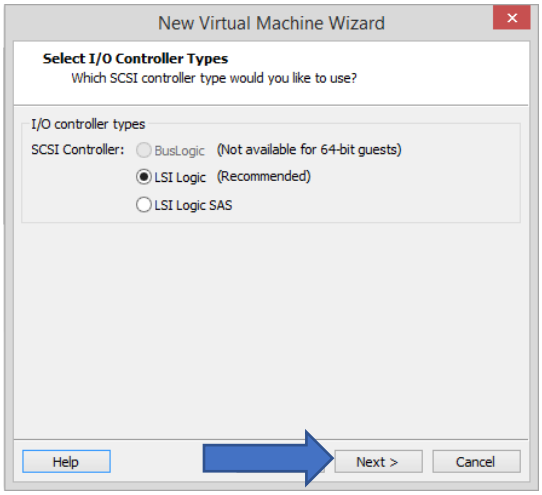


Figura D2 10.Tipo de Kernel

Fuente: VMware

- Tipo de periférico q utiliza el disco duro virtual, se mantiene por defecto, click en siguiente.

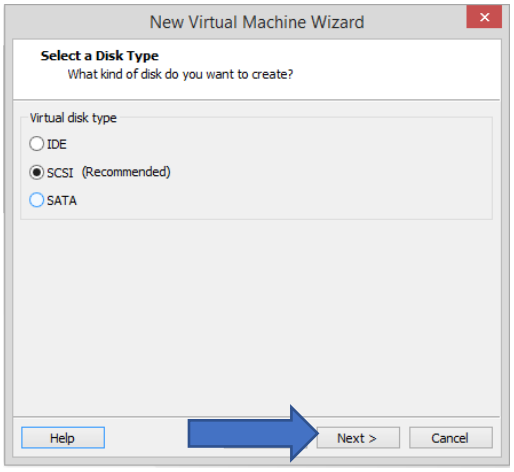


Figura D2 11. Tipo de periférico que utiliza el disco duro

Fuente: VMware

- Para crear un disco duro virtual, elegir la primera opción y dar click en siguiente.

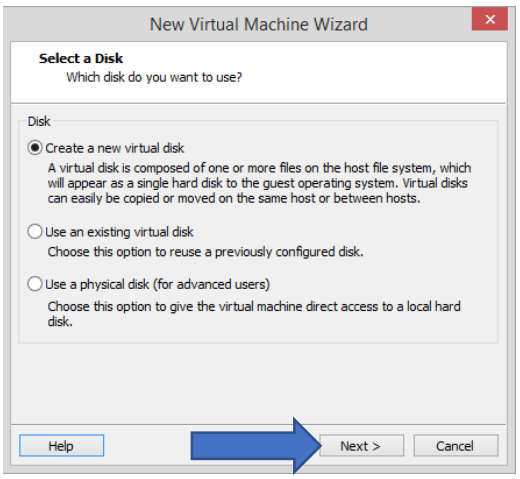


Figura D2 12. Creación de nuevo disco duro viertual

Fuente: VMware

- Especificar la capacidad del disco que se quiera dar a la máquina virtual y click en siguiente.

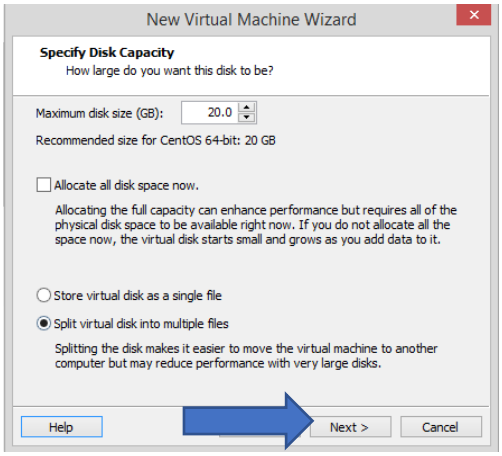


Figura D2 13. Capacidad del disco duro

Fuente: VMware

- Archivo de inicio de la máquina Virtual, mantener por defecto, click en siguiente.

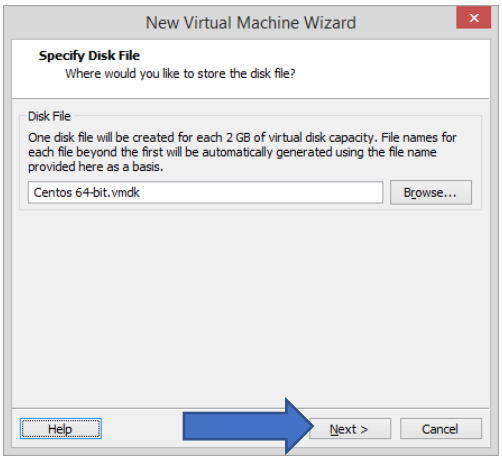


Figura D2 14. Archivo de Inicio

Fuente: Vmware

- Esta ventana muestra un registro de todo lo escogido anteriormente (funcionamiento de la maquina). Click en Finalizar.

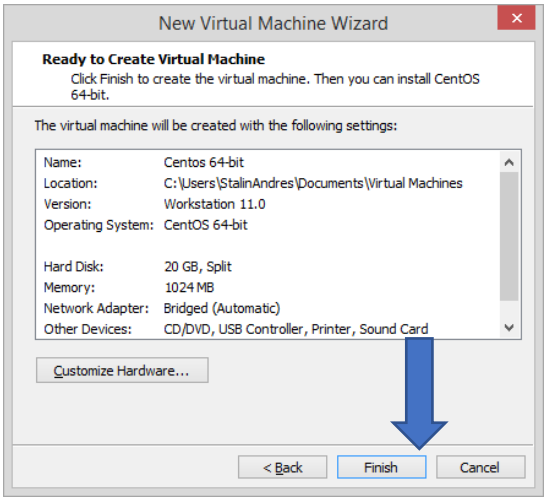


Figura D2 15. Registro de lo escogido

Fuente: VMware

- Se puede observar que ya está creada la máquina virtual, en la parte superior izquierda en el nombre especificado para la máquina virtual en este caso Centos 64-bit, dar click derecho y luego en Preferencias.

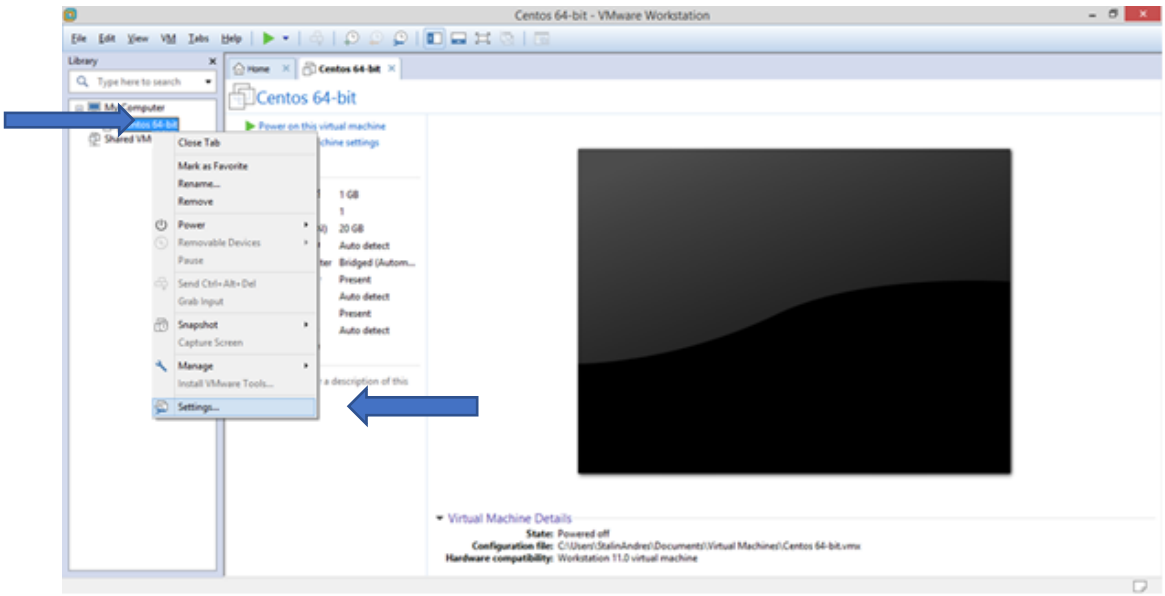


Figura D2 16. Muestra de la máquina virtual creada

Fuente: VMware

- En esta ventana en la opción CD/DVD, se debe cargar el archivo de imagen ISO para que la máquina virtual arranque con el Sistema Operativo que se desea, click en OK

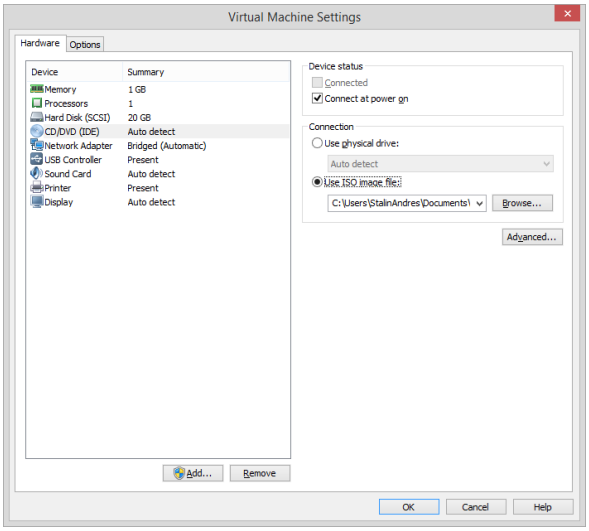


Figura D2 17. Carga del Archivo de imagen ISO

Fuente: VMware

- Y como último paso dar Play en la Máquina Virtual

- Luego de dar Play en la Máquina Virtual, en la pantalla inicial de CentOS escoger la opción que mejor convenga al usuario

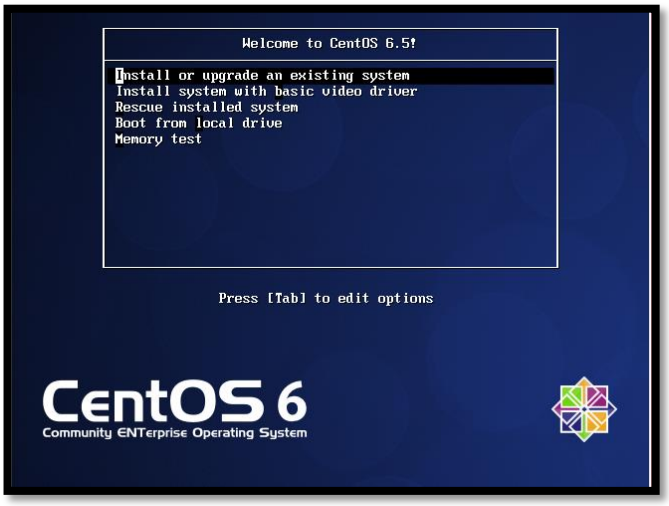


Figura D2 18. Pantalla Inicial de CentOS

Fuente: CentOS

- En la opción Disco encontrado se debe escoger Skip

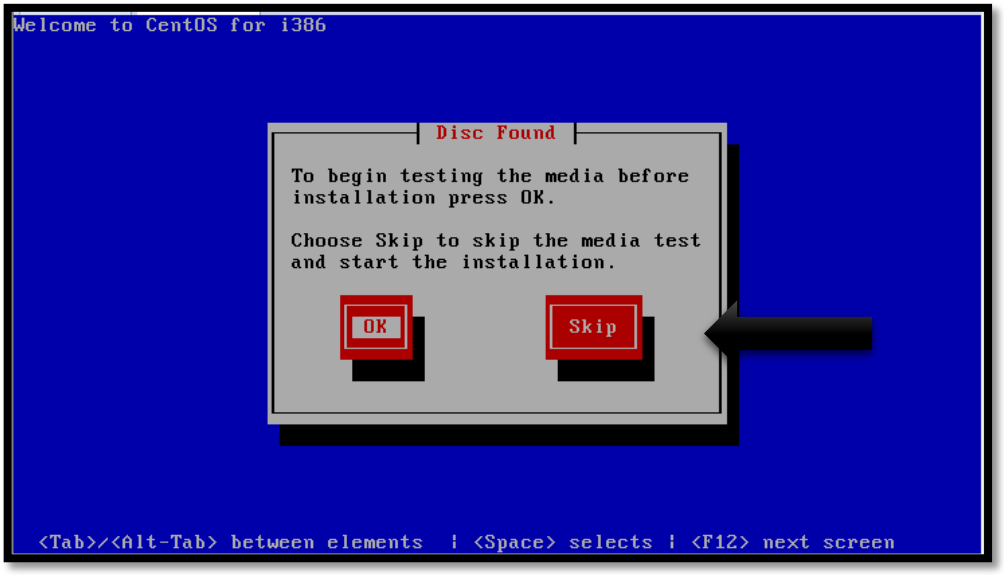


Figura D2 19. Opción Disco encontrado

Fuente: CentOS

- Aparece la pantalla de inicio de instalación de CentOS, dar click en siguiente.

Figura D2 20. Inicio de Instalación de CentOS

Fuente: CentOS

- Escoger el idioma del sistema operativo, click en siguiente.

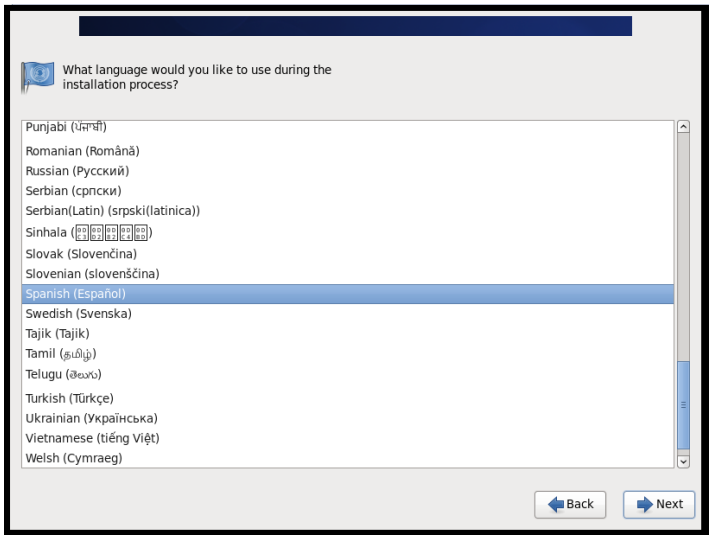


Figura D2 21. Elección del Idioma del S.O.

Fuente: CentOS

- Escoger el idioma del teclado

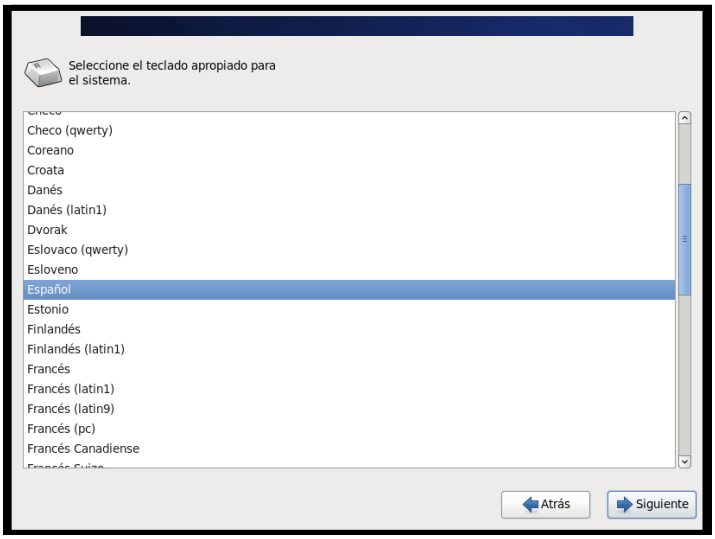


Figura D2 22. Elección del Idioma del teclado

Fuente: CentOS

- Escoger la opción dispositivos de almacenamiento básicos, click en siguiente.

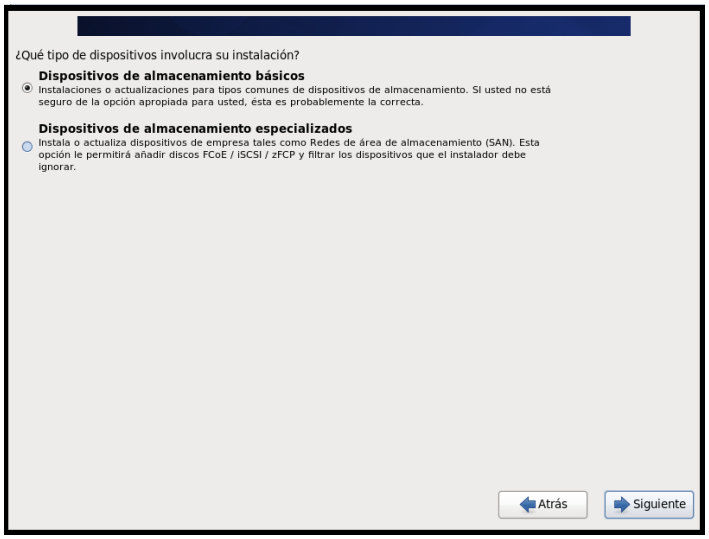


Figura D2 23. Almacenamiento básico

Fuente: CentOS

- Escoger la opción para el dispositivo de almacenamiento y dar click en siguiente.

Figura D2 24. Opciones para el dispositivo de almacenamiento

Fuente: CentOS

- Asignar el nombre del host, por lo general se mantiene el nombre q sale por defecto. Click en siguiente.

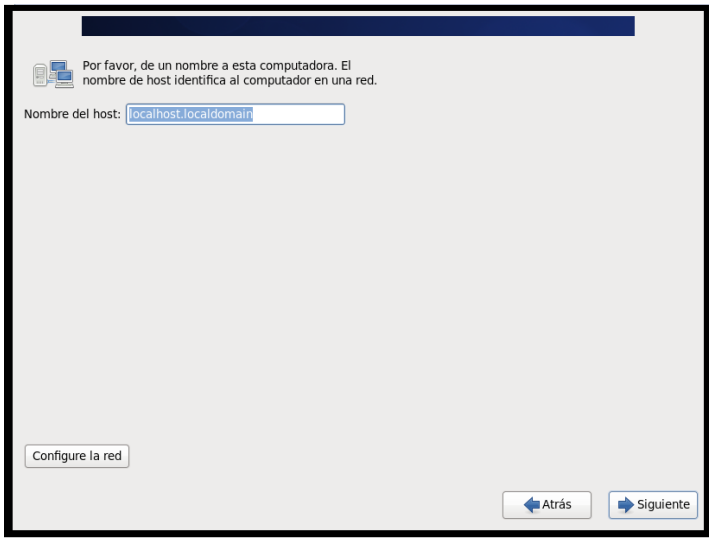


Figura D2 25. Nombre del Host

Fuente: CeontOS

- Se debe escoger la región en que se encuentra la PC para establecer la zona horaria, click en siguiente.

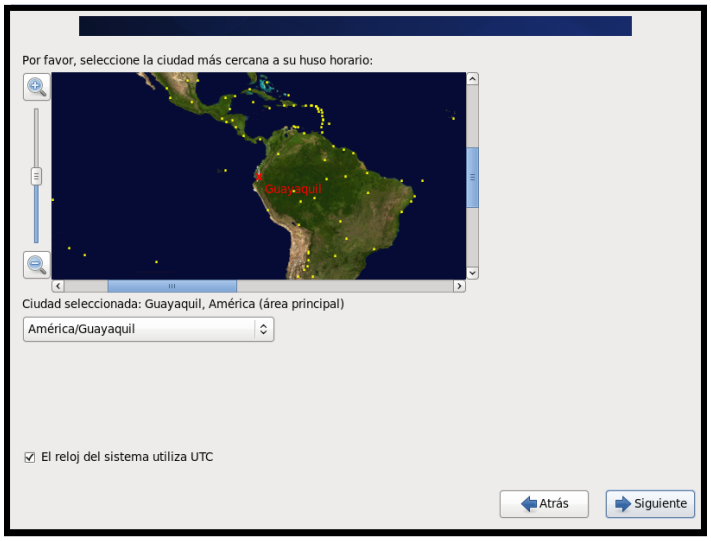


Figura D2 26. Zona Horaria

Fuente: CentOS

- Digitar una contraseña para root, debe ser una contraseña que recuerde siempre, ya que al iniciar el sistema requiere de ella. Click en siguiente.

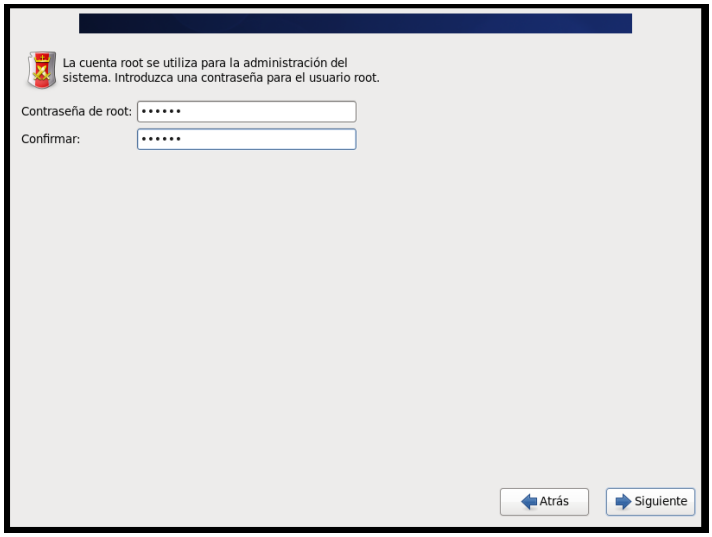


Figura D2 27. Contraseña de root

Fuente: CentOS

- Elegir la opción de la forma en que se desee instalar, click en siguiente.

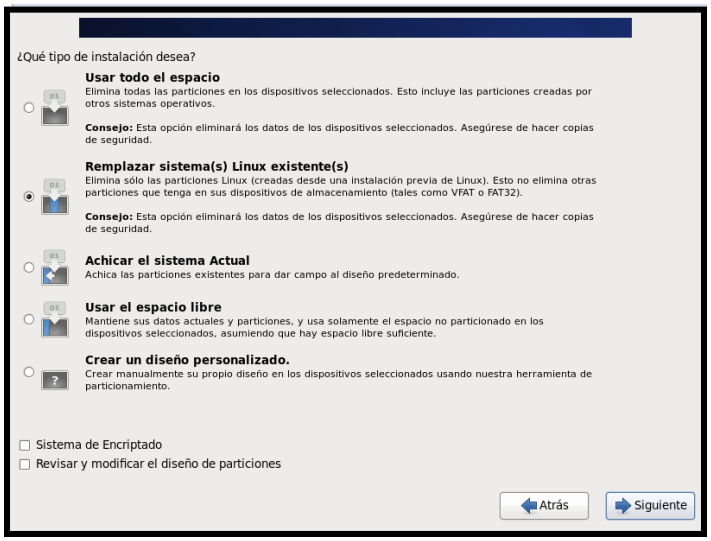


Figura D2 28. Tipo de Instalación

Fuente: CentOS

- Escoger la opción para escribir cambios al disco, click en siguiente.

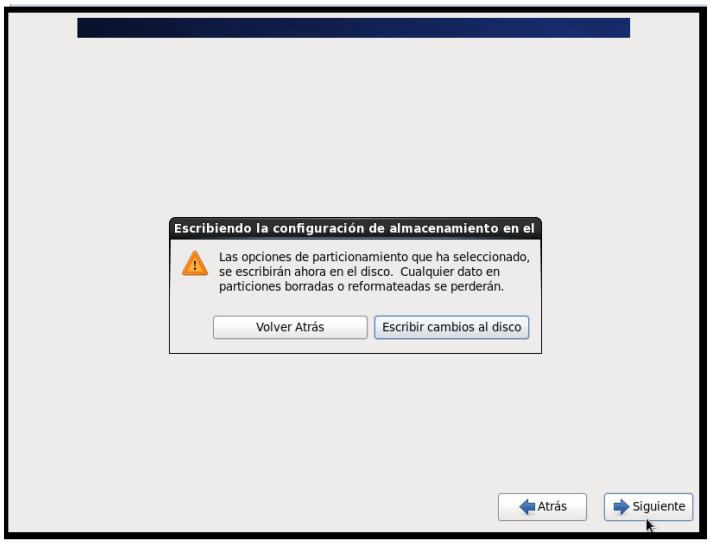


Figura D2 29. Opción para escribir cambios al disco

Fuente: CentOS

- Escoger la opción de escritorio, click en siguiente.

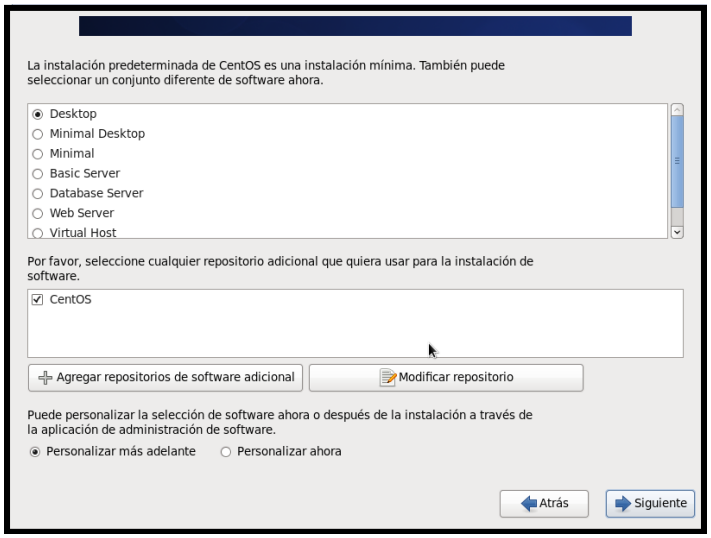


Figura D2 30. Instalación predeterminada

Fuente: CentOS

- Esperar a que se descarguen todos los paquetes necesarios para la instalación.

Figura D2 31. Inicio de instalación

Fuente: CentOS

Figura D2 32. Paquetes de Instalación

Fuente: CentOS

- Finalizar la instalación.

Figura D2 33. Fin de instalación

Fuente: CentOS

- Configurar el inicio de sesion CentOS.

Figura D2 34. Bienvenida a CentOS

Fuente: CentOS

- Aceptar el acuerdo de licencia

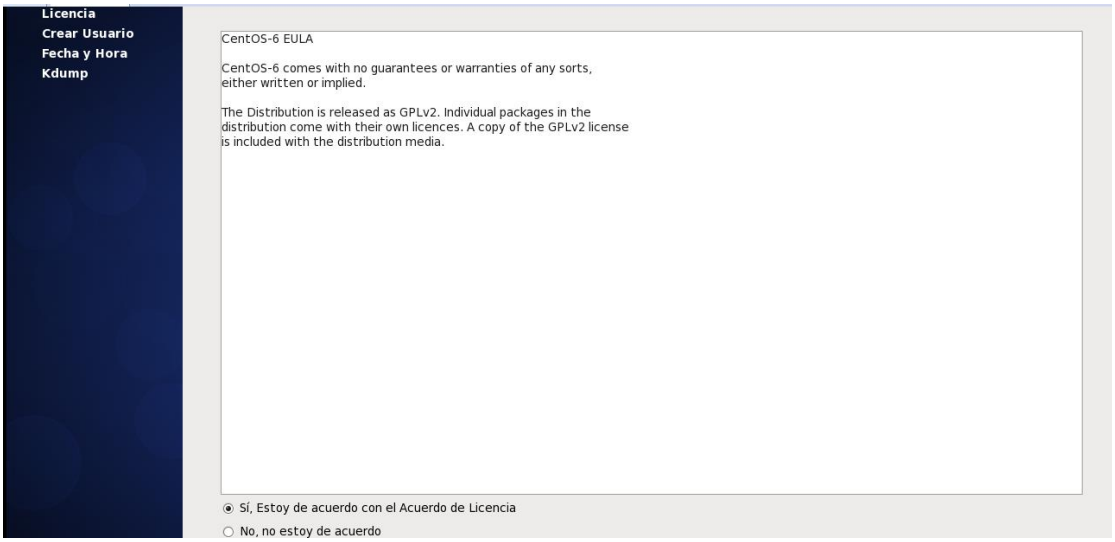


Figura D2 35. Acuerdo de Licencia

Fuente: CentOS

- Si se desea se debe crear el usuario para inicio de sesión

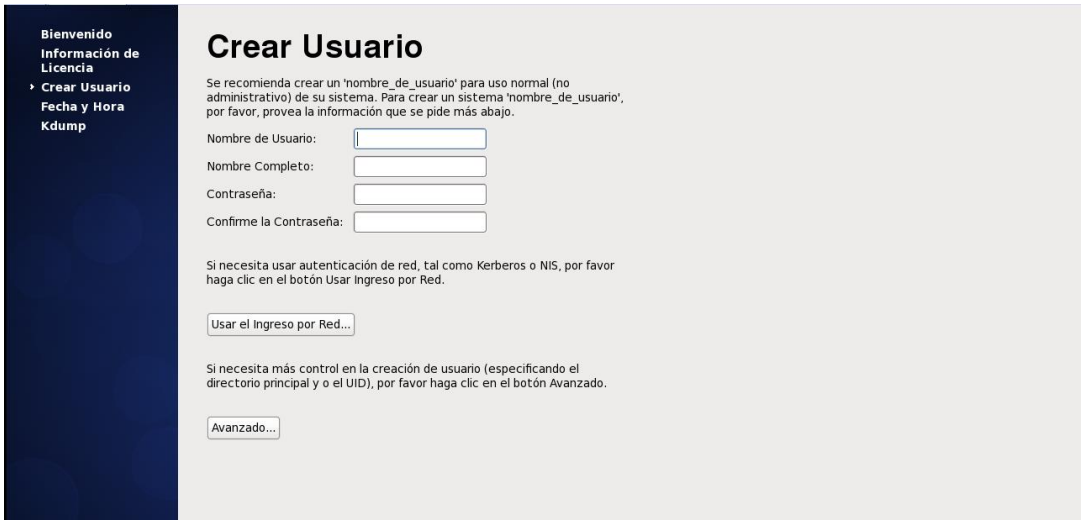


Figura D2 36. Usuario para inicio de sesión

Fuente: CentOS

- Configurar la fecha y hora del sistema

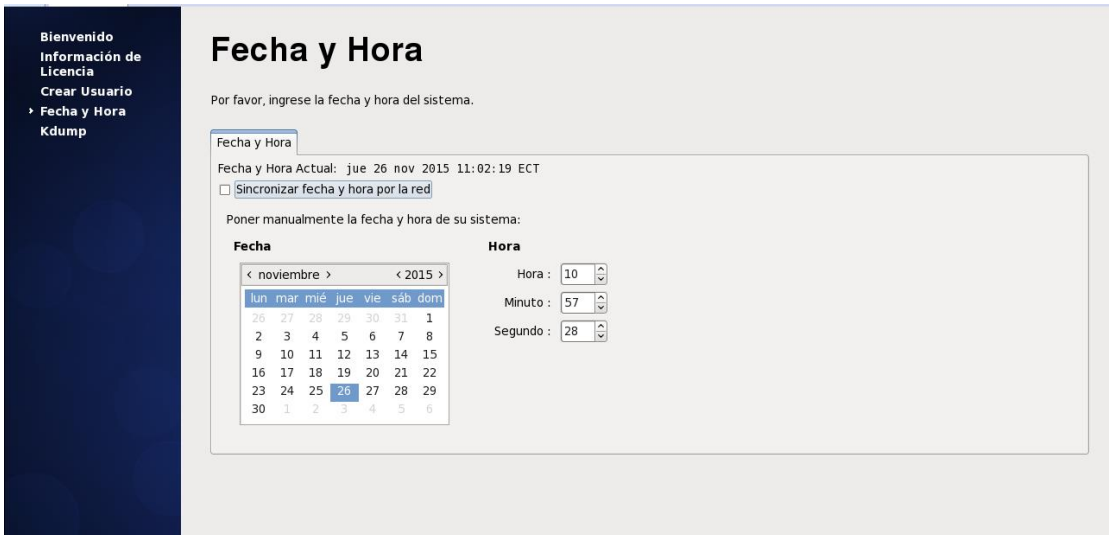


Figura D2 37. Fecha y Hora del Sistema

Fuente: CentOS

- Al finalizar la configuración ya se puede ingresar al sistema operativo e iniciar sesión.

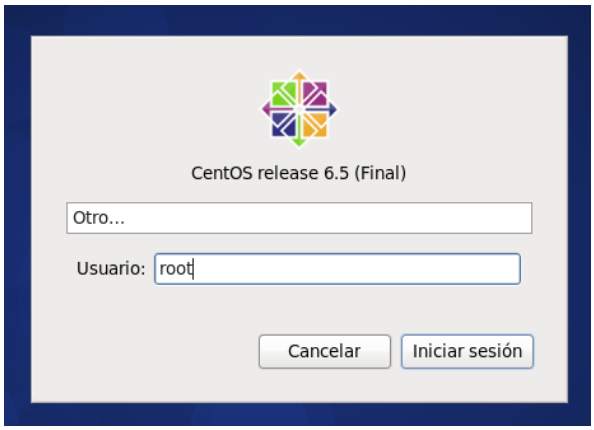


Figura D2 38. Inicio de Sesión

Fuente: CentOS

D3. INSTALACIÓN DE ELASTIX

- Una vez cargado el software nos aparecerá la inicialización del ELASTIX, y en la opción de boot dar enter o espacio para iniciar la instalación.

Figura D3 1. Inicio de ELASTIX

Fuente: ELASTIX

- Escoger el idioma Spanish y dar enter en aceptar para continuar.

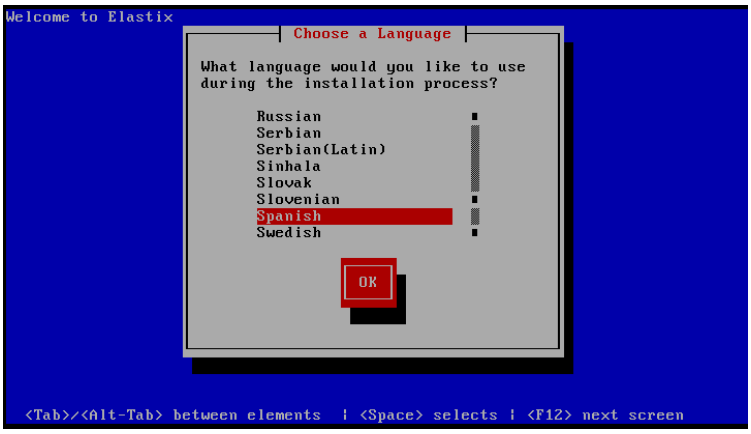


Figura D3 2. Elección de idioma

Fuente: ELASTIX

- En esta ventana seleccionar el tipo de teclado, escoger “es” para español y dar un enter en aceptar para continuar.

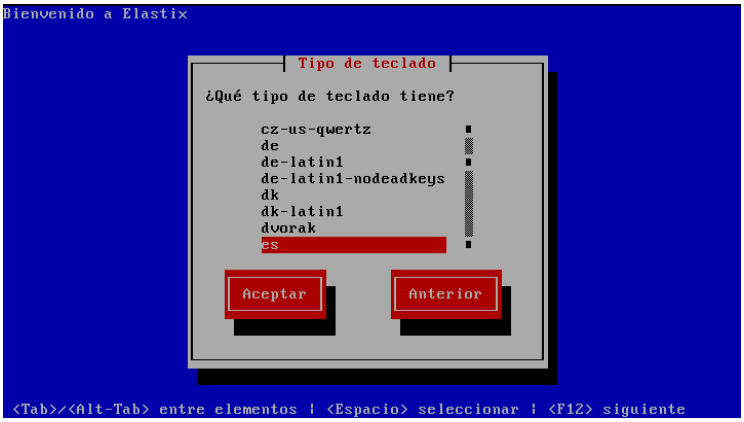


Figura D3 3. Idioma de teclado

Fuente: ELASTIX

- Inicializar los datos para la instalación escogiendo la opción SI

Figura D3 4. Inicializar datos de instalación

Fuente: ELASTIX

- Luego realizar una partición para el servidor, de acuerdo al espacio libre disponible.

Figura D3 5. Particionamiento para el servidor

Fuente: ELASTIX

- Visualización de las particiones que tiene el disco y el tamaño que ocupa cada una.

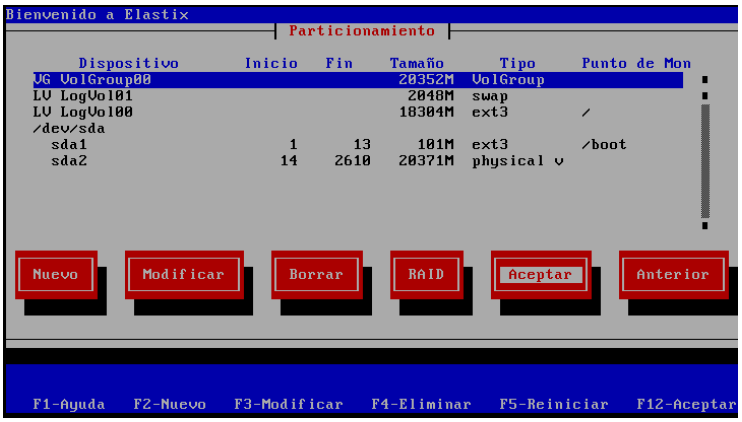


Figura D3 6. Visualización de particiones

Fuente: ELASTIX

- A continuación, configurar la interfaz de red eth0 en el sistema, seleccionando SI

Figura D3 7. Configurar interfaz de red

Fuente: ELASTIX

- Ahora se configura la interfaz eth0 de forma manual y con IPv4.

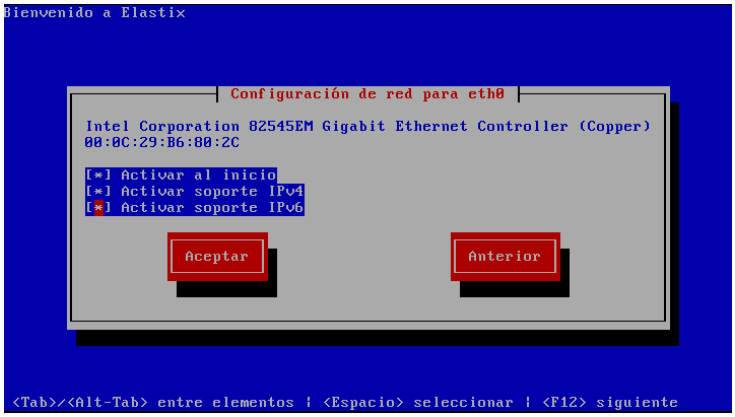


Figura D3 8. Configuración de red para eth0

Fuente: ELASTIX

- Seleccionamos la configuración DHCP para el direccionamiento IPv4 de eth0 recordando que este es la IP del servidor de voz.

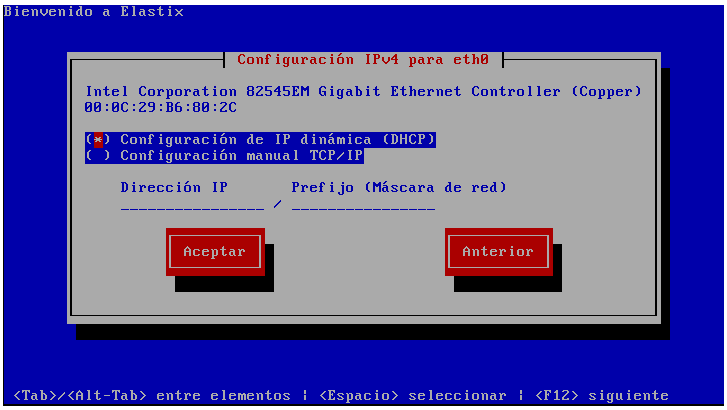


Figura D3 9. Configuración IPv4 para eth0

Fuente: ELASTIX

- Seleccionar descubrimiento automático de vecino para el direccionamiento IPv6 de eth0

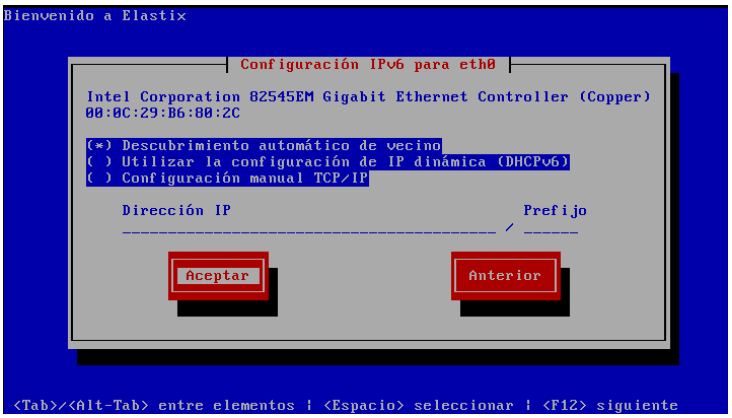


Figura D3 10. Configuración IPv6 para eth0

Fuente: ELASTIX

- En la ventana de configuración de un nombre para el host seleccionar la opción Automáticamente a través de DHCP.

Figura D3 11. Configuración del nombre del host

Fuente: ELASTIX

- En uso horario escoger el reloj del sistema y buscar América/Guayaquil y dar enter en aceptar.

Figura D3 12. Selección del uso horario

Fuente: ELASTIX

- Luego pide que se ingrese la contraseña para root, en este caso es elastix1234, confirmar la contraseña y dar un enter en aceptar para continuar.

Figura D3 13. Contraseña de root

Fuente: ELASTIX

- Finalmente se inicia la instalación, esperar porque esto tarda algunos minutos.

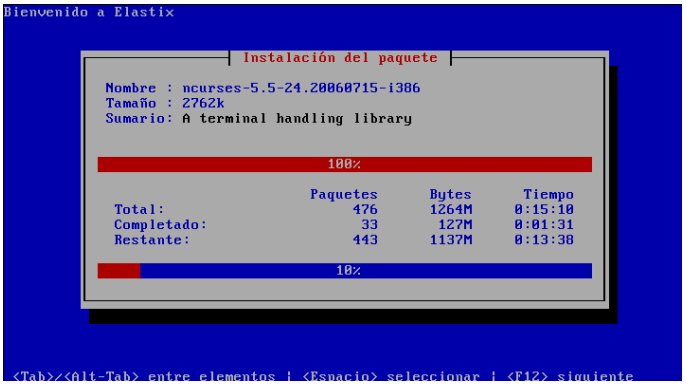


Figura D3 14. Instalación de paquetes

Fuente: ELASTIX

- Se observa una inicialización del servicio en modo consola.

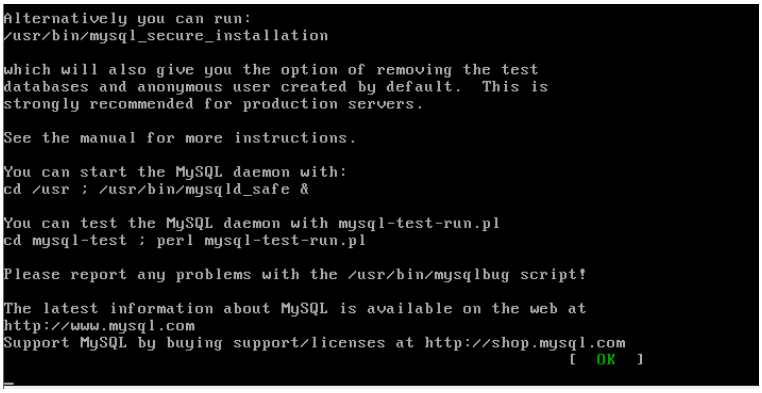


Figura D3 15. Inicio de servicio en modo consola

Fuente: ELASTIX

- A continuación, se solicitará una contraseña para la base de datos MySQL en este caso será elastix1234

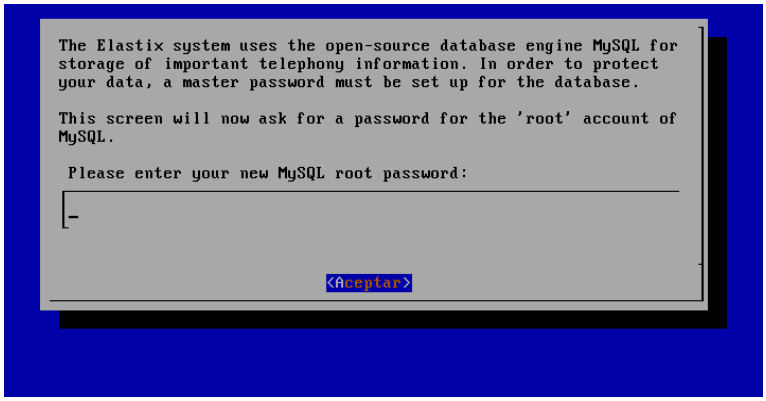


Figura D3 16. Contraseña de MySQL

Fuente: ELASTIX

- Confirmar la clave de root, dar un Enter en aceptar para continuar.

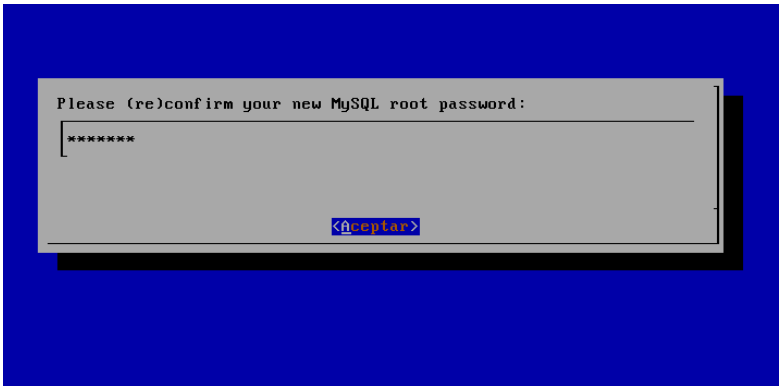


Figura D3 17. Confirmación de contraseña de MySQL

Fuente: ELASTIX

- Para el ingreso por vía web se debe colocar una contraseña para admin que en este caso será elastix1234.

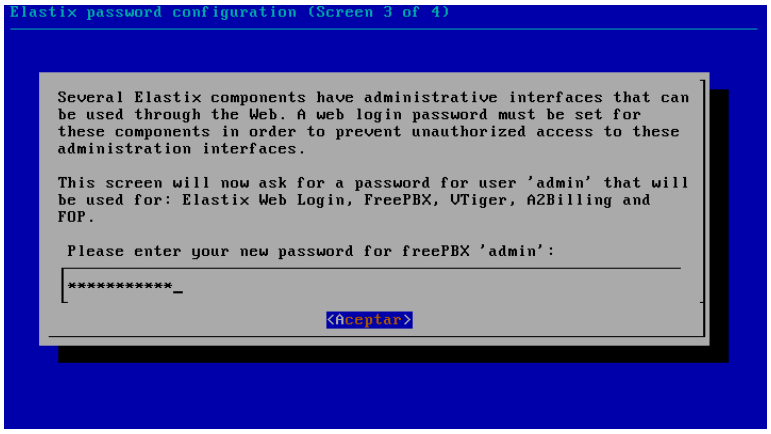


Figura D3 18. Contraseña de admin

Fuente: ELASTIX

- Confirmar la contraseña para admin

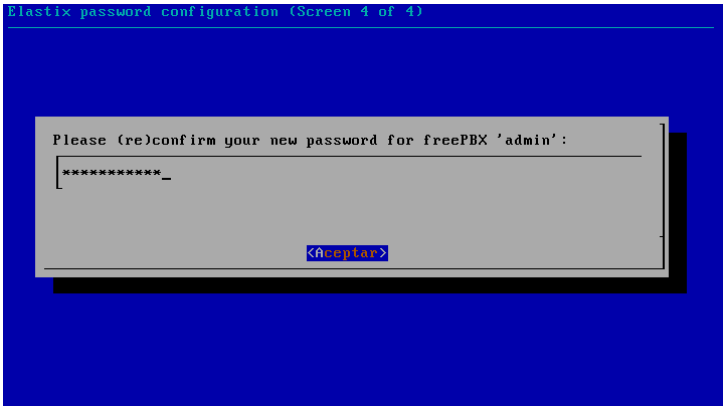


Figura D3 19. Confirmación de contraseña de admin

Fuente: ELASTIX

- En la consola del servidor en modo root escribir el comando setup para realizar la configuración de la red.

Figura D3 20. Consola del servidor en modo root

Fuente: ELASTIX

- Escoger la herramienta de configuración de red y dar Enter en aceptar para continuar.

Figura D3 21. Herramienta de configuración de red

Fuente: ELASTIX

- En la ventana de selección de acción escoger la opción Editar dispositivos, guardar y cerrar.

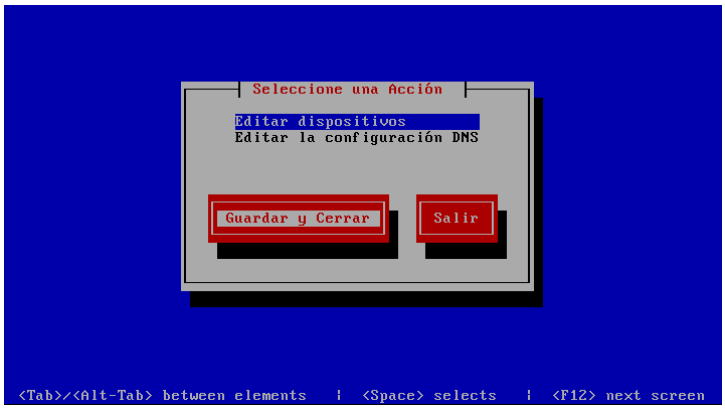


Figura D3 22. Selección de acción

Fuente: ELASTIX

- Escoger la interfaz de red eth0 y guardar para continuar con la configuración.

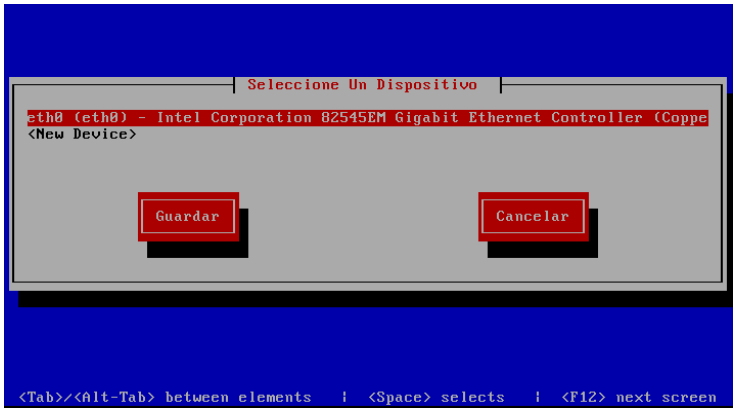


Figura D3 23. Selección de dispositivo

Fuente: ELASTIX

- Luego añadir una dirección IP estática al servidor Elastix, con su respectiva máscara y puerta de enlace.

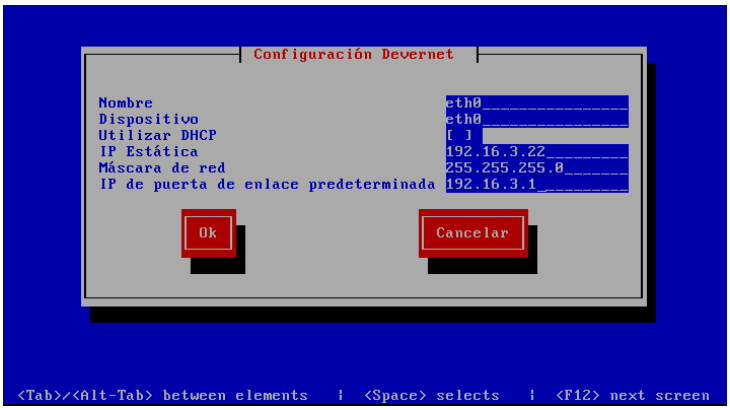


Figura D3 24. Asignación de dirección IP del servidor

Fuente: ELASTIX

- Guardar los cambios que se realiza en la configuración de red y cerrar.

Figura D3 25. Guardar cambios

Fuente: ELASTIX

- Se debe realizar un reinicio de las interfaces, para esto ingresar el siguiente comando ➔ service network restart

Figura D3 26. Reinicio de interfaces

Fuente: ELASTIX

- Para verificar que la dirección IP se asignó a la interfaz eth0 correctamente, ingresar el comando ifconfig

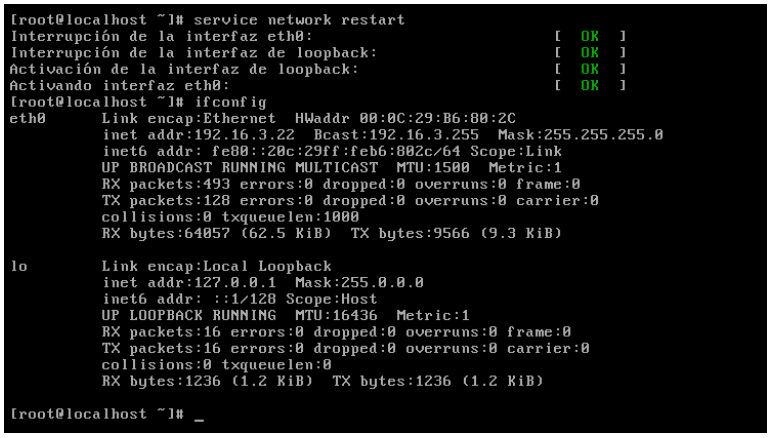


Figura D3 27. Verificación de IP en la interfaz eth0

Fuente: ELASTIX

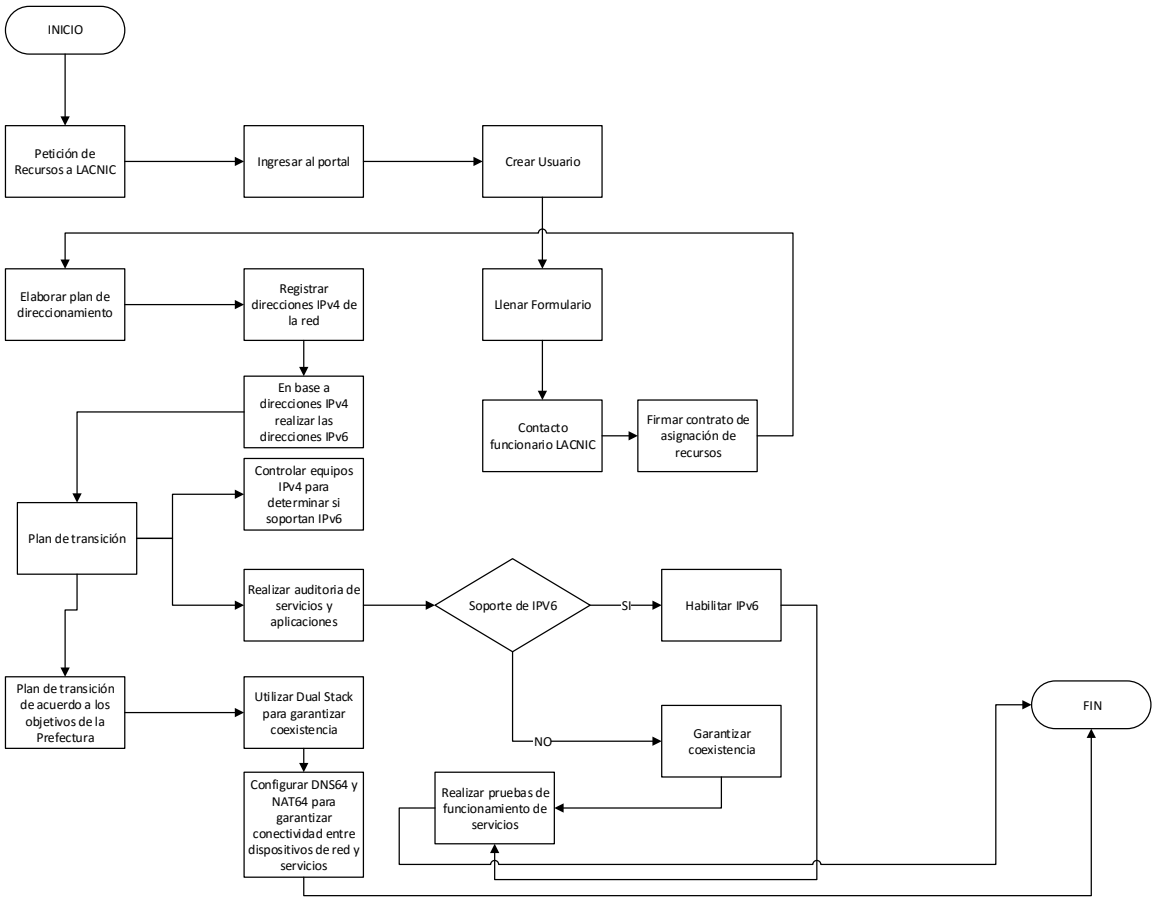
Anexo E. Manual de Procedimientos

El presente manual de procedimientos está estructurado en base a los procedimientos para realizar una coexistencia entre el protocolo IPv4 e IPv6 en la Prefectura de Imbabura, el cuál deberá ser utilizado por el administrador de red en una futura implementación del proyecto.

<table>
<tr><th colspan="4">PREFECTURA DE IMBABURA</th></tr>
<tr><td>PREFECTURA DE IMBABURA</td><td colspan="3">PROCEDIMIENTOS PARA LA ETAPA DE ELABORACIÓN DEL PLAN DE TRANSICIÓN</td></tr>
<tr><td rowspan="2">Versión: 1.0</td><td colspan="3">Revisado por: Ing. Fernando Miño / Director de Departamento de Tecnologías de la Información</td></tr>
<tr><td colspan="3">Elaborado por: Stalin Andrés Hidrobo Mafla</td></tr>
<tr><td>Código: MP-PI-001</td><td colspan="3">GAD PROVINCIAL DE IMBABURA</td></tr>
<tr><th>N°</th><th>Actividad</th><th>Descripción</th><th>Responsable</th></tr>
<tr><td>1</td><td>Petición de Recursos</td><td>- Ingresar al portal IPv6 de LACNIC.
- Crear un usuario en LACNIC
- Llenar el formulario de petición de recursos
- Esperar contacto de funcionarios de LACNIC
- Firmar contrato de asignación de recursos</td><td>Director de TIC’s</td></tr>
<tr><td>2</td><td>Elaboración del plan de direccionamiento</td><td>- Registrar las direcciones IPv4 de la red.</td><td>Administrador de la red</td></tr>
</table>

		- Tomar como base direcciones IPv4 para realizar el direccionamiento IPv6	
3	Plan de transición de acuerdo a los objetivos de la Prefectura de Imbabura	- Utilizar Dual Stack, para coexistir entre protocolos IPv4 e IPv6 en la red - Utilizar servicios de traducción para brindar la conectividad a los usuarios IPv6 que necesitan tener acceso a servicios y aplicaciones en IPv4. Este proceso se consigue llevar a cabo con el levantamiento de NAT64 y DNS64. - Supervisar el proceso y efectos de la transición de IPv6 mediante pruebas.	
4	Plan de transición	- Controlar los equipos IPv4: switchs, servidores, PCs y dispositivos móviles de usuarios, para determinar los que admiten IPv6. - Realizar una auditoría de los Servicios y Aplicaciones para identificar los que están habilitados el protocolo IPv6.	

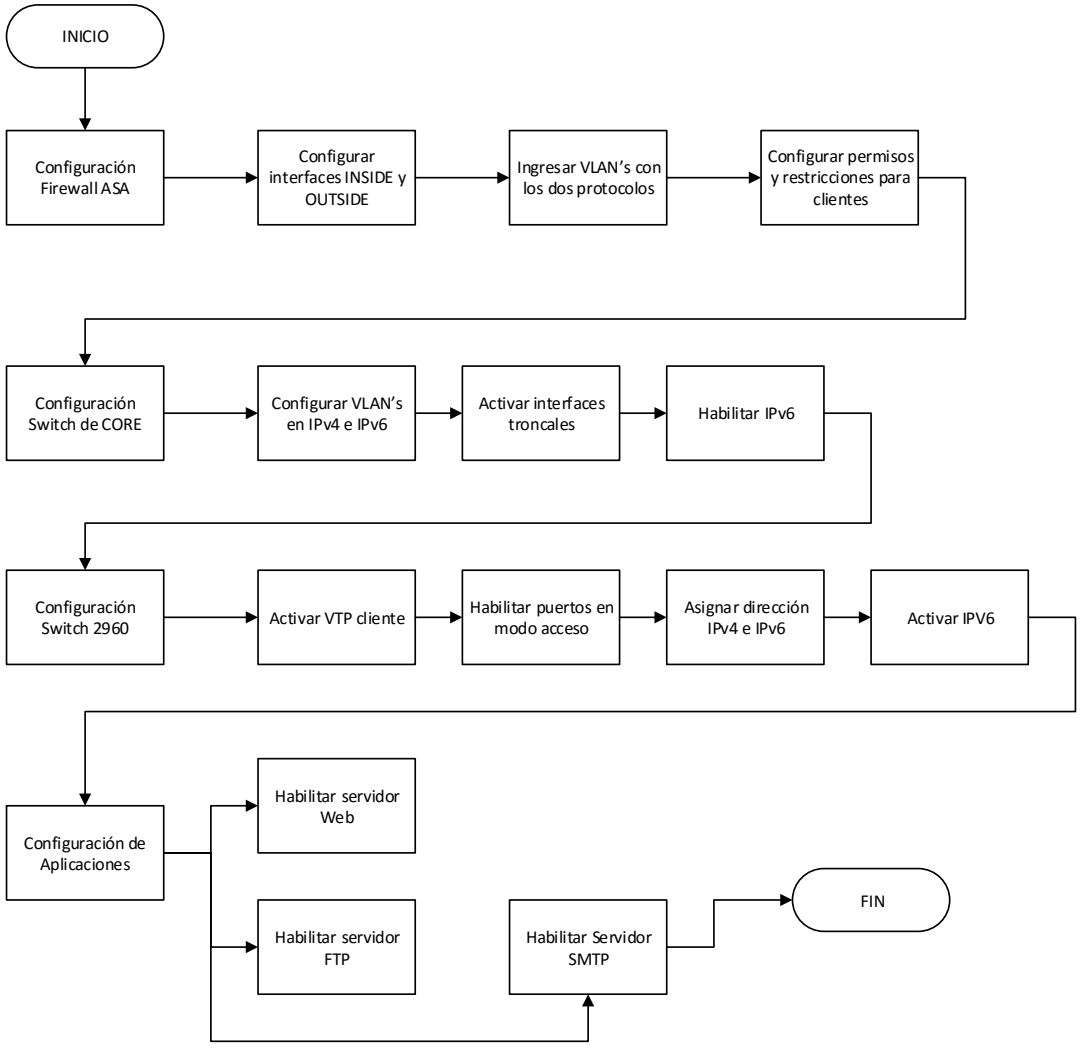
FLUJOGRAMA


INICIO
Petición de Recursos a LACNIC
Ingresar al portal
Crear Usuario
Elaborar plan de direccionamiento
Registrar direcciones IPv4 de la red
Llenar Formulario
En base a direcciones IPv4 realizar las direcciones IPv6
Contacto funcionario LACNIC
Firmar contrato de asignación de recursos
Controlar equipos IPv4 para determinar si soportan IPv6
Plan de transición
Realizar auditoria de servicios y aplicaciones
Soporte de IPV6
SI
Habilitar IPv6
Plan de transición de acuerdo a los objetivos de la Prefectura
Utilizar Dual Stack para garantizar coexistencia
NO
Garantizar coexistencia
FIN
Configurar DNS64 y NAT64 para garantizar conectividad entre dispositivos de red y servicios
Realizar pruebas de funcionamiento de servicios

<table>
<tr><th colspan="4">PREFECTURA DE IMBABURA</th></tr>
<tr><td>PREFECTURA DE IMBABURA</td><td colspan="3">PROCEDIMIENTOS PARA LA ETAPA DE IMPLEMENTACIÓN Y CONFIGURACIÓN</td></tr>
<tr><td rowspan="2">Versión: 1.0</td><td colspan="3">Revisado por: Ing. Fernando Miño / Director de Departamento de Tecnologías de la Información</td></tr>
<tr><td colspan="3">Elaborado por: Stalin Andrés Hidrobo Mafla</td></tr>
<tr><td>Código: MP-PI-002</td><td colspan="3">GAD PROVINCIAL DE IMBABURA</td></tr>
<tr><th>N°</th><th>Actividad</th><th>Descripción</th><th>Responsable</th></tr>
<tr><td>1</td><td>Configuración Firewall ASA</td><td>- Configurar interfaces INSIDE y OUTSIDE
- Ingresar VLAN’s utilizando los dos protocolos.
- Configurar permisos y restricciones para los clientes.</td><td>Administrador de la red</td></tr>
<tr><td>2</td><td>Configuración Switch de CORE</td><td>- Configurar VLAN´s en IPv4 e IPv6
- Activar interfaces troncales
- Habilitar IPv6</td><td>Administrador de la red</td></tr>
<tr><td>3</td><td>Configuración Switch 2960</td><td>- Activar VTP cliente para que se propaguen las VLAN’s configurada.
- Habilitar puertos en modo acceso
- Asignar direcciones IPv4 a IPv6.
- Activar IPv6</td><td></td></tr>
<tr><td>4</td><td>Configuración de aplicaciones</td><td>- Habilitación de Servidor Web</td><td>Administrador de red</td></tr>
</table>

		- Habilitación de Servidor FTP - Habilitación de Servidor SMTP	

FLUJOGRAMA



Anexo F. Aplicaciones Adicionales

F1. Instalación de PostFix

- Instalar el paquete de PostFix con el siguiente comando #yum install postfix

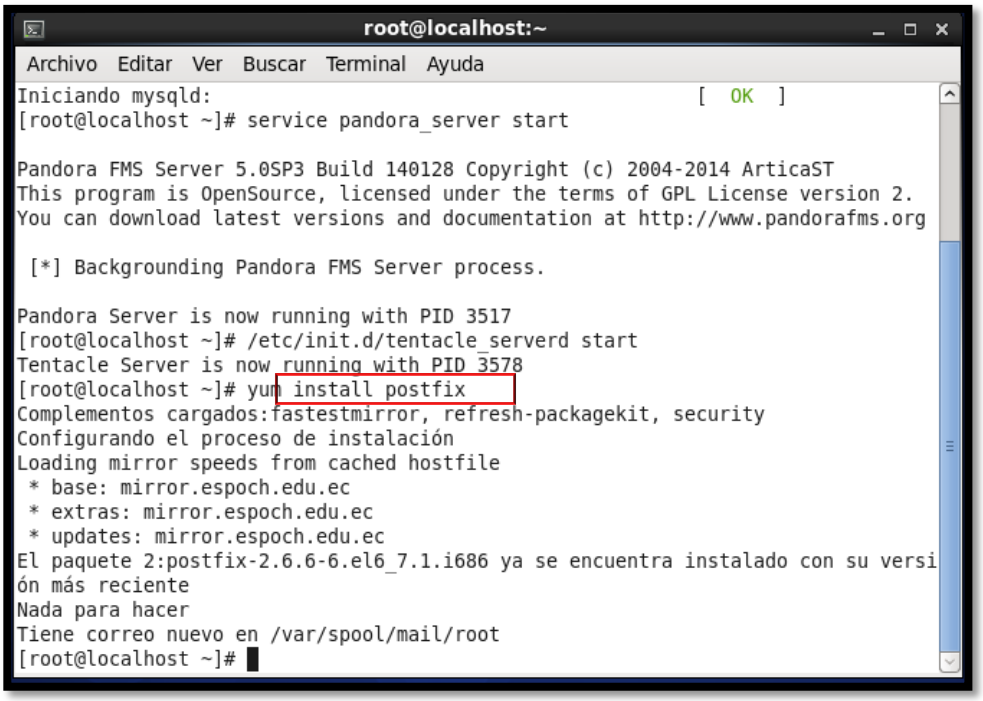


Figura F1 1. Instalación de PostFix

Fuente: Consola CentOS

- Se procede a modificar la configuración de PostFix en el siguiente archivo #/etc/postfix/main.cf

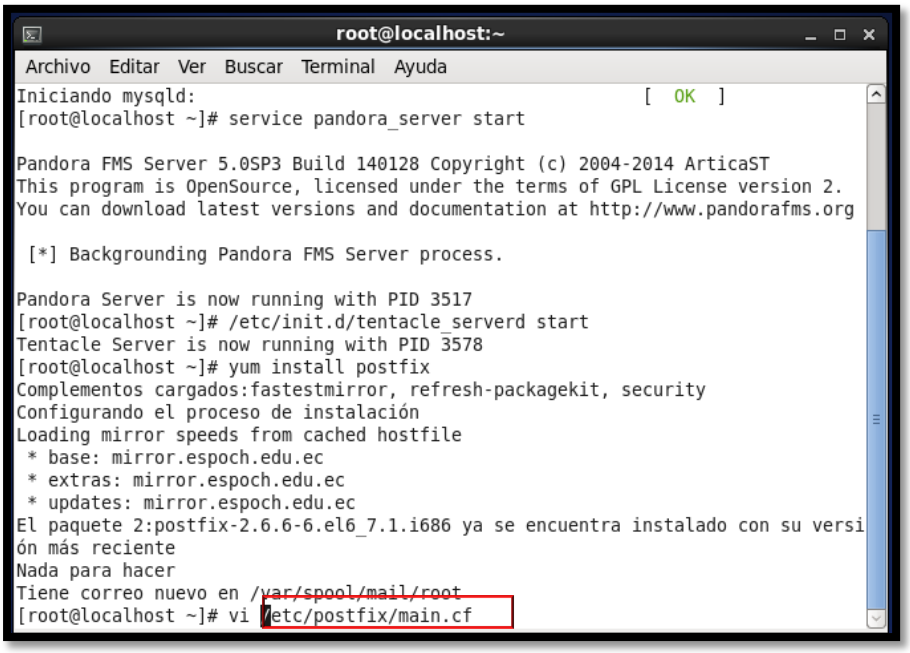


Figura F1 2. Comando para configurar archivo de PostFix

Fuente: Consola CentOS

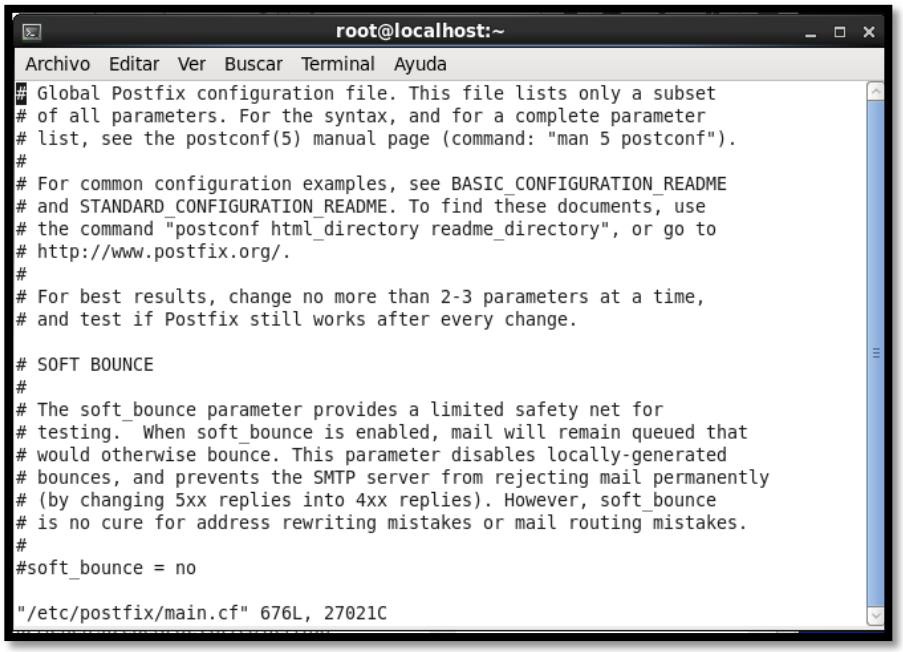


Figura F1 3. Archivo de Configuración de PostFix

Fuente: Consola CentOS

- Dentro de este archivo se debe editar las siguientes líneas

inet_interfaces = all
mydomain = midominio.org
myorigin = $mydomain
mydestination = $mydomain, $myhostname, localhost
home_mailbox = Maildir/

- Añadir el servicio al inicio del sistema con el siguiente comando

#chkconfig postfix on

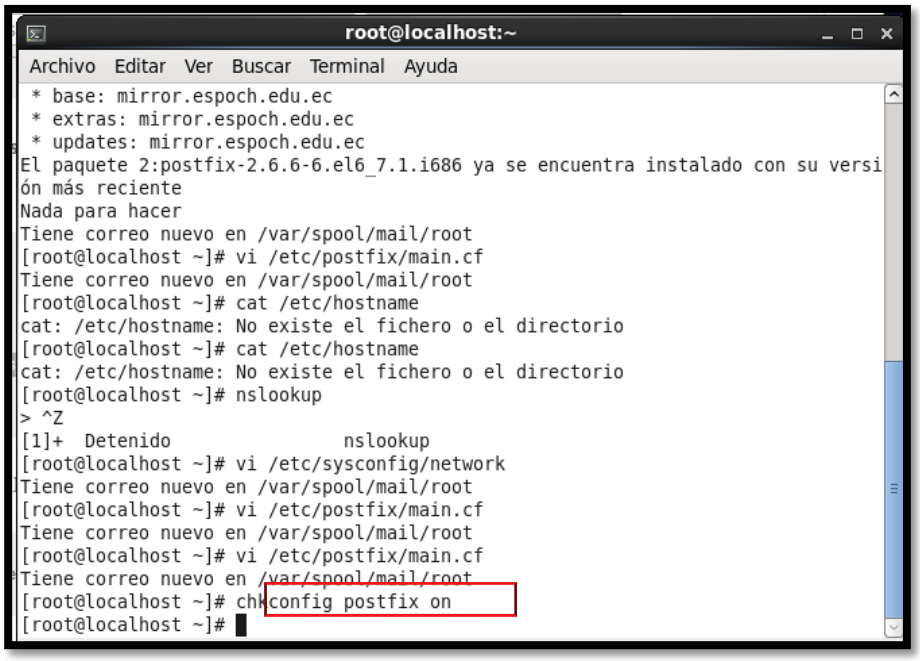


Figura F1 4. Inicio de Servicio PostFix al iniciar el Sistema Operativo

Fuente: Consola CentOS

- Reiniciar el servicio con el comando

#service postfix restart

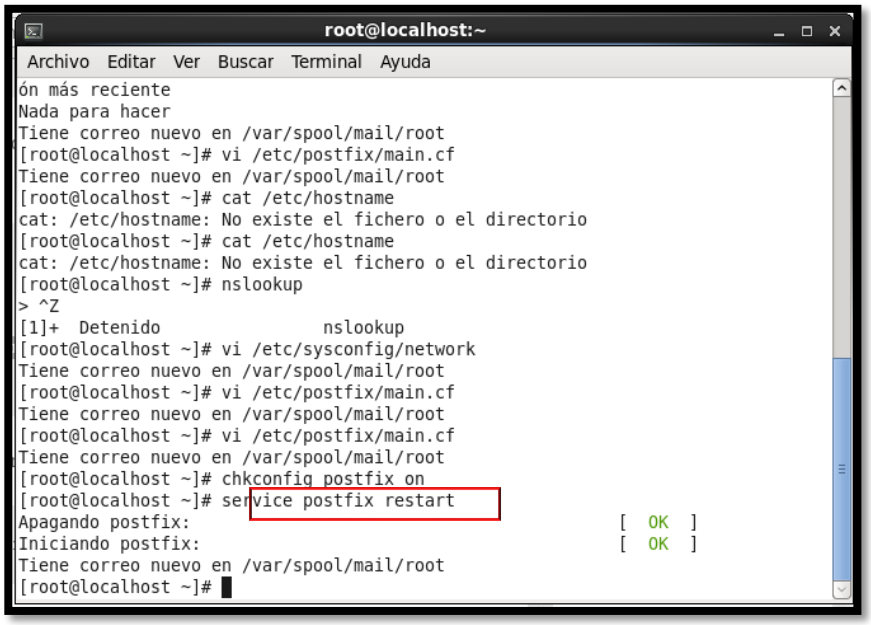


Figura F1 5. Reinicio del Servicio PostFix

Fuente: Consola CentOS

- Por defecto todos los usuarios definidos en el sistema tienen su cuenta de correo de la siguiente manera: usuario@midominio.org

- Crear la carpeta Maildir en el directorio mostrado para que se guarden en ella automáticamente los usuarios añadidos al sistema y los correos electrónicos recibidos.

mkdir /etc/skel/Maildir

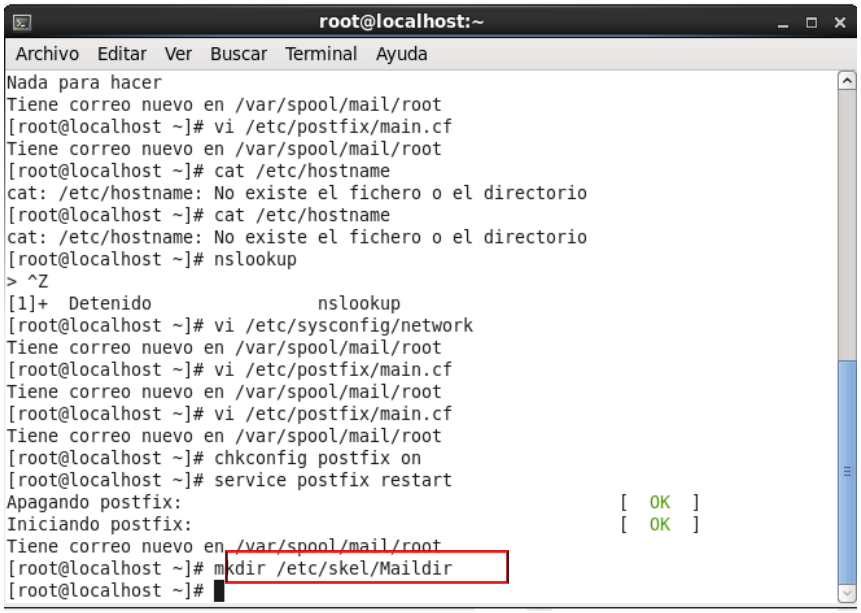


Figura F1 6. Creación de carpeta Maildir

Fuente: Consola CentOS

- Crear el archivo para leer el contenido de la carpeta creada con el siguiente comando

touch /etc/skel/.muttrc

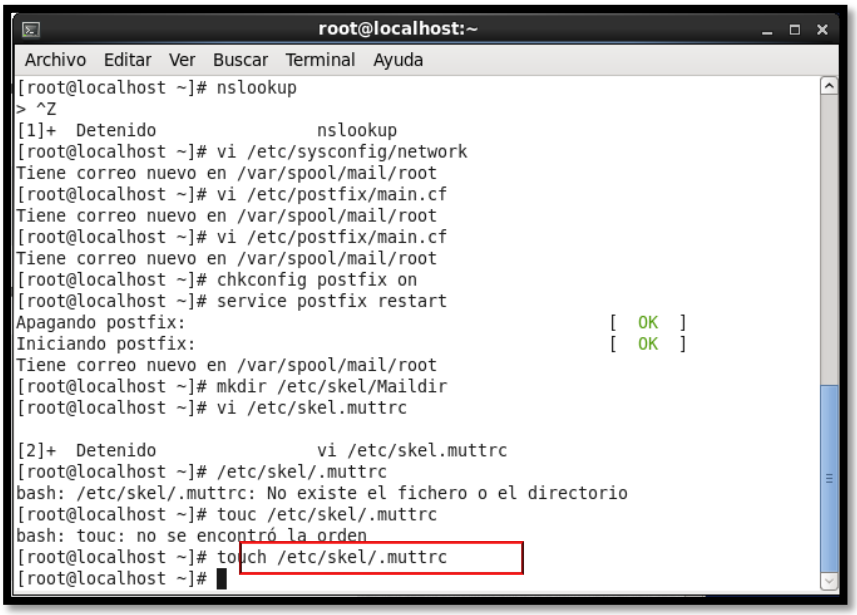


Figura F1 7. Creación de archivo para lectura de correos

Fuente: Consola CentOS

- Editar el archivo con las configuraciones mostradas en la figura

Figura F1 8. Configuración de archivo para recibir correos

Fuente: Consola CentOS

- Crear usuarios para probar el envío de correos

Figura F1 9. Creación de Usuario para prueba

Fuente: Consola CentOS

- Para comprobar el envío de correo es necesario tener instalado telnet para esto se debe instalar el paquete con los siguiente comandos.

yum –y install telnet

#yum install telnet-server

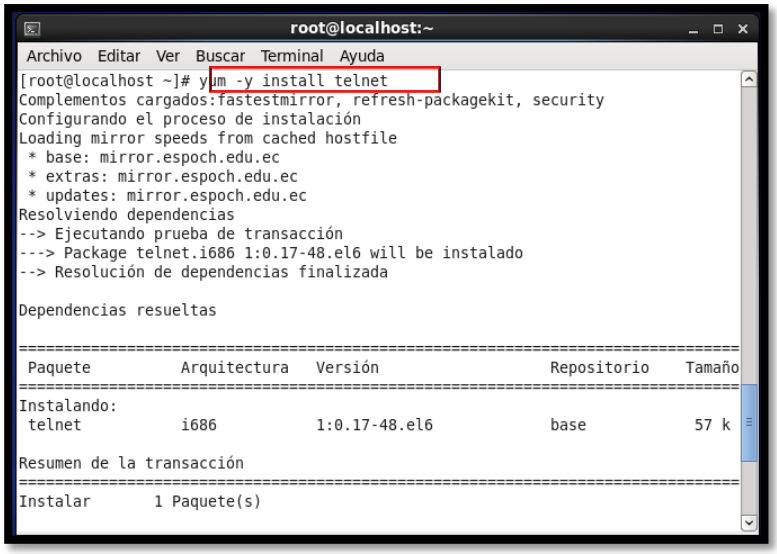


Figura F1 10. Comando para instalar Telnet

Fuente: Consola CentOS

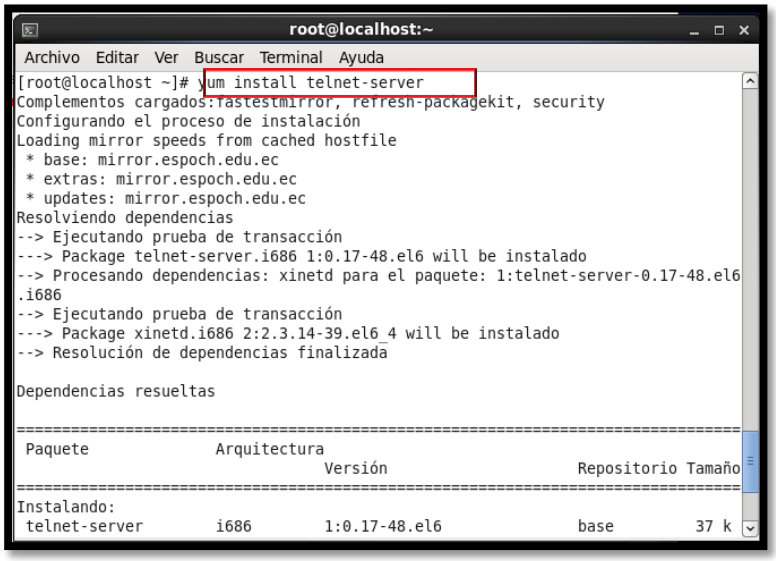


Figura F1 11. Comando para instalación de Telnet

Fuente: Consola CentOS

- Acceder al archivo /etc/xineted.d/telnet

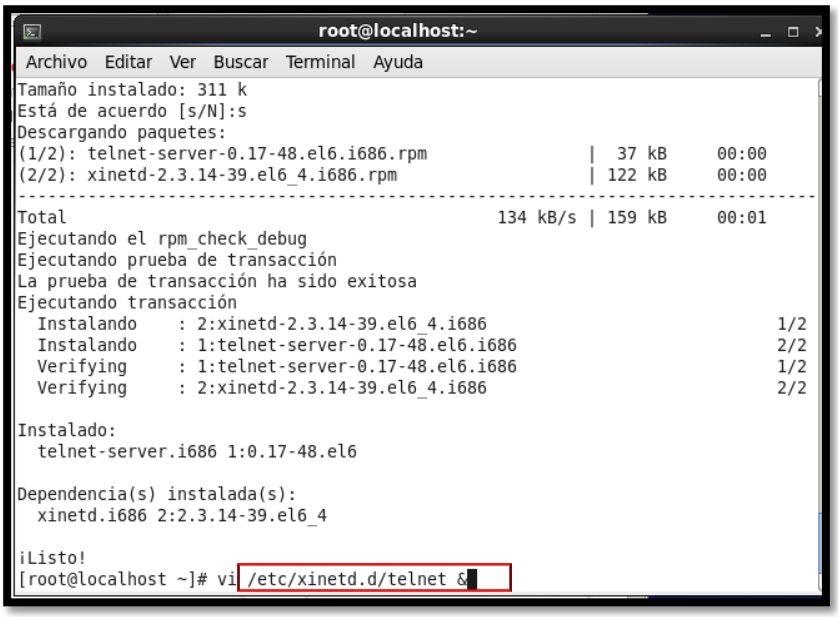


Figura F1 12. Ingreso al archivo de configuración de Telnet

Fuente: Consola CentOS

- Dentro de este archivo cambiar la línea disable=yes por disable=no

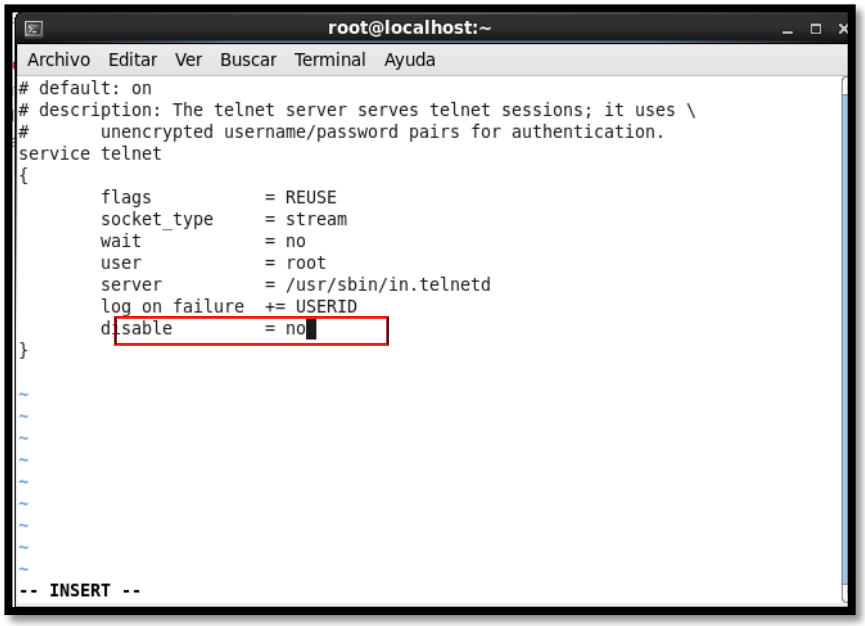


Figura F1 13. Archivo de configuración de Telnet

Fuente: Consola CentOS

- A continuación abrir el puerto 23 del firewall para permitir el acceso Telnet, esto se realiza en el menú sistema, escoger administración y luego cortafuegos.

Figura F1 14. Menú Sistema

Fuente: CentOS

- En la opción otros puertos escoger añadir y escoger el puerto 23 de Telnet, luego hacer clic en aceptar y el puerto se añade.

Figura F1 15. Añadir el Puerto para Telnet

Fuente: CentOS

Figura F1 16. Puerto 23 de Telnet

Fuente: CentOS

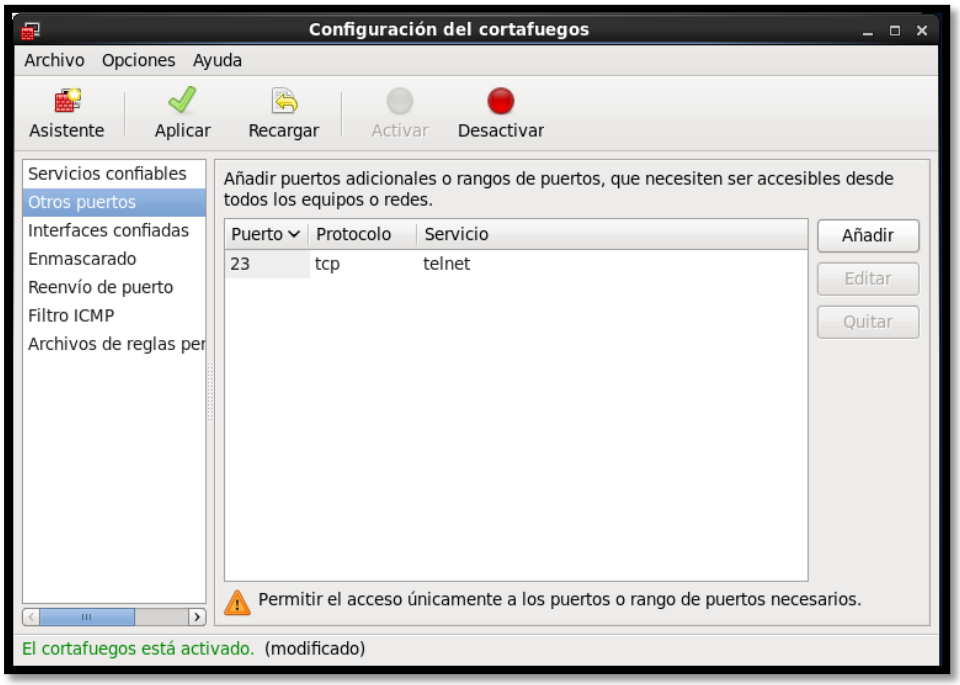


Figura F1 17. Puerto Telnet añadido

Fuente: CentOS

- Probar Telnet con el protocolo SMTP

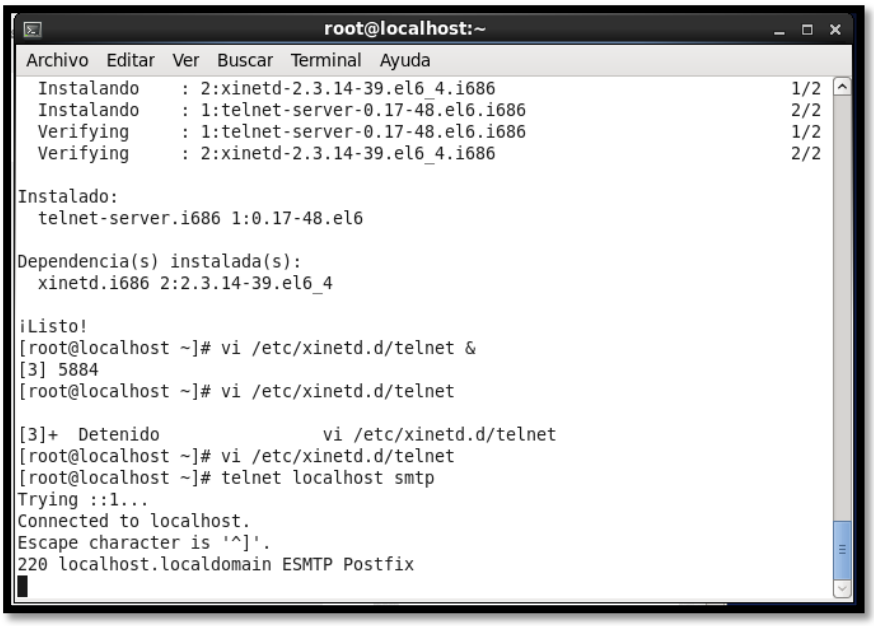


Figura F1 18. Telnet al protocolo SMTP

Fuente: Consola CentOS

- Añadir las siguientes líneas para envió de correo.

220 mail.midominio.org ESMTP Postfix

ehlo local

250-mail.midominio.org

250-PIPELINING

250-SIZE 10240000

250-VRFY

250-ETRN

250-ENHANCEDSTATUSCODES

250-8BITMIME

250 DSN

mail from: test@test.org

250 2.1.0 Ok

rcpt to: user1@midominio.org

250 2.1.5 Ok

data

354 End data with <CR><LF>.<CR><LF>

subject: hola

primer correo de prueba.

250 2.0.0 Ok: queued as 0E32477

- Comprobar en el log que se haya enviado el correo esto permite identificar si el servidor PostFix estará funcionando correctamente.

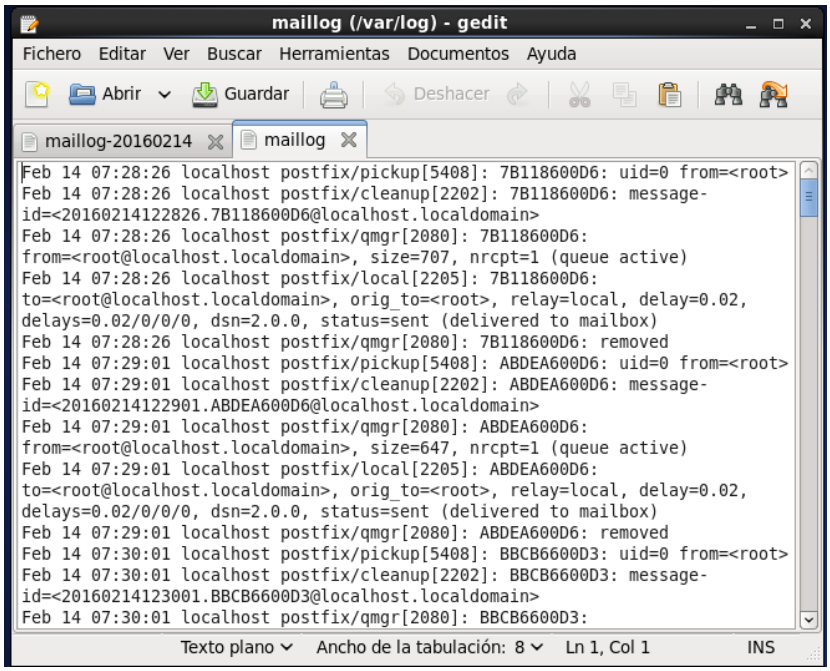


Figura F1 19. Comprobación de Correo enviado

Fuente: Consola CentOS

- Para enviar y recibir correo electrónico se debe crear una cuenta de correo electrónico para vincular a Postfix, en este caso se utilizó Outlook.

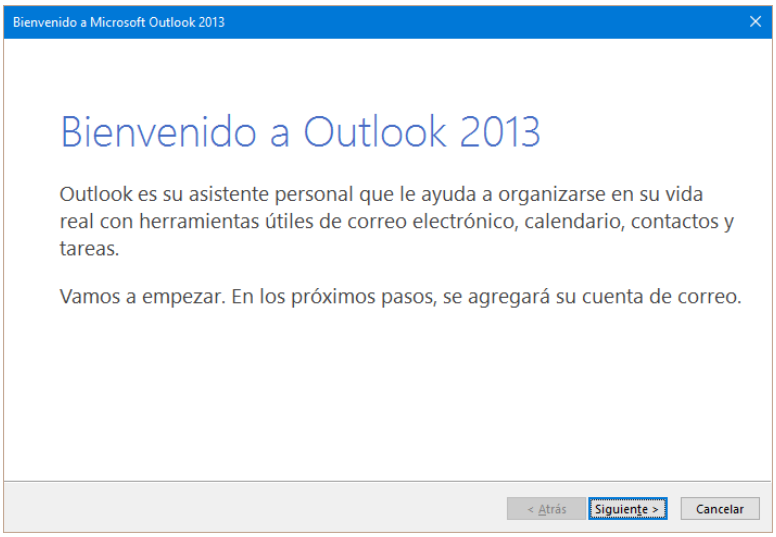


Figura F1 20. Pantalla de Inicio de Outlook

Fuente: Aplicación Outlook

- Para agregar la cuenta escoger la opción si

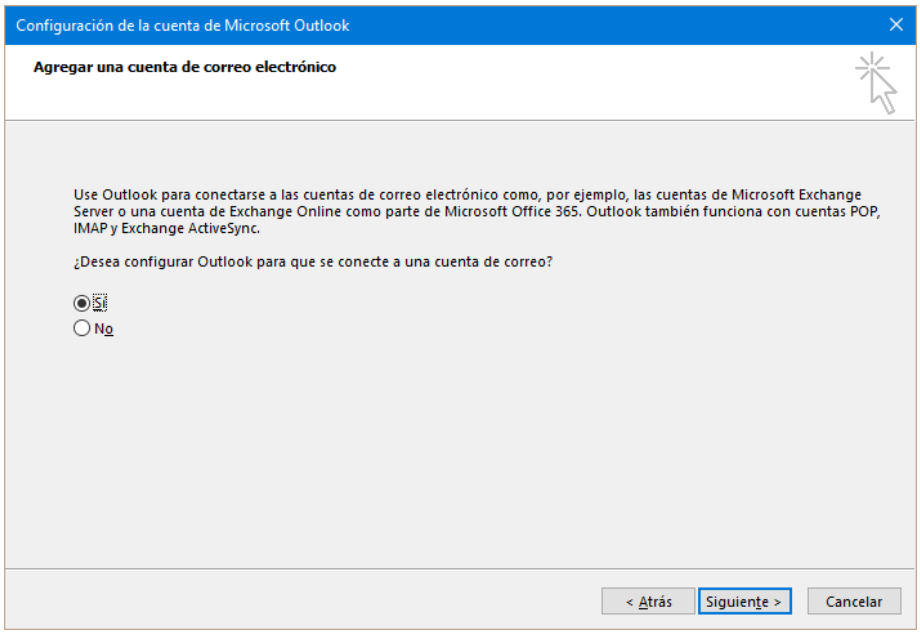


Figura F1 21. Configuración de Outlook

Fuente: Aplicación Outlook

- Escoger la opción Configuración manual o tipos de servidores adicionales.

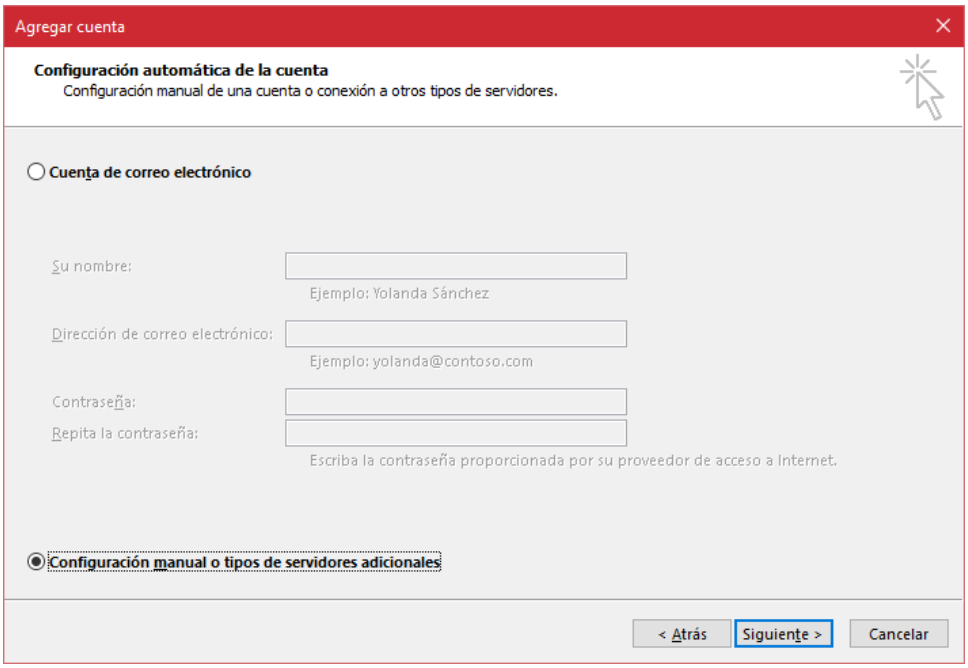


Figura F1 22. Opción configuración manual

Fuente: Aplicación Outlook

- Escoger el servicio POP o IMAP

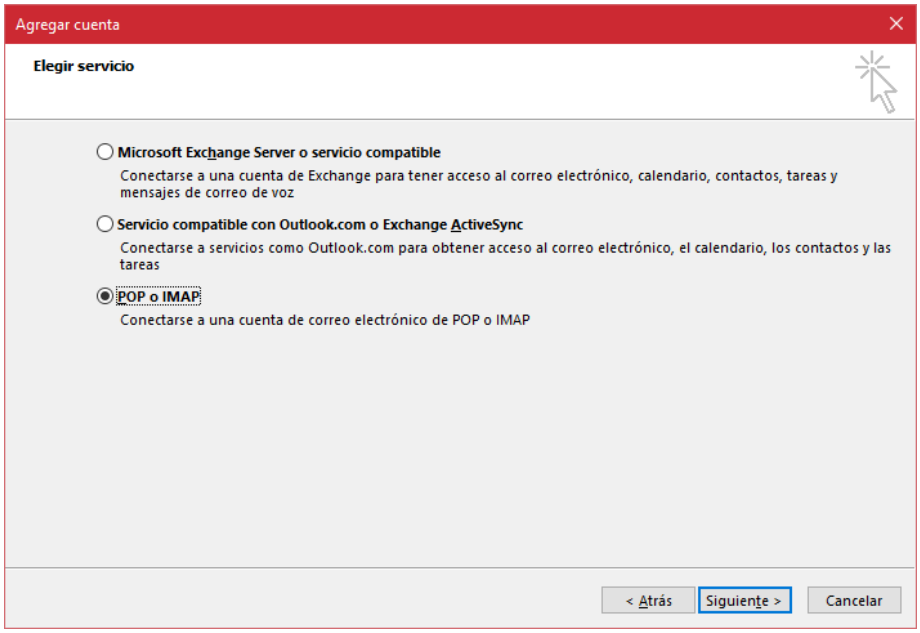


Figura F1 23. Elección del Tipo de Servicio a configurar

Fuente: Aplicación Outlook

- Configurar la cuenta con los datos de usuario creado en el servidor PostFix

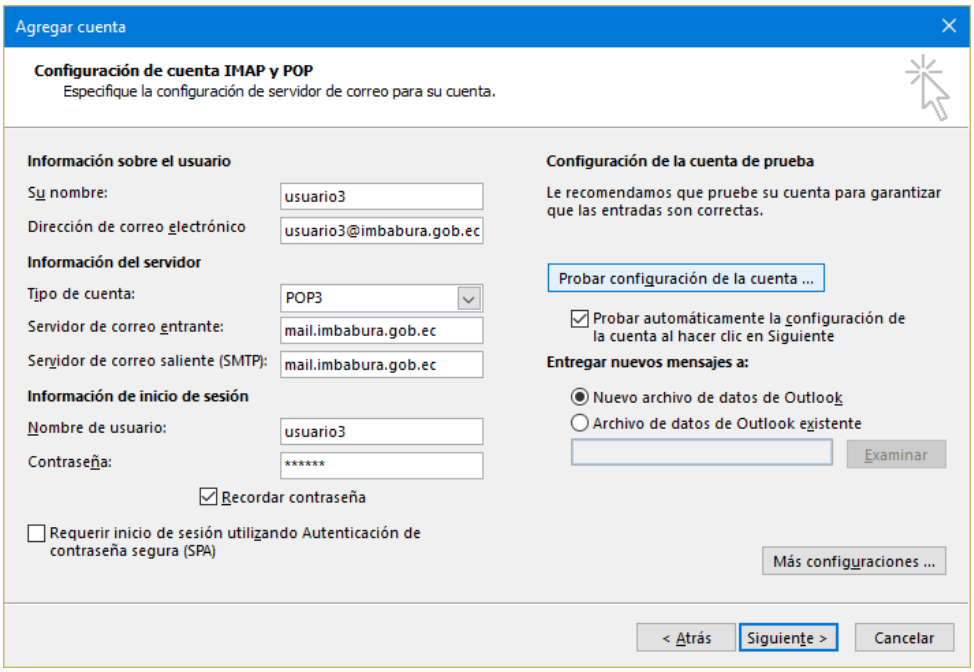


Figura F1 24. Configuración de cuenta

Fuente: Aplicación Outlook

- Realizar prueba de conexión de la cuenta con el Servidor Postfix.

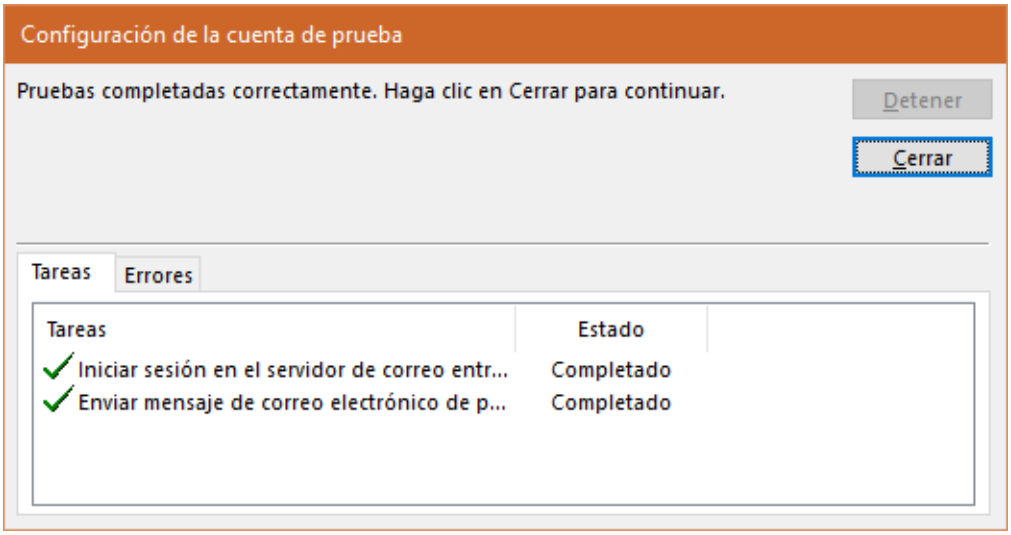


Figura F1 25. Prueba de conexión con Postfix

Fuente: Aplicación Outlook

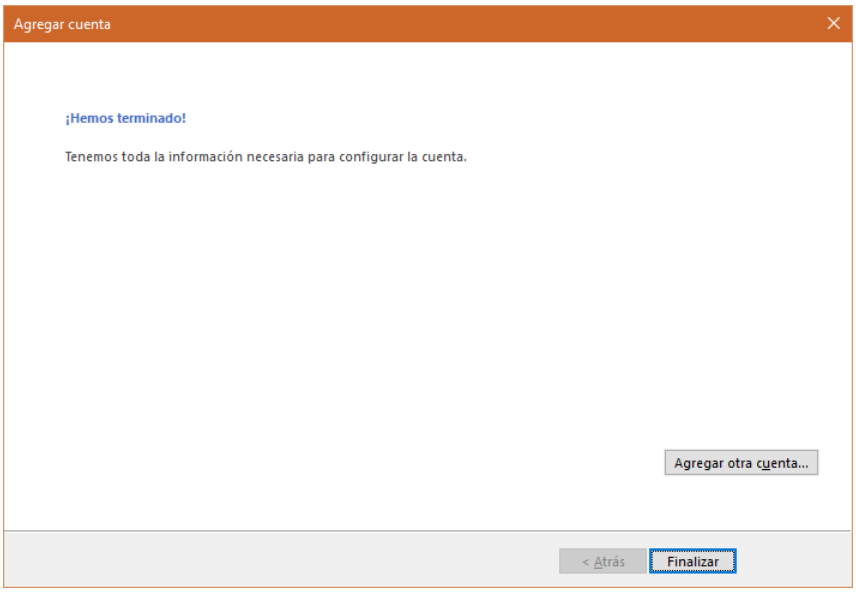


Figura F1 26. Finalización de configuración de correo

Fuente: Aplicación Outlook

F2. Instalación de Servidor FTP

- Ingresar al terminal e instalar el paquete de ftp mediante el comando

  #yum install vsftpd

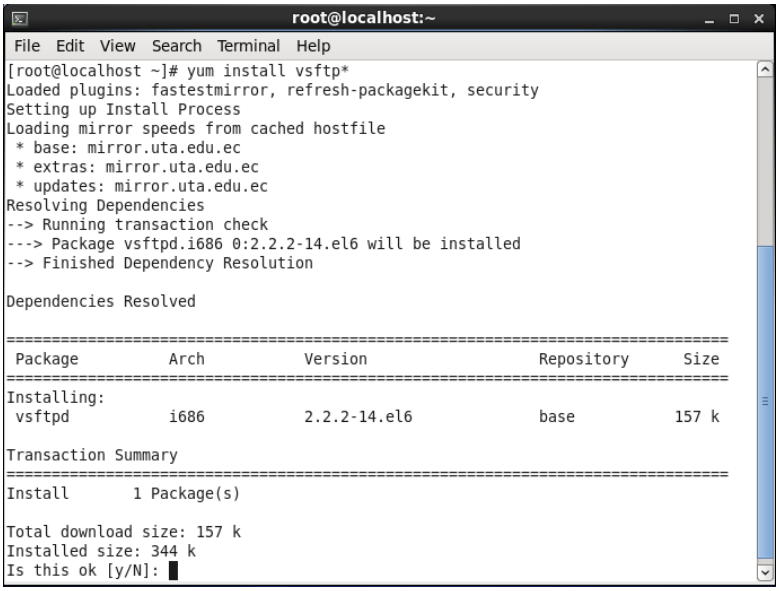


Figura F2 1. Instalación paquete FTP

Fuente: Consola CentOS

- Ingresar el comando mostrado a continuación para ingresar al archivo de configuración de FTP.

  #nano /etc/vsftpd/vsftpd.conf

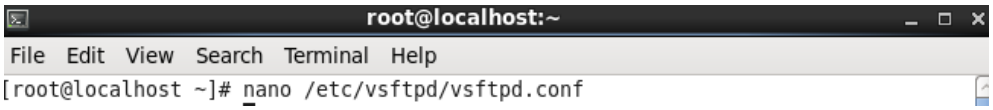


Figura F2 2. Ingreso al archivo de Configuración FTP

Fuente: Consola CentOS

- Verificar que las siguientes líneas estén activadas, de esta manera se garantiza que FTP está funcionando correctamente.

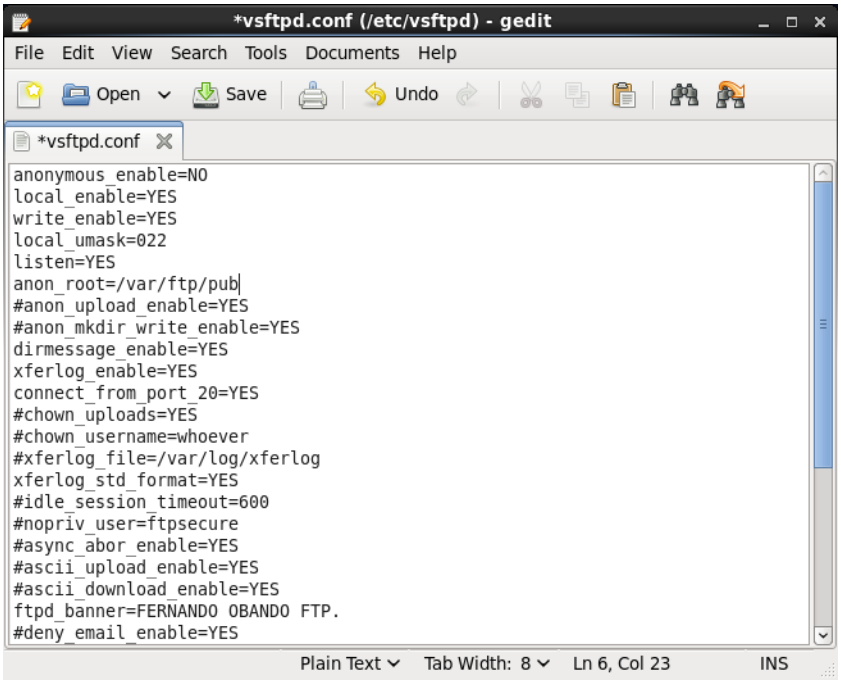


Figura F2 3. Archivo de Configuración FTP

Fuente: Consola CentOS

Ibarra, 15 de abril del 2016

Ing. Fernando Miño Ortega, Director de Tecnologías de la Información del Gobierno Provincial de Imbabura.

CERTIFICADO:

La Dirección de Tecnologías de la Información del Gobierno Provincial de Imbabura certifica que el proyecto de Tesis "METODOLOGÍA DE TRANSICIÓN DEL PROTOCOLO DE INTERNET VERSION 4 A VERSION 6 EN EL GOBIERNO PROVINCIAL DE IMBABURA" propuesto por el Sr. Hidrobo Mafla Stalin Andrés, con número de cédula 1003444617, estudiante de la Carrera de Ingeniería en Electrónica y Redes de Comunicación de la Facultad de Ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte, ha sido culminado y revisado por el personal técnico de esta Dirección y de esta manera cumple con el objetivo del proyecto propuesto.

Atentamente,

Ing. Fernando Miño Ortega
DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN
GOBIERNO PROVINCIAL DE IMBABURA