



UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE

COMUNICACIÓN

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE

INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

“PROPUESTA DE TRANSICIÓN DE SERVICIOS DE IPv4 A IPv6 PARA

LA RED DE DATOS CABLEADA DEL GOBIERNO AUTÓNOMO

DESCENTRALIZADO MUNICIPAL SAN MIGUEL DE IBARRA.”

AUTOR: GABRIELA ESTEFANÍA MERA TERÁN

DIRECTOR: MSc. FABIÁN CUZME

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:

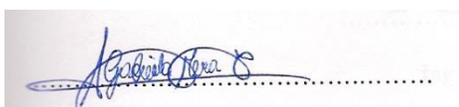
DATOS DEL CONTACTO			
CÉDULA DE IDENTIDAD:		1003487467	
APELLIDOS Y NOMBRES:		Mera Terán Gabriela Estefanía	
DIRECCIÓN:		Conjunto Parque Sol “Los Ceibos”	
EMAIL:		gembra@utn.edu.ec	
TELÉFONO FIJO:	062950131	TELÉFONO MÓVIL	0999197851
DATOS DE LA OBRA			
TÍTULO:		“Propuesta de transición de servicios de IPv4 a IPv6 para la red de datos cableada del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra.”	
AUTOR(ES):		Gabriela Estefanía Mera Terán	
FECHA:			
PROGRAMA:		Pregrado	
TÍTULO POR EL QUE OPTA:		Ingeniería en Electrónica y Redes de Comunicación	
ASESOR/DIRECTOR:		MSc. Fabián Cuzme	

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Gabriela Estefanía Mera Terán, con cédula de identidad Nro.100348746-7, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en formato 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 del 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.



Firma.....

Nombres: Gabriela Estefanía Mera Terán

Cédula: 100348746-7

Ibarra, 24 de octubre del 2016



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, GABRIELA ESTEFANÍA MERA TERÁN, con cédula de identidad Nro. 100348746-7, 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: “PROPUESTA DE TRANSICIÓN DE SERVICIOS DE IPv4 A IPv6 PARA LA RED DE DATOS CABLEADA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL SAN MIGUEL DE IBARRA”, 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 24 de octubre del 2016

Gabriela Estefanía Mera Terán

100348746-7



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DECLARACIÓN

Yo, Gabriela Estefanía Mera Terán, 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

Gabriela Estefanía Mera Terán

100348746-7



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

vi

CERTIFICACIÓN

Certifico que la Tesis “PROPUESTA DE TRANSICIÓN DE SERVICIOS DE IPv4 A IPv6 PARA LA RED DE DATOS CABLEADA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL SAN MIGUEL DE IBARRA” ha sido realizada en su totalidad por: GABRIELA ESTEFANÍA MERA TERÁN portadora de la cédula de identidad número: 100348746-7.

Ing. Fabián Cuzme

Director de Tesis

DEDICATORIA

Dedico este proyecto de titulación a mis padres: Willians Mera y Sayonara Terán quienes son mi ejemplo a seguir, por todo lo que me han brindado día a día y el apoyo que incondicionalmente he recibido de ellos en todo momento de mi vida.

A mi esposo Patricio Estévez, quien me ha acompañado muchas noches en vela a terminar mis tareas, a mi hija Doménica quien es la motivación de esfuerzo y dedicación para convertirme en una buena madre y excelente profesional.

A mis hermanos Kevin y Andrea quienes han estado siempre a mi lado, son mi inspiración, mi orgullo.

A quienes han motivado con mucho amor la superación de cualquier obstáculo de mi vida y han hecho posible que logre muchos triunfos.

A toda mi familia, quienes confiaron en mí y me ayudaron cuando los he necesitado.

Gaby Mera

AGRADECIMIENTO

A Dios, quien guio mi camino en cada etapa de mi vida estudiantil, dándome fuerzas, esperanzas, salud para seguir en el camino.

A mis padres quienes, creyeron en mí y me brindaron su apoyo emocional como económico, dándome ejemplo de superación, porque hoy gracias a ellos cumplo uno de los sueños más anhelados que también es parte de su triunfo.

A mi esposo, que, con mucho amor, me ayudó a realizar mis trabajos con responsabilidad, y me dio fuerzas para culminar esta etapa de mi vida.

A mi hija, que es la inspiración, motivo y fuerza que impulsó que concluya una de las metas que me quedan por cumplir.

A mis hermanos, mis abuelitos, mis tíos quienes, con palabras de aliento, estuvieron apoyando en la realización de cada una de mis actividades universitarias.

A mi director de trabajo de grado, Ingeniero Fabián Cuzme, quien con su experiencia y conocimiento guio la realización de este proyecto.

A un gran amigo, el Ingeniero Fernando Obando, quien con sus conocimientos me ayudó a la culminación de este proyecto.

A la Universidad Técnica del Norte y la Facultad de Ingeniería en Ciencias Aplicadas, por el conocimiento que me ha brindado en el tiempo que ha durado la carrera.

Al Gobierno Autónomo Descentralizado de la ciudad de Ibarra, quienes permitieron que realice este proyecto, ayudándome con la información que se requería para la realización del mismo.

Gabriela Mera

ÍNDICE DE CONTENIDOS

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	¡Error! Marcador no definido.
DEDICATORIA	vii
AGRADECIMIENTO	viii
ÍNDICE DE CONTENIDOS	ix
ÍNDICE DE TABLAS	xiii
ÍNDICE DE FIGURAS.....	xiv
RESUMEN	xvii
ABSTRACT.....	xviii
PRESENTACIÓN.....	xix
Capítulo I	20
1. Antecedentes	20
1.1 Introducción	20
1.2 Problema	21
1.3 Objetivos.....	22
1.3.1 Objetivo General.....	22
1.3.2 Objetivos Específicos.....	22
1.4 Alcance	22
1.5 Justificación	23
Capítulo II.....	25
2 Marco teórico.....	25
2.1 Introducción	25
2.2 Protocolo de Internet versión cuatro.....	26
2.2.1 Formato de la cabecera IPv4.....	26

	x
2.2.2 Nomenclatura IPv4.	28
2.2.3 Limitaciones de IPv4.	28
2.3 Protocolo de Internet versión seis	29
2.3.1 Características de IPv6.....	30
2.3.2 Formato de cabecera IPv6.....	30
2.3.3 Nomenclatura IPv6.	32
2.3.4 Direccionamiento IPv6.	32
2.3.4.1 Reglas para escribir una dirección IPv6.	32
2.3.5 Prefijos de red.	33
2.3.5.1 Identificar los bits de red y bits de host o de interfaz.	34
2.3.6 Tipo de direcciones en IPv6.....	34
2.3.6.1 Direcciones Unicast.	35
2.3.7 Resolución de nombres con IPv6.....	37
2.3.7.1 Tipo de registro.....	37
2.3.8 Protocolos utilizados en IPv6.	37
2.3.8.1 Protocolo ICMPv6.....	37
2.3.9 Enrutamiento IPv6.	39
2.3.9.1 Enrutamiento estático.	39
2.3.9.2 Enrutamiento dinámico.....	39
2.3.10 Protocolos de enrutamiento para IPv6.	39
2.3.10.1 Enrutamiento Interno IGP.....	40
2.3.10.2 Enrutamiento externo EGP.....	42
2.3.11 Seguridad en IPv6.....	42
2.3.11.1 IPsec.....	43
2.3.11.2 Algoritmo de Resumen o Hash.....	44
2.3.11.3 Algoritmos de cifrado.....	44
2.3.11.4 Asociaciones y políticas de seguridad.	44
2.4 Comparación de IPv4 con IPv6.	48
2.5 Mecanismos de transición.....	49
2.5.1 Dual Stack (Doble Pila).	49

	xi
2.5.2 Túneles.....	50
2.5.2.1 Túneles manuales:	50
2.5.2.2 Túneles automáticos:	50
2.5.3 Traducción	53
2.6 Servidores	53
2.6.1 Tipos de Servidores.	53
Capítulo III.....	60
3. Planteamiento de Modelo De Transición y Análisis de Seguridad en IPv6	60
3.1 Plan de acción propuesto por el Ministerio de Telecomunicaciones (MINTEL)	60
3.2 Modelo De Transición de IPv4 a IPv6 para la red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra	61
3.2.1 FASE I: Planificación.	61
3.2.1.1 Selección del personal.	61
3.2.1.2 Capacitación y entrenamiento.....	61
3.2.1.3 Cronograma de actividades.....	62
3.2.2 FASE II: Diseño.....	63
3.2.2.1 Análisis de la situación actual.....	63
3.2.2.2 Análisis de Hardware o Equipamiento de la Red.	84
3.2.2.3 Análisis de Software de los Equipos.	86
3.2.2.4 Selección de los servicios y aplicaciones seleccionadas para IPv6.....	88
3.2.2.5 Pool de direcciones IPv6.	88
3.2.2.6 Análisis del protocolo de seguridad IPsec para IPv6.....	88
3.2.2.7 Elección del mecanismo más eficiente para la transición de IPv4 a IPv6 para la red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra.	90
3.2.2.8 Aspectos legales con IPv6.	93
3.3.3 FASE III: Implementación y Análisis de pruebas	94
3.3.3.1 Plan de direccionamiento IPv6.	94
3.3.3.2 Actualizaciones en Hardware y Software.....	99
3.3.3.3 Configuraciones de los equipos con IPv6.....	102
3.3.3.4 Pruebas de funcionamiento.....	103

	xii
3.3.3.5 Monitorización de la red con la implementación de IPv6.....	129
3.3.3.6 Riesgos y plan de contingencia con IPv6	135
Capítulo IV.....	137
4. Análisis Costo-Beneficio	137
4.1 Costo Social	137
4.2 Recurso Humano/Tecnológico.....	137
4.2.1 Costo de capacitación e implementación.....	138
4.3 Hardware.....	138
4.3.1 Costos de Hardware.....	139
4.4 Software	139
4.4.1 Costo de Software.....	139
4.5 Costo total del proyecto	140
4.6 Razón Beneficio Costo.....	141
CONCLUSIONES	144
RECOMENDACIONES.....	146
GLOSARIO DE TÉRMINOS.....	148
BIBLIOGRAFÍA	152
ANEXOS	156
ANEXO A: Especificaciones técnicas de switches del Cuarto de Equipos del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra	156
ANEXO B: Creación de la máquina virtual en VMWare e instalación de Centos 6.....	164
ANEXO C: Manual de Administrador para la instalación del Servidor de Correo Electrónico, servidor WEB, servidor DNS64NAT64 y configuración de doble pila	182
ANEXO D: Instalación de GNS3	210
ANEXO E: Instalación del Firewall Checkpoint en VMWare.....	229
ANEXO F: Precios de equipos	252
ANEXO G: Proforma del proyecto.....	256
ANEXO H: Publicación de la página WEB del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra en la Internet, utilizando una red con mecanismo Doble Pila o Dual Stack	257

ÍNDICE DE TABLAS

Tabla 1. <i>Tipos de direcciones en IPv6</i>	35
Tabla 2. <i>Comparación IPv4 e IPv6</i>	48
Tabla 3. <i>Distribución de los departamentos del Edificio Principal del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra.</i>	68
Tabla 4. <i>Distribución de Departamentos del Edificio Antiguo del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra.</i>	69
Tabla 5. <i>Equipamiento del Cuarto de Telecomunicaciones del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra.</i>	72
Tabla 6. <i>Descripción de las VLAN's del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra</i>	76
Tabla 7. <i>Descripción de Switches Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra</i>	79
Tabla 8. <i>Descripción de los Servidores Físicos y Virtuales</i>	80
Tabla 9. <i>Descripción de Equipos en Edificio Antiguo</i>	83
Tabla 10. <i>Descripción del Equipamiento en la casa de la Ibarreñidad</i>	84
Tabla 11: <i>Comparación de SSL e IPsec</i>	89
Tabla 12: <i>Comparación de Mecanismos de Transición</i>	91
Tabla 13. <i>Subneteo de vlans en IPv6</i>	96
Tabla 14. <i>Subredes Ipv6 con el correspondiente número de usuarios.</i>	97
Tabla 15: <i>Riesgos de Implementación de IPv6</i>	135
Tabla 16: <i>Riesgos de no implementar IPv6.</i>	135
Tabla 17. <i>Plan de contingencia</i>	136
Tabla 18: <i>Presupuesto de Capacitación e Implementación.</i>	138
Tabla 19: <i>Presupuesto de Hardware.</i>	139
Tabla 20: <i>Presupuesto de Software</i>	140
Tabla 21: <i>Presupuesto Total del proyecto</i>	140

ÍNDICE DE FIGURAS

Figura 1: <i>Formato de Cabecera IPv4</i>	27
Figura 2: <i>Formato de Cabecera IPv6</i>	31
Figura 3: <i>Representación de una dirección IPv6 en octetos</i>	32
Figura 4: <i>Longitud de prefijo para IPv6</i>	33
Figura 5: <i>Identificación de Id de interfaz</i>	34
Figura 6: <i>Dirección IPv6 compatible con IPv4</i>	36
Figura 7: <i>Formato mensaje ICMPv6</i>	38
Figura 8: <i>Funcionamiento AH</i>	45
Figura 9: <i>Funcionamiento ESP</i>	46
Figura 10: <i>Túnel 6to4</i>	51
Figura 11: <i>Túnel 6over4</i>	52
Figura 12: <i>Túnel Teredo</i>	52
Figura 13: <i>Página WEB del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra</i>	56
Figura 14: <i>Envío y recepción de emails protocolo POP</i>	57
Figura 15: <i>Funcionamiento del protocolo IMAP</i>	58
Figura 16: <i>Acceso al correo Institucional del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra</i>	59
Figura 17: <i>Transición y Coexistencia de IPv4 e IPv6 en Ecuador</i>	60
Figura 18: <i>Cronograma de actividades para el proyecto</i>	62
Figura 19: <i>Ubicación del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra</i>	64
Figura 20: <i>Simbología de la estructura del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra</i>	65
Figura 21: <i>Organigrama del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra</i>	66
Figura 22: <i>Organigrama Gestión de Tecnologías de Información</i>	67
Figura 23: <i>Topología Física de la Red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra</i>	75

Figura 24: <i>Funcionamiento Dual Stack</i>	92
Figura 25: <i>Mecanismo de Traducción</i>	93
Figura 26: <i>Acceso a configuraciones de tarjeta inalámbrica</i>	100
Figura 27: <i>Habilitación de IPv6 en Windows 7</i>	101
Figura 28. <i>Topología planteada para el entorno propuesto del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra</i>	103
Figura 29. <i>Configuración tarjeta de red con IPv4</i>	104
Figura 30. <i>Verificación dominio en IPv4</i>	105
Figura 31. <i>Configuración tarjeta de red con IPv6</i>	105
Figura 32. <i>DNS en IPv6</i>	106
Figura 33. <i>Verificación de conectividad con usuario Dual Stack</i>	106
Figura 34. <i>Página del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra con Dual Stack</i>	107
Figura 35. <i>Acceso a página Web con la dirección IPv4</i>	107
Figura 36. <i>Ejecución del servicio NAT64</i>	108
Figura 37. <i>Verificación del funcionamiento de NAT64 en Centos 6.5</i>	109
Figura 38. <i>Verificación de acceso de un cliente IPv6 a un servicio con IPv4</i>	109
Figura 39. <i>Verificación de un usuario interno al servicio WEB</i>	110
Figura 40. <i>Acceso a Outlook 2016</i>	111
Figura 41. <i>Pantalla de Inicio de Outlook</i>	111
Figura 42. <i>Agregar una cuenta en Outlook 2016</i>	112
Figura 43. <i>Configuración manual de servidores</i>	112
Figura 44. <i>Configuración de protocolos</i>	113
Figura 45. <i>Configuración de servidor de correo entrante y saliente</i>	114
Figura 46. <i>Más configuraciones de la cuenta</i>	114
Figura 47. <i>Configuración de puertos</i>	115
Figura 48. <i>Configuración del servidor como entrante y saliente con IPv6</i>	115
Figura 49. <i>Verificación de la creación de la cuenta</i>	116
Figura 50. <i>Envío de correo en IPv6</i>	116
Figura 51. <i>Verificación de recepción de correo en IPv6</i>	117

Figura 52. Verificación de un usuario interno al servicio de Correo Electrónico	117
Figura 53. Verificación de un usuario externo al servicio WEB	118
Figura 54. Verificación de funcionamiento del correo electrónico	119
Figura 55. Configuración de Interfaz fa0/0 en Ipv6	119
Figura 56. Configuración de Interfaz fa1/0 en Ipv6	120
Figura 57. Implementación de protocolo de enrutamiento OSPFv3	120
Figura 58. Configuración de Interfaces R2.....	121
Figura 59. Implementación de protocolo de enrutamiento OSPFv3 en R2	121
Figura 60. Aplicación de IKE.....	122
Figura 61. Verificación de Políticas de seguridad.....	122
Figura 62. Aplicación de IKE en R2	123
Figura 63. Configuración de clave en R1	123
Figura 64. Configuración de clave en R2	124
Figura 65. Especificación de Algoritmos de cifrado a tráfico de datos.....	124
Figura 66. Especificación de Algoritmos de cifrado a tráfico de datos en R2	125
Figura 67. Especificación modo túnel en R1	125
Figura 68. Especificación modo túnel en R2	126
Figura 69. Verificación de conectividad extremo a extremo	126
Figura 70. Verificación de conectividad extremo a extremo	127
Figura 71. Verificación de utilización de protocolo ESP	127
Figura 72. Cabecera ESP (51)	128

RESUMEN

El protocolo de internet (IP, por sus siglas en inglés) versión cuatro, permite que los dispositivos tengan acceso a la Internet. Este recurso, con el evidente avance tecnológico que se experimenta en la actualidad, se está agotando significativamente. IPv4 dispone de alrededor de cuatro mil millones de direcciones y debido al gran surgimiento de Internet, se está terminando día a día. Por esta razón, el grupo de Trabajo de Ingeniería de Internet IETF crea el nuevo protocolo IPv6, como solución a la escasez de direcciones.

El nuevo protocolo IPv6, permite direccionar alrededor de trescientos cuarenta sextillones de dispositivos, que frente a IPv4 es incomparable. El nuevo protocolo está siendo ya implementado en las redes y lo que se espera, es que coexista con IPv4 hasta que todo sea manejado con IPv6. Entonces, se necesita de un mecanismo de transición que permita manejar los dos protocolos, en tanto que IPv4 siga existiendo.

En Ecuador, el Ministerio de Telecomunicaciones y Sociedad de la información, mediante acuerdo ministerial No. 007-2012, ejecutó un plan de acciones para que se lleve a cabo una transición ordenada y coexistente de IPv4 a IPv6 con operadores, ISP (Proveedor de Internet), entidades y organismos del sector público y privado. Es por ello, que en sus plataformas electrónicas debe empezar a generarse tráfico IPv6. De acuerdo a lo establecido, surgió la propuesta para el Gobierno Autónomo Descentralizado Municipal de San Miguel de Ibarra, de empezar a utilizar este nuevo protocolo en los servicios WEB y Correo Electrónico.

El estudio de este proyecto, consiste en desarrollar un modelo de transición que permita utilizar un mecanismo para la coexistencia de los protocolos IPv4 e IPv6, basándose en las acciones que se encuentran en el acuerdo ministerial. Para ello, se va a realizar un análisis de la situación actual de la empresa, para verificar el soporte del protocolo IPv6 en cuanto a hardware, software, así como también de las aplicaciones y servicios.

Para finalizar, se realiza la configuración en equipos y servicios con un simulador de red, que permita evidenciar la coexistencia de los dos protocolos.

ABSTRACT

IP internet protocol version four (IP), allows that the devices have internet access, this resource, with the obvious technological advancement is running out significantly. IPv4 has approximately four billion addresses and because of the emergence of the Internet, it has completed day by day. For this reason, the Internet Engineering staff IETF, has created the new IPv6 protocol, as a solution to the shortage of addresses.

The new IPv6 protocol enables to route three around three hundred forty sextillions devices, that compared to IPv4 it's unbeatable. The new protocol has been already implemented in networks it is expected to coexist with IPv4 until everything is handled with IPv6. So, it is necessary a transition mechanism to handle both protocols, while IPv4 continues to exist.

In Ecuador, the Ministry of Telecommunications and Information Society, by ministerial agreement No. 007-2012, executed an action plan to be carried out with operators in an orderly and coexistent transition from IPv4 to IPv6, ISP (Internet Service Provider), public and private entities and institutions. Therefore, in their electronic platforms should be generate IPv6 traffic. According to the provisions, the proposal for Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, starts using this new protocol on the web and email services.

This project is to develop to use a transition mechanism for the coexistence of IPv4 and IPv6 protocols, based on the actions that the ministerial agreement has. To do this, it will be made an analysis of the current situation of the company, to verify the IPv6 support for hardware, software as well as, applications and services.

Finally, configuration is performed on equipment and services with a simulator of network, allowing to demonstrate the coexistence of the two protocols.



PRESENTACIÓN

El proyecto de titulación “PROPUESTA DE TRANSICIÓN DE SERVICIOS DE IPv4 A IPv6 PARA LA RED DE DATOS CABLEADA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL SAN MIGUEL DE IBARRA”, está compuesto de los siguientes capítulos:

CAPÍTULO I: Se presenta el planteamiento del problema, los objetivos (general y específicos), el alcance y la justificación del proyecto.

CAPÍTULO II: Contiene la fundamentación teórica, es decir, se detalla la información referente a los protocolos IPv4/IPv6, ventajas y desventajas, comparación de los mismos, así como también la descripción de los servicios WEB y Correo electrónico.

CAPÍTULO III: Se presenta un modelo de transición en el cual se describen los pasos a seguir para la adopción del protocolo IPv6, analizando el estado de situación actual de la empresa, verificación del soporte para IPv6 en cuanto a hardware, software, servicios, aplicaciones y de esta manera elegir el mecanismo más adecuado para lograr la coexistencia de IPv4 con IPv6. También se realiza el análisis de IPsec, el cual debe aplicarse en la red para garantizar seguridad.

CAPÍTULO IV: Se realiza un análisis costo-beneficio (social), donde se exponen las ventajas que el Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra ofrecerá a los usuarios, en caso de que esta propuesta llegue a ser implementada.

Capítulo I

1. Antecedentes

En este capítulo se detallan las debilidades del protocolo IPv4, se realiza una comparación muy general con el protocolo IPv6, de esta manera se determinan las actividades a planificar para que los dos protocolos coexistan y puedan ser implementados en la red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra.

1.1 Introducción

La internet, conocido también como la red de redes, en la actualidad, es uno de los servicios más importantes que permiten conectar a varios usuarios ubicados en cualquier parte del mundo, para acceder a la información que necesite cualquier persona, realizar pagos electrónicos, consultar valores a pagar, chatear, observar imágenes, escuchar música, descargar o subir videos entre otros.

Para acceder a la información, las redes tienen como necesidad manejar cierto tipo de reglas o protocolos para dar lugar a la comunicación, tal es el caso del protocolo TCP/IP que se describirá más adelante. Para ello se debe tomar en cuenta una dirección IP, que es un identificador que va a permitir a un dispositivo navegar en el Internet.

El protocolo IP utilizado para establecer la comunicación es IPv4, que es una dirección de 32 bits de longitud y que permite contar con 4,294,967,296 de direcciones únicas, sin embargo, este direccionamiento está siendo reemplazado por el protocolo IPv6, debido a que en él se manejan direcciones de 128 bits dando lugar a 340.282.366.920.938.463.463.374.607.431.768.211.456 direcciones válidas. En consecuencia, las redes están ya migrando al nuevo protocolo IPv6 debido al crecimiento masivo de las redes como lo es IoT (Internet de las Cosas).

1.2 Problema

Actualmente, la gran mayoría de los dispositivos en Internet utilizan direccionamiento IPv4. Sin embargo, con el aumento de la población de Internet y limitación de direcciones IPv4, se comienza a dar pie a la transición a IPv6 para que las redes no tengan límites y se desarrollen cada vez más y proporcionen a los usuarios el acceso a servicios que cada día tienen cosas nuevas que mostrar al mundo. IPv6 tiene un mayor espacio de direcciones de 128 bits, lo que permite obtener 340 sextillones direcciones IP, IPv4 ya tiene la mayoría de sus direcciones ocupadas.

Sin embargo, los protocolos IPv4 e IPv6 no son compatibles, por lo tanto, si no se tienen nodos que soporten IPv6, simplemente los paquetes van a ser rechazados, perdiendo así la información. Como se evidencia en la actualidad la mayoría de Proveedores de Internet (por sus siglas en inglés ISP: Internet Service Provider) están ya implementando este protocolo lo que hace necesario que las empresas empiecen a buscar un mecanismo que permita la adopción de IPv6, sin que afecte a la información que maneja el protocolo IPv4.

En las próximas generaciones, las redes de datos, especialmente las inalámbricas que se crean a partir de las redes cableadas, al no contar con el manejo de IPv6, perderán la implementación de nuevas tecnologías y la conectividad con redes que utilizan el protocolo IPv6, por tanto una entidad importante como es el Gobierno Autónomo Descentralizado Municipal de San Miguel de Ibarra que no cuenta con proyecciones ni estudios que permitan implementar este protocolo, debe realizar un análisis que admita en un futuro la implementación de este nuevo protocolo para prestar sus servicios a cualquier usuario.

El protocolo IPv4 tiene varias falencias, entre ellas se puede decir que su encabezado de datagrama es el doble que el de IPv6, lo que implica que los equipos tengan mayor procesamiento de información, IPv4 tiene de forma opcional IPSec, protocolo que brinda mayor seguridad a las comunicaciones, mientras que en IPv6 se lo utiliza de forma obligatoria. IPv4 no es un protocolo escalable ya que utiliza para poder satisfacer la demanda de direcciones el protocolo NAT (traducción de direcciones de red) que debe redirigir el flujo de datos de la red interna a la externa.

1.3 Objetivos

1.3.1 Objetivo General.

Proponer la transición de servicios IPv4 a IPv6 de la red cableada en el Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra mediante la aplicación de un modelo de transición aplicando el mecanismo idóneo para permitir la coexistencia de los dos protocolos antes mencionados.

1.3.2 Objetivos Específicos.

- Realizar un estudio del fundamento teórico mediante la investigación bibliográfica y documental que permita sustentar cada uno de los parámetros que se establezcan para la transición y convivencia entre IPv4 e IPv6.
- Analizar la estructura actual de la red física y de datos que tiene implementada el Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra para el correspondiente estudio de plan de transición, de los servicios WEB y Correo electrónico que brinda a los usuarios internos y externos.
- Plantear y diseñar un modelo de transición que permita la coexistencia de los protocolos IPv4 e IPv6 en la red de datos del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, garantizando además que permita aplicar niveles de seguridad utilizando el protocolo IPsec.
- Realizar un análisis costo-beneficio (social) para la implementación del modelo de transición IPv4 a IPv6 con la finalidad de identificar los beneficios que se van a generar para todos los usuarios.

1.4 Alcance

Este proyecto tiene como finalidad presentar un modelo de transición que posibilite la coexistencia de los protocolos IPv4 e IPv6 respectivamente, es decir que usuarios, aplicaciones y servicios puedan manejarse con ambos protocolos en la red del Gobierno Autónomo

Descentralizado Municipal San Miguel de Ibarra eligiendo un mecanismo que se ajuste a las características de la red.

En el Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, se debe analizar la infraestructura de red física como lógica de datos para así determinar la situación actual de acuerdo al recurso que disponen. De la misma manera, es importante el estudio en cuanto a software y hardware para verificar si se tiene el soporte para IPv6, y cuáles serían las acciones a tomar en cuenta en caso de no cumplir con este requisito.

Para el desarrollo de este proyecto, se va a utilizar software libre que va a permitir simular los servicios WEB y Correo Electrónico, así como también el servidor DNS64-NAT64. La configuración de los equipos se va a realizar utilizando un simulador de red. También se va a aprovechar la implementación del protocolo IPsec, ya que en IPv6 su uso debería ser aplicado para implementar seguridad a la red.

Para finalizar, se realizará un análisis en cuanto al costo de una posible implementación de este proyecto, determinando así que se obtengan beneficios para los usuarios que acceden a los recursos de la red en cuanto a los servicios descritos anteriormente.

1.5 Justificación

El protocolo IPv6, será el que las redes manejen en un futuro, por esta razón es que todas ellas deberán migrar por completo en los siguientes años, para mejorar e incrementar los servicios que brinden a los usuarios. El protocolo IPv4 va a ir desapareciendo, y las instituciones públicas como privadas deberán implementar como protocolo nativo IPv6.

En Ecuador, mediante acuerdo ministerial N^o 007-2012 del 18 de enero del 2012, el Ministro de Telecomunicaciones y de la Sociedad de la Información, el Ing. Jaime Guerrero Ruiz, estableció el requerimiento de que las entidades del sector público manejen el protocolo IPv6 en sus sitios WEB y plataformas de servicios electrónicos, de manera coexistente con el actual protocolo IPv4, con la finalidad de que se genere tráfico IPv6 a nivel nacional, permitiendo que los recursos

públicos sigan siendo visibles a nivel mundial. (Ministerio de Telecomunicaciones y Sociedad de la Información, 2012)

Con IPv6, se puede aplicar calidad de servicio (QoS), que permite dar prioridad a los paquetes que se deseen o tengan mayor prioridad como son datos multimedia o de voz. También implementar el protocolo IPSEC, que en IPv4 es opcional, mientras que en IPv6 su uso es obligatorio permitiendo aplicar seguridad extremo a extremo y eliminando la utilización de NAT. (Ministerio de Industria, energía y turismo de España, 2013)

El estudio del protocolo de nueva generación permitirá que se desarrollen tecnologías nuevas como domótica, IoT, movilidad IP, entre otras. Es importante destacar que el desarrollo de este proyecto aportará para que las demás empresas públicas empiecen a desarrollar modelos o metodologías de transición para que las redes empiecen a implementar IPv6 y de la misma manera estarán cumpliendo con los requerimientos que dispone el MINTEL.

De igual manera, los estudiantes de la carrera de Ingeniería en Electrónica y Redes de Comunicación, podrán utilizar el análisis que se realizará en este proyecto para futuros estudios o implementaciones en temas similares, con lo que podrán aplicar y mejorar las actividades que se realicen con respecto a la propuesta para el Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra.

Capítulo II

2 Marco teórico

Este capítulo contiene la descripción de cada uno de los protocolos IPv4 e IPv6, en la que se analizan las ventajas del protocolo versión seis, de la misma manera realizando un análisis comparativo en el que se especifica porque se debe implementar el protocolo de nueva generación en las redes actuales.

2.1 Introducción

La Internet es una herramienta de emisión mundial, un mecanismo para compartir información de cualquier tipo y un medio para la colaboración y la interacción entre personas y sus ordenadores, sin tener en cuenta su ubicación geográfica. Esto ha sido posible debido al gran crecimiento de las redes que hacen posible que la comunicación se pueda realizar, de la misma manera se puede considerar como la creación más exitosa que ha evolucionado en los últimos años y con ello es posible cualquier cosa. (Internet Society, 2016)

En la actualidad, para que las comunicaciones se puedan realizar, se han creado ciertos protocolos, que son el conjunto de reglas que permiten compartir información. Internet maneja IP (Internet Protocol, por sus siglas en inglés) que es parte de la capa de red de la pila TCP/IP. Por tanto, se va a proceder a explicar el protocolo IP que va a ser la base para la comprensión de este tema.

El protocolo de Internet (IP), pertenece a la capa de red del modelo OSI, y es un protocolo que realiza su máximo esfuerzo para la entrega de la información, es decir no garantiza la entrega de paquetes al destino, lo que lo define como no confiable ni orientado a la conexión. De la misma manera si un paquete se daña o pierde en el camino no se podrán recuperar.

Gracias a este protocolo se pueden interconectar las redes, lo que quiere decir que se caracteriza por proporcionar un esquema de red que permite el envío de información de un origen a un destino sin preocuparse si él se encuentra en la misma o diferente red. La unidad de información que se utiliza para la comunicación a este nivel es el datagrama. Para que la comunicación se pueda

establecer se debe contar con una IP que se va a encontrar tanto en el origen como el destino. (MacDonald, 2008)

El protocolo IP que se ha utilizado desde hace mucho tiempo y la primera versión ha sido el IPv4, pero actualmente algunas empresas ya manejan el protocolo IPv6, debido al gran crecimiento de las redes que existe en la actualidad y seguramente en un futuro sean mucho más extensas. Cada dispositivo final, usuario, computador que quiera acceder a la red debe contar con una dirección IP única, ya sea IPv4 o IPv6. (Cicileo, 2009)

2.2 Protocolo de Internet versión cuatro

Porque hablar directamente de IPv4 y no desde IPv1, pues las versiones IPv1, IPv2 e Ipv3 fueron extensiones del protocolo TCP, que se usaron hasta 1979. Pero entonces se logró estandarizar el protocolo IPv4 que se le considera independientemente de cualquier otro protocolo y se define en el RFC 791, publicado en 1981, el cual ha sido utilizado actualmente. (Lujan, 2015)

2.2.1 Formato de la cabecera IPv4. La cabecera IP contiene las instrucciones para manipulación y entrega de un paquete IP. Por ejemplo, cuando un paquete llega a la interfaz de un router, éste necesita saber si ese paquete es de tipo IPv4 o IPv6. Para eso, se examina un campo específico de la cabecera. Esta cabecera contiene también información de direccionamiento y otros datos de cómo manipular el paquete a lo largo de su trayectoria. (MacDonald, 2008)

A continuación, se va a observar la Figura 1, que indica la cabecera de un paquete IP. Existen diversos campos en la misma, y cada red utiliza los que más le interesa. Hay campos destacados que son importantes para comprender y la forma en cómo ayuda al router la cabecera IP para dirigir con éxito los paquetes.

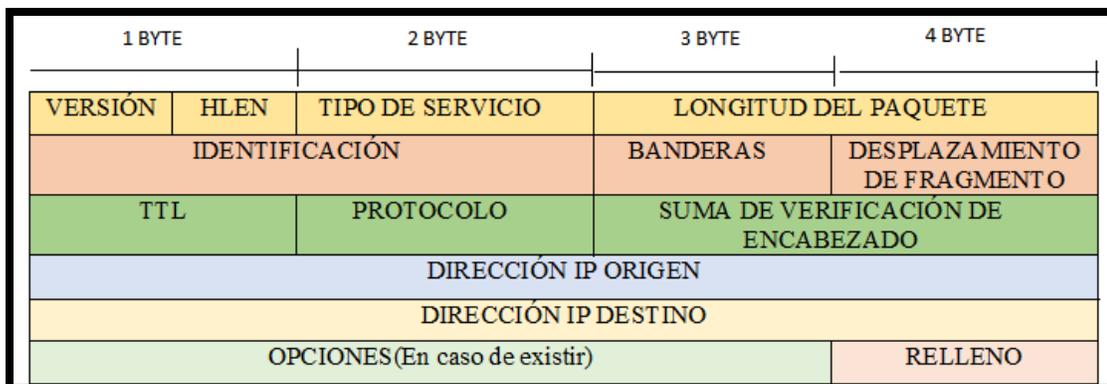


Figura 1: *Formato de Cabecera IPv4*

Fuente: (MacDonald, 2008)

Los campos más importantes para un análisis son:

- **Versión:** Indica si es la versión IPv4 o IPv6.
- **HLEN:** Indica al Router cuan larga es la cabecera.
- **Tipo de Servicio (ToS):** Los 8 bits de este campo pueden describir el nivel de prioridad de rendimiento que el router debe usar a la hora de procesar el paquete.
- **Longitud del paquete:** longitud total del datagrama, y la mínima es 20 bytes (cabecera sin datos) y la máxima es de 65.535 bytes.
- **Identificación:** Es el que se envía por el remitente para re ensamblar los fragmentos.
- **Dirección IP Origen:** Representa un host que envía el paquete y tiene una longitud de 32 bits.
- **Dirección IP Destino:** Representa al host que recibirá el paquete y de 32 bits de longitud. Este es el dato que utilizará el router para enviar el dato a la red correcta.
- **TTL (Tiempo de vida, Time to Live).** Utiliza 8 bits y comprende el número máximo de saltos que el paquete puede dar antes de ser considerado como 'perdido' o 'no entregable'.
- **Banderas y desplazamiento de fragmento:** Cuando el paquete es demasiado grande, en ocasiones el router debe fragmentar el paquete para poder enviarlo de un medio a otro con una MTU más pequeña. Entonces el paquete IPv4 usa el desplazamiento de fragmento y la bandera para poder reconstruir el dato cuando llegue al destino.
- **Protocolo:** Campo de 8 bits que indica el protocolo de capa superior (ICMP, UDP, TCP), que es la capa transporte que recibirá el paquete lo va a des encapsular.

- **Suma de Verificación de Encabezado:** Empleado para indicar la longitud de la cabecera y es comprobado por cada router a lo largo del camino. Cada router ejecuta un algoritmo y, en caso de que la suma de comprobación sea incorrecta, se asume que el paquete está corrompido y se descarta.
- **Opciones:** Utilizado para ofrecer servicios especiales de enrutamiento.
- **Relleno.** Se utiliza para completar con bits cuando los datos de la cabecera no terminan en un límite de 32 bits.

2.2.2 Nomenclatura IPv4. IPv4 utiliza un tamaño de 32 bits, utilizando unos y ceros, en otras palabras, contiene cuatro bytes, cada uno de ellos compuestos de ocho bits, separados por un punto “.”. Permite obtener $2^{32} = 4,294,967,296$ millones de direcciones válidas, pero con el incremento de redes que se ha dado en los últimos tiempos, éstas llegan a ser insuficientes. Se pueden escribir en dos formatos:

En forma binaria: 11000000.10101000.00000010.00000001

En forma decimal: 192.168.2.1

2.2.3 Limitaciones de IPv4. El protocolo IPv4 se ha mantenido desde la recomendación RFC 791, pese a ello, la gran demanda que ha surgido para las redes actuales no se anticiparon en el diseño de IPv4 por lo tanto se tienen las siguientes debilidades:

- **Agotamiento de direcciones IP:** Aunque se manejen 4.294.967.296 millones de direcciones, no es suficiente para la creciente demanda de redes que existen hoy en día. Por esta razón se ha utilizado NAT, para asignar una dirección pública a varias privadas, es un buen método para poder reutilizar las direcciones privadas, pero entonces va a conllevar a que en las comunicaciones se produzcan cuellos de botella.
- **Soporte para la entrega de datos en tiempo real:** Aplicaciones nuevas como video y audio, requieren QoS, por ello, se necesita una arquitectura flexible que permita afrontar el reto que supone la movilidad de sus usuarios.
- **Requerimientos de Seguridad a nivel IP:** Se utiliza para garantizar entrega de paquetes, y la norma es IPsec. En Ipv4 este campo es opcional, mientras que en IPv6 es obligatoria.

- **Expansión en la tabla de enrutamiento de Internet:** Con el aumento de nodos o servidores que están conectados a Internet, aumentan las rutas de red por lo que los routers deben manejar tablas de enrutamiento con mayor información y esto produce un aumento de recursos de la red en cuanto a memoria y procesamiento.

2.3 Protocolo de Internet versión seis

Se lo conoce también como el protocolo Next Generation o de nueva generación (IPng) y fue creado por la IETF (Internet Engineering Task Force) y se presentó en el año de 1994. En el RFC 1752 se especifican los requisitos de IPv6, especificando el formato de la PDU y señalando las técnicas de IPng en las áreas de direccionamiento, encaminamiento y seguridad. Más detalles específicos referentes a IPv6, se incluyen en el RFC 2460. (Tanenbaum, 2011)

El protocolo IPv4, dispone sólo de 32 bits de direcciones proporcionando un espacio teórico de 2^{32} (aproximadamente cuatro mil millones) interfaces de red únicas globalmente. IPv6 en cambio, tiene un espacio de direcciones de 128 bits y por tanto puede direccionar 2^{128} interfaces de red (340.282.366.920.938.463.463.374.607.431.768.211.456), esto quiere decir que IPv6 abastecerá gran cantidad de usuarios en los próximos años. (LACNIC, 2012)

Actualmente, IPv6 continúa añadiendo nueva funcionalidad para fortalecer su protocolo y ya se lo considera lo suficientemente apto para que soporte la operación de Internet en sustitución con IPv4. Esto gracias a la expansión de direcciones que se ha realizado al protocolo IPv4, siendo así, permite la interconexión de muchos dispositivos (tabletas, teléfonos móviles, y televisiones inteligentes), entre otros.

IPv4 dejará de utilizarse en cualquier momento debido a que el Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC), que es responsable de la asignación de recursos para esta región, anunció el agotamiento del stock de direcciones IPv4 y expresó su preocupación por la demora de operadores y gobiernos en desplegar el protocolo de Internet (IPv6) en la región. (LACNIC, 2012)

Por esta razón al momento de iniciarse con planes de transición o de migración de redes IPv4 a redes IPv6 representará quizás el cambio más importante en la historia del Internet ya que es necesario para que la red de redes pueda seguir desarrollándose de una forma segura y estable.

2.3.1 Características de IPv6. Las características primordiales son las siguientes:

- **Mayor espacio para direccionamiento de redes:** El protocolo IPv6 tiene una longitud de 128 bits para direcciones tanto de origen como de destino, en otras palabras 2^{128} posibles direcciones, a diferencia de Ipv4 que tiene 2^{32} direcciones.
- **Direccionamiento más eficiente y jerárquico:** Permite que los routers principales dirijan el tráfico de manera más rápida e incluso que sus tablas de enrutamiento sean mucho más pequeñas.
- **Nuevo formato de cabecera:** Se desarrolló para que los routers realicen un consumo menor de procesamiento al manejar la información.
- **Configuración de direcciones:** Con IPv6 se puede simplificar la configuración en los hosts, permite el uso de un servidor DHCP para las direcciones con estado, y de igual manera se admite también las direcciones sin estado que son las que no utilizan un servidor DHCP.
- **QoS:** Esto permite darle cierto tipo de prioridad a un tráfico de datos, mediante un campo en la cabecera de IPv6 (Class Traffic), permitiendo que los routers proporcionen tratamiento especial a un flujo determinado de paquetes.
- **Seguridad:** en IPv6 es obligatorio el campo IPSEC, que permite seguridad de encriptación a la carga útil y autenticación de la fuente de comunicación.
- **Interacción con nodos vecino:** Utilizando el protocolo Neighbor Discovery que Ipv6 dispone es capaz de manejar una serie de mensajes que va a permitir la interacción con los nodos vecinos.

2.3.2 Formato de cabecera IPv6. La cabecera IPv6 con relación a IPv4, tiene campos que se han simplificado, de tal forma que se puede reducir la redundancia que IPv4 incluye. De igual forma algunos campos son modificados, tal es el caso del campo desplazamiento de

fragmentación, ya que en IPv6 los encaminadores no fragmentan los paquetes, ya que esta fragmentación/desfragmentación se la realiza de extremo a extremo. (6SOS, 2004)

A continuación, en la Figura 2, se puede ver que IPv6 cuenta con ocho de los doce campos que IPv4 tiene, y de igual forma se procede a explicar cada uno de ellos:



Figura 2: *Formato de Cabecera IPv6*

Fuente: Recuperado de: http://www.6sos.org/documentos/6SOS_El_Protocolo_IPv6_v4_0.pdf

Campos renombrados:

- **Versión:** Simplemente cambia de IPv4 a IPv6.
- **Longitud del paquete:** longitud de carga útil, que es la longitud de los propios datos y puede ser de hasta 65536 bytes, con un tamaño de 2 bytes.
- **Protocolo:** siguiente cabecera, en lugar de utilizar cabeceras de longitud variable, se emplean cabeceras encadenadas, por lo que desaparece el campo opciones, utilizada mayoritariamente de extremo a extremo con 1 byte de longitud.
- **TTL:** Límite de saltos y tiene un byte de longitud.
- **Dirección de origen y dirección de destino:** amplían su tamaño de 32 a 128 bits.

Los nuevos campos son:

- **Clase de tráfico:** Indica prioridad a un paquete y es equivalente a ToS en IPv4 y con longitud de un byte.
- **Etiqueta de Flujo:** permite tráfico en tiempo real y tiene 20 bits de longitud.

En resumen, estos dos campos van a permitir que un paquete sea tratado con prioridades distintas a los demás y lo que caracteriza a IPv6.

2.3.3 Nomenclatura IPv6. El sistema Hexadecimal está en base **16**, sus números están representados por los 10 primeros dígitos de la numeración decimal, y el intervalo que va del número 10 al 15 están representados por las letras del alfabeto de la A hasta la F. IPv6 utiliza este sistema en su direccionamiento, para lo cual es necesario saber cómo se compone una dirección en este formato. (INSAT, s.f.)

2.3.4 Direccionamiento IPv6. IPv6 extiende su dirección de 32 a 128 bits, que por el momento es suficiente para cubrir la gran demanda de usuarios en el futuro. Cuatro bits, representan un dígito hexadecimal, por lo tanto, una dirección IPv6 consta de 32 valores hexadecimales. A continuación, se va a presentar un ejemplo para ayudar a la comprensión del mismo en la Figura 3: (CISCO, 2013)

Dirección IPv6: **2001:0DB8:0GGG:1111:0000:0000:0000:0001 /64**

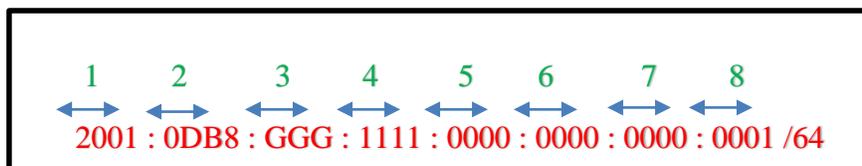


Figura 3: *Representación de una dirección IPv6 en octetos*

Fuente: Elaboración propia

2.3.4.1 Reglas para escribir una dirección IPv6. Se van a describir dos reglas importantes para representar una dirección en IPv6:

- **Utilización de mayúsculas o minúsculas**

No hay problema si una dirección es escrita en mayúsculas o minúsculas. Por ejemplo, es lo mismo decir “AB01” que “ab01”

- **Ceros Iniciales**

✓ Los ceros iniciales en cada segmento de 16 bits no se deben escribir. Por ejemplo:

3fdd : 0404 : 0001 : 1000 : 0034 : 0000 : 0ef0 : bc00

Como se puede escribir: 3fdd:404:1:34:0:ef0:bc00

✓ Optimizar los ceros en cada segmento. Por ejemplo:

2008:db8:0000:0000:0000:0000:0000

Como se puede escribir: 2008:db8:0:0:0:0:0

- **Dobles dos puntos**

Esta regla reduce mucho más una dirección IPv6.

✓ Es posible la reducción de ceros contiguos, una sola vez, es cualquier segmento de 16 bits por dobles dos puntos así:

AA02 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0300

AA02 : 0000 : 0000 : 0000 : 0000 : 0000 : 0300

Como se puede escribir: AA02::0300

✓ Se debe aplicar la regla una sola vez para evitar ambigüedades.

2008 : 0d52 : 0000 : 0000 : 0011 : 0000 : 0000 : 00B5

Como se puede escribir: 2008:d52::11:0000:0000:B5 o también

2008:d52:0000:0000:11::B5

2.3.5 Prefijos de red. En IPv4, el prefijo o la parte de red de la dirección, se puede identificar por la máscara decimal o por la cuenta de bits 255.255.255.0 o /24. Con el direccionamiento IPv6 se obtiene siempre de la cuenta de bits (longitud del prefijo). En la Figura 4 se indica la longitud del prefijo

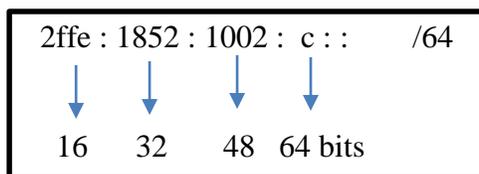


Figura 4: Longitud de prefijo para IPv6

Fuente: Elaboración propia

En la Tabla 1, se puede observar cada tipo de dirección Ipv6 y sus correspondientes subdivisiones:

Tabla 1. *Tipos de direcciones en IPv6*

Tipo de dirección IPv6	Subdivisión
Unicast	Link local (Enlace local)
	Site local (Sitio local)
	Loopback
	Sin especificar
	Agregable global
	Compatible con IPv4
Anycast	Link local (Enlace local)
	Site local (Sitio local)
	Agregable global
Multicast	Nodo Solitario
	Asignada

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

2.3.6.1 Direcciones Unicast.

- **Enlace local:** Utilizadas en enlaces sencillos y no deben ser enrutadas. Útil en redes temporales y empiezan por “FE80:”, sirven para el ID de interfaces de un mismo enlace.
- **Sitio Local:** Utilizadas para identificar interfaces en la misma área de red, es decir, del mismo sitio como puede ser el campus universitario. Estas direcciones empiezan por “FEC0:”
- **Agregable Global:** Direcciones utilizadas para el tráfico genérico en el Internet de IPv6 y son similares a las direcciones unicast usadas para comunicarse a través del Internet de con el protocolo IPv4. Se caracterizan por permitir limitar el tamaño de la tabla de enrutamiento global de Internet.

Este tipo de direcciones consta de tres partes:

- ✓ **Prefijo recibido del proveedor:** el prefijo asignado a una organización por un proveedor debe ser al menos de 48 bits.
- ✓ **Sitio:** con el prefijo recibido del proveedor, existe la posibilidad de tener 65,535 subredes. La organización puede usar los bits 49 a 64 (16 bits) del prefijo recibido para subredes.
- ✓ **Computadora:** representa los 64 bits de más bajo orden de la dirección, es llamada Identificador de Interface. (Network Information Center México S.C., 2010)
- **Loopback:** En IPv4, cada dispositivo tiene una dirección loopback, que es usada por el nodo mismo. De la misma manera en Ipv6 y se representa por ::1.
- **Sin-Especificar:** Indica la ausencia de una dirección y es usada para propósitos especiales. Es representada por :: .
- **Compatible con IPv4:** Es utilizada por los mecanismos de transición en computadoras y ruteadores para crear automáticamente túneles IPv4. De esa forma se entregan paquetes IPv6 sobre redes IPv4. (Network Information Center México S.C., 2010)

En la Figura 6 se va a indicar una dirección IPv6 compatible con una IPv4. Se puede observar que el prefijo se crea con el bit puesto a cero del de más alto nivel de los 96 bits, los bits restantes (32) de menor nivel, representan una dirección IPv4.

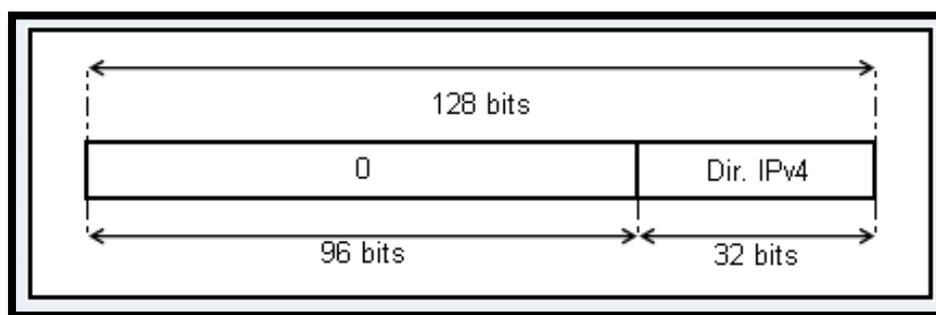


Figura 6: Dirección IPv6 compatible con IPv4

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

Se van a tener en cuenta únicamente las direcciones Unicast Global, por lo que se va a trabajar sobre ellas en el respectivo análisis del protocolo IPv6.

2.3.7 Resolución de nombres con IPv6. El DNS, conocido como sistema de nombre de dominios, no puede ser extendido para dar un eficiente soporte a IPv6 porque al realizar una petición por parte de una aplicación únicamente va a retornar una dirección de 32 bits. Para que puedan dar soporte a IPv6 se debe realizar lo siguiente (Carlos, s.f.):

- Un nuevo tipo de registro que permita relacionar el nombre de un dominio con una dirección IPv6.
- Un nuevo dominio que permita que una dirección IPv6 pueda brindar el soporte adecuado para las correspondientes búsquedas que se necesite.

Con la creación de un nuevo tipo de registro se va a permitir que un host, pueda almacenar su dirección IPv6. Sin embargo, existen casos en que un host va a tener más de una dirección IPv6 por lo cual deberá tener más de un registro parecido.

2.3.7.1 Tipo de registro. El protocolo IPv4 utiliza el registro A, mientras que IPv6 va a utilizar el AAAA, que tiene como función almacenar una sola dirección. El proceso de resolución inversa del nombre de dominio IPv6 utiliza el PTR que también se lo utiliza en IPv4. Una dirección IPv6 está representada por una secuencia de nibbles, separados por un punto y con el sufijo “.IP6.INT”. Esta secuencia se codifica en inverso, es decir, primero se codifica el de menor orden hasta continuar con el más alto. (CISCO, 2013)

2.3.8 Protocolos utilizados en IPv6.

2.3.8.1 Protocolo ICMPv6. En IPv4 se utiliza el protocolo ICMP, y tiene como función informar si se tuvo algún error durante el procesamiento de la información y realizar pruebas respectivas en la capa de Internet como es el famoso “Ping”. Estos mensajes pueden ser de dos tipos:

1. Mensajes de error: En el campo “tipo de mensaje”, se encuentra el 0 y se define de 0 a 127 valores.
2. Mensajes informativos: Valores desde los 128 hasta los 255. (Deering, 2011)

En la Figura 7, se indica el formato de mensaje ICMPv6

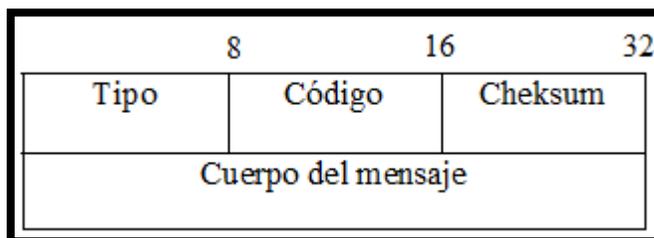


Figura 7: *Formato mensaje ICMPv6*

Fuente: Recuperado de <http://es.slideshare.net/DavidMarzaHerrera/i-pv6-9310591>

- **Descubrimiento de Vecinos (Neighbor Discovery):** Conocido también como ND, puede ser utilizado por un nodo, un router o un host y sus funciones son las siguientes:

En un nodo:

- ✓ Resuelve la dirección IPv6 de un nodo vecino.
- ✓ Determina si se puede enviar o recibir paquetes IPv6 de un vecino.
- ✓ En el Router:
 - ✓ Permite notificar de su presencia mediante una configuración realizada en el host.
 - ✓ Notifica a cualquier host, sobre la mejor dirección del siguiente salto.
- ✓ En el host:
 - ✓ Descubre enrutadores vecinos.
 - ✓ Descubrir vecinos y parámetros de configuración. (Alonso, 2001)
- **MLD o descubrimiento de una escucha multidifusión:** Se basa en enviar una serie de mensajes ICMPv6 a un solo destinatario, sin embargo, el procesamiento se realiza en múltiples hosts. Tiene las siguientes características:
 - ✓ Cuando un conjunto de hosts atiende a una dirección multidifusión, se lo conoce como grupo multidifusión.
 - ✓ Si un host quiere juntarse a un grupo multidifusión, debe enviar un mensaje.
 - ✓ Los grupos multidifusión son dinámicos.
 - ✓ Un host, puede enviar tráfico a diferentes direcciones de grupo. (Microsoft, 2005)

2.3.9 Enrutamiento IPv6. Este proceso permite mantener las tablas de enrutamiento actualizadas, ya sea manualmente o dinámicamente, procedimiento que se realiza también en IPv4. Para enviar un paquete se necesita un enrutador IPv6, los enrutadores verifican la dirección destino del paquete IPv6 y buscan el prefijo que le corresponde dentro de sus tablas de enrutamiento. Cuando ya se haya encontrado este prefijo que se dirige al destino, entonces el paquete se reenvía de acuerdo a la información del siguiente salto. (Universidad de San Carlos de Guatemala, 2009)

2.3.9.1 Enrutamiento estático. Se basa en las tablas de enrutamiento que son manualmente configuradas y no cambian con un posible reajuste en la topología de red. Un router que haya configurado manualmente su tabla de enrutamiento es llamado un router estático. Un router estático funciona muy bien en redes pequeñas, pero no recomendable en redes demasiado grandes o que estén en constante cambio, ya que su administración debe realizarse manualmente.

2.3.9.2 Enrutamiento dinámico. Las tablas de enrutamiento se van a actualizar automáticamente para los cambios que se den en la topología de la red y un router que realice estas actividades es conocido como router dinámico. Esto se realiza con la permanente comunicación entre los routers y se facilita con la implementación de un protocolo de enrutamiento que envían mensajes periódicos con información que se intercambia entre ellos. Los routers dinámicos requieren poco mantenimiento y son excelentes para funcionar en redes de gran escala.

2.3.10 Protocolos de enrutamiento para IPv6. Es utilizado para facilitar el intercambio de información con respecto a rutas entre routers. Poseen un elemento importante para detectar y recuperarse de fallas en la red, esta información se propaga a través de toda la red. Cuando los routers mantengan la información de todos los demás con la correcta información de cada una de las tablas de enrutamiento, se puede decir que la red es convergente y cuando ya se logra la convergencia de la red, se puede decir que está en un estado estable.

Por ello, toman relevancia el AS (Autonomous System) o sistema autónomo, que es un conjunto de redes que están bajo una misma administración, que cuenta con sus propias reglas y políticas, y comparten una estrategia de enrutamiento común hacia el exterior, esto significa que

todos los routers dentro del mismo AS comparten la misma tabla de enrutamiento. Estos AS son asignados por la ARIN (es el Registro Regional de Internet para América). (Universidad de San Carlos de Guatemala, 2009)

2.3.10.1 Enrutamiento Interno IGP. Los protocolos de enrutamiento que se pueden utilizar para IPv6 son:

- ✓ RIPng para IPv6
- ✓ OSPFv3
- ✓ EIGRP para IPv6

- **RIPng para IPv6**

Tiene una estructura simple de paquetes y usa el puerto UDP 521 para anunciar constantemente sus rutas y asincrónicamente sus cambios de ruta. Es un protocolo de vector distancia, adaptación del protocolo RIPv2. El número máximo de saltos es 15 para alcanzar el destino y con una distancia de 16 saltos el destino es inalcanzable. Usualmente se lo utiliza en redes pequeñas. (TRIPOD, 2016)

Cuando está configurado este protocolo, anuncia todas las rutas en su tabla de enrutamiento en todas las interfaces, el router también envía un mensaje de solicitud general a todas las interfaces y todos los routers vecinos envían el contenido de sus tablas de enrutamiento en respuesta al mensaje y esas respuestas son las que forman la tabla inicial de enrutamiento. Estas rutas aprendidas tienen un tiempo de vida de tres minutos antes de que se eliminen de la tabla de enrutamiento.

Después de la inicialización de RIPng, se anuncia periódicamente cada 30 segundos las rutas en su tabla a través de cada interfaz. De la misma forma, si ocurre un cambio en la red de los routers IPv6 con RIPng se pueden enviar las actualizaciones instantáneas en lugar de esperar un anuncio previo. Cada red tendrá un prefijo de su dirección IPv6 en el destino asociado a la métrica los cuales son establecidos por el administrador del sistema de forma específica.

- **OSPFv3**

Está diseñado para trabajar en sistemas autónomos, OSPF para IPv6 es una adaptación del protocolo OSPF para IPv4. Para cada enlace, el costo es único y es asignado por el administrador de la red y puede incluir factores como retraso, ancho de banda y costo monetario. El protocolo de estado de enlace para IPv6 presenta los siguientes cambios en relación a la versión 2:

- ✓ Nuevas LSAs son definidas para los prefijos y direcciones en IPv6.
- ✓ La estructura de los paquetes ha sido modificada para poder eliminar dependencias con el protocolo IPv4.
- ✓ Se ejecuta en cada enlace en lugar de ejecutarse en cada subred.
- ✓ Ya no proporciona autenticación, ya que OSPF se basa en la cabecera y el tráiler del mensaje para realizar tareas de autenticación. (CISCO Systems, 2010)

Este protocolo usa el término “link” indicado la facilidad de comunicación o el medio donde los nodos se comunican a la capa enlace; varias subredes IPv6 se pueden asignar a un solo enlace, a su vez dos nodos pueden interactuar sobre un único enlace así no compartan la misma subred IPv6. OSPF delimita la cantidad de routers y enlaces que pueden existir en una red debido a que requiere procesamiento y ancho de banda, para que esto no sea un problema el protocolo permite dividir la red en áreas, pero si la red es pequeña puede definirse en una sola área sin restricciones en la topología.

- **EIGRP para IPv6**

EIGRP es de propiedad de Cisco Systems, a diferencia de IPv4 en IPv6 se agrega un protocolo de capa 3 para poder utilizarlo y que soporte dicho protocolo. Las principales características de EIGRP para IPv6 son: (CISCO Academy Network, 2009)

- ✓ Establecimiento de adyacencias
- ✓ Tablas de topología y de vecinos
- ✓ Ancho de banda definido en 1544 Kbps

- ✓ Distancia administrativa interna 90 y 170 externa
- ✓ Uso de algoritmo DUAL
- ✓ Actualizaciones parciales generadas por eventos.

2.3.10.2 Enrutamiento externo EGP. Se encarga de proveer el enrutamiento entre sistemas autónomos, se puede decir que es el tipo de protocolos que utiliza un ISP (Internet Service Provider), y de igual forma se lo implementa en los routers principales que componen el Internet. Para ello, se necesita un conjunto de información antes de comenzar su funcionamiento, una lista de los routers vecinos, una lista de las redes que van a ser publicadas como accesos directos y un número de sistema autónomo del router local.

- **BGP**

Un protocolo de enrutamiento externo es BGP (Border Gateway Protocol), que se caracteriza por la robustez que se utiliza entre sistemas autónomos, es esta razón por la que se convirtió en el protocolo más utilizado en Internet. Para lograr escalabilidad a este nivel, BGP utiliza varios parámetros denominados atributos, con la finalidad de definir las políticas de enrutamiento y mantener un ambiente estable de enrutamiento. (Moya, 2009)

Incluso para poder reducir el tamaño de las tablas de enrutamiento, BGP hace uso de CIDR (Classless Interdomain Routing). En las actualizaciones de las tablas de enrutamiento que se realizan entre vecinos, primero se debe de establecer una conexión TCP entre dichos vecinos y así únicamente cuando se produce un cambio en alguna ruta, estos cambios son anunciados a los vecinos.

2.3.11 Seguridad en IPv6. La IETF, consideró que IPsec fuera obligatoriamente configurado con el protocolo IPv6, también es usado en IPv4, siendo opcional. Este tipo de seguridad que IPv6 aplica es únicamente en la capa IP, o capa de red y no es una arquitectura. Uno de los beneficios de aplicar seguridad en IPv6 es que ahora se debe intentar entre 2^{64} posibilidades en una subred

para poder atacarla, resultando mucho más complicada. (Ministerio de Industria, energía y turismo de España, 2013)

Debido a la gran disponibilidad de direcciones IPv6 que permite asignar direcciones IP únicas en todo el mundo a varios dispositivos, de esta manera, elimina el direccionamiento privado y también el NAT de traducción de direcciones de red. Es así que se considera importante el análisis e implementación del protocolo IPsec, que proporciona seguridad a las redes actuales que utilizan el protocolo IPv6. (Amelines, 2012)

2.3.11.1 IPsec. Es un estándar que proporciona seguridad de la información, caracterizado por ser potente y flexible. Se ha creado debido a las falencias que tiene el protocolo IP que es la seguridad, esto permite que las redes actuales accedan a aplicaciones críticas como es la de manejar información que involucre transacciones empresariales. Del mismo modo, proporciona seguridad independientemente de alguna aplicación, de tal forma que lo convierte en una pieza imprescindible de las redes actuales. (Pérez, 2001)

Por lo tanto, IPsec se ha convertido en un componente básico de las redes IP, por ello se puede considerar una tecnología bastante madura para implantarla en redes cuya prioridad sea la seguridad. Si se habla de seguridad se refiere a la confidencialidad y la integridad de los datos que para muchas compañías es un requisito fundamental que sus redes deben proporcionar a los clientes.

En otras palabras, IPsec es el conjunto de estándares para integrar en IP funciones de seguridad basadas en criptografía. Se caracteriza por proporcionar: confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública (RSA), algoritmos de cifrado (DES, 3DES, IDEA, Blowfish), algoritmos de hash (MD5, SHA-1) y certificados digitales. (Iglesias, 2011) IPsec se compone de:

- Dos protocolos de seguridad: IP Authentication Header (AH) e IP Encapsulating Security Payload (ESP) que proporcionan mecanismos de seguridad para proteger el tráfico IP.

- Un protocolo de gestión de claves: Internet Key Exchange (IKE) que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

2.3.11.2 Algoritmo de Resumen o Hash. Realizan autenticación y verifican la integridad de un paquete. Éste entrega una secuencia de bits de pequeña longitud, las asocia a al paquete y resulta muy difícil de falsificar. Los más conocidos son:

- SHA-1: Genera un resumen de 160 bits.
- MD5: Genera un resumen de 128 bits.

Estos dos algoritmos son parte de las especificaciones de IPsec, siendo más seguro SHA-1. (Pérez, 2001)

2.3.11.3 Algoritmos de cifrado. IPsec emplea algoritmos de cifrado simétrico, es decir, que utiliza la misma clave el emisor como receptor del paquete. La clave es utilizada para cifrar y descifrar el mensaje y cuanto más grande sea más segura es. El modo de trabajo es dividir el mensaje en bloques de tamaño fijo y lo interesante es que aplican sobre cada uno de ellos operaciones de confusión y difusión. (De la Luz, 2010)

La confusión oculta la relación entre el mensaje claro, el mensaje cifrado y la clave, mientras que la difusión reparte la influencia de cada bit del mensaje original lo más cercano entre el mensaje cifrado. Entre algunos de ellos están DES, 3DES, AES. Se considera DES como inseguro debido a debilidades encontradas que fueron mejoradas con 3DES. AES uno de los más seguros actualmente. Pero para consideraciones de IPsec se utilizan DES Y 3DES. (Pérez, 2001)

2.3.11.4 Asociaciones y políticas de seguridad. Una SA (Asociación de seguridad), es un grupo de parámetros como algoritmos de cifrado, de resumen, clave, etc., que se utilizan para establecer una comunicación segura. De la misma forma, las direcciones origen y destino forman parte de una SA como también los protocolos AH o ESP, utilizados como modo transporte o modo túnel y la referencia de SA es llamado SPI. (Pérez, 2001)

- **Protocolo AH:** Se utiliza para garantizar autenticación e integridad de los paquetes, pero no proporciona confidencialidad. Se inserta entre la cabecera IPv6 y los datos transportados.

Su funcionamiento se basa en los siguientes pasos:

- ✓ Un algoritmo de hashing es aplicado a la combinación del mensaje de entrada y una clave.
- ✓ Esto genera como salida la representación del mensaje en forma de una cadena de dígitos que se denomina MAC, igual a una huella digital de los datos.
- ✓ Este MAC se copia en el campo datos autenticados del paquete AH, creando así el paquete IPsec el cual se envía a través de la red.
- ✓ En el receptor, se aplica el algoritmo hash y se realiza el cálculo del MAC, se compara con el recibido en el paquete, si son iguales, el receptor tiene la seguridad de que el paquete no ha sido modificado durante la comunicación y que proviene efectivamente del origen esperado. (De la Luz, 2010)

En la Figura 8 se indica gráficamente el proceso de funcionamiento del protocolo AH.

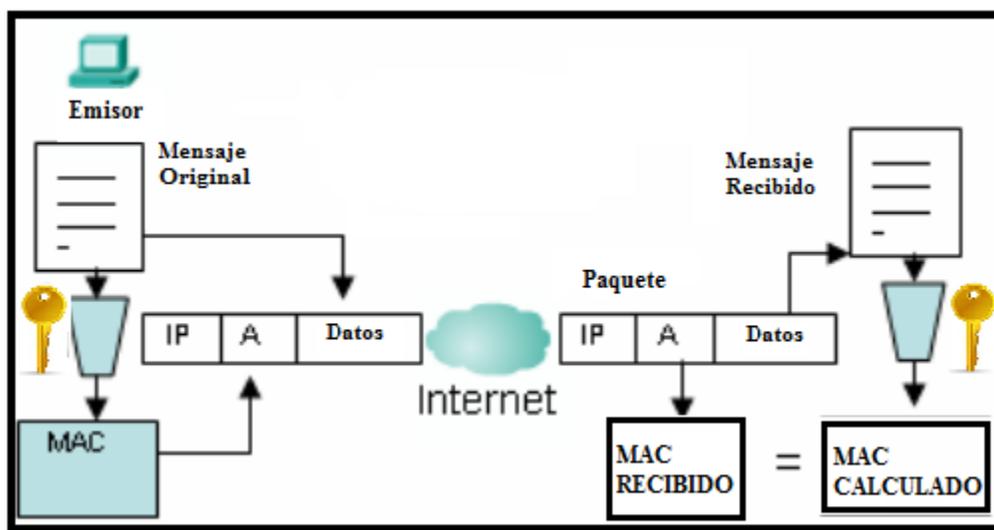


Figura 8: *Funcionamiento AH*

Fuente: (Pérez, 2001)

- **Protocolo ESP:** Tiene como objetivo principal brindar confidencialidad. Describe el modo de cifrar los datos que se desean enviar y como éstos se incluyen en el paquete IPv6. También

ofrece servicios de integridad y autenticación del origen de los datos empleando mecanismos similares como AH. (Pérez, 2001)

Realiza un cifrado con un algoritmo simétrico de clave simétrica. Este maneja cifrado de bloque, de manera que la longitud del mensaje tiene que ser múltiplo del tamaño del bloque (8 o 16 bytes, en la mayoría de los casos). Por esta razón, existe un campo de relleno en la cabecera de cifrado de seguridad ESP. (Pérez, 2001)

Su funcionamiento se basa en los siguientes pasos:

- ✓ El emisor, toma el mensaje original, y le aplica el algoritmo de criptografía simétrica que puede ser 3DES.
- ✓ El mensaje cifrado se incluye en el paquete IPSec, a continuación de la cabecera ESP. En caso de que el paquete es interceptado por un tercero en su trayecto, éste obtendrá un conjunto de bits incoherentes.
- ✓ En el destino, el receptor aplica de nuevo el algoritmo de cifrado recuperando los datos originales. (Iglesias, 2011)

La seguridad que proporciona esta cabecera, tiene que ver con el cifrado que se emplea, debido a que la clave ESP, la conocen únicamente el emisor y el receptor y un atacante no podrá descifrar los datos sin conocer ésta clave. En la Figura 9 se indica el funcionamiento del protocolo ESP.

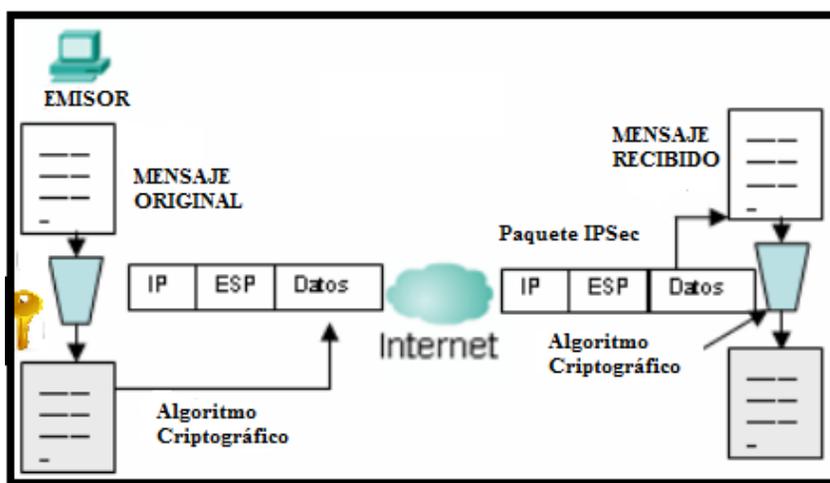


Figura 9: *Funcionamiento ESP*

Fuente: (Pérez, 2001)

- *Protocolo IKE*. Es el protocolo de control que se encarga de entablar comunicación y realizar la negociación de claves y otros elementos con IPsec entre dos computadores. Por esta razón, el IETF ha definido el protocolo IKE para realizar tanto esta función de gestión automática de claves como el establecimiento de las asociaciones de seguridad correspondientes. IKE es un protocolo híbrido que ha resultado de la integración de dos protocolos complementarios: *ISAKMP* y *OAKLEY*. (Iglesias, 2011)

ISAKMP define de forma genérica el protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE, esto facilita los procedimientos y formatos del paquete para establecer, negociar, modificar y eliminar asociaciones de seguridad. OAKLEY especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente. (Iglesias, 2011)

De igual manera IPsec puede trabajar en dos modos: transporte y túnel:

- ✓ **Modo transporte:** el contenido transportado dentro del datagrama AH o ESP son datos de la capa de transporte (por ejemplo, datos TCP o UDP). Entonces, la cabecera IPsec se luego de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. Este modo tiene la ventaja de asegurar la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPsec.
- ✓ **Modo Túnel:** el contenido del datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. Así que, a un datagrama IP se añade inicialmente una cabecera AH o ESP, luego de ello, se añade una nueva cabecera IP que es la que se utiliza para encaminar los paquetes a través de la red. El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPsec.

2.4 Comparación de IPv4 con IPv6.

A continuación, se va a mencionar las principales características de cada uno de los protocolos mediante una tabla comparativa (Tabla 2) que permita visualizar las principales diferencias de IPv4 con IPv6:

Tabla 2. *Comparación IPv4 e IPv6*

IPv4	IPv6
Las direcciones tanto de origen como destino son de 32 bits de longitud (4 Bytes)	Las direcciones de origen y destino son de 128 bits de longitud (16 Bytes).
IPSec es un protocolo opcional.	IPSec es una obligatoriedad.
No existe identificación de paquetes QoS que manejen los routers en sus cabeceras.	Con la utilización del campo flow label, se tiene entendido que se está manejando QoS
La fragmentación de un paquete lo realiza el host como el router, que produce retardos.	La fragmentación en IPv6 lo realiza únicamente el host, porque el paquete es procesado en el nodo final de destino.
Su cabecera tiene un checksum.	Es eliminado el campo checksum.
Se emplean solicitudes ARP para resolver direcciones IPv4, en una dirección de capa física	Las tramas ARP, son reemplazadas con mensajes multicast neighbor Discovery
Usan registros A, para la resolución de direcciones IPv4 a dominios.	Usan registros AAAA, para la resolución de las direcciones IPv6.
Se utilizan las direcciones Broadcast, para enviar un paquete a todos los nodos de las subredes.	Se utiliza una dirección multicast para poder enviar la información a los nodos de un ámbito local del vínculo.
Se debe configurar las direcciones de manera manual o utilizando DHCP.	No requiere de configuraciones manuales o utilizar DHCP.

Fuente: (Nuñez, 2009)

2.5 Mecanismos de transición

La transición de IPv4 a IPv6 no será posible de realizarla de un día para otro, por ello, es importante buscar alguna solución para que los dos protocolos puedan convivir un tiempo mientras todas las redes migren a IPv6 completamente. Por ejemplo, tratar de realizar actualizaciones de software en los nodos IPv4 actuales y definir que equipos son los que se debería cambiar para que manejen IPv6.

Las características de configuración que IPv6 proporciona, permiten que las redes sean más fáciles de mantener, algo nuevo para los ISP's, pero de la misma manera el despliegue de su infraestructura es muy rápido. Hay que tomar en cuenta que las aplicaciones también deben utilizar el protocolo IPv6 para llevar a cabo la comunicación, aunque hoy en día ya es posible. (LACNIC, 2012)

Los principales mecanismos de transición se clasifican en tres grupos y son:

- Dual Stack (Doble Pila)
- Túneles
- Traducción (LACNIC, 2012)

2.5.1 Dual Stack (Doble Pila). Es el método más utilizado porque utiliza un nodo de doble pila IPv6/IPv4 y puede comunicar tanto un nodo IPv4 como un nodo IPv6. Para conseguirlo, se debe configurar los dos tipos de direccionamiento a cada uno de ellos. Este mecanismo permite activar o desactivar una de las pilas, por ello va a funcionar de tres maneras:

- Si está activada la pila IPv4, se comportará como un solo nodo IPv4.
- Si está activada la pila IPv6, se comportará como un solo nodo IPv6.
- Cuando estén activadas las dos pilas funcionará con los dos protocolos.

Recordar que IPv4 utiliza para configurar las direcciones utiliza DHCP o la forma estática, mientras que IPv6 utiliza configuración estática o DHCPv6. De la misma manera, el DNS, debe

ser capaz de resolver los nombres de las direcciones en IPv4 como en IPv6, por lo tanto, debe manejar un nodo IPv6/IPv4. (LACNIC, 2012)

2.5.2 Túneles. El mecanismo túnel es utilizado para el transporte de paquetes IPv6 utilizando una infraestructura IPv4. Además, computadoras aisladas IPv6 pueden establecer sesiones IPv6 extremo a extremo utilizando IPv4 como la capa de transporte. Los túneles tienen como finalidad encapsular paquetes IPv6 dentro de paquetes IPv4, que luego serán encapsulados a un nodo destino IPv4 sobre una red que maneje IPv4.

Luego el nodo destino realizará la desencapsulación y extraerá los paquetes IPv6. Tomar en cuenta que, para poder aplicar este mecanismo, es necesario que los nodos extremos del túnel soporten Pila Dual. (Network Information Center México S.C., 2010)

Este mecanismo puede ser dividido en dos grupos:

2.5.2.1 Túneles manuales: Aquellos que para transportar un paquete IPv6 deben encapsularse en un paquete IPv4, por tanto, son túneles punto a punto que deben ser configurados manualmente. La configuración de túneles entre host y routers se puede realizar de las siguientes maneras:

- **Host a Host:** los host IPv6/IPv4 que están conectados con infraestructura IPv4, pueden encapsular paquetes IPv6 entre ellos mismos.
- **Router a Host:** los routers IPv6/IPv4 pueden encapsular paquetes IPv6 a su destino final.

2.5.2.2 Túneles automáticos: Los nodos IPv6 pueden utilizar direcciones que sean compatibles con IPv4, con IPv6 o 6to4, es un túnel dinámico de paquetes IPv6 sobre una infraestructura de enrutamiento IPv4.

La configuración de túneles entre host y routers se puede realizar de las siguientes maneras:

- **Router a Router:** utiliza el túnel automático en donde los routers IPv6/IPv4, separados por una infraestructura IPv4 pueden encapsular paquetes IPv6 entre ellos mismos.

- **Host a Router:** Un host IPv6/IPv4 puede encapsular paquetes IPv6 a un router intermedio IPv6/IPv4 al cual se puede acceder mediante la infraestructura de enrutamiento IPv4.

Ahora se van a describir las tecnologías del túnel automático:

- **Túnel 6to4:** especifica un mecanismo para que los sitios IPv6 puedan comunicarse entre sí a través de la red IPv4 sin establecer configuraciones explícitas del túnel. La red IPv4 se comporta como una capa de enlace punto a punto de unidifusión en donde dominios de IPv6 se comunican a través de routers 6to4 llamados puertas de enlace 6to4.

Este método utiliza el prefijo de dirección global: 2002:WWXX:YYZZ::/48, WWXX:YYZZ: corresponde al ID de agregación del siguiente nivel de una dirección global. En la Figura 10 se indica la infraestructura de un túnel 6to4.

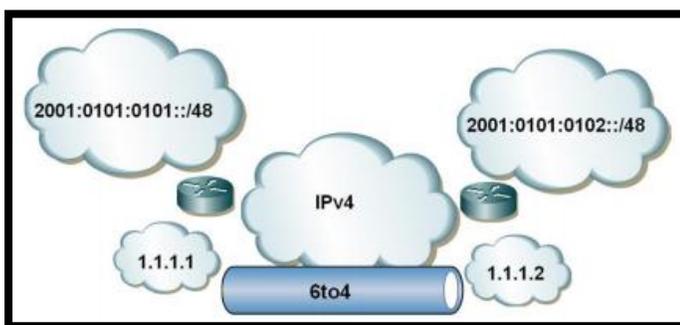


Figura 10: Túnel 6to4

Fuente: (Cedeño., 2013)

- **Túnel 6over4:** se lo llama también túnel de multidifusión de IPv4, donde 6over4 admite la comunicación entre nodos IPv6 e IPv4 a través de infraestructura IPv4, con capacidad de multidifusión. Para el buen desempeño de 6over4, la infraestructura IPv4 debe estar habilitada para multidifusión IPv4.

En este mecanismo, se debe crear un enlace virtual a través de un grupo IPv4 multicast con ámbito local – organizacional, recordando que el mecanismo multicast en IPv4 es opcional. Por tanto, las direcciones IPv6 multicast mapean direcciones IPv4 multicast para ejecutar. Para el

encaminamiento entre IPv6 y el dominio 6over4 es suficiente configurar un router al menos en una de sus interfaces. (Cedeño., 2013)

En la Figura 11 se indica la infraestructura del túnel 6over4

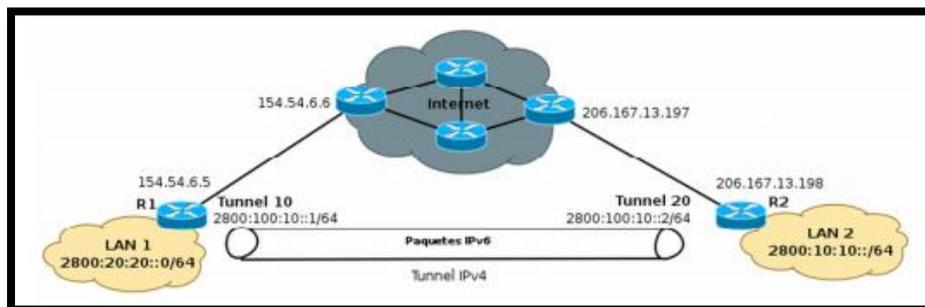


Figura 11: *Túnel 6over4*

Fuente: (Cedeño., 2013)

- **Túnel Teredo:** fue diseñado para garantizar las conectividades IPv6 de los nodos dual stack, localizados detrás de los dispositivos NAT sobre dominios IPv4, es decir, que define el encapsulamiento de paquetes IPv6 en datagramas UDP IPv4 para ser dirigidas a través de dispositivos NAT y en internet IPv4. En la Figura 12 se indica un cliente se comunica a través de un túnel Teredo con hosts IPv6 nativos. (Palet, 2007)

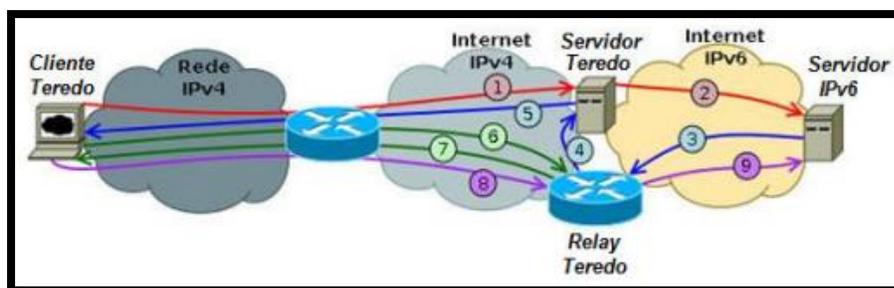


Figura 12: *Túnel Teredo*

Fuente: (Palet, 2007)

- **ISATAP:** Permite crear túneles IPv4/IPv6 de forma automática dentro de una infraestructura IPv4. Con respecto a 6over4 tiene algunas ventajas, por ejemplo, no necesita utilizar direcciones multicast IPv4 y soluciona problemas en redes remotas, como la baja escalabilidad en la agregación.

2.5.3 Traducción. Este método permite un enrutamiento de forma transparente de la comunicación entre nodos que soporten ya sea la versión cuatro, la versión 6 o el mecanismo de doble pila. Operan de distintas maneras o capas, puede ser, traduciendo cabeceras IPv4 en cabeceras IPv6 y viceversa, conversiones en las direcciones o el intercambio del tráfico TCP a UDP (LACNIC, 2012)

2.6 Servidores

Un servidor es un equipo que es parte de una red y provee de servicios a cualquier otro cliente. Debe cumplir características en cuanto a hardware y software, además ser especializada con altas capacidades de proceso que permita almacenar varias aplicaciones y que éstas sean accesibles por parte de los usuarios de una red, si así lo requieren. (APR, 2016)

2.6.1 Tipos de Servidores. Un servidor puede ser dedicado o compartido. En el caso de ser dedicado, éste va a prestar todos sus recursos para atender peticiones que un cliente realice y si es compartido, va a ser utilizado para trabajar localmente en una red en el que se lo coloque. (APR, 2016)

Existen algunos tipos de servicios como:

- Base de Datos (BDD)
- DNS
- DHCP
- FTP
- Mail (Correo/mensajería)
- Proxy
- SSH
- Transmisión Multimedia
- Telnet
- Web

En este caso se estudiarán los servicios que se proponen para la transición de IPv4 a IPv6 que son: WEB y correo electrónico. La elección se ha realizado tomando en cuenta la disponibilidad de funcionamiento de los servicios que brinda a los usuarios internos como externos.

- **Servidor WEB.** La palabra WEB es asociada a Internet, debido a que existen navegadores disponibles en cualquier dispositivo con acceso a la red para acceder a estos sitios que ofrecen diferente tipo de información como: archivos, música, videos entre otros. (Corporación Digital Colombia, 2016)

Por lo tanto, un servidor web es un lugar que alberga cualquier tipo de información que el usuario requiera por medio de un navegador que realiza el intercambio de información entre el usuario y el servidor mediante HTTP que generalmente en la navegación web usa el puerto 80 y se basa en el modelo cliente servidor y de igual manera HTTPS con el puerto 443. (Herramientas WEB, 2013)

Este servidor presenta un total de datos enviados de 45,5 MBytes y recibidos de 6,0 MBytes, es el quinto servidor considerado como prioritario y crítico porque además es uno de los servidores que más consumen el protocolo HTTP, aquí se alojan las aplicaciones web para el intercambio de datos. Este servidor mantiene las páginas de alarmas, turismo, sismert, consulta de documentos, consulta de impuestos. (Ibarra, 2015)

Este servidor se encuentra virtualizado, su sistema operativo es Debian 7. El servidor tiene las siguientes funcionalidades:

- Recaudación de impuestos para parroquias rurales, brinda la funcionalidad de realizar operaciones de cobro y pago de impuesto predial a través de la web.
- El sistema se relaciona con el Sistema de Actividades Económicas y permite el registro de las actividades turísticas del cantón en base al catastro turístico del Ministerio de Turismo, realiza la re-categorización de las mismas, la emisión de la tasa de turismo individual o en bloque y la impresión de la Licencia Única Anual de Funcionamiento LUAF.

- El Sistema registra: Multas generadas por los inspectores, Emisión de certificados de no adeudar, permite la creación de grupos de inspectores con su respectiva asignación de ruta de control, realiza el registro de ventas de tickets por inspector y supervisor, registra el cuadro del dinero recaudado, proporciona reportes de la información registrada.
- El Sistema de Archivo Documental cumple con la funcionalidad de gestionar el almacenamiento y consulta de documentos generados en el Municipio de Ibarra, tales como Ordenanzas, Contratos, Convenios, Reglamentos, Proyectos, Actas y Resoluciones.
- El Sistema de Participación Ciudadana maneja los siguientes ejes: Organización Social y Territorial, Planificación Participativa, Presupuesto Participativo y Mecanismos de Participación Ciudadana y Control Social.
- En el sistema informático constan los siguientes módulos: Censo Socioeconómico, registro de Organizaciones Sociales y Territoriales, Registro de Convocatorias Participativas, Registro de reuniones y Asambleas, emisión de certificados participativos, Administración del Sistema y Reportes.
- El Sistema realiza el registro y consulta de obras, mingas y vallas del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, las mismas que pueden ser observadas en el mapa y visualizar las fotografías subidas en cada opción.
- Redmine es una herramienta para la gestión de proyectos que incluye un sistema de seguimiento de incidentes con seguimiento de errores, calendario de actividades, diagramas de Gantt para la representación visual de la línea del tiempo de los proyectos, wiki, foro, visor del repositorio de control de versiones, RSS, control de flujo de trabajo basado en roles e integración con correo electrónico. En la Dirección TIC se instaló ésta herramienta para la administración de Actividades del Personal, Documentación de Procesos y Procedimientos, Documentación de Sistemas, entre otros.
- Consulta de impuestos, predios, valores a pagar del SISMERT y sistemas de boletín de noticias. La tecnología que usan estos módulos es la siguiente:
- El portal web del Cantón Ibarra es un canal informativo que contiene datos del cantón en las siguientes temáticas: Gobierno, Cultura, Turismo y Archivo histórico. Cada uno corresponde a un sitio web totalmente independiente que conserva sus características propias de cada tema. El portal web encuentra en un servidor compartido arrendado con la empresa Inprise.ec. (Ibarra, 2015)

El servidor WEB, está destinado para el uso de usuarios internos como usuarios externos que hacen uso de las diferentes actividades que se han descrito.

En la Figura 13, se encuentra la página WEB del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra.

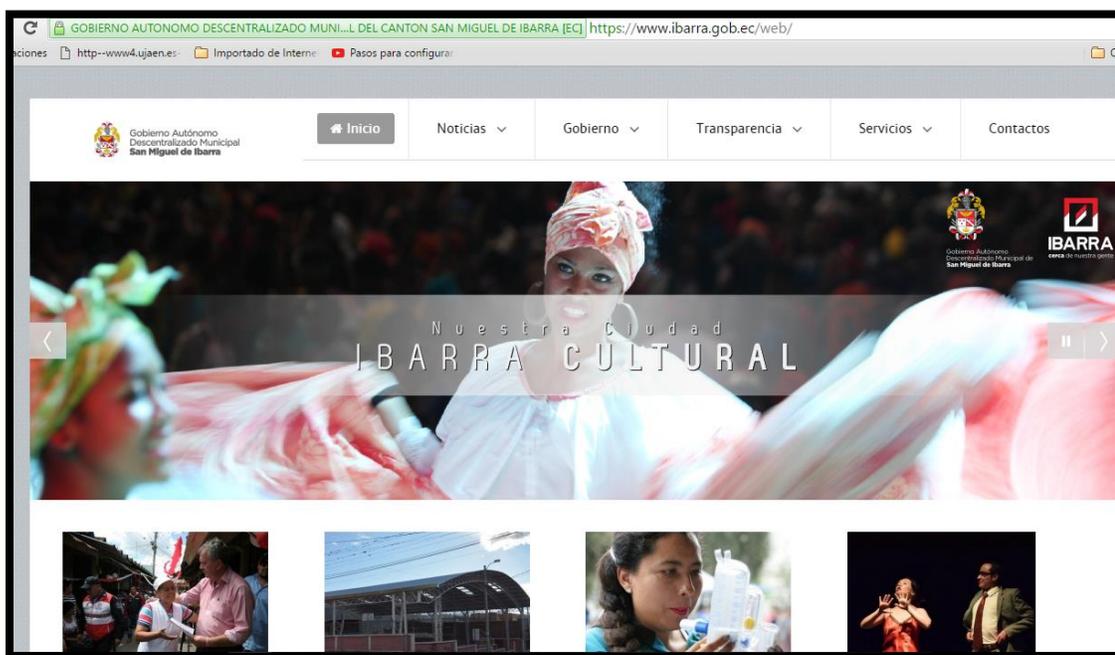


Figura 13: *Página WEB del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra*

Fuente: <https://www.ibarra.gob.ec/web/>

- **Servidor de correo electrónico.** El mail o correo electrónico, es el sistema que permite enviar, recibir y gestionar mensajes de usuarios o clientes, unos a otros conectados en una misma red o usuarios de otras redes como el Internet. El intercambio de estos mensajes se realiza de forma asíncrona, para lograr la efectiva comunicación se necesita de algunos protocolos que son: POP, IMAP y SMTP. Estos protocolos proporcionan la interacción (transmisión y recepción) de correo electrónico entre ordenadores y servidores, con funciones características o específicas entre cada uno.

- **POP (Post Office Protocol)**

Es el protocolo utilizado por clientes de email (Windows Mail, Outlook, etc) para recoger mensajes en el servidor de email. Los mensajes son transferidos desde el servidor hacia la computadora local cuando el usuario se conecta al servidor. Una vez que se reciben los mensajes, la conexión puede interrumpirse, procediéndose a la lectura de los mensajes sin necesidad de seguir conectado al servidor. (Fundamentos de Redes, 2013)

Es decir, que se puede leer el correo sin necesidad de seguir conectado a la red, por tanto, la función de este protocolo es mandar a llamar a él o los mensajes, descargarlos para el computador. En la Figura 14 se indica el funcionamiento de envío y recepción de correos.

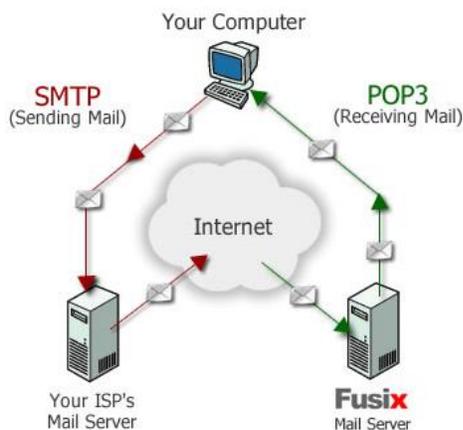


Figura 14: *Envío y recepción de emails protocolo POP*

Fuente: Recuperado de <https://sites.google.com/site/fundamentosderedesuteztic1h/protocolos-pop-imap-y-smtp>

- **IMAP (Internet Message Access Protocol)**

De la misma manera es utilizado para tener acceso a los mensajes que llegan al servidor de correo, pero a diferencia del POP, entre la computadora local y el servidor de email, la comunicación debe estar siempre activa pues hay una constante interacción entre ambos. Los mensajes se mantienen en el servidor de email, aunque el usuario accede como si estuvieran localmente. Esta opción es útil para las personas que leen sus e-mails en diferentes computadoras. (Fundamentos de Redes, 2013)

De esta forma, al verse interrumpida la conexión al servidor, se perderá la información y así se pierde la posibilidad de lectura de los mensajes. En la Figura 15 se indica el funcionamiento de este protocolo.

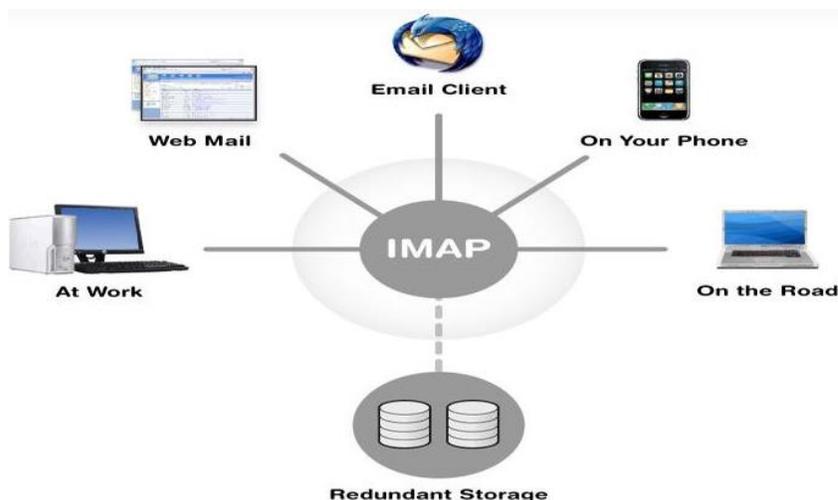


Figura 15: *Funcionamiento del protocolo IMAP*

Fuente: Recuperado de <https://sites.google.com/site/fundamentosderedesuteztic1h/protocolos-pop-imap-y-smtp>

- **SMTP (Simple Mail Transfer Protocol)**

Se considera un estándar internacional utilizado para transferencia de correo electrónico (email) entre computadoras. Es utilizado exclusivamente para el envío de correos.

Este protocolo funciona en línea, de manera que opera en los servicios de correo electrónico. Sin embargo, este protocolo posee algunas limitaciones en cuanto a la recepción de mensajes en el servidor de destino (cola de mensajes recibidos). Como alternativa a esta limitación se asocia normalmente a este protocolo con otros, como el POP o IMAP, otorgando a SMTP la tarea específica de enviar correo, y recibirlos empleando los otros protocolos antes mencionados (POP O IMAP). (Fundamentos de Redes, 2013)

Este servidor al igual que el WEB, se encuentra virtualizado utilizando el sistema operativo Centos 7 y se utiliza el correo institucional con la herramienta Zimbra versión 8. El servidor de correo presenta un total de datos enviados de 4,0 GBytes y recibidos de 1,5 GBytes, es el primero

de los servidores prioritarios y críticos, debe estar funcionando correctamente porque la entidad trabaja solamente con cuentas de correo institucionales debido a que la información que se envía o recibe es de uso exclusivo y confidencial de la entidad. (Ibarra, 2015)

El uso de este servidor es únicamente para los usuarios internos, se manejan alrededor de 700 cuentas y la razón por la que se encuentra utilizando una plataforma libre es porque las entidades gubernamentales lo utilizan. De la misma manera, el Ingeniero Gabriel Bucheli, administrador de la red, manifestó que, si se manejara este servidor con software pagado, el costo de cada cuenta de usuario, estaría alrededor de unos tres dólares americanos, por lo bajo, resultando un costo mensual de alrededor de dos mil dólares, lo que con software libre no tiene este costo.

Con respecto a la seguridad de este servidor, se encuentran instaladas políticas de seguridad en el Firewall Checkpoint que, ante cualquier spam u otra clase de ataques, se realice el filtro de estos problemas que pueden afectar al servidor de correo. En la Figura 16, se indica la interfaz de acceso al servidor de correo.



The image shows a login interface for the institutional email system. At the top left is the logo of the 'Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra'. At the top right is the 'zimbra' logo. Below these are two input fields: 'Nombre de usuario:' and 'Contraseña:'. To the right of the password field is a checkbox labeled 'Recordarme' and a button labeled 'Iniciar sesión'. At the bottom left, there is a 'Versión:' label and a dropdown menu currently set to 'Predeterminada'. To the right of the dropdown is a link that says '¿Qué es esto?'. The entire interface is set against a blue background.

Figura 16: Acceso al correo Institucional del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra

Fuente: Recuperado de <https://correo.ibarra.gob.ec>

Capítulo III

3. Planteamiento de Modelo De Transición y Análisis de Seguridad en IPv6

En este capítulo se diseña un modelo de transición en el cual se puedan implementar las acciones estipuladas en el plan maestro que se encuentra en el acuerdo ministerial, que permita realizar una transición ordenada y coexistente de los dos protocolos. Así mismo, analizar los puntos críticos en los cuales se debería implementar el protocolo IPsec que permitan brindar seguridad a la red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra.

3.1 Plan de acción propuesto por el Ministerio de Telecomunicaciones (MINTEL)

Aquí se explican los lineamientos generales que el MINTEL ha propuesto para que se lleve a cabo la transición de IPv4 a IPv6. En la Figura 17 se explica un modelo generalizado de la metodología empleada.

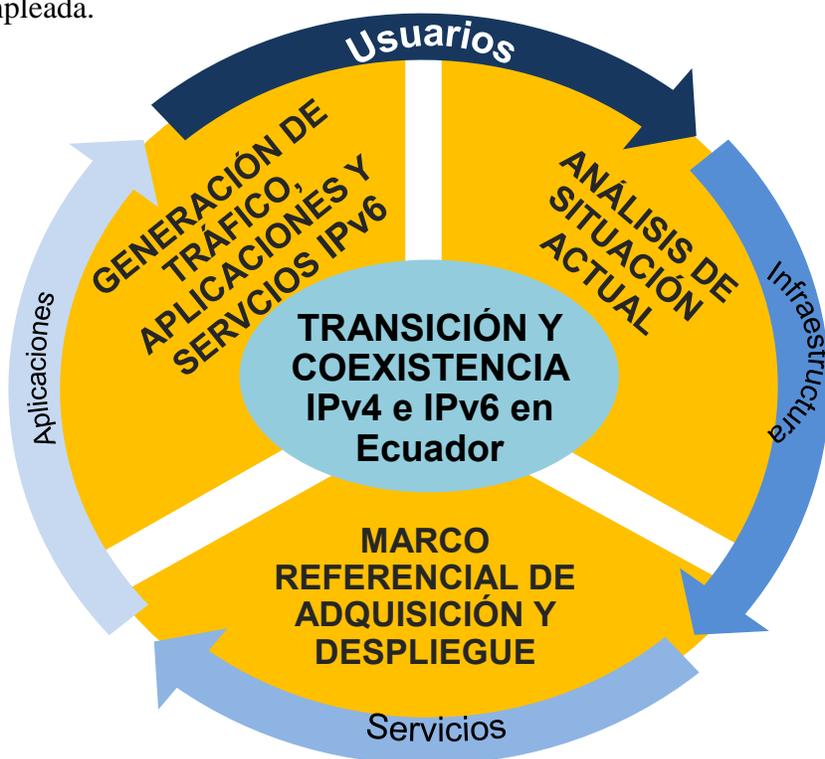


Figura 17: *Transición y Coexistencia de IPv4 e IPv6 en Ecuador*

Fuente: Recuperado de <http://www.telecomunicaciones.gob.ec/>

3.2 Modelo De Transición de IPv4 a IPv6 para la red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra

Para poder llevar a cabo la transición de IPv4 a IPv6 en esta empresa, es necesario que se ajusten las actividades de acuerdo al plan de transición propuesto por el MINTEL, es así como se ha diseñado el modelo de transición para el Gobierno Autónomo Descentralizado Municipal de San Miguel de Ibarra en el que se incluyen las actividades realizadas en fases.

3.2.1 FASE I: Planificación.

En esta fase es importante identificar y establecer los planes a futuro para la adopción del protocolo IPv6, determinando el recurso humano requerido para la delegación de funciones y responsabilidades en cada área y llevar a cabo el proceso de transición y coexistencia del protocolo IPv4 e IPv6.

3.2.1.1 Selección del personal. Se debe elegir a los ingenieros que trabajan en el departamento TIC's de la entidad, para cumplir con todas las actividades que este proyecto demanda. En este departamento se encuentran las siguientes personas:

- El Director de la Dirección de Tecnologías Informáticas el Ingeniero Carlos Gudiño.
- El administrador de la red el Ingeniero Gabriel Bucheli.
- El encargado de hardware y software el licenciado Miguel Tobar.
- El analista de sistemas el Tecnólogo Víctor Hugo Dávila.
- El analista de sistemas el Ingeniero Esteban Páez.

3.2.1.2 Capacitación y entrenamiento. Se debe realizar al personal de TIC's del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, con la finalidad de llevar a cabo el proyecto con responsabilidad que se requiere. Como alternativa se presenta en el **Anexo G**, la propuesta de la empresa Imbatec que dispone de personal capacitado para el presente proyecto. Cabe recalcar que se tomó a esta empresa debido a la pronta respuesta a la solicitud de proforma. El Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra puede llamar a

licitaciones para elegir a la empresa de su conveniencia o convenio con cualquier institución educativa que tenga conocimiento en el tema como lo es la Universidad Técnica del Norte.

3.2.1.3 Cronograma de actividades. Esto va a permitir controlar que se realicen las actividades dispuestas en cada fase. Se debe tratar de establecer un periodo aproximado de tiempo en el que se culminará este proceso. En la Figura 18 se ha elaborado un modelo de cronograma de actividades.

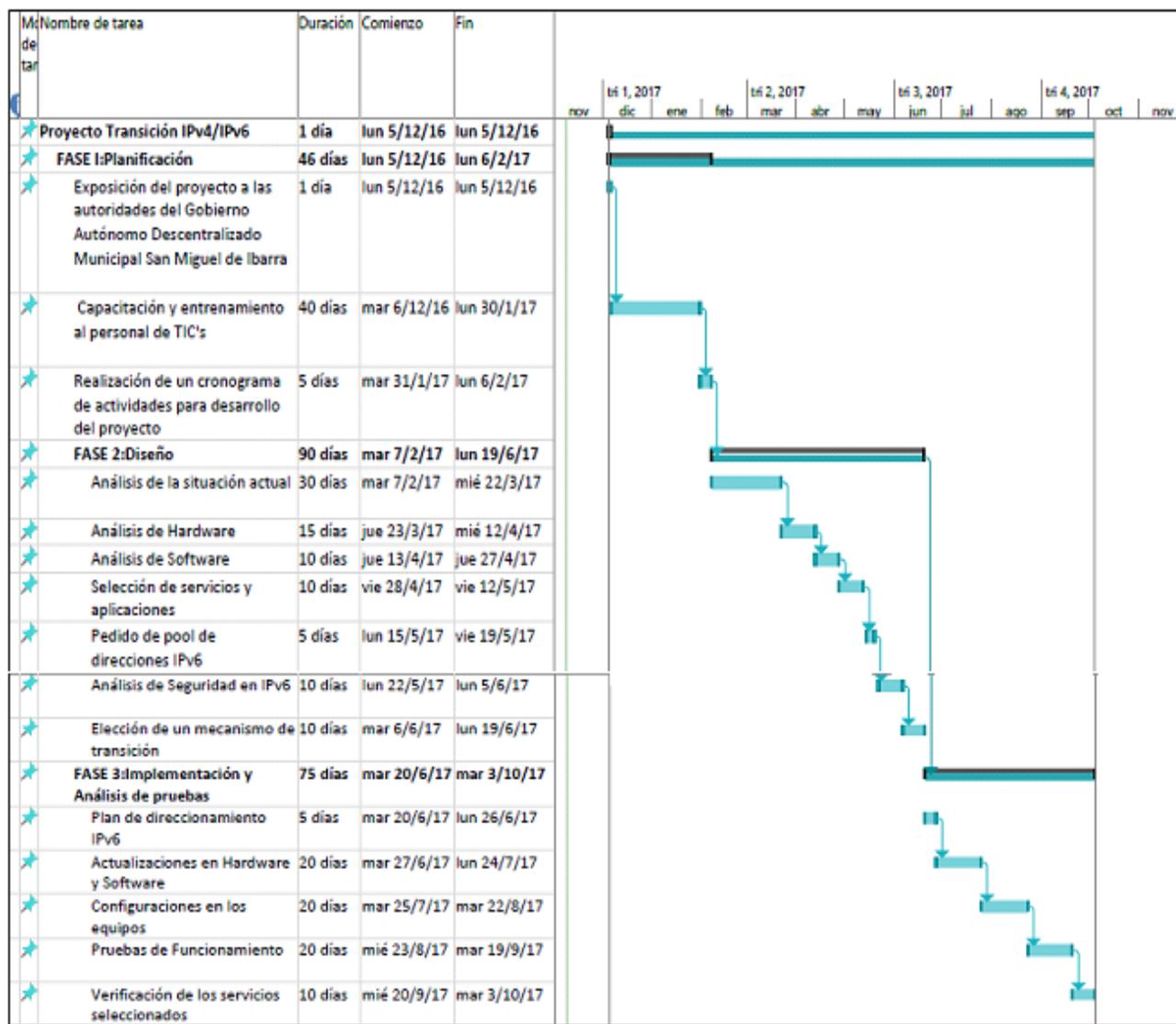


Figura 18: Cronograma de actividades para el proyecto

Fuente: Captura propia extraída de Project 2016

Este cronograma está planificado para realizarse en un periodo de va alrededor de los 200 días, las fechas que se han señalado son una referencia, para especificar el tiempo que va a durar cada actividad.

3.2.2 FASE II: Diseño

Esta etapa tiene como objetivo realizar el análisis actual de la empresa, identificando las áreas en donde se va a implementar IPv6, la topología de red, entre otros, para verificar el soporte del protocolo IPv6, de la misma manera seleccionar los servicios y aplicaciones que se van a manejar con el nuevo protocolo.

3.2.2.1 Análisis de la situación actual.

- **Descripción de la Institución**

Gobierno Autónomo Descentralizado Municipal San Miguel Ibarra

El Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, se encuentra en la provincia de Imbabura, en el cantón Ibarra. Es una entidad de Derecho Público conformada por una comunidad humana, administrando sus propios recursos económicos. Tiene como objetivos principales:

1. Organización del territorio cantonal con soluciones para las deficiencias de ordenamiento, infraestructura, equipamiento de servicios públicos, movilidad, vivienda ambiente y gestión de riesgos.
2. Mejorar las condiciones sociales de los ibarreños, a través de la construcción de políticas públicas locales, promoción cultural, servicios sociales incluyentes de calidad, fomentando una sociedad culta, participativa y segura.
3. Alcanzar un crecimiento equitativo de la producción, el comercio y los servicios, de forma consensuada entre el municipio y los diferentes actores locales.
4. Fortalecer la Gestión Institucional del GAD, mediante la implementación del sistema de calidad, rendición de cuentas y participación ciudadana, para satisfacer las necesidades de

la colectividad. (Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, 2015)

- **Ubicación:** El Ilustre Municipio de San Miguel de Ibarra, es en donde se encuentra Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra y está ubicado entre las calles García Moreno 6-31 y Simón Bolívar Esquina. En la Figura 19, se indica gráficamente la ubicación de la entidad.



Figura 19: *Ubicación del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra*

Fuente: Recuperado de <https://www.google.com.ec/maps/@0.3512708,-78.1193806,290m/data=!3m1!1e3>

Misión

Somos un gobierno municipal que, a través de una administración eficiente, fomenta el desarrollo integral del cantón, brindando servicios de calidad enmarcados en valores, principios y normativas, para mejorar las condiciones de vida de sus habitantes. (Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, 2015)

Visión

Ser un gobierno incluyente, reconocido por la ciudadanía por brindar servicios públicos de calidad, cumpliendo con los principios de gobernabilidad, para alcanzar un desarrollo ordenado, económico, social, turístico, productivo y seguro. Posicionando al cantón Ibarra en el año 2019 como referente nacional e internacional. (Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, 2015)

- **Estructura Administrativa:** Está basado en la parte de administración estratégica que el Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra propone a la ciudadanía. A continuación, en la Figura 20, se indica la simbología de la estructura de la entidad.

SIMBOLOGÍA

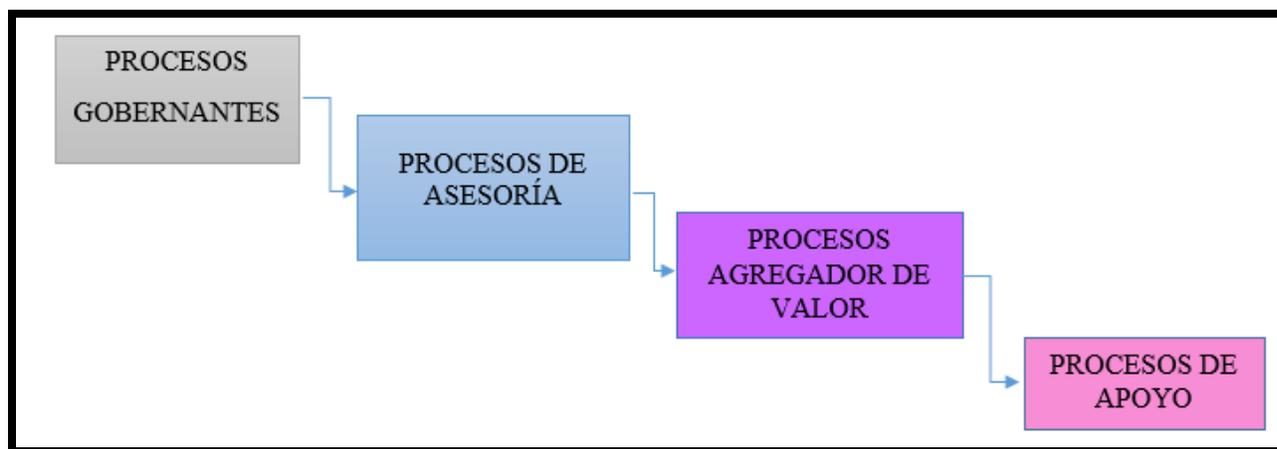


Figura 20: *Simbología de la estructura del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra*

Fuente: Recuperado de <https://www.ibarra.gob.ec/web/index.php/gobierno/planificacion-estrategica/2015-08-26-22-53-45>

En la Figura 21, se indican el organigrama de la Institución.

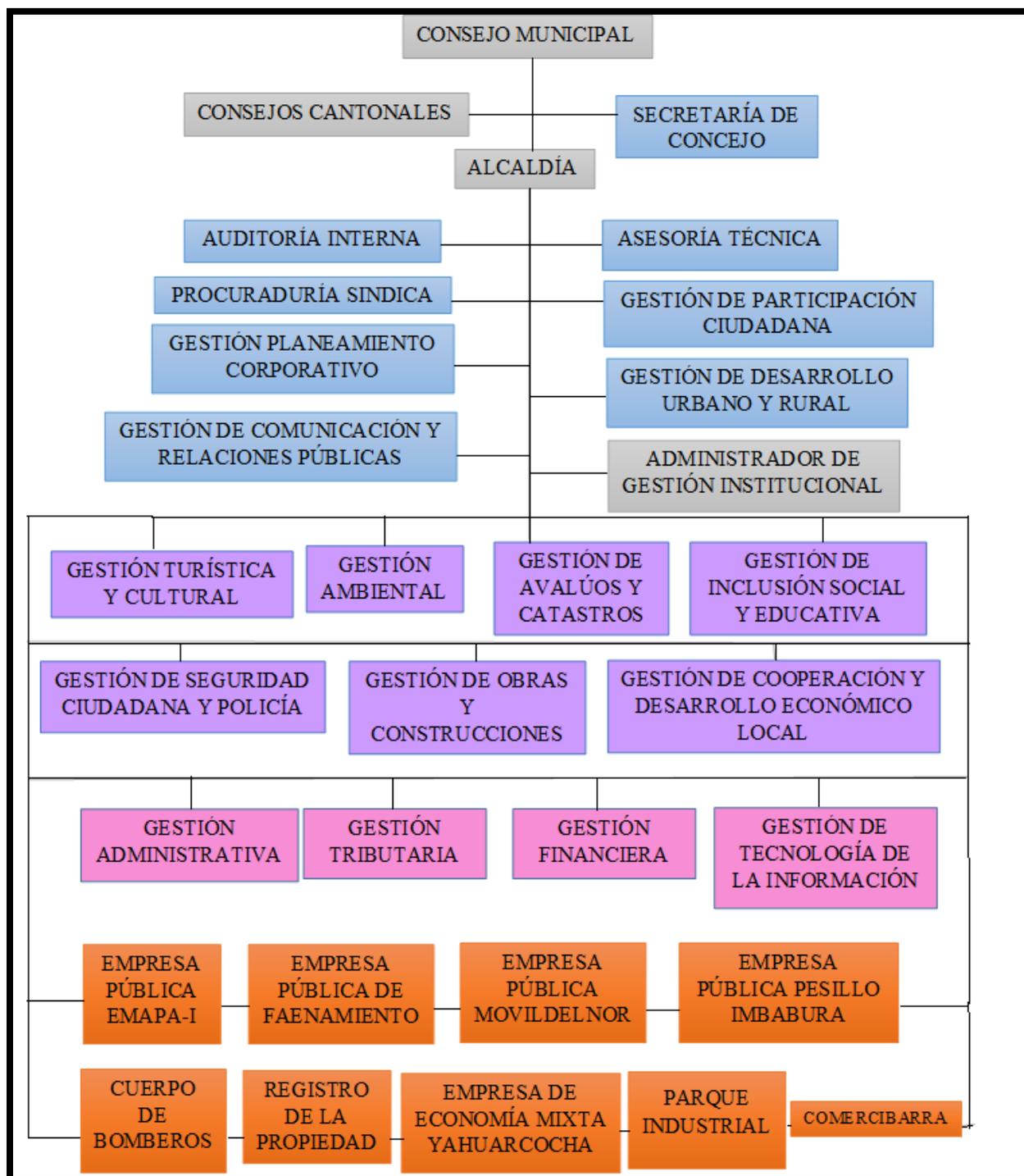


Figura 21: Organigrama del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra

Fuente: Recuperado de <https://www.ibarra.gob.ec/web/index.php/gobierno/planificacion-estrategica/2015-08-26-22-53-45>

- **Gestión de Tecnología de la Información:** Este departamento tiene como objetivo proporcionar tecnología de información de vanguardia para satisfacer los requerimientos y expectativas de los usuarios, a través de una plataforma de conectividad, hardware y software, que permita a las distintas unidades de la Municipalidad de Ibarra operar de manera integrada con información disponible en los diferentes niveles para la toma de decisiones. (Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, 2015)

A continuación, en la Figura 22, se va a presentar el organigrama del Departamento de Gestión de Tecnología de la Información.

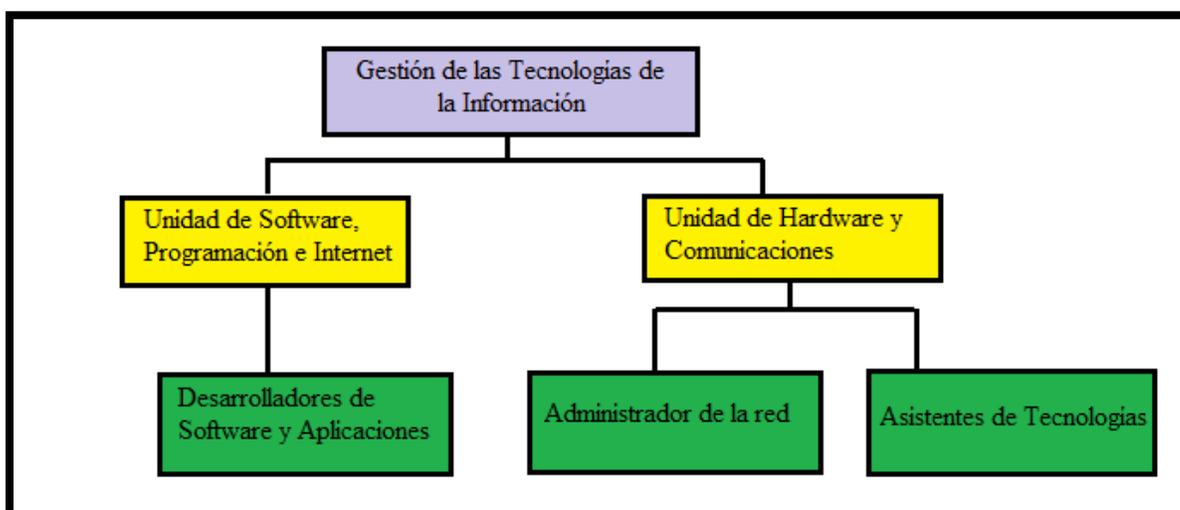


Figura 22: *Organigrama Gestión de Tecnologías de Información*

Fuente: (Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, 2015)

- **Detalle de las dependencias Internas y externas del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra**

Esta información ha sido proporcionada a algunos estudiantes que han realizado trabajos de tesis y por lo tanto se van a referir nuevamente para el análisis de este proyecto.

Dependencias Internas

- ✓ *Edificio Principal*

Esta dependencia se encuentra ubicada en el centro de la ciudad de Ibarra, en las calles Gabriel García Moreno 6-31 y Simón Bolívar. Se encuentra dividida en tres plantas como se detalla en la Tabla 3 y aproximadamente se encuentran trabajando 201 empleados, quienes cumplen funciones acordes a cada departamento.

Tabla 3. *Distribución de los departamentos del Edificio Principal del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra.*

	Departamentos	Número de Empleados
Planta Baja	<ul style="list-style-type: none"> • Atención al cliente • Rentas • Coactivas • Tesorería • Dirección de Comunicación Social • Recursos Humanos y Capacitación • Auditorio 	44
Primera Planta	<ul style="list-style-type: none"> • Alcaldía • Sala de Sesiones • Auditoria Interna • Procuraduría Municipal • Secretaria General • Administración General • Dirección de Gestión Administrativa • Dirección de Gestión Financiera • Presupuesto • Finanzas • Contabilidad • Copiadora 	51
	<ul style="list-style-type: none"> • Dirección de Planificación • Dirección de Avalúos y Catastros Urbano 	

Segunda Planta	<ul style="list-style-type: none"> • Dirección de Tecnologías de la información y Comunicación (TIC) • Dirección de Obras Públicas • Archivo Histórico 	98
Tercera Planta	<ul style="list-style-type: none"> • Gestión de Avalúos y Catastros Rural 	8
TOTAL DE EMPLEADOS		201

Fuente: GAD-I 2016

✓ *Edificio Antiguo*

Se encuentra ubicado en la calle Simón Bolívar entre las calles Juan José Flores y Gabriel García Moreno, junto al Edificio Principal, la distribución del mismo se detalla en la Tabla 4 y tiene un aproximado de 80 usuarios:

Tabla 4. *Distribución de Departamentos del Edificio Antiguo del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra.*

Planta	Departamentos	Número de Empleados
Planta Baja	<ul style="list-style-type: none"> • Comisaria de Construcciones • Comisaria de Higiene • Archivo Institucional • Recaudación • Dirección de Medio Ambiente • Plan de Ordenamiento Territorial • Biblioteca • Unidad de proyectos • Central de Operadora Telefónica 	40
	<ul style="list-style-type: none"> • Secretaria de Comisiones /Concejales 	

Primera Planta	<ul style="list-style-type: none"> • Radio • SISMERT • Secretaría de Comisiones /Concejales • Radio • SISMERT • Tránsito y Transporte • Dirección de Salud y Medio Ambiente • Tránsito y Transporte • Dirección de Salud y Medio Ambiente 	40
TOTAL DE EMPLEADOS		80

Fuente: (Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, 2015)

El total de usuarios en las dependencias Internas suman un total de 281 empleados actualmente.

Dependencias Externas.

Cuenta con importantes funciones que son parte del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra y por ende necesitan estar comunicadas y éstas son:

- *Dirección de Cultura, Proyecto Parque Ciudad Blanca*

Se localiza en las calles Simón Bolívar y Juan José Flores (esquina) en la casa de la Ibarreñidad, en la cual, la primera planta corresponde al proyecto parque Ciudad Blanca y en la tercera planta el departamento de Cultura, y cuenta con 20 usuarios. (Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, 2015)

- *Dirección de Turismo*

Se encuentra ubicada en las calles Miguel Oviedo y Antonio José de Sucre de la ciudad de Ibarra y cuenta con una cantidad de 18 usuarios. (Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, 2015)

- *Bodega Municipal*

La ubicación es en la Avenida Víctor Manuel Guzmán y calle Uruguay junto al Instituto ecuatoriano de Seguridad Social (Hospital del Seguro Social) de la ciudad de Ibarra. Aquí

se realiza el almacenamiento de materiales, equipos y maquinaria perteneciente al GAD-Ibarra, además también se encuentra el área de Mecánica, Reciclaje y Desechos Sólidos, la Dirección de Gestión de Seguridad Industrial y Salud Ocupacional. Esta dependencia cuenta con 10 usuarios. (Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, 2015)

- *Administración de Mercado Amazonas*

Se encuentra ubicada en la Avenida Pérez Guerrero y cuenta con 5 usuarios. (Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, 2015)

El total de empleados de dependencias externas es de 53 usuarios.

El número de empleados total del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, tomando en cuenta las dependencias internas como externas suman un total de 281 usuarios.

- **Análisis de la infraestructura física de la red de datos**

El cuarto principal de telecomunicaciones del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra se ubica en la segunda planta dentro de la dirección de Gestión de Tecnologías de la Información y se va a detallar los principales componentes con los que se cuenta.

- *Data Center*

Este centro de procesamiento de datos, es el espacio físico que se encuentra en el departamento TIC del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, que ha sido diseñado y construido bajo normas internacionales de seguridad y es donde se interconectan todo el equipamiento de la red de datos tanto de dependencias internas como externas.

Cumple con ciertas especificaciones de la norma TIA-942, el cual provee lineamientos como diseño eléctrico, control ambiental, protección contra riesgos físicos, almacenamiento de archivos, además por seguridad de acuerdo a las normas posee un sistema de acceso restringido. A continuación, se presentan algunas características:

- La red local de datos se basa en la tecnología Ethernet.
- Utiliza la topología tipo estrella.
- Se han configurado VLAN's para los equipos de red y para los equipos de VoIP.
- El cableado vertical y horizontal de la red es UTP Categoría 6 y el cableado estructurado del edificio principal cuenta con un periodo de vida útil de 15 años a partir del año 2010.
- Posee el sistema de puesta a tierra tipo malla, ubicada en la parte del edificio antiguo, no dispone de un generador eléctrico.

En la Tabla 5, se describen los equipos que se encuentran en el Data Center del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra

Tabla 5. *Equipamiento del Cuarto de Telecomunicaciones del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra.*

Cantidad	Equipos	Marca/Modelo
16	Switch Administrables	▪ Cisco, 3COM
10	Servidores Físicos	▪ HP ProLiant DL, BL, ML
20	Servidores Virtuales	-
1	Firewall	▪ Chekpoint 4610
1	Chasis Blade System	▪ HP c3000
16	Patch Panel categoría 6 para voz y datos	-
6	Convertidores de fibra óptica	-
2	Equipos de proveedores de internet	-
	▪ Un módem	
	▪ Un conversor de fibra óptica	
1	Sistema de detección de incendios	▪ Marca: Chemetron ▪ Panel de Control: Micro 1012
2	Sistemas de aire acondicionado	▪ Aire acondicionado marca Lenux ▪ Sistema de aire acondicionado de precisión Marca Liebel
1	Sistema de seguridad física del cuarto de comunicaciones	▪ Marca: iGuard LM Series
2	Monitores	▪ Un monitor Samsung ▪ Un monitor Hacer

4	UPS14 (Sistema de Alimentación Ininterrumpida)	<ul style="list-style-type: none"> ▪ UPS Marca PowerWare 9170 Plus de 12KVA ▪ UPS Marca Tripplite de 3KVA ▪ UPS Marca APP de 1.5 KVA
1	Tablero PDU	

Fuente: (Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, 2015)

- ***Cableado Horizontal o de distribución***

Se utiliza cable UTP Categoría 6, permite interconectar el backbone con las áreas de trabajo. Para los equipos terminales, se tienen cajetines sobrepuestos para tomas simples y dobles, con tapas de protección para las salidas RJ-45 para voz y datos.

La interconexión del cableado horizontal entre el edificio principal y el edificio antiguo al correspondiente backbone, se encuentra sobre el cielo falso utilizando las bandejas metálicas y para los puntos de las áreas de trabajo está distribuido con canaletas.

- ***Cableado Vertical o Backbone***

Este cableado cumple la función de interconectar el cableado de distribución de cada uno de los diferentes pisos del edificio principal con la utilización de fibra óptica y cable UTP con cada uno de los equipos de comunicación que se encuentran en el Data Center.

El backbone del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra se interconecta con los equipos de comunicación que se sitúan en: el edificio antiguo, la dirección de Turismo y la dirección de Cultura mediante fibra óptica, éstos llegan al área de distribución principal MDF, ubicada en el departamento de Gestión de Tecnologías de la Información edificio principal. Las áreas de distribución secundarias SDF se encuentran en: el edificio antiguo primera planta, en la primera planta de dirección de turismo y en la dirección de cultura en la tercera planta.

La fibra óptica es de tipo multimodo para la conexión entre las dependencias externas del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra y monomodo entre

entidades independientes. Presenta una certificación ISO 9001 y cumple con las especificaciones ISO/IEC 11801 certificación Tier 1 en fibra óptica.

- Áreas de trabajo.

Los dispositivos terminales como son computadoras, impresoras y teléfonos utilizan patch cord UTP categoría 6/Clase E, con conectores RJ-45 a los dos lados cumpliendo con las normas del cableado estructurado EIA y TIA.

- **Topología Física de la Red de Datos del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra**

Para conocer y determinar los equipos que soportan el protocolo IPv6, es importante conocer la situación actual de la infraestructura física. En la actualidad, la red es capaz de transmitir y receptor señales de voz, datos y video, acceso a Internet y también permite la compartición de archivos.

De la misma manera internamente posee servicios como correo interno institucional, consultas de los correspondientes sistemas prediales, sistemas administrativos, financieros, entre otros servicios que favorecen al desempeño de las actividades de la entidad. Todo se maneja con el protocolo IPv4, más no se tiene ninguna relación de convivencia con el protocolo IPv6.

De la misma manera, se puede ver la conexión del switch core con fibra óptica con el enlace del proveedor Telconet, que proporciona un ancho de banda de 18 Mbps al Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra También la conexión de los servidores físicos albergados en el Data Center. Aunque en este proyecto no se tomen en cuenta los enlaces inalámbricos, se los puede visualizar y son los enlaces conectados de color rojo. En la Figura 23, se describe la estructura física de la red local de datos, en la cual se pueden visualizar las conexiones de los enlaces LAN que van hacia los edificios de las dependencias tanto internas como externas.

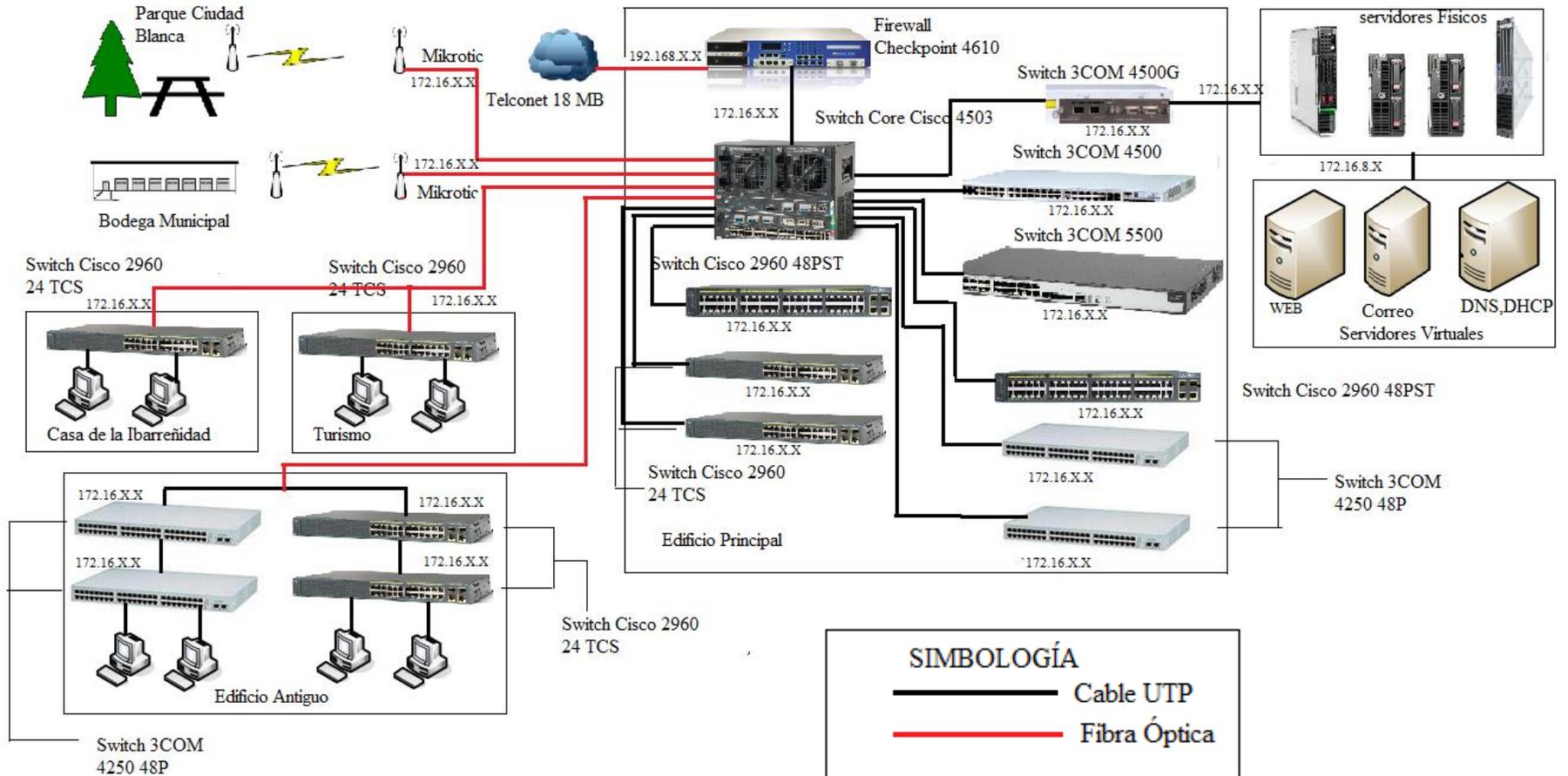


Figura 23: Topología Física de la Red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra

Fuente: Departamento de Gestión de la Información Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra

- **Análisis de la infraestructura lógica de la red de datos:**

La LAN del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, dispone un direccionamiento IPv4 Clase B (172.X.X.X) con una máscara de red 255.255.248.0 que por el momento satisface la capacidad de usuarios que maneja la entidad y mediante el equipamiento existente garantiza la disponibilidad de sus servicios, además permite a la red un gran crecimiento y escalabilidad.

Para una mejor administración de la red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, se ha distribuido la red en VLAN's. En la tabla 6 se detalla la distribución de cada una de ellas con su correspondiente direccionamiento IPv4.

Tabla 6. Descripción de las VLAN's del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra

NOMBRE VLAN	ID VLAN	RED	GATEWAY	INTERVALOS
Servidores	2	172.16.8.0	172.16.8.1	172.16.8.2 - 172.16.8.62
Admin. Equipos	3	172.16.8.64	172.16.8.1	172.16.8.65 - 172.16.8.126
Dirección Informática	4	172.16.8.128	172.16.8.1	172.16.8.129 - 172.16.8.190
Alcaldía	5	172.16.8.192	172.16.8.1	172.16.8.193 - 172.16.8.254
Auditoria interna	6	172.16.9.0	172.16.9.1	172.16.9.2 - 172.16.9.62
Procuraduría	7	172.16.9.64	172.16.9.1	172.16.9.65 - 172.16.9.126
Planificación	8	172.16.9.128	172.16.9.1	172.16.9.129 - 172.16.9.190
Comunicación	9	172.16.9.192	172.16.9.1	172.16.9.193 - 172.16.9.254
Secretaria General	10	172.16.10.0	172.16.10.1	172.16.10.2 - 172.16.10.62
Finanzas	11	172.16.10.64	172.16.10.1	172.16.10.65 - 172.16.10.126
Recursos Humanos	15	172.16.10.128	172.16.10.1	172.16.10.129 - 172.16.10.190
Avalúos	18	172.16.10.192	172.16.10.1	172.16.10.193 - 172.16.10.254

Administración	20	172.16.11.0	172.16.11.1	172.16.11.2 - 172.16.11.62
Obras Públicas	21	172.16.11.64	172.16.11.1	172.16.11.65 - 172.16.11.126
Participación Ciudadana	22	172.16.11.128	172.16.11.1	172.16.11.129 - 172.16.11.190
Cultura	23	172.16.11.192	172.16.11.1	172.16.11.193 - 172.16.11.254
Seguridad	28	172.16.12.0	172.16.12.1	172.16.12.2 - 172.16.12.62
Turismo	30	172.16.12.64	172.16.12.1	172.16.12.65 - 172.16.12.126
Mercado	31	172.16.12.128	172.16.12.1	172.16.12.129 - 172.16.12.190
Higiene	32	172.16.12.192	172.16.12.1	172.16.12.193 - 172.16.12.254
Proyecto C.N.H	33	172.16.13.0	172.16.13.1	172.16.13.2 - 172.16.13.62
Concejales	34	172.16.13.64	172.16.13.1	172.16.13.65 - 172.16.13.126
Wireless Municipio	35	172.16.13.128	172.16.13.1	172.16.13.129 - 172.16.13.190
Wireless-Ibarra Digital	36	172.16.13.192	172.16.13.1	172.16.13.193 - 172.16.13.254
Cámaras	37	172.16.14.0	172.16.14.1	172.16.14.2 - 172.16.14.62
Telefonía	38	172.16.14.64	172.16.14.1	172.16.14.65 - 172.16.14.190
Enlace de Equipos	39	172.16.14.192	172.16.14.1	172.16.14.193 - 172.16.14.254
Biométricos	40	172.16.15.0	172.16.15.1	172.16.15.2 - 172.16.15.62

Fuente: Dirección de Gestión de Tecnologías de la Información

- **Proveedor de Internet**

El Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, tiene como proveedor de Internet a Telconet, con un ancho de banda de 18 Mbps. Posee enrutamiento con IPv4, pero no para IPv6. Para obtener un bloque IPv6, es necesario que el administrador de la red, realice el pedido al proveedor de Internet, Telconet es el ISP, que maneja ya IPv6 en las redes y

proporcionará un direccionamiento IPv6 con un /48, porque es el rango que se asigna a las empresas, en este caso a la entidad gubernamental.

- **Descripción General de los Equipos del Data Center**

El cuarto de equipos del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra se encuentra ubicado en el departamento de Gestión de Tecnologías de la Información, cabe recalcar que aquí llegan todas las conexiones directamente para ser administradas a cada equipo. A continuación, se va a detallar los principales equipos que se encuentran albergados en el mismo:

- **Firewall Checkpoint 4610**

Hoy en día, la seguridad de las redes, es un punto muy importante que debe garantizar la protección de la información. El Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, dispone de un firewall Checkpoint serie 4610 que es un dispositivo de seguridad que filtra cada vez un mayor número de amenazas sofisticadas. Como una puerta de enlace de seguridad empresarial se debe utilizar varias tecnologías para el control de acceso a la red, detectar ataques sofisticados y proporcionar capacidades de seguridad adicionales, como la prevención de pérdida de datos y la protección de las amenazas basadas en la Web. (CHECKPOINT, 2015)

La marca Point, combinan tecnologías de redes rápidas con alto rendimiento que proporciona capacidades de multi-núcleo del más alto nivel de seguridad sin comprometer la velocidad de la red para mantener sus datos, la red y los empleados seguro. Cada aparato es capaz de ejecutar cualquier combinación de software cuchillas de proporcionar la flexibilidad y el nivel exacto de seguridad para cualquier negocio en todos los puntos de la red mediante la consolidación de múltiples tecnologías de seguridad en una única solución integrada. (CHECKPOINT, 2015)

En el **Anexo A**, se indican las características más importantes de cada uno de los equipos.

- **Switches**

Estos dispositivos de red, permiten dividir una gran LAN en los segmentos que sean necesarios. En la tabla 7, se describen las características más importantes de los mismos que se utilizan en el Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra. En el **Anexo A**, se describen las especificaciones técnicas de estos switches para verificar si tienen el soporte de IPv6.

Tabla 7. Descripción de Switches Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra

Switch	Características Generales	Memoria	Función
Cisco Catalyst 4503- E	48 GigaEthernet 10/100/1000 Mbps 8 puertos SPF 1000 BASE-T Conmutador: Capas 2, 3 y 4	RAM: 256MB FLASH: 32MB	Interconexión entre dependencias externas e internas con fibra óptica y UTP.
Cisco Catalyst 2960	24/48 FastEthernet 10/100 Mbps 2 Giga Ethernet:10/100/1000 Mbps Conmutador: Capa 2	RAM: 64 MB, FLASH: 32MB	Conectan los segmentos de red del edificio principal
3COM 4500 G	24 GigaEthernet 10/100/1000 Mbps 4 puertos de uso dual 10/100/1000 Conmutador: Capas 2, 3	FLASH: 28MB	Interconectan los servidores físicos del cuarto de comunicaciones
3COM 5500 SI	48 Fast Ethernet - 10/100 Mbps 4 Giga Ethernet - 1000 Mbps Conmutador: Capas 2, 3	-	Utilizado para interconectar los segmentos de red del edificio principal
3COM 4500	48 Fast Ethernet - 10/100 Mbps 2 Giga Ethernet – 1000 Mbps Conmutador: Capas 2, 3	SDRAM: 64 MB FLASH: 8 MB	Interconectan los segmentos de red del edificio principal
3COM 4250T	48 Fast Ethernet -10/100 Mbps 2 Giga Ethernet - 10/100/1000 Mbps Conmutador: Capa 2	-	Interconectan los segmentos de red del edificio principal

Fuente: Dirección de Gestión de Tecnologías de la Información

- Servidores Físicos y Virtuales

Los servidores físicos albergan a los servidores virtuales y en la Tabla 8 se detalla la distribución de cada uno de ellos en forma muy general, y se va a dar prioridad a los servidores WEB y correo electrónico como ya se había planteado, dando una mayor explicación.

Tabla 8. Descripción de los Servidores Físicos y Virtuales

Servidor	Tipo	Sistema operativo	Memoria RAM y Capacidad	Procesador	Función
SERVIDOR HP BL 460 G6	Físico	Debian 6.0.1	Memoria: 8 GB Disco Duro: 1.4 TB	Intel(R) Xeon(R) E55600 @ 2.8GHz	Se considera el master de virtualización para gestión de servidores
FREE NAS	Virtual	FreeNAS	Memoria: 1 GB Disco Duro: 1.4 TB	2	Permite simplificar el mantenimiento de los datos
SERVIDOR DOCUMENTAL	Virtual	Debian 7.0.1	Memoria:1 GB Disco Duro: 40 GB	2	Almacena documentos electrónicos
SERVIDOR SUBVERSIÓN GID	Virtual	Debian 7.0.1	Memoria:1 GB Disco Duro: 30 GB	2	Modificación de versiones antiguas-actuales
SERVIDOR CONTROL DE PERSONAL	Virtual	Windows Server 2003	Memoria:1 GB Disco Duro: 20 GB	2	Control de Personal de la entidad
SERVIDOR HP BL 460 G6	Físico	Debian 6.0.1	Memoria: 16 GB Disco Duro: 683 GB	Intel(R) Xeon(R) E55600 @ 2.8GHz	Master de virtualización para gestión de servidores
SERVIDOR REPOSITORIOS	Virtual	Debian 6.0.1	Memoria:2 GB Disco Duro: 292 GB	1	Evita descargar paquetes nuevamente
SERVIDOR DE CORREO	Virtual	Centos 7	Memoria:2 GB Disco Duro: 176 GB	2	Correo institucional con la herramienta zimbra
SERVIDOR DE SERVICIOS DE RED	Virtual	Centos 7	Memoria: 1 GB Disco Duro: 10 GB	2	Funciones de DNS (Servidor de Dominio de Nombres) y DHCP (Direccionamiento IP dinámico)
SERVIDOR DE REDMINE	Virtual	Debian 6.0.1	Memoria: 512 MB Disco Duro: 15 GB	1	Para el seguimiento de errores y gestión de proyectos (aplicaciones web)
SERVIDOR NTP	Virtual	Debian 6.0.1	Memoria: 256 MB Disco Duro: 5 GB	1	Para la sincronización de relojes de sistemas computacionales a través de red

SERVIDOR DE VENTANILLA ÚNICA	Virtual	Ubuntu 10.0.4	Memoria:1 GB Disco Duro: 10 GB	4	Aplicación web en Java para cobros y registros, en ventanilla
SERVIDOR SRI	Virtual	Windows Server 2003	Memoria:1 GB Disco Duro: 50 GB	2	Transacciones SRI
SERVIDOR WEBSERVICE	Virtual	Debian 7	Memoria:512 MB Disco Duro: 5 GB	1	Comunicación de servicios web con instituciones financieras
SERVIDOR HP 160 G5 (Srv3)	Físico	Debian 5.0.1	Memoria:4 GB Disco Duro: 250 GB	Procesador Intel Xeon 2.0 GHz	Master de Virtualización para Gestión de servidores. Permite emular hardware para cada servidor.
SISTEMA DOCUMENTAL QUIPUX	Virtual	Debian 5.0.1	Memoria:1 GB Disco Duro: 50 GB	2	Para sistema documental interno.
SERVIDOR DE BALANCE SCORD CARD	Virtual	Windows Server 2000	Memoria: 256 MB Disco Duro: 10 GB	2	Administrador de gestión de proyectos
SERVIDOR PROMOX HP DL 380 G5 (Srv5)	Físico	PROMOX	Memoria:8 GB Disco Duro: 100 GB	Intel(R) Xeon(TM) CPU 3.60GHz	Servidor Master de virtualización para gestión de servidores.
SERVIDOR DE BASE DE DATOS POSTGRES Pruebas (deb101)	Virtual	Debian 5.0.1	Memoria:2 GB Disco Duro: 80 GB	4	Base de Datos de prueba
SERVIDOR MOODLE	Virtual	Debian 5.0.1	Memoria:512 MB Disco Duro: 20 GB	1	Sistema de gestión de aprendizaje
SERVIDOR HP BL 460 G8	Físico	Debian 7.0.1	Memoria:47 GB Disco Duro: 300 GB	Xeon(R) CPU E5-2650 0 @ 2.00GHz	
SERVIDOR APLICACIONES WEB	Virtual	Debian 7.0.1	Memoria:4 GB Disco Duro: 32 GB	4	Proporciona servicios de aplicación a los usuarios
SERVIDOR VIRTUAL MAPAS (MAPSERVER)	Virtual	Debian 7.0.1	Memoria:8 GB Disco Duro: 22 GB	8	Servidor de mapas. Aplicaciones web.

SERVIDOR BDD POSTGIS	Virtual	Debian 7.0.1	Memoria:8 GB Disco Duro: 102 GB	8	Servidor de base de datos basado en Postgres para aplicaciones Geoespacial.
SERVIDOR SISTEMA DOCUMENTAL QUIPUX (MIGRAR)	Virtual	Debian 7.0.1	Memoria: 4 GB Disco Duro: 60 GB	4	Servidor documental
SERVIDOR DE BDD POSTGRESQL	Físico	Debian 5.0.1	Memoria: 8 GB Disco Duro: 440 GB	Intel(R) Xeon(TM) CPU 3.60GHz	Usado para aplicaciones internas municipales Sistema de Base de Datos
SERVIDOR DE APLICACIONES TERCEROS OLYMPO	Físico	Windows Server 2003	Memoria: 3 GB Disco Duro: 101 GB	Intel(R) Xeon(TM) CPU 3.20GHz	Aplicaciones de escritorio para Windows de terceros
SERVIDOR DE ANTIVIRUS	Físico	Windows Server 2003	Memoria:1 GB Disco Duro: 80 GB	Intel Pentium 4	Antivirus de la entidad

Fuente: Dirección de Gestión de Tecnologías de la Información

- **Equipamiento en el edificio antiguo**

Se encuentra un rack en la primera planta del edificio antiguo, tiene 19 pulgadas y permite la comunicación con todos los departamentos del edificio y llega al edificio central a través del backbone de fibra óptica. En la Tabla 9 se indican los equipos de comunicación que se encuentran en este lugar:

Tabla 9. *Descripción de Equipos en Edificio Antiguo*

Nro.	Dispositivo	Modelo	Descripción General
		Cisco Catalyst 2960	Puertos Fast Ethernet: 24 (10 /100) Conexión: permite la conectividad con el cuarto de equipos a través de fibra óptica.
		Cisco Catalyst 2960	Puertos Fast Ethernet: 24 (10 /100) Conexión: está en stack con el switch Cisco 2960 anterior.
4	Switch Administrables	Superstack 3COM, 3C16471	Serie Puertos Fast Ethernet: 24 (10 /100) Conexión: brinda conectividad a una parte del edificio antiguo.
		3COM 4250T, 3C17302	Serie Puertos Fast Ethernet: 48 (10 /100) Conexión: brinda conectividad a una parte del edificio antiguo.
4	Patch panel		Un patch panel de 24 puertos y dos patch panel de 48 puertos Marca: HUBBEL Para cableado UTP Categoría 6
1	Patch Panel de Fibra		Conexión: Permite establecer un enlace de fibra óptica con el Data Center. Utiliza un hilo de fibra monomodo
6	Organizadores de cable UTP		Permiten distribuir de mejor manera el cableado de la red.

Fuente: Dirección de Gestión de Tecnologías de la Información

- **Equipamiento en la casa de la Ibarreñidad**

Localizado en la segunda planta en el departamento de Cultura, es un rack cerrado de 19 pulgadas y permite conectividad entre los departamentos de Cultura y el departamento del Proyecto

parque ciudad Blanca con el cuarto de equipos del edificio principal. En la Tabla 10 se indican los elementos que se encuentran en el rack:

Tabla 10. *Descripción del Equipamiento en la casa de la Ibarreñidad*

Nro.	DISPOSITIVO	DESCRIPCIÓN
1	Switch Administrable	Modelo: CISCO 2960 Puertos Fast Ethernet: 24 Puertos Gigabit Ethernet: 2 Conexión: Permite la conectividad mediante fibra óptica con el cuarto de equipos del edificio principal. Además, interconecta los segmentos de red de la unidad de cultura, y proyecto parque ciudad blanca
1	Patch Panel	Patch Panel de 24 puertos para cableado UTP Categoría 6
1	Patch Panel de Fibra óptica	Permite la conectividad con el cuarto de equipos del edificio principal
1	Organizadores de cable UTP	Permiten distribuir de mejor manera el cableado de la red.

Fuente: Dirección de Gestión de Tecnologías de la Información

- **Acceso a usuarios finales**

Para los usuarios finales, se tiene acceso a los recursos de la red mediante computadores de escritorio y computadores portátiles que aproximadamente suman unos 26 portátiles y 390 de escritorio, contabilizando tanto las dependencias internas como externas.

3.2.2.2 Análisis de Hardware o Equipamiento de la Red. A continuación, se va a detallar el inventario de Hardware proporcionado por el Departamento de Tecnologías Informáticas, en el cual se encuentran los equipos de comunicaciones de red y cada uno de ellos con las respectivas características las cuales se van a analizar detenidamente:

- ✚ **Tiempo de uso/ años:** Los equipos de red, tienen una vida útil de tres años, es decir su funcionamiento va a ser óptimo en este tiempo, pero no deben sobrepasar los diez años de uso. (Universidad Técnica Particular de Loja, 2010)
- ✚ **Sistema operativo IOS:** Las versiones desde 12.0()TS o T en adelante, tienen el soporte IPv6. (CISCO, 2016)

Por lo tanto, en el inventario realizado, los equipos switch marca 3COM, deben ser sustituidos, por no soportar las características para el buen desempeño de la red con IPv6. El equipamiento CISCO, funciona correctamente y sus IOS son compatibles con IPv6. En caso de tener un IOS, distinto se recomienda actualizarlo a versiones superiores a la 12.0()TS.

En cuanto a los servidores físicos, se puede decir que están actualizados los sistemas operativos que albergan a los servidores virtuales. Po lo tanto el análisis propio de cada sistema operativo se analiza en el siguiente punto.

El inventario en cuanto a hardware, permitirá a la presente administración de la red conocer los equipos aptos para la implementación del nuevo protocolo, o para actualizaciones en cualquier equipo que no disponga de las características que se ha analizado en este apartado. De la misma manera, en el **Anexo A**, se encuentra más detallado las características de los equipos y el soporte para IPv6.

3.2.2.3 Análisis de Software de los Equipos. El software o sistemas operativos de los servidores, computadoras, en los cuales se encuentran los servicios y aplicaciones es importante que también sea verificado por lo tanto el inventario en cuanto a software es el siguiente:

Se ha realizado un análisis en cuanto a los sistemas operativos que manejan los servidores virtuales y las computadoras de los usuarios que tiene el Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, en la que la mayoría de usuarios finales utilizan en sus computadoras Windows 7 y Windows 8, y tienen el soporte para IPv6.

3.2.2.4 Selección de los servicios y aplicaciones seleccionadas para IPv6. Como se ha propuesto la transición de IPv4 a IPv6 para los servicios WEB y Correo Electrónico, se ha explicado ya la importancia que tienen para la entidad por lo tanto tener en consideración las siguientes recomendaciones:

- ✓ Se debe tener en cuenta de que dependen los otros servicios, por ejemplo, en el caso de servidor WEB, depende del servidor de base de datos, por lo tanto, este servicio también debe tener compatibilidad con IPv6.
- ✓ Debe existir la compatibilidad IPv4/IPv6, ya que algunos servicios no van a poder manejar los dos protocolos, por eso, hasta que adopten IPv6 elegir un mecanismo que permita mantener coexistencia entre estos dos protocolos.

3.2.2.5 Pool de direcciones IPv6. Debe realizarse el pedido al proveedor de servicios Telconet. Este ISP, actualmente maneja y permite tener direccionamiento IPv6, el administrador de la red, debe realizar el trámite requerido para la asignación de un bloque IPv6. En caso de que no tuvieran este soporte, existe el trámite directo en la página de LACNIC: <http://www.lacnic.net/web/lacnic/ipv6-end-user>.

3.2.2.6 Análisis del protocolo de seguridad IPsec para IPv6. IPsec (Internet Protocol Security), es un estándar creado por la IETF que permite proporcionar niveles de seguridad a la capa de red IP y a otros protocolos de capas superiores como TCP, UDP, entre otros. IPsec tiene soporte para IPv4 como para IPv6, pero en IPv4 el uso no es obligatorio, mientras que para IPv6 está integrado y su uso es obligatorio.

Los principales servicios de seguridad que IPsec proporciona son:

- **Integridad:** Aquellos paquetes que no han sido cambiados o modificados en el trayecto de la comunicación.
- **Confidencialidad:** Se garantiza que el contenido de los paquetes solo sea conocido tanto por el emisor y por el receptor.
- **Autenticidad:** Se dice que el emisor del mensaje, es quien dice ser.

Para la implementación de este protocolo IPsec en la red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, se va a realizar utilizando ESP modo túnel. Es importante considerar que este protocolo se puede implementar en usuarios finales, en servidores o como en este caso que será implementado en los gateways de los switches. Para una mejor comprensión de la aplicación de este protocolo se va a detallar en las pruebas de funcionamiento que se han realizado para la red del municipio de Ibarra.

SSL, de la misma forma es el protocolo de seguridad que se implementa en las comunicaciones de la entidad, pero frente a IPsec, ¿cuál sería el más eficaz? Pues se van a determinar las características más importantes en la Tabla 11.

Tabla 11: *Comparación de SSL e IPsec*

Características	SSL	IPsec
Aplicaciones	Habilitadas en web, uso compartido de archivos, correo electrónico	Soportado para todas las aplicaciones IP.
Cifrado	En la escala de moderado a seguro debido a la longitud de clave de 40 a 256 bits.	En la escala de seguro, porque la longitud de claves es de 56 a 256bits.
Autenticidad	En la escala moderada, es unidireccional o bidireccional.	En la escala segura, debido a autenticación bilateral mediante secretos compartidos o con certificados digitales.

Complejidad de Conexión	En la escala baja porque se requiere de un navegador Web.	En la escala media debido a que puede resultar complicado sin los suficientes conocimientos técnicos.
Opciones de conexión	Cualquier dispositivo se puede conectar	Ciertos dispositivos con configuración específica

Fuente: Recuperado de: <http://ecovi.uagro.mx/ccna4/course/module7/7.4.2.4/7.4.2.4.html>

IPsec supera a SSL en muchas formas importantes:

- La cantidad de aplicaciones que admite
- La solidez del cifrado
- La solidez de la autenticación
- La seguridad general

Cuando la seguridad representa un problema, IPsec es la mejor opción. Si el soporte y la facilidad de implementación son los principales problemas, considerar utilizar SSL. Pero en este proyecto se utilizará IPsec para verificar el funcionamiento con el protocolo IPv6.

3.2.2.7 Elección del mecanismo más eficiente para la transición de IPv4 a IPv6 para la red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra. Es importante recalcar, que la transición de IPv4 a IPv6, para los ISP's y las empresas deben realizarla gradualmente y de la misma manera se debe mantener la interoperabilidad si esta llegara a efectuarse. Es por ello que se busca un mecanismo de transición que permita preservar las grandes inversiones que se han realizado en redes IPv4, y los mecanismos que se han revisado en el capítulo II permiten que las redes IPv4 con IPv6 mantengan interconexión entre ellas.

La migración de IPv4 a IPv6, puede ser complejo en grandes organizaciones, pero utilizando varias estrategias o mecanismos de convivencia van a ayudar en este proceso de transición. El objetivo de que este proceso se llegara a realizar, es con la finalidad de que los costos de transición y el impacto que produzca en una organización o empresa sean mínimos.

Para explicar las ventajas y desventajas de cada uno de los mecanismos estudiados, se va a presentar la Tabla 12 (comparativa) de cada uno de ellos para una correcta selección de transición:

Tabla 12: *Comparación de Mecanismos de Transición*

MECANISMOS DE TRANSICIÓN		
	Ventajas	Desventajas
Dual Stack	<ul style="list-style-type: none"> • Fácil de implementar. • Solución inmediata más accesible. • No hay necesidad de traducción ni encapsulamiento • Si falla la red IPv4, estará disponible la IPv6, y viceversa. 	<ul style="list-style-type: none"> • Se debe mantener dos redes. • No hay reducción de demanda de direcciones IPv4.
Túneles	<ul style="list-style-type: none"> • Soportan varias plataformas como CISCO, Linux, entre otros. 	<ul style="list-style-type: none"> • Se requieren conocer las dos direcciones IPv4 (origen y destino), las dos direcciones IPv6 (origen y destino), para la encapsulación. • Se necesita implementar dual Stack en cada uno de los puntos del túnel. • Requieren mayor configuración que la de los otros mecanismos. • Si se deja de manejar IPv4, esta infraestructura de red deberá migrar desde cero a IPv6.
Traducción	<ul style="list-style-type: none"> • Brinda escalabilidad a la red. • Permite el acceso a las dos redes en el caso de que un dispositivo IPv4 se quiera comunicar con un IPv6 y viceversa. 	<ul style="list-style-type: none"> • Se tienen los mismos problemas que NAT en IPv4. • Produce cuellos de botella. • Se pierden los beneficios de IPv6. • Tiene cierta incompatibilidad con algunas aplicaciones.

Fuente: (Cedeño., 2013)

Después de haber identificado ventajas y desventajas entre de los mecanismos de transición, se va a elegir el que permita que se ajuste a las características de la red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra. Es por eso, que se va a elegir el mecanismo doble pila o Dual Stack, debido a que permite implementar el protocolo IPv6 sobre una red de infraestructura IPv4.

De la misma manera, se puede manejar los dos protocolos conjuntamente, es decir, tener usuarios IPv4 que se conecten con otros IPv4 y usuarios que tengan IPv6 con otros que también manejen IPv6, permitiendo una transición de manera controlada que no se traduzca a un cambio instantáneo y permita que se realice por etapas. En la Figura 24 se explica el funcionamiento del mecanismo doble pila.

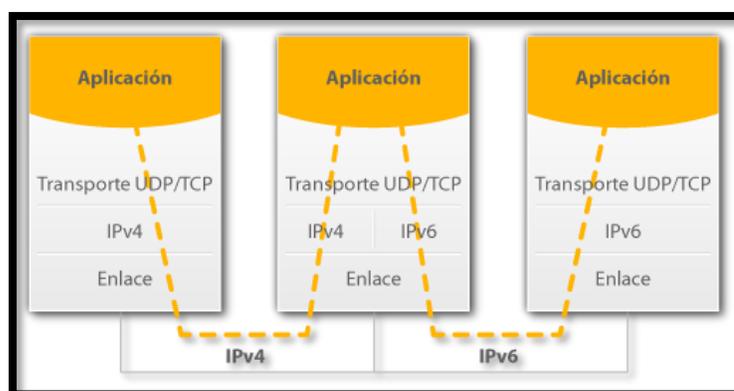


Figura 24: *Funcionamiento Dual Stack*

Fuente: Recuperado de <http://portalipv6.lacnic.net/mecanismos-de-transicion/>

Otros mecanismos que se van a utilizar son el NAT64 y el DNS64. Cuando la red es IPv6 nativa y necesita llegar a sitios que son sólo IPv4 se realiza una traducción usando NAT, mediante un mapeo entre los paquetes IPv6 e IPv4. Se utiliza un prefijo especial para mapear direcciones IPv4 a IPv6: 64:ff9b::/96, el cual se encuentra definido en el RFC 6052.

Es necesario también realizar una modificación al DNS, llamada DNS64, que permite generar un registro AAAA aun cuando el destino no tenga dirección IPv6 (es decir, el DNS responda sólo con registros de tipo A).

Los usuarios nativos IPv6 acceden directamente a internet o a la nube de aplicaciones IPv6, pero cuando se necesita ir desde un usuario nativo IPv6 hacia la nube de aplicaciones IPv4, NAT64 realiza el mapeo que se necesita para comunicar a estos usuarios. Al usar un prefijo /96 se consigue que se realice una asignación de los últimos 32 bits de una dirección IPv6 con los 32 bits de una dirección IPv4

Una dirección IPv6 se encuentra expresada en números hexadecimales, en cambio una dirección IPv4 está en números decimales, por tanto, NAT64 realiza el cálculo que permite la conversión. En la Figura 24 se evidencia el proceso de este mecanismo.

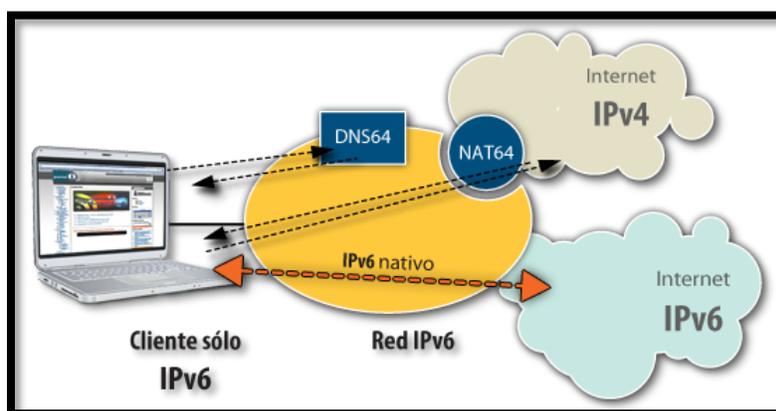


Figura 25: *Mecanismo de Traducción*

Fuente: Recuperado de <http://portalipv6.lacnic.net/mecanismos-de-transicion/>

3.2.2.8 Aspectos legales con IPv6.

- Situación Regulatoria: Acuerdo número 0133 del 25 de marzo del 2011 emitido por el MINTEL, señala que, las instituciones y organismos señalados en el art. 225 de la Constitución de la república del Ecuador, en la adquisición de equipamiento tecnológico, productos o aplicaciones a partir de la fecha señalada para el despliegue de IPv6, sean compatibles y tengan el soporte con el protocolo IPv6.
- Ley especial de telecomunicaciones No. 184 modificada el 13 de octubre del 2011, que está vigente: Indica que IPv6 es un aspecto a tener en cuenta refiriéndose a la explotación y

comercialización de servicios, y se debe homologar a los equipos para que empiecen a generar tráfico IPv6.

- En decreto No.1790 de la ley especial de telecomunicaciones, se establece que las redes públicas de telecomunicaciones tenderán a un diseño de red libre, es decir que no tengan protocolos ni especificaciones de tipo propietario de tal forma que se permita la interconexión con los planes emitidos por la CONATEL, indicando que IPv6 cuente como un requisito.
- Con respecto al resto de aspectos regulatorios de Cibercafés, buscapersonas, audio y video, radiofrecuencia, cable submarino, interconexión, comercio electrónico, redes de acceso universal de Internet, VoIP, telefonía, no hay cambios ni modificaciones, sin embargo, es indispensable que se empiece a incorporar en estos servicios que implementen IP, el protocolo IPv6. (Palet J. , 2011)

3.3.3 FASE III: Implementación y Análisis de pruebas

La etapa final en la que se realizan las configuraciones en los equipos y se realizan las pruebas necesarias de funcionamiento para la coexistencia de IPv4 con IPv6.

3.3.3.1 Plan de direccionamiento IPv6. El Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra al tener como proveedor de servicios de Internet a Telconet, puede realizar un pedido para obtener un pool de direcciones IPv6 a esta empresa, debido a que es uno de los ISP's en el Ecuador, que ya manejan sus redes con el nuevo protocolo. Este requerimiento es inmediato, debido a que ya manejan un bloque de asignación IPv4, por lo tanto, el bloque de asignación IPv6 debería ser concebido sin ningún inconveniente.

Telconet asignará al Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra un bloque de direccionamiento con prefijo /48. Para este caso de estudio, se va a utilizar la red 2001:0db8:20:x:x::/48, debido a que en el RFC 3849 estas direcciones están especificadas para

realizar pruebas de funcionamiento, por lo tanto pueden utilizarse para describir modelos de red , esto, mientras que se realice el trámite de petición de bloque IPv6.

En el momento que ya se haya obtenido el pool de direccionamiento IPv6, se procede a reemplazar al rango de dirección con el que se están realizando las pruebas respectivas. Para realizar el direccionamiento IPv6 es necesario distribuir las IP's de tal manera que permitan optimizar la utilización del recurso IPv6, a pesar de que se tienen suficientes direcciones y tomando en cuenta el RFC 4291, que recomienda que las subredes cuenten con una máscara de /64.

Sin embargo, se va a realizar el subnetting IPv6, para lo cual se va a utilizar los 16 bits del campo de subred, mientras que, el prefijo global otorgado por el ISP, en este caso 2001:db8:20:/48, va a permanecer fijo.

2001:db8:20:0000:0000:0000:0000:0000

Ahora se va a realizar el subnetting con los bits restantes, para lo cual, hay que tomar en cuenta que cada segmento de 16 bits tiene 4 decimales, y cada decimal es llamado un nibble. Estos se encuentran con un color como se indica en la dirección IPv6

2001:db8:20:0000:0000:0000:0000:0000

Una vez reconocidos los nibbles, se va a determinar la cantidad de usuarios con los que se cuenta en cada una de las vlans y así determinar la subred IPv6 correspondiente.

Se tienen 28 vlans, por lo tanto, se realiza el cálculo de 2^n , en este caso 2^5 , que son 32, las cuatro restantes se planifican para un futuro crecimiento.

Recordar que se debe realizar el subnetting con los bits del cuarto hexeto.

nibble 1	nibble 2	nibble 3	nibble 4
0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0

1 1 1 1 1 1 0 0 0 0 0 0 0 0 <----- $2^6=64$

Es importante que en el subnetting en IPv6 no se tomen bits individuales de un nibble, sino tomar el nibble completo, para evitar que el subneteo sea muy complejo. Esto significa que en realidad tendremos $2^8=256$ prefijos para 256 vlans.

El prefijo sería sumar a los 48 bits que ya están definidos los 8 bits de los dos nibbles, obteniendo así un prefijo /56. El cambio se realiza en el primer y segundo nibble, como se indica en la Tabla 13.

Tabla 13. *Subneteo de vlans en IPv6*

Servidores	2001:db8:20:0000::/56	Participación Ciudadana	2001:db8:20:0E00::/56
Admin. Equipos	2001:db8:20:0100::/56	Cultura	2001:db8:20:0F00::/56
Dirección Informática	2001:db8:20:0200::/56	Seguridad	2001:db8:20:1000::/56
Alcaldía	2001:db8:20:0300::/56	Turismo	2001:db8:20:2000::/56
Auditoría interna	2001:db8:20:0400::/56	Mercado	2001:db8:20:3000::/56
Procuraduría	2001:db8:20:0500::/56	Higiene	2001:db8:20:4000::/56
Planificación	2001:db8:20:0600::/56	Proyecto C.N.H	2001:db8:20:5000::/56
Comunicación	2001:db8:20:0700::/56	Concejales	2001:db8:20:6000::/56
Secretaria General	2001:db8:20:0800::/56	Wireless Municipio	2001:db8:20:7000::/56
Finanzas	2001:db8:20:0900::/56	Wireless-Ibarra Digital	2001:db8:20:8000::/56
Recursos Humanos	2001:db8:20:0A00::/56	Cámaras	2001:db8:20:9000::/56
Avalúos	2001:db8:20:0B00::/56	Telefonía	2001:db8:20:A000::/56
Administración	2001:db8:20:0C00::/56	Enlace de Equipos	2001:db8:20:B000::/56

Obras Públicas	2001:db8:20:0D00::/56	Biométricos	2001:db8:20:C000::/56
-----------------------	-----------------------	--------------------	-----------------------

Fuente: Elaboración propia con datos del Departamento de Tecnología e Informática

Luego se va a realizar la asignación para los usuarios de cada una de las Vlans, para ello se va a tomar el tercer y cuarto nibble, tomando en cuenta la cantidad de usuarios para cada uno. Se va a indicar la primera y segunda vlan, lo demás ya está sobreentendido. En la Tabla 14 se especifican las subredes y la cantidad de usuarios por cada subred de cada vlan.

Tabla 14. *Subredes Ipv6 con el correspondiente número de usuarios.*

NOMBRE VLAN	SUBREDES	# USUARIOS
Servidores	2001:db8:20:0000::/56	40
Admin. Equipos	2001:db8:20:0100::/56	5
Dirección Informática	2001:db8:20:0200::/56	15
Alcaldía	2001:db8:20:0300::/56	8
Auditoria interna	2001:db8:20:0400::/56	20
Procuraduría	2001:db8:20:0500::/56	11
Planificación	2001:db8:20:0600::/56	15
Comunicación	2001:db8:20:0700::/56	8
Secretaria General	2001:db8:20:0800::/56	4
Finanzas	2001:db8:20:0900::/56	7
Recursos Humanos	2001:db8:20:0A00::/56	9
Avalúos	2001:db8:20:0B00::/56	13
Administración	2001:db8:20:0C00::/56	6
Obras Públicas	2001:db8:20:0D00::/56	20
Participación Ciudadana	2001:db8:20:0E00::/56	14
Cultura	2001:db8:20:0F00::/56	12
Seguridad	2001:db8:20:1000::/56	7
Turismo	2001:db8:20:2000::/56	20
Mercado	2001:db8:20:3000::/56	18
Higiene	2001:db8:20:4000::/56	5
Proyecto C.N.H	2001:db8:20:5000::/56	13

Concejales	2001:db8:20:6000::/56	25
Wireless Municipio	2001:db8:20:7000::/56	60
Wireless-Ibarra Digital	2001:db8:20:8000::/56	18
Cámaras	2001:db8:20:9000::/56	60
Telefonía	2001:db8:20:A000::/56	100
Enlace de Equipos	2001:db8:20:B000::/56	40
Biométricos	2001:db8:20:C000::/56	30

Fuente: Elaboración propia con los datos del Departamento de Tecnologías e Informática

La Vlan servidores necesita IP's para 40 usuarios, para lo cual se va a utilizar 2^6 , que son 64, las 24 direcciones restantes, serán para un futuro crecimiento de la red. Se va a utilizar el tercer y cuarto nibble.

Servidores la subred es 2001:db8:20:0000::/56

Usuario 1 2001:db8:20:0000::/62

Usuario 2 2001:db8:20:0001::/62

Usuario 3 2001:db8:20:0002::/62

.....Hasta llegar al usuario 40

Usuario 40 2001:db8:20:002E::/62

La Vlan Admin. Equipos necesita IP's para 5 usuarios, para lo cual se va a utilizar 2^3 .

Admin. Equipos la subred es 2001:db8:20:0100::/56

Usuario 1 2001:db8:20:0100::/59

Usuario 2 2001:db8:20:0101::/59

Usuario 3 2001:db8:20:0102::/59

Usuario 4 2001:db8:20:0103::/59

Usuario 5 2001:db8:20:0104::/59

Y así sucesivamente con todas las subredes que se han creado, cuidadosamente utilizando el sistema hexadecimal para la asignación de cada IP.

3.3.3.2 Actualizaciones en Hardware y Software. En cuanto al hardware, se necesita adquirir nuevo equipamiento en caso de no cumplir con las especificaciones para el soporte IPv6, en este caso los switches de la marca 3COM, deben ser adquiridos y este análisis de costo se encuentra en el capítulo 4.

En el caso de software, para los equipos CISCO, que no tienen una versión igual o superior a la 12.0(TS), se debe efectuar la actualización del IOS, de la siguiente manera:

- 1.- Ingresar a la terminal del equipo
- 2.- Verificar la versión con el comando *#show versión*
- 3.- Descargar la .ISO por ejemplo: 12-2.55.SE1
4. Borrar la versión anterior con el comando *#delete /f/r flash1:c2960-ipbase-mz.122.35-35.SE5*
- 5.- Copiar la nueva versión con el comando *#copy tpft flash1*
- 6.- Escribir en la memoria, y reiniciar con los comandos *#write mem* y *#reload*.

Finalmente se habilita IPv6:

***** Habilitación de ipv6*****

```
Switch# configure terminal
```

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
```

```
Switch(config)# end
```

```
Switch# reload
```

```
*****
```

En el caso de software se va a tener en cuenta los siguientes sistemas operativos:

- ✓ Windows
- ✓ Linux

Instalación en Windows:

En algunas versiones, la habilitación de protocolo IPv6, está únicamente deshabilitada, para activarla en usuarios de Windows 7 en adelante se realizan las siguientes configuraciones:

1.- Dirigirse a la tarjeta de red, en este caso la inalámbrica y seleccionar propiedades como se indica en la Figura 26:

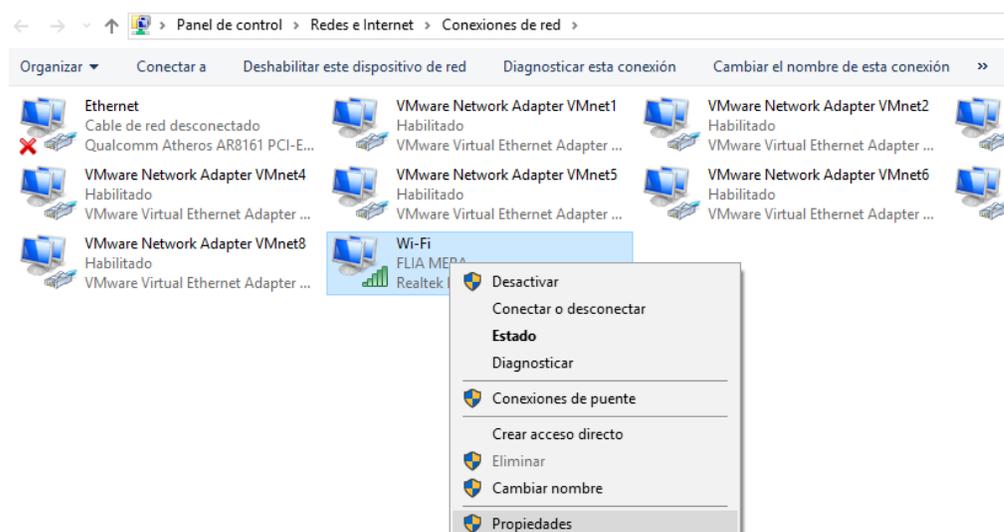


Figura 26: Acceso a configuraciones de tarjeta inalámbrica

Fuente: Captura propia extraída de Windows 7

2.- En la imagen derecha se encuentra deshabilitado, y en la segunda se activa la habilitación de IPv6 como se indica en la Figura 27.

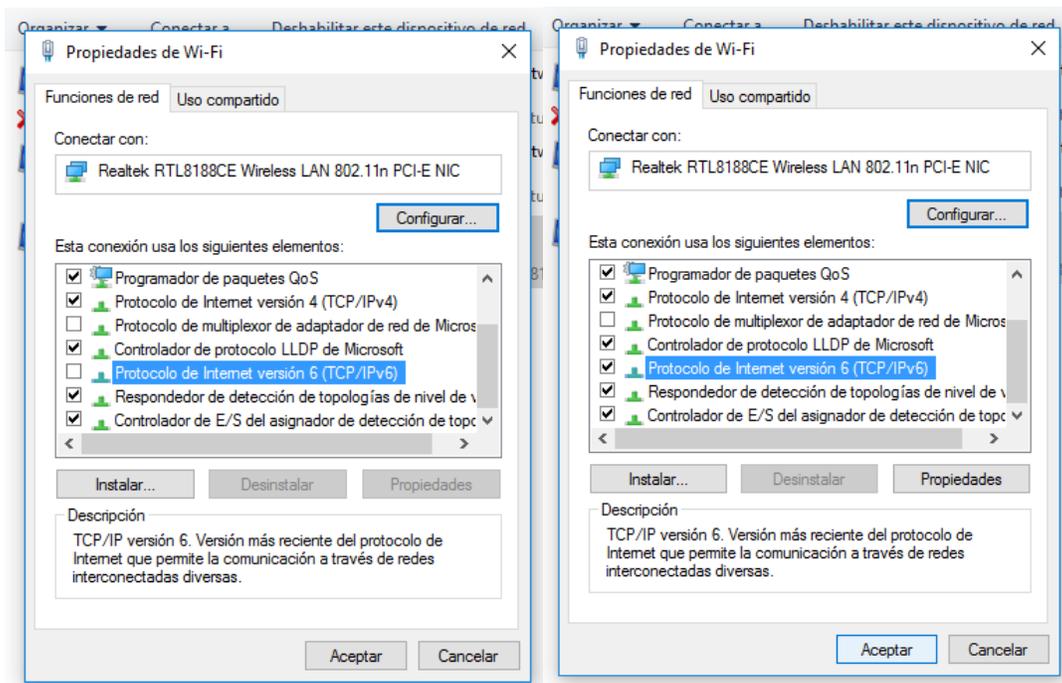


Figura 27: *Habilitación de IPv6 en Windows 7*

Fuente: Captura propia extraída de Windows 7

Estas configuraciones se realizan también en las versiones superiores a Windows 7, como la 8, 8.1 o la actual versión 10.

Instalación en Linux:

IPv6 está soportado a partir de versión del kernel 2.4.x.

Para comprobar si está instalado:

```
#test -f /proc/net/if_inet6 && echo "Kernel actual soporta IPv6"
```

Para instalar el módulo IPv6:

```
#modprobe ipv6
```

Se puede comprobar el módulo con:

```
#lsmod |grep -w 'ipv6' && echo "modulo IPv6 cargado" (Cicileo, 2009)
```

- **Configuración en Red Hat**

Añadir a */etc/sysconfig/network*:

```
NETWORKING_IPV6=yes
```

Reiniciar la red:

```
# service network restart
```

- **Configuración en Debian**

Con el módulo IPv6 cargado se edita */etc/network/interfaces*:

```
iface eth0 inet6 static
pre-up modprobe ipv6
address 2001:DB8:1234:5::1:1
```

Se reinicia o:

```
# ifup --force eth0
```

Con estos comandos y activaciones los equipos tanto en hardware como en software están listos para ser configurados con IPv6 y con el correspondiente mecanismo de transición elegido.

3.3.3.3 Configuraciones de los equipos con IPv6. En general, para los switches CISCO, que se encuentran en la topología de la red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, se debe habilitar IPv6 con los siguientes comandos:

```
*****Habilitación de protocolo IPv6*****
```

```
Switch# configure terminal
```

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
```

```
Switch(config)# end
```

Switch# reload

Para la configuración de los servidores, se ha realizado un manual de administrador en el que se indican las instrucciones de instalación de IPv6 en los servidores WEB, Correo Electrónico y en el DNS64NAT64, se encuentran en los **Anexos C, D y E**.

3.3.3.4 Pruebas de funcionamiento. Para el correspondiente plan de pruebas se va a realizar utilizando la siguiente topología indicada en la Figura 28

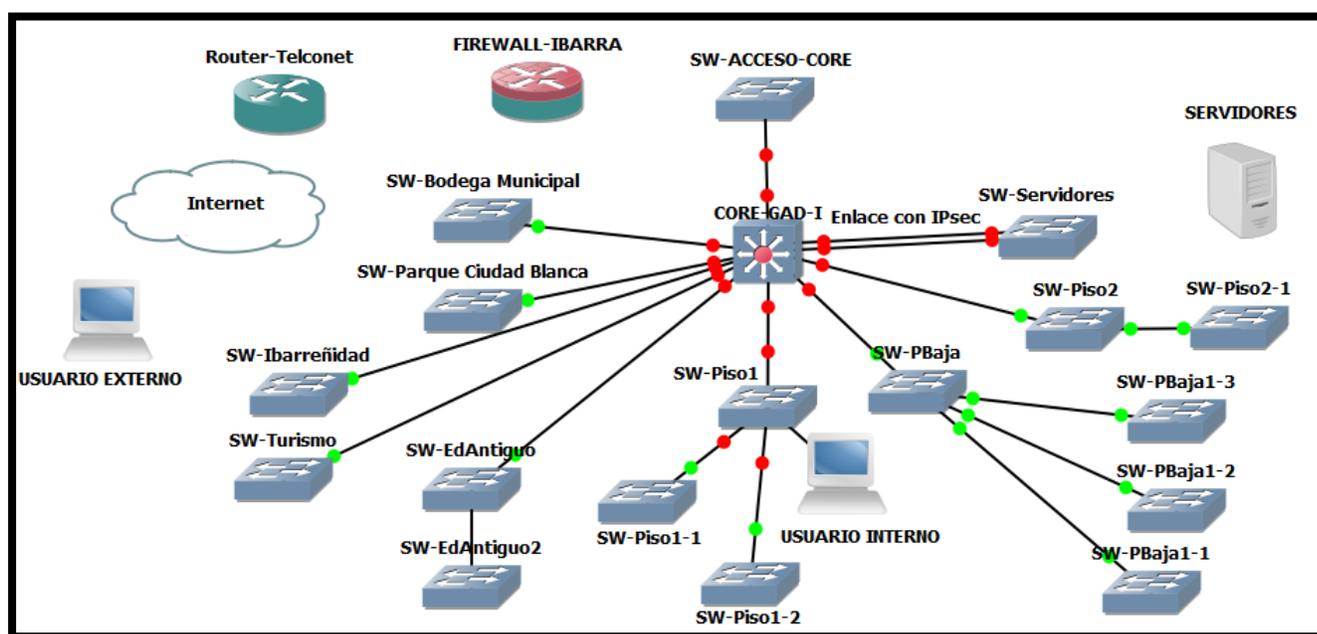


Figura 28. Topología planteada para el entorno propuesto del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra

Fuente: Captura propia extraída de software GNS3

Las Configuraciones realizadas son:

RED INTERNA:

- FIREWALL IBARRA: Doble pila.
- CORE, SW de acceso: Doble pila.
- Servidores: WEB (Sólo IPv4), DNS (servidor dns64nat64 doble pila), SMTP o Correo (Sólo IPv6), todos con sistema operativo Centos 6.7. La razón de utilizar estos sistemas

operativos, es porque se manejan bajo estos parámetros, así se permitirá presentar una propuesta para un entorno muy parecido al de la red de esta entidad.

- USUARIO INTERNO (Windows 10, Doble pila). Se utilizó este sistema operativo debido a que la mayor parte de los usuarios manejan Windows en cada una de las oficinas de los usuarios.

RED EXTERNA:

- Usuario IPv6 (Windows 7, Sólo IPv6). Se maneja este usuario con este sistema operativo debido a que como se conoce la mayoría de las personas lo utilizan.

✓ Configuración de la tarjeta de red para un usuario IPv4

Se configura la tarjeta del usuario con una dirección válida en IPv4.

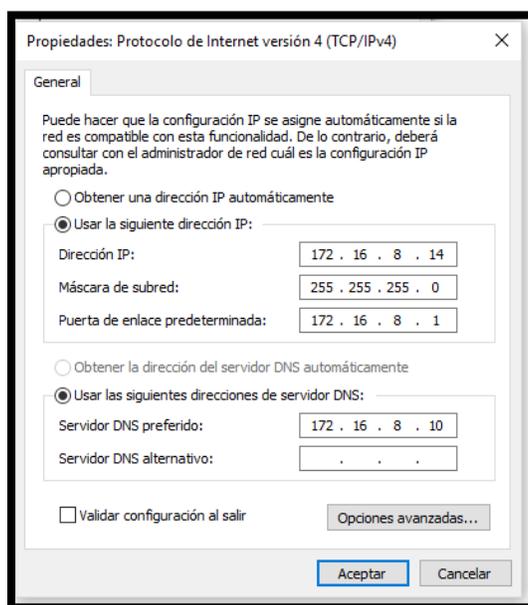


Figura 29. Configuración tarjeta de red con IPv4

Fuente: Captura propia extraída de sistema operativo windows 10

Se utiliza el comando `ipconfig /flushdns` que limpiará la cache para que resuelva sin problema el nuevo dominio configurado y con el comando `nslookup` se verifica que el servidor está

respondiendo a la petición. Como se puede observar responde al dominio dns.gad-i.gob.ec que es el que se encuentra configurado en el servidor DNS.

```
C:\Users\GABY>ipconfig /flushdns

Configuración IP de Windows

Se vació correctamente la caché de resolución de DNS.

C:\Users\GABY>nslookup
Servidor predeterminado: dns.gad-i.gob.ec
Address: 172.16.8.10
```

Figura 30. Verificación dominio en IPv4

Fuente: Captura propia extraída de sistema operativo Windows 10

✓ Configuración de la tarjeta de red para un usuario con IPv6

Se configura la IPv6 en el equipo

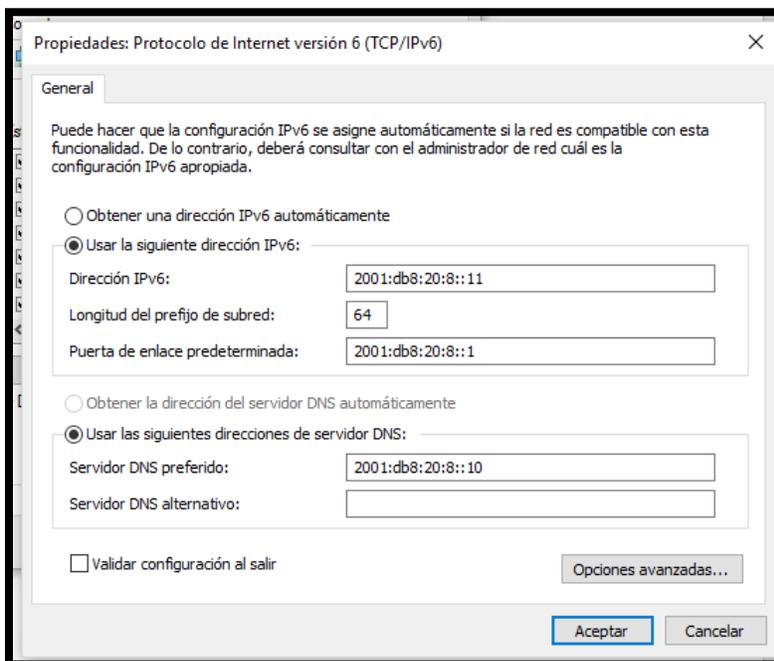
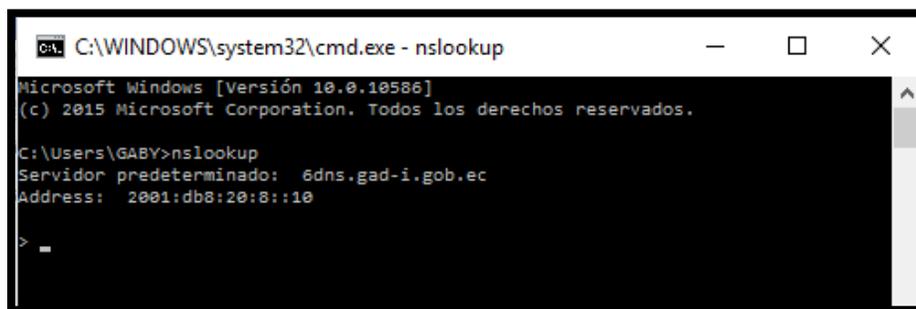


Figura 31. Configuración tarjeta de red con IPv6

Fuente: Captura propia extraída de sistema operativo Windows 10

Ahora de la misma manera, se ejecuta el comando nslookup para determinar cuál servidor y con qué Ip está resolviendo el dominio. Se observa que efectivamente es el IPv6



```

C:\WINDOWS\system32\cmd.exe - nslookup
Microsoft Windows [Versión 10.0.10586]
(c) 2015 Microsoft Corporation. Todos los derechos reservados.

C:\Users\GABY>nslookup
Servidor predeterminado: 6dns.gad-i.gob.ec
Address: 2001:db8:20:8::10

>

```

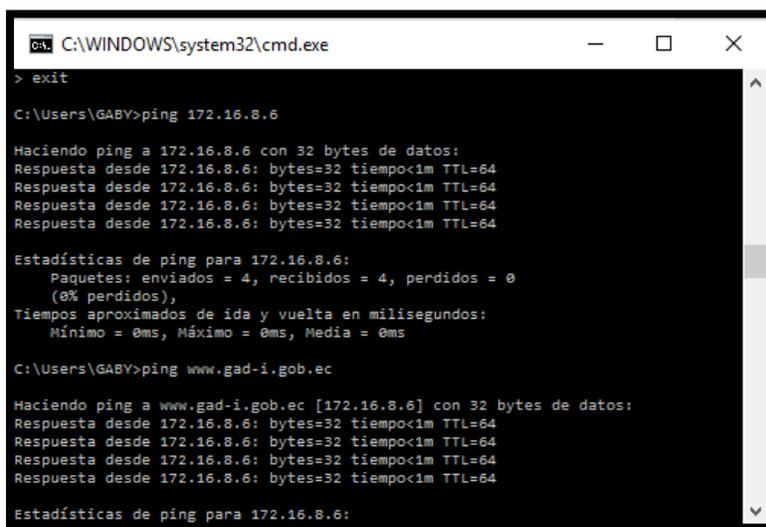
Figura 32. *DNS en IPv6*

Fuente: Captura propia extraída de sistema operativo Windows 10

- **Verificación de los servicios seleccionados**

Servidor WEB desde la red interna

Se realiza una solicitud ICMP o ping a la página del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra. Se puede observar que responde a esta petición el servidor configurado con IPv4, desde el usuario configurado con doble pila.



```

C:\WINDOWS\system32\cmd.exe
> exit

C:\Users\GABY>ping 172.16.8.6

Haciendo ping a 172.16.8.6 con 32 bytes de datos:
Respuesta desde 172.16.8.6: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 172.16.8.6:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\GABY>ping www.gad-i.gob.ec

Haciendo ping a www.gad-i.gob.ec [172.16.8.6] con 32 bytes de datos:
Respuesta desde 172.16.8.6: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 172.16.8.6:

```

Figura 33. *Verificación de conectividad con usuario Dual Stack*

Fuente: Captura propia extraída de sistema operativo Windows 10

Ahora se verifica el acceso a la página del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, tanto con el dominio como con la dirección IPv4.



Figura 34. *Página del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra con Dual Stack*

Fuente: Captura propia extraída de sistema operativo Windows 10

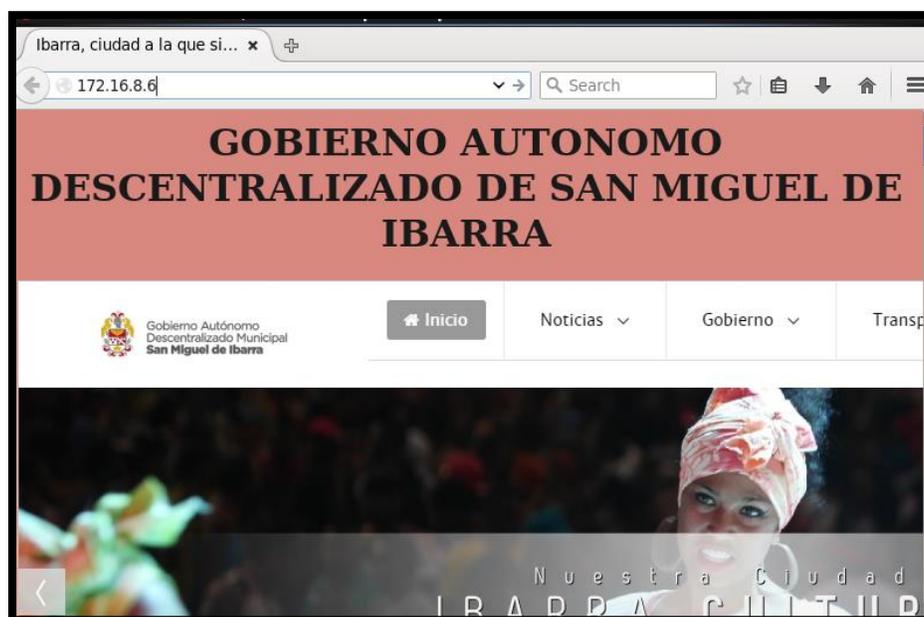
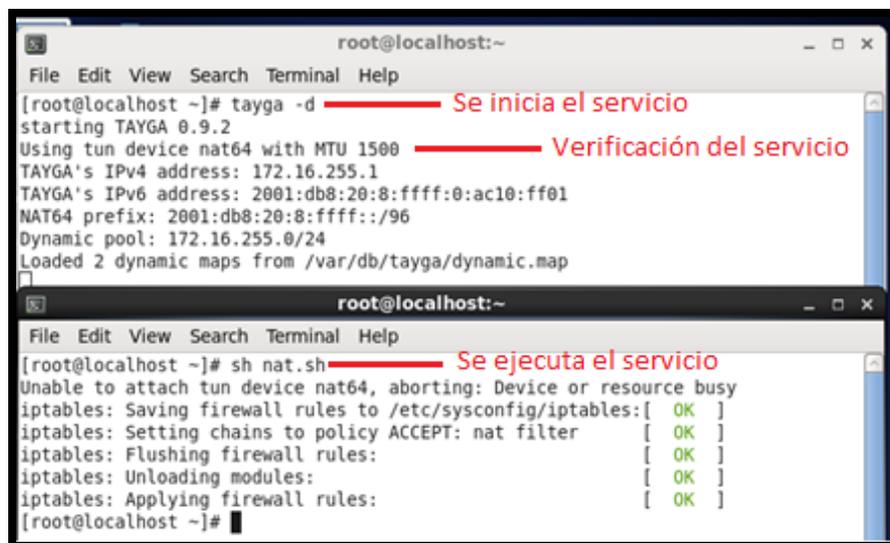


Figura 35. *Acceso a página Web con la dirección IPv4*

Fuente: Captura propia extraída de sistema operativo Windows 10

Para que funcione correctamente el dns64 y nat64 se debe iniciar el servicio con el siguiente comando.

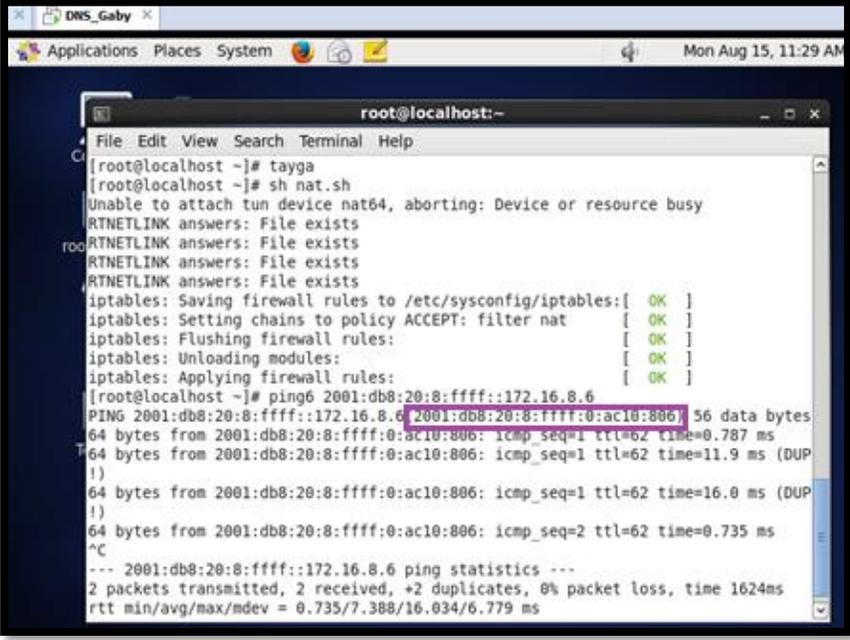


```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# tayga -d Se inicia el servicio  
starting TAYGA 0.9.2  
Using tun device nat64 with MTU 1500 Verificación del servicio  
TAYGA's IPv4 address: 172.16.255.1  
TAYGA's IPv6 address: 2001:db8:20:8:ffff:0:ac10:ff01  
NAT64 prefix: 2001:db8:20:8:ffff::/96  
Dynamic pool: 172.16.255.0/24  
Loaded 2 dynamic maps from /var/db/tayga/dynamic.map  
[root@localhost ~]#  
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# sh nat.sh Se ejecuta el servicio  
Unable to attach tun device nat64, aborting: Device or resource busy  
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]  
iptables: Setting chains to policy ACCEPT: nat filter [ OK ]  
iptables: Flushing firewall rules: [ OK ]  
iptables: Unloading modules: [ OK ]  
iptables: Applying firewall rules: [ OK ]  
[root@localhost ~]#
```

Figura 36. Ejecución del servicio NAT64

Fuente: Captura propia extraída de sistema operativo centos 6.7

En el servidor DNS, se puede visualizar que, al servidor WEB, que sólo se encuentra con direccionamiento IPv4, con la ejecución del servicio tayga, se crea una dirección IPv6 como se visualiza en la Figura 37.



```

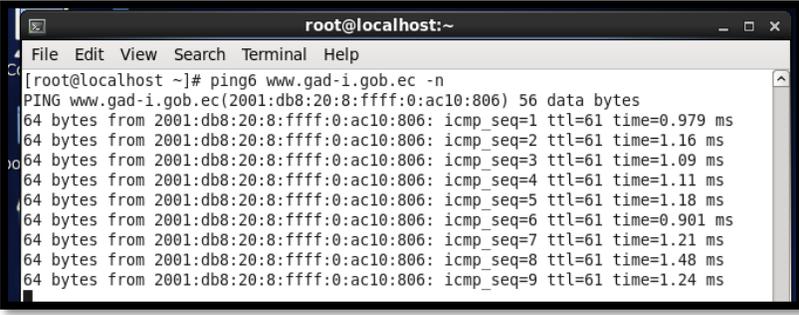
root@localhost:~# tayga
root@localhost ~]# sh nat.sh
Unable to attach tun device nat64, aborting: Device or resource busy
RTNETLINK answers: File exists
RTNETLINK answers: File exists
RTNETLINK answers: File exists
RTNETLINK answers: File exists
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
iptables: Setting chains to policy ACCEPT: filter nat [ OK ]
iptables: Flushing firewall rules: [ OK ]
iptables: Unloading modules: [ OK ]
iptables: Applying firewall rules: [ OK ]
root@localhost ~]# ping6 2001:db8:20:8::ffff::172.16.8.6
PING 2001:db8:20:8::ffff::172.16.8.6: 56 data bytes
64 bytes from 2001:db8:20:8::ffff:0:ac10:806: icmp_seq=1 ttl=62 time=0.787 ms
64 bytes from 2001:db8:20:8::ffff:0:ac10:806: icmp_seq=1 ttl=62 time=11.9 ms (DUP
!)
64 bytes from 2001:db8:20:8::ffff:0:ac10:806: icmp_seq=1 ttl=62 time=16.0 ms (DUP
!)
64 bytes from 2001:db8:20:8::ffff:0:ac10:806: icmp_seq=2 ttl=62 time=0.735 ms
^C
--- 2001:db8:20:8::ffff::172.16.8.6 ping statistics ---
2 packets transmitted, 2 received, +2 duplicates, 0% packet loss, time 1624ms
rtt min/avg/max/mdev = 0.735/7.388/16.034/6.779 ms

```

Figura 37. Verificación del funcionamiento de NAT64 en Centos 6.5

Fuente: Captura propia extraída de sistema operativo centos 6.5

En el servidor de correo SMTP, que sólo cuenta con direccionamiento IPv6, puede acceder al servidor WEB, verificando el servicio que se encuentra funcionando perfectamente, comprobando que, aunque sólo cuente con IPv6, accede a un servicio que sólo cuenta con direccionamiento IPv4.



```

root@localhost:~# ping6 www.gad-i.gob.ec -n
PING www.gad-i.gob.ec(2001:db8:20:8::ffff:0:ac10:806) 56 data bytes
64 bytes from 2001:db8:20:8::ffff:0:ac10:806: icmp_seq=1 ttl=61 time=0.979 ms
64 bytes from 2001:db8:20:8::ffff:0:ac10:806: icmp_seq=2 ttl=61 time=1.16 ms
64 bytes from 2001:db8:20:8::ffff:0:ac10:806: icmp_seq=3 ttl=61 time=1.09 ms
64 bytes from 2001:db8:20:8::ffff:0:ac10:806: icmp_seq=4 ttl=61 time=1.11 ms
64 bytes from 2001:db8:20:8::ffff:0:ac10:806: icmp_seq=5 ttl=61 time=1.18 ms
64 bytes from 2001:db8:20:8::ffff:0:ac10:806: icmp_seq=6 ttl=61 time=0.901 ms
64 bytes from 2001:db8:20:8::ffff:0:ac10:806: icmp_seq=7 ttl=61 time=1.21 ms
64 bytes from 2001:db8:20:8::ffff:0:ac10:806: icmp_seq=8 ttl=61 time=1.48 ms
64 bytes from 2001:db8:20:8::ffff:0:ac10:806: icmp_seq=9 ttl=61 time=1.24 ms

```

Figura 38. Verificación de acceso de un cliente IPv6 a un servicio con IPv4

Fuente: Captura propia extraída de sistema operativo centos 6.5

Se puede visualizar el acceso al servidor WEB con la configuración dual stack en este usuario.

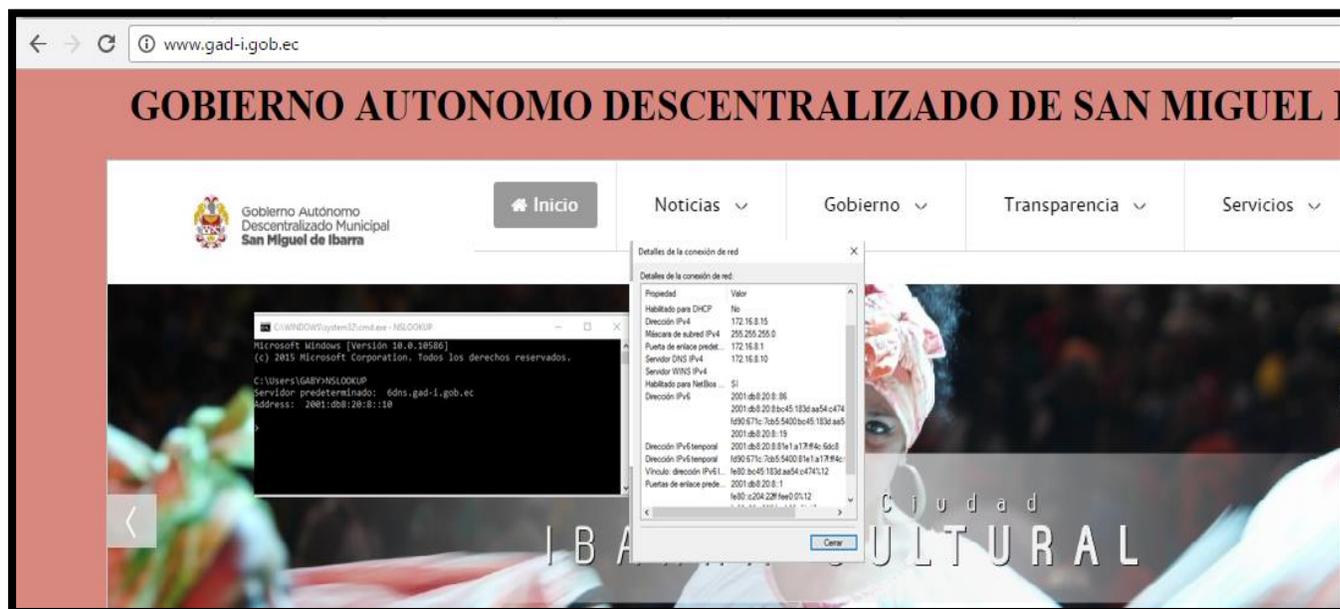


Figura 39. Verificación de un usuario interno al servicio WEB

Fuente: Captura propia extraída de sistema operativo Windows 10

Servidor de Correo Electrónico desde la red interna

Se realizó la prueba utilizando un correo corporativo utilizando Outlook 2016, debido a que en los usuarios finales se tiene vinculado al gestor Zimbra, porque para los usuarios es mucho más fácil manejar esta plataforma. Por eso se utilizará para usuarios tanto IPv4 como IPv6, o Dual Stack

Se ejecuta el correspondiente Outlook 2016 desde el usuario.

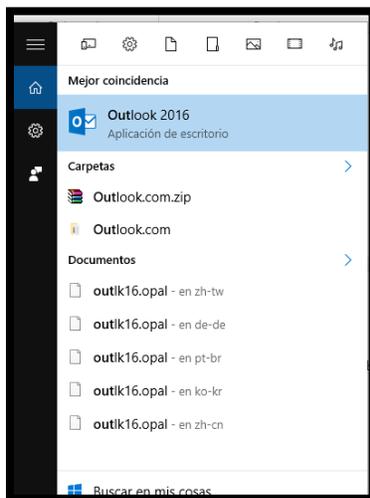


Figura 40. Acceso a Outlook 2016

Fuente: Captura propia extraída de sistema operativo Windows 10

La pantalla de bienvenida es la presentada en la Figura 107, dirigirse a archivo

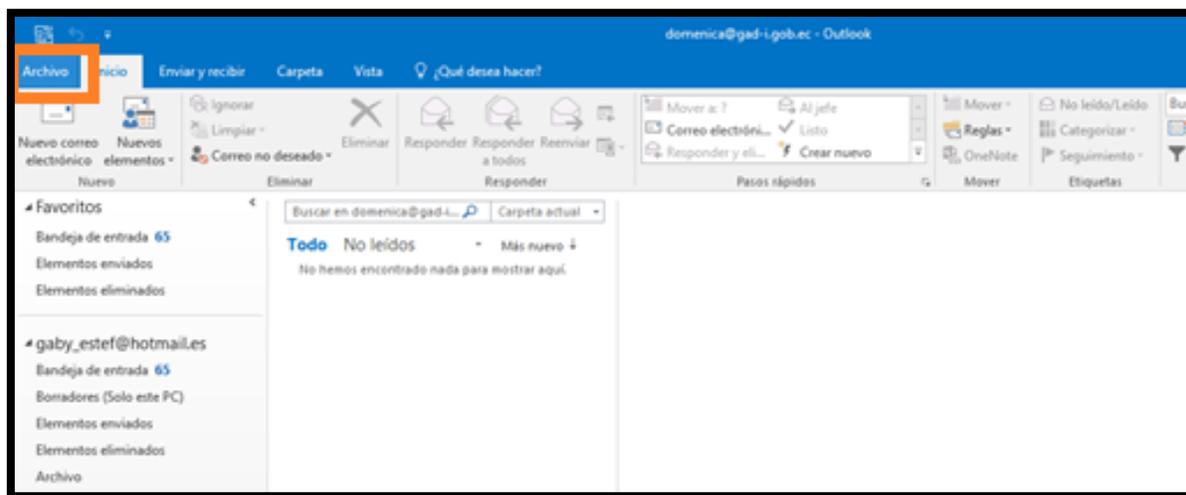


Figura 41. Pantalla de Inicio de Outlook

Fuente: Captura propia extraída de sistema operativo Windows 10

Y se escoge agregar cuenta

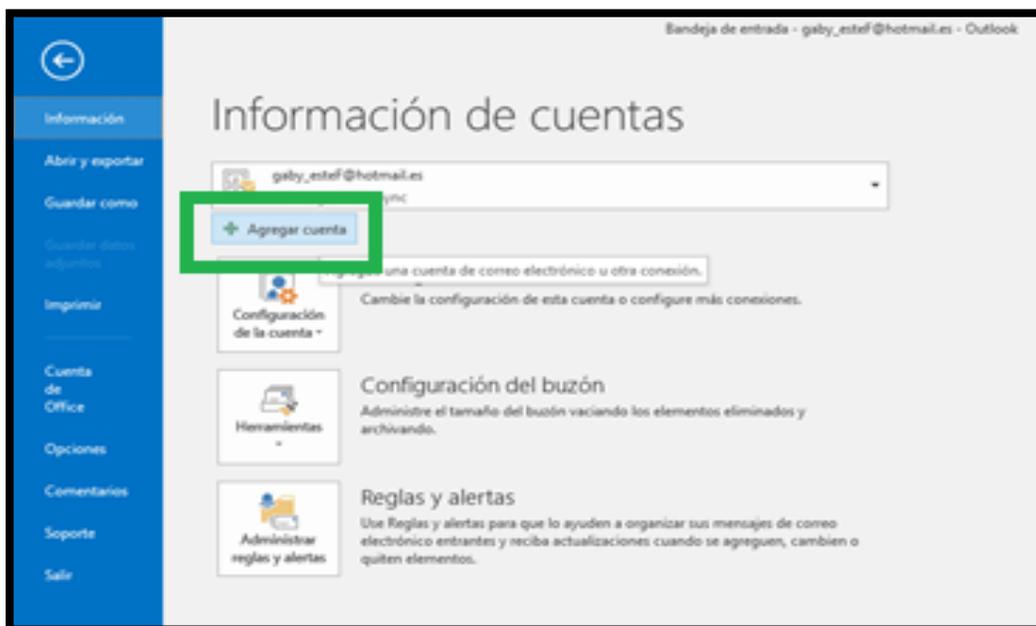


Figura 42. *Agregar una cuenta en Outlook 2016*

Fuente: Captura propia extraída de sistema operativo Windows 10

Se escoge la opción de configuración manual y se presiona siguiente.

Figura 43. *Configuración manual de servidores*

Fuente: Captura propia extraída de sistema operativo Windows 10

Se elige el servicio POP o IMAP, porque son los protocolos con los que se está trabajando en el servidor y se presiona siguiente.

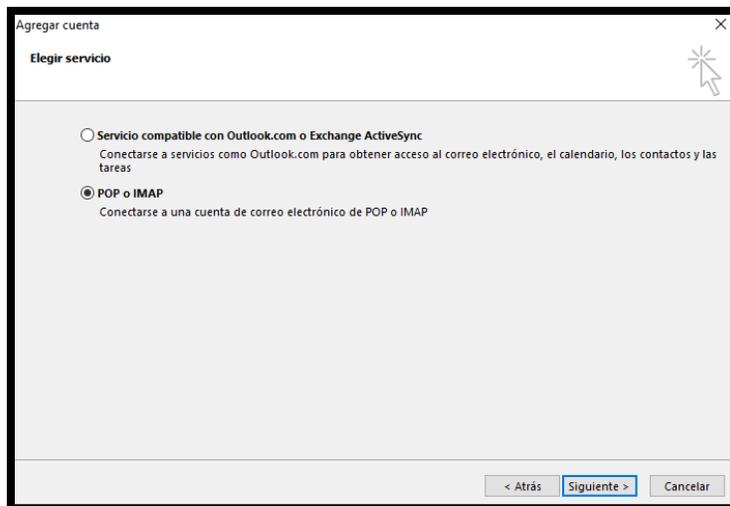


Figura 44. *Configuración de protocolos*

Fuente: Captura propia extraída de sistema operativo Windows 10

Este punto es importante, para configurar el nombre de usuario se debe colocar uno que esté registrado en el servidor de correo en este caso en Centos. De la misma manera el correo electrónico con el dominio creado.

En el punto de servidores se puede colocar el dominio que se ha creado, es decir mail.gad-i.gob.ec o escribir la Ip del servidor con su dirección IPv4 o IPv6, en este caso como se ha especificado en el plan de pruebas sólo funcionara como usuario IPv6. En caso de que se desee utilizar una IPv4 el procedimiento es el mismo.

En información del inicio de sesión se debe colocar la información del correo en Centos con su respectiva contraseña.

Una vez realizados estos pasos se coloca siguiente.

Agregar cuenta

Configuración de cuenta IMAP y POP
Especifique la configuración de servidor de correo para su cuenta.

Información sobre el usuario
 Su nombre: Pato
 Dirección de correo electrónico: pato@gad-l.gob.ec

Información del servidor
 Tipo de cuenta: POP3
 Servidor de correo entrante: mail.gad-l.gob.ec
 Servidor de correo saliente (SMTP): mail.gad-l.gob.ec

Información de inicio de sesión
 Nombre de usuario: pato
 Contraseña: *****
 Recordar contraseña

Requerir inicio de sesión utilizando Autenticación de contraseña segura (SPA)

Configuración de la cuenta de prueba
 Le recomendamos que pruebe su cuenta para garantizar que las entradas son correctas.
 Probar configuración de la cuenta ...
 Probar automáticamente la configuración de la cuenta al hacer clic en Siguiente

Entregar nuevos mensajes a:
 Nuevo archivo de datos de Outlook
 Archivo de datos de Outlook existente

Más configuraciones ...

< Atrás **Siguiente >** Cancelar

Figura 45. Configuración de servidor de correo entrante y saliente

Fuente: Captura propia extraída de sistema operativo Windows 10

Dirigirse a más configuraciones:

Cambiar cuenta

Configuración de cuenta IMAP y POP
Especifique la configuración de servidor de correo para su cuenta.

Información sobre el usuario
 Su nombre: pato
 Dirección de correo electrónico: pato@gad-l.gob.ec

Información del servidor
 Tipo de cuenta: POP3
 Servidor de correo entrante: mail.gad-l.gob.ec
 Servidor de correo saliente (SMTP): mail.gad-l.gob.ec

Información de inicio de sesión
 Nombre de usuario: pato
 Contraseña: *****
 Recordar contraseña

Requerir inicio de sesión utilizando Autenticación de contraseña segura (SPA)

Configuración de la cuenta de prueba
 Le recomendamos que pruebe su cuenta para garantizar que las entradas son correctas.
 Probar configuración de la cuenta ...
 Probar automáticamente la configuración de la cuenta al hacer clic en Siguiente

Más configuraciones ...

< Atrás **Siguiente >** Cancelar

Figura 46. Más configuraciones de la cuenta

Fuente: Captura propia extraída de sistema operativo Windows 10

En la opción avanzada, se debe tener en cuenta que estos dos puertos estén configurados, en este caso como se va a realizar pruebas locales SMTP, utilizará el puerto 25.

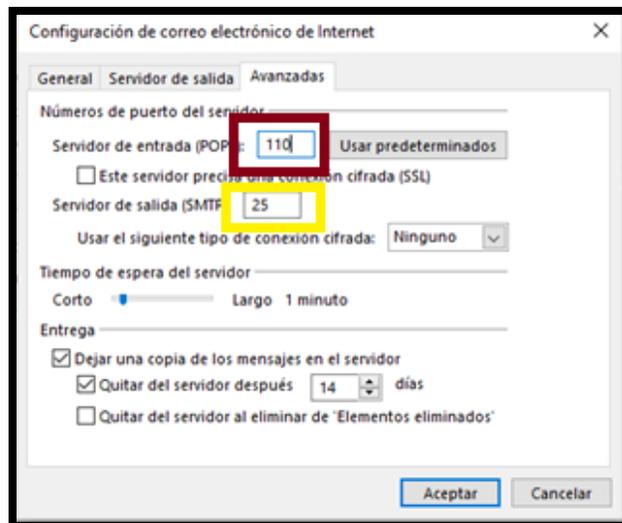


Figura 47. Configuración de puertos

Fuente: Captura propia extraída de sistema operativo Windows 10

Ahora se va a colocar aceptar y de la misma forma se coloca siguiente

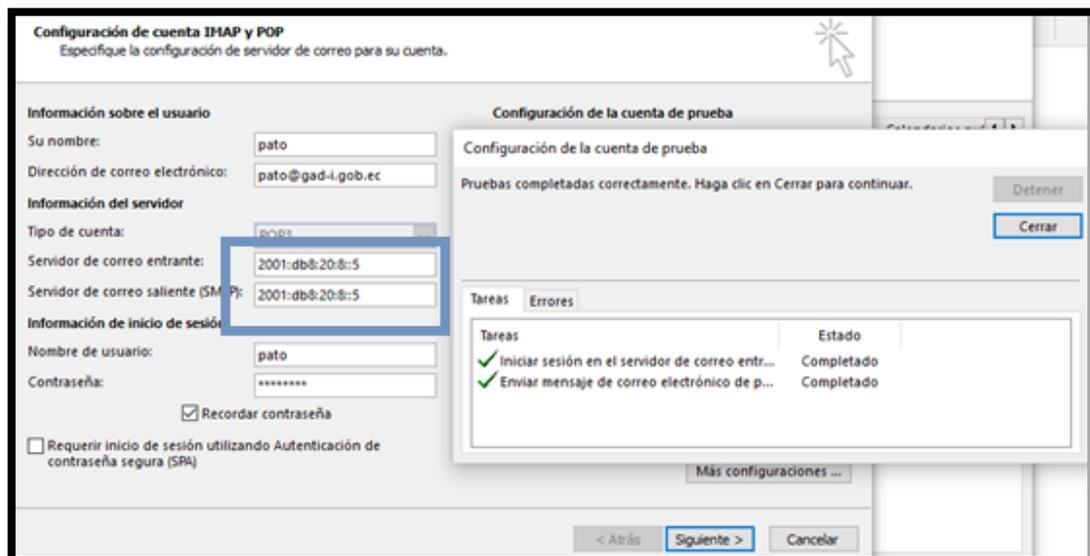


Figura 48. Configuración del servidor como entrante y saliente con IPv6

Fuente: Captura propia extraída de sistema operativo Windows 10

Si las dos tareas están con un check verde, está configurado correctamente el correo corporativo.

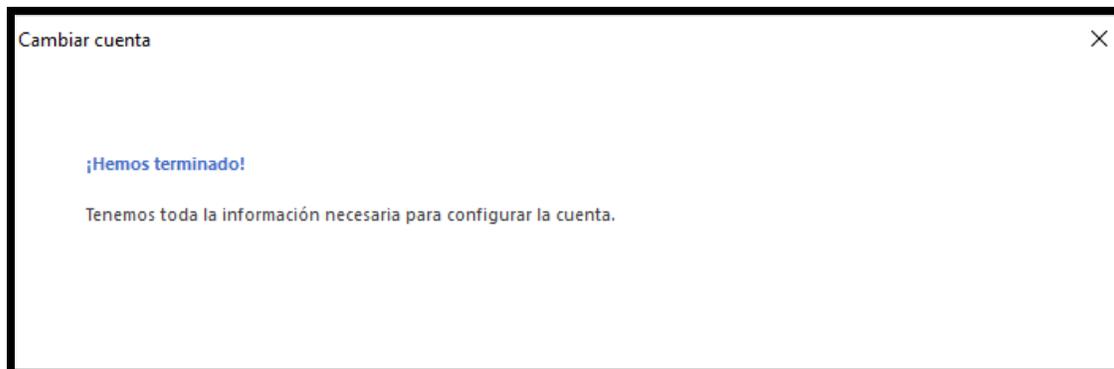


Figura 49. Verificación de la creación de la cuenta

Fuente: Captura propia extraída de sistema operativo Windows 10

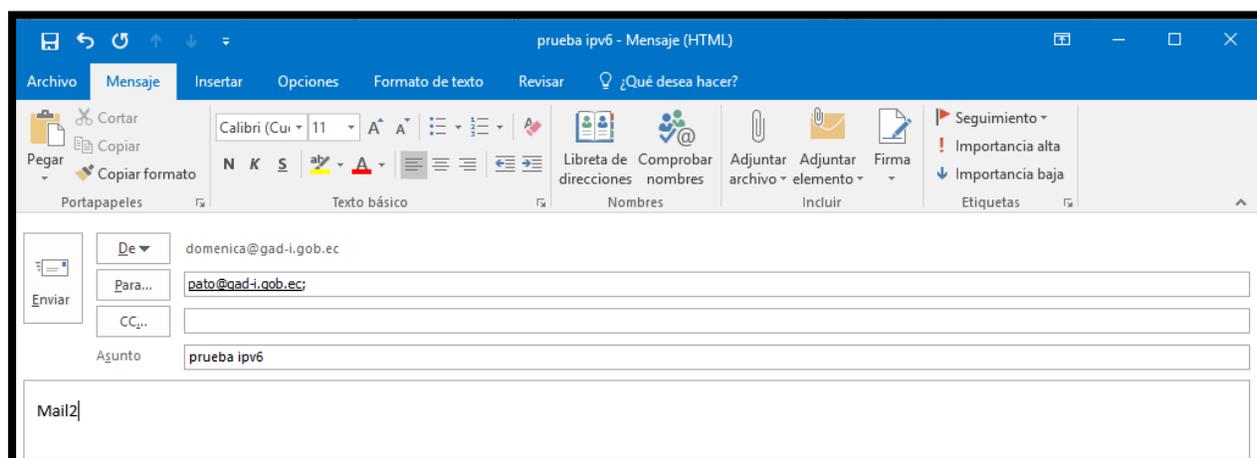


Figura 50. Envío de correo en IPv6

Fuente: Captura propia extraída de sistema operativo Windows 10

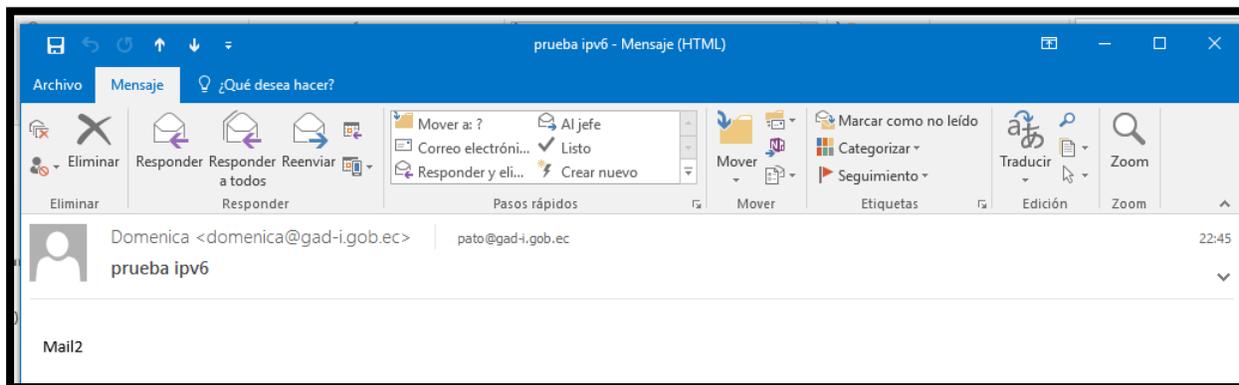


Figura 51. Verificación de recepción de correo en IPv6

Fuente: Captura propia extraída de sistema operativo Windows 10

Ahora se ha probado de igual manera con el servicio Correo electrónico, verificando el envío y recepción de los emails.

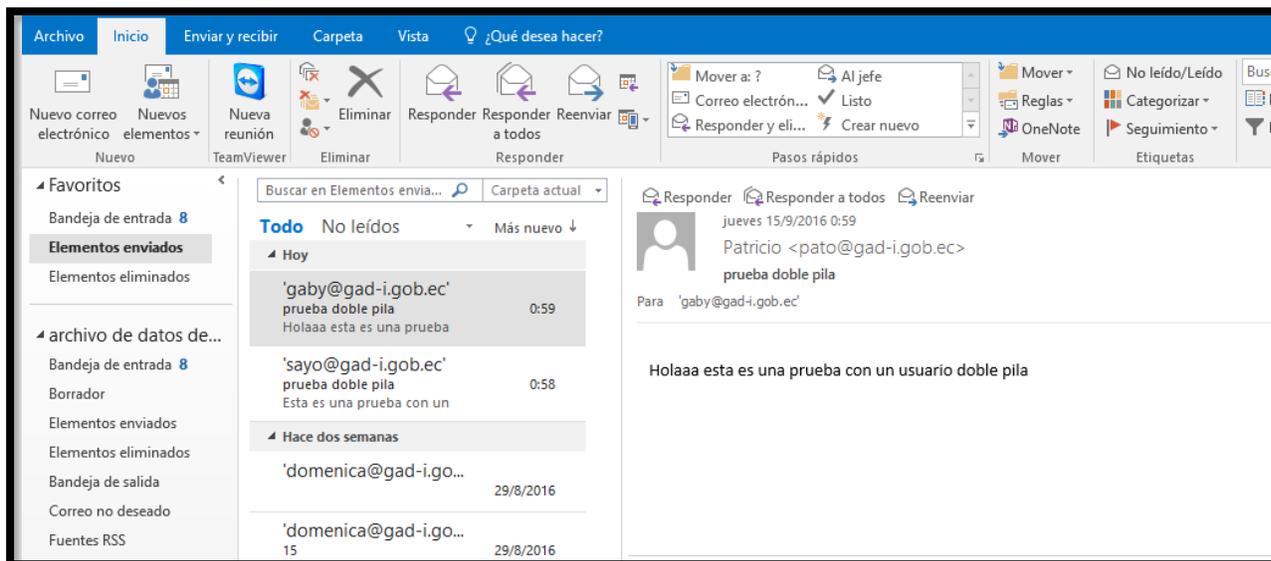


Figura 52. Verificación de un usuario interno al servicio de Correo Electrónico

Fuente: Captura propia extraída de sistema operativo Windows 10

Servidor WEB desde un usuario externo

Se puede observar el acceso desde un usuario IPv6 al servidor WEB, que se encuentra únicamente con direccionamiento IPv4.

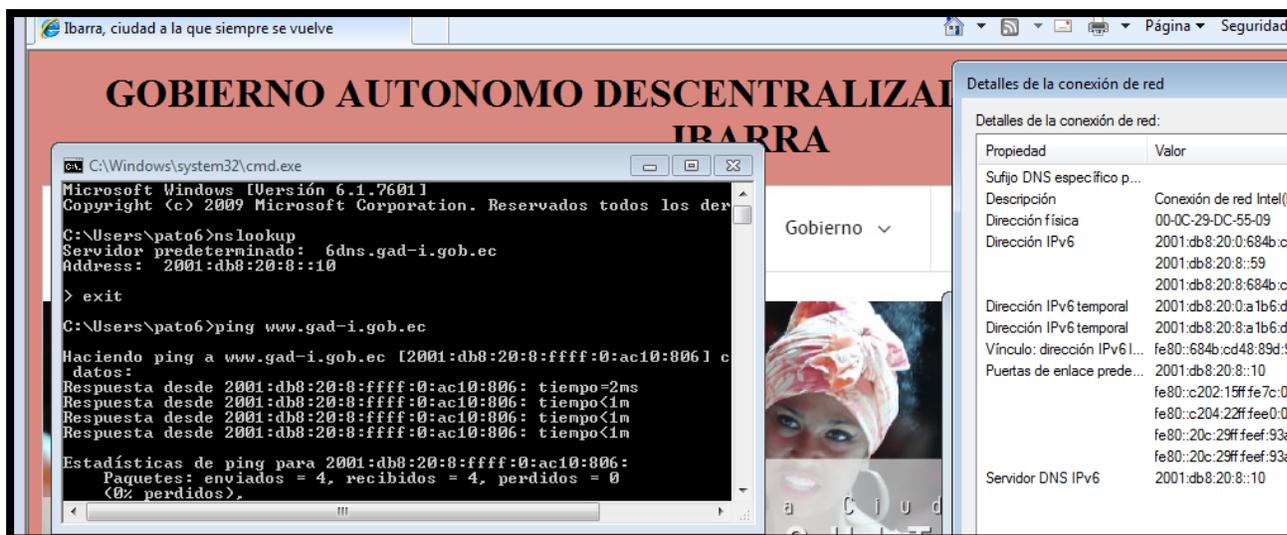


Figura 53. Verificación de un usuario externo al servicio WEB

Fuente: Captura propia extraída de sistema operativo Windows 10

Servidor de Correo Electrónico desde un usuario externo

De la misma forma se instaló en Windows 7 el servicio de Windows Live Mail, y se verificó de la misma forma el servicio de Correo Electrónico.

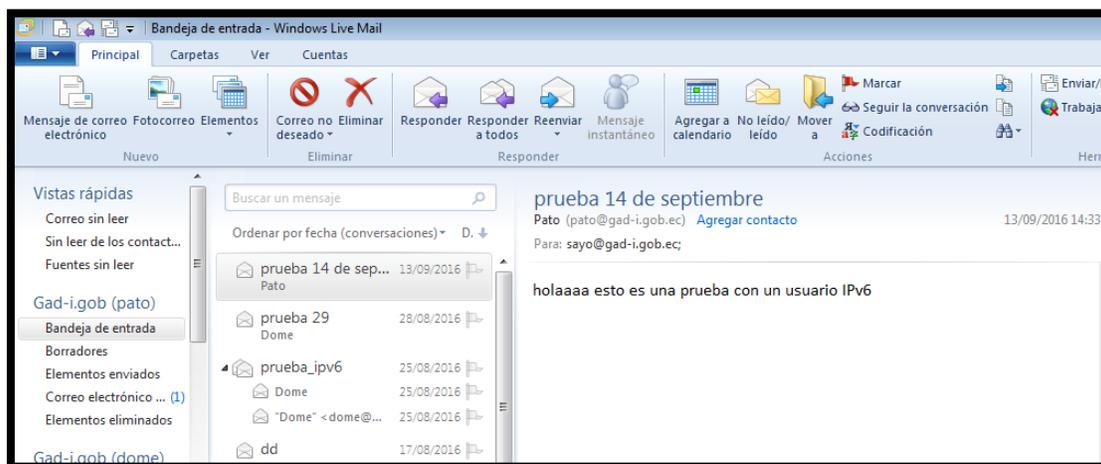


Figura 54. Verificación de funcionamiento del correo electrónico

Fuente: Captura propia extraída de sistema operativo Windows 10

Configuraciones de seguridad

1. Se configuran las interfaces fastethernet con sus respectivas direcciones Ipv6

```

R1#
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int fa0/0
R1(config-if)#ipv
R1(config-if)#ipv6 e
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 add 2001:db7::1/64
R1(config-if)#no shut
R1(config-if)#
*Jul  7 18:03:12.519: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
R1(config-if)#
*Jul  7 18:03:12.519: %ENTITY_ALARM-6-INFO: CLEAR INFO Fa0/0 Physical Port Administrative State Down
*Jul  7 18:03:13.519: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#exit

```

Figura 55. Configuración de Interfaz fa0/0 en Ipv6

Fuente: Captura propia extraída de software GNS3

```

Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int fa 1/0
R1(config-if)#ipv6 en
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 add
R1(config-if)#ipv6 address 2001:db8::1/64
R1(config-if)#no shut
R1(config-if)#
*Jul  7 18:14:22.579: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
R1(config-if)#
*Jul  7 18:14:22.579: %ENTITY_ALARM-6-INFO: CLEAR INFO Fa1/0 Physical Port Administrative State Down
*Jul  7 18:14:23.579: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
R1(config-if)#

```

Figura 56. Configuración de Interfaz fa1/0 en Ipv6

Fuente: Captura propia extraída de software GNS3

2. Se configura un protocolo de enrutamiento en este caso OSPFv3 y se configura en cada red.

```

R1(config-if)#exit
R1(config)#ipv6 un
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 r
R1(config)#ipv6 router o
R1(config)#ipv6 router ospf 1
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#exit
R1(config)#int fa1/0
R1(config-if)#ipv6 o
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#exit
R1(config)#int fa0/0
R1(config-if)#ip
R1(config-if)#ipv6 os
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#

```

Figura 57. Implementación de protocolo de enrutamiento OSPFv3

Fuente: Captura propia extraída de software GNS3

3. Se realizan las mismas configuraciones en R2 con sus correspondientes redes.

```

R2(config)#int fa1/0
R2(config-if)#ipv6 en
R2(config-if)#ipv6 enable
R2(config-if)#ipv6 ad
R2(config-if)#ipv6 address 2001:db8::2/64
R2(config-if)#no shut
R2(config-if)#
*Jul  7 18:20:38.791: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
R2(config-if)#
*Jul  7 18:20:38.791: %ENTITY_ALARM-6-INFO: CLEAR INFO Fa1/0 Physical Port Administrative State Down
*Jul  7 18:20:39.791: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
R2(config-if)#exit
R2(config)#int fa0/0
R2(config-if)#ipv6 e
R2(config-if)#ipv6 enable
R2(config-if)#ipv6 ad
R2(config-if)#ipv6 address 2001:db9::1/64
R2(config-if)#no shut
R2(config-if)#
*Jul  7 18:21:38.127: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
R2(config-if)#
*Jul  7 18:21:38.127: %ENTITY_ALARM-6-INFO: CLEAR INFO Fa0/0 Physical Port Administrative State Down
*Jul  7 18:21:39.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R2(config-if)#

```

Figura 58. *Configuración de Interfaces R2*

Fuente: Captura propia extraída de software GNS3

4. Se configura el protocolo de enrutamiento, OSPFv3

```

R2(config)#ipv6 router ospf 1
R2(config-rtr)#
*Jul  7 18:22:34.239: %OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,
please configure manually
R2(config-rtr)#router-id 1.1.1.2
R2(config-rtr)#exit
R2(config)#int fa0/0
R2(config-if)#ipv6 o
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#exit
R2(config)#int fa1/0
R2(config-if)#ip
R2(config-if)#ipv
R2(config-if)#ipv6 os
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#exit
R2(config)#exit
R2#copy ru
*Jul  7 18:23:54.907: %SYS-5-CONFIG_I: Configured from console by console
R2#copy ru st
Destination filename [startup-config]?
Building configuration...
[OK]
R2#

```

Figura 59. *Implementación de protocolo de enrutamiento OSPFv3 en R2*

Fuente: Captura propia extraída de software GNS3

5. Se definen políticas IKE (Internet Key Exchange) y se especifica el uso de llaves pre-shared como método de autenticación.

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB7::6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/11/16 ms
R1#
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#cry
R1(config)#crypto is
R1(config)#crypto isakmp po
R1(config)#crypto isakmp policy 4
R1(config-isakmp)#enc
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#ha
R1(config-isakmp)#hash md5
R1(config-isakmp)#au
R1(config-isakmp)#authentication p
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#li
R1(config-isakmp)#lifetime 86400
R1(config-isakmp)#exit
R1(config)#
```

Figura 60. *Aplicación de IKE*

Fuente: Captura propia extraída de software GNS3

6. El comando do show hist, permite verificar las configuraciones de enrutamiento y encriptación que se ha configurado en el router.

```
R1(config)#do show hist
no shut
exit
ipv6 unicast-routing
ipv6 router ospf 1
router-id 1.1.1.1
exit
int fa1/0
ipv6 ospf 1 area 0
exit
int fa0/0
ipv6 ospf 1 area 0
exit
crypto isakmp policy 4
encryption 3des
hash md5
authentication pre-share
group 2
lifetime 86400
exit
do show hist
R1(config)#
```

Figura 61. *Verificación de Políticas de seguridad*

Fuente: Captura propia extraída de software GNS3

7. Se realizan las mismas configuraciones en el Router 2.

```

R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#cry
R2(config)#crypto is
R2(config-isakmp)#encr
R2(config-isakmp)#encryption 3des
R2(config-isakmp)#has
R2(config-isakmp)#hash md5
R2(config-isakmp)#aut
R2(config-isakmp)#authentication pr
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 2
R2(config-isakmp)#lifetime 86400
R2(config-isakmp)#exit
R2(config)#end
R2#copy
*Jul  7 18:32:39.443: %SYS-5-CONFIG_I: Configured from console by console
R2#copy ru st
Destination filename [startup-config]?
Building configuration...
[OK]
R2#

```

Figura 62. Aplicación de IKE en R2

Fuente: Captura propia extraída de software GNS3

8. Se define una clave (key), y como se ha escogido utilizar claves pre-configuradas que se intercambien en la negociación inicial es necesario configurarla en cada extremo

```

lifetime 86400
exit
do show hist
R1(config)#exit
R1#copy ru
*Jul  7 18:31:18.803: %SYS-5-CONFIG_I: Configured from console by console
R1#copy ru st
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#cry
R1(config)#crypto is
R1(config)#crypto isakmp keep
R1(config)#crypto isakmp keepalive 30 30
R1(config)#cryp
R1(config)#crypto is
R1(config)#crypto isakmp key 6 asd10 address ipv6 2001:db8::2
% Incomplete command.

R1(config)#crypto isakmp key 6 asd10 address ipv6 2001:db8::2/64
R1(config)#

```

Figura 63. Configuración de clave en R1

Fuente: Captura propia extraída de software GNS3

```

R2(config-isakmp)#authentication pr
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 2
R2(config-isakmp)#lifetime 86400
R2(config-isakmp)#exit
R2(config)#end
R2#copy
*Jul  7 18:32:39.443: %SYS-5-CONFIG_I: Configured from console by console
R2#copy ru st
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#crypt
R2(config)#crypto is
R2(config)#crypto isakmp kee
R2(config)#crypto isakmp keepalive 30 30
R2(config)#crypto s
R2(config)#crypto is
R2(config)#crypto isakmp ke
R2(config)#crypto isakmp key 6 asd10 add ipv6 2001:db8::1/64
R2(config)#

```

Figura 64. Configuración de clave en R2

Fuente: Captura propia extraída de software GNS3

9. El transform set se utiliza para definir las políticas de seguridad que serán aplicadas al tráfico que entra o sale de una interfaz.

```

R1(config)#crypto ipsec tr
R1(config)#crypto ipsec transform-set ipv6?
WORD

R1(config)#crypto ipsec transform-set ipv6_tr
R1(config)#crypto ipsec transform-set ipv6_trans a
R1(config)#crypto ipsec transform-set ipv6_trans ah-sh
R1(config)#crypto ipsec transform-set ipv6_trans ah-sha-hmac es
R1(config)#crypto ipsec transform-set ipv6_trans ah-sha-hmac esp-3
R1(config)#crypto ipsec transform-set ipv6_trans ah-sha-hmac esp-3des
R1(cfg-crypto-trans)#exit
R1(config)#cry
R1(config)#crypto ip
R1(config)#crypto ipsec pro
R1(config)#crypto ipsec profile ipv6?
WORD

R1(config)#crypto ipsec profile ipv6_profile
R1(ipsec-profile)#set t
R1(ipsec-profile)#set transform-set ipv6?
WORD

R1(ipsec-profile)#set transform-set ipv6_trans
R1(ipsec-profile)#

```

Figura 65. Especificación de Algoritmos de cifrado a tráfico de datos

Fuente: Captura propia extraída de software GNS3

```

R2#
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#cryp
R2(config)#crypto is
R2(config)#crypto isakmp kee
R2(config)#crypto isakmp keepalive 30 30
R2(config)#crypto s
R2(config)#crypto is
R2(config)#crypto isakmp ke
R2(config)#crypto isakmp key 6 asd10 add ipv6 2001:db8::1/64
R2(config)#cr
R2(config)#crypto ipsec tr
R2(config)#crypto ipsec transform-set ipv6_trans a
R2(config)#crypto ipsec transform-set ipv6_trans ah-sh
R2(config)#crypto ipsec transform-set ipv6_trans ah-sha-hmac es
R2(config)#crypto ipsec transform-set ipv6_trans ah-sha-hmac esp-3
R2(config)#crypto ipsec transform-set ipv6_trans ah-sha-hmac esp-3des
R2(cfg-crypto-trans)#exit
R2(config)#cry
R2(config)#crypto ipsec profile ipv6_profile
R2(ipsec-profile)#set tr
R2(ipsec-profile)#set transform-set ipv6_trans
R2(ipsec-profile)#

```

Figura 66. Especificación de Algoritmos de cifrado a tráfico de datos en R2

Fuente: Captura propia extraída de software GNS3

10. Se crea el túnel que va a permitir la conexión de un extremo al otro para definir sus propios parámetros de seguridad

```

R1#copy ru st
Destination filename [startup-config]?
Building configuration...
[OK]
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int tunnel 0
R1(config-if)#
*Jul 7 18:45:48.067: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
R1(config-if)#ipv6 en
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 add 2002:db8::1/64
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#tun
R1(config-if)#tunnel sou
R1(config-if)#tunnel source fa1/0
R1(config-if)#tunnel des
R1(config-if)#tunnel destination 2001:db8::2
R1(config-if)#tunnel mode ipsec ipv6
R1(config-if)#tunnel pro
R1(config-if)#tunnel protection ipsec profile ipv6_profile
R1(config-if)#
*Jul 7 18:52:55.847: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#

```

Figura 67. Especificación modo túnel en R1

Fuente: Captura propia extraída de software GNS3

```

Destination filename [startup-config]?
Building configuration...
[OK]
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int tunnel 0
R2(config-if)#ipv6 ena
*Jul  7 18:47:22.691: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
R2(config-if)#ipv6 ena
R2(config-if)#ipv6 enable
R2(config-if)#ipv6 add 2002:db8::2/64
R2(config-if)#ipv6 ospf
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#tunnel source fal/0
R2(config-if)#tunnel des
R2(config-if)#tunnel destination 2001:db8::1
R2(config-if)#tunnel mode ipsec ipv6
R2(config-if)#tunnel protect
R2(config-if)#tunnel protection ipsec profile ipv6_profile
R2(config-if)#
*Jul  7 18:54:44.859: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R2(config-if)#
*Jul  7 18:54:46.027: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
R2(config-if)#

```

Figura 68. *Especificación modo túnel en R2*

Fuente: Captura propia extraída de software GNS3

- Una vez configurados estos parámetros se observa que se empieza a visualizar las actualizaciones de OPSFv3 y de la misma manera se comprueba conectividad de un extremo a otro en los correspondientes Routers.

```

R2(config-if)#ipv6 ena
R2(config-if)#ipv6 enable
R2(config-if)#ipv6 add 2002:db8::2/64
R2(config-if)#ipv6 ospf
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#tunnel source fal/0
R2(config-if)#tunnel des
R2(config-if)#tunnel destination 2001:db8::1
R2(config-if)#tunnel mode ipsec ipv6
R2(config-if)#tunnel protect
R2(config-if)#tunnel protection ipsec profile ipv6_profile
R2(config-if)#
*Jul  7 18:54:44.859: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R2(config-if)#
*Jul  7 18:54:46.027: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
R2(config-if)#
*Jul  7 18:54:57.099: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Tunnel0 from LOADING to FULL, Loading Done
R2(config-if)#do ping 2002:db8::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:DB8::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/24 ms
R2(config-if)#

```

Figura 69. *Verificación de conectividad extremo a extremo*

Fuente: Captura propia extraída de software GNS3

```

R1(config-if)#ipv6 enable
R1(config-if)#ipv6 add 2002:db8::1/64
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#tun
R1(config-if)#tunnel sou
R1(config-if)#tunnel source fa1/0
R1(config-if)#tunnel des
R1(config-if)#tunnel destination 2001:db8::2
R1(config-if)#tunnel mode ipsec ipv6
R1(config-if)#tunnel pro
R1(config-if)#tunnel protection ipsec profile ipv6_profile
R1(config-if)#
*Jul 7 18:52:55.847: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
*Jul 7 18:54:57.179: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
R1(config-if)#
*Jul 7 18:55:08.255: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.2 on Tunnel0 from LOADING to FULL, Loading Done
R1(config-if)#do ping 2002:db8::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:DB8::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms
R1(config-if)#

```

Figura 70. Verificación de conectividad extremo a extremo

Fuente: Captura propia extraída de software GNS3

12. Una vez realizada esta configuración, se va a capturar los paquetes de la interfaz fa1/0 que es la que está configurada en modo túnel y comprobar que los paquetes estén siendo cifrados y verificar el protocolo ESP esté funcionando. Como se logre observar los paquetes están siendo cifrados con un algoritmo y en código ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
71	75.3926760	fe80::c802:1cff:fe2fe80::c801:18ff:fe4	fe80::c801:18ff:fe4	ICMPv6	86	Neighbor solicitation for fe80::c801:18ff:fe40:1c from ca:02:1c:24:00:1c
72	75.3926760	2001:db8::2	2001:db8::1	ESP	182	ESP (SPI=0xf874afa)
73	75.3926760	fe80::c801:18ff:fe4fe80::c802:1cff:fe2	fe80::c802:1cff:fe24:1c	ICMPv6	86	Neighbor solicitation for fe80::c802:1cff:fe24:1c from ca:01:18:40:00:1c
74	75.4026830	fe80::c802:1cff:fe2fe80::c801:18ff:fe4	fe80::c802:1cff:fe24:1c	ICMPv6	78	Neighbor Advertisement fe80::c802:1cff:fe24:1c (rtr, sol)
75	75.4026830	fe80::c801:18ff:fe4fe80::c802:1cff:fe2	fe80::c801:18ff:fe40:1c	ICMPv6	78	Neighbor Advertisement fe80::c801:18ff:fe40:1c (rtr, sol)
76	78.8059500	fe80::c801:18ff:fe4ff02::5	fe80::c802:1cff:fe2ff02::5	OSPF	94	Hello Packet
77	79.9967380	fe80::c802:1cff:fe2ff02::5	fe80::c802:1cff:fe2ff02::5	OSPF	94	Hello Packet
78	80.4570430	2001:db8::1	2001:db8::2	ESP	206	ESP (SPI=0xaf8bd5c1)
79	80.4670500	2002:db8::2	2001:db7::6	ICMPv6	118	Echo (ping) reply id=0xf9ec, seq=1, hop limit=64
80	80.4870630	2001:db8::1	2001:db8::2	ESP	206	ESP (SPI=0xaf8bd5c1)
81	80.4970690	2002:db8::2	2001:db7::6	ICMPv6	118	Echo (ping) reply id=0xf9ec, seq=2, hop limit=64
82	80.5170830	2001:db8::1	2001:db8::2	ESP	206	ESP (SPI=0xaf8bd5c1)
83	80.5270890	2002:db8::2	2001:db7::6	ICMPv6	118	Echo (ping) reply id=0xf9ec, seq=3, hop limit=64
84	80.5471030	2001:db8::1	2001:db8::2	ESP	206	ESP (SPI=0xaf8bd5c1)
85	80.5571090	2002:db8::2	2001:db7::6	ICMPv6	118	Echo (ping) reply id=0xf9ec, seq=4, hop limit=64
86	80.5771220	2001:db8::1	2001:db8::2	ESP	206	ESP (SPI=0xaf8bd5c1)
87	80.5871290	2002:db8::2	2001:db7::6	ICMPv6	118	Echo (ping) reply id=0xf9ec, seq=5, hop limit=64
88	81.5477650	ca:01:18:40:00:1c	ca:01:18:40:00:1c	LOOP	60	Reply
89	82.7085490	ca:02:1c:24:00:1c	ca:02:1c:24:00:1c	LOOP	60	Reply

Figura 71. Verificación de utilización de protocolo ESP

Fuente: Captura propia extraída de software Wireshark

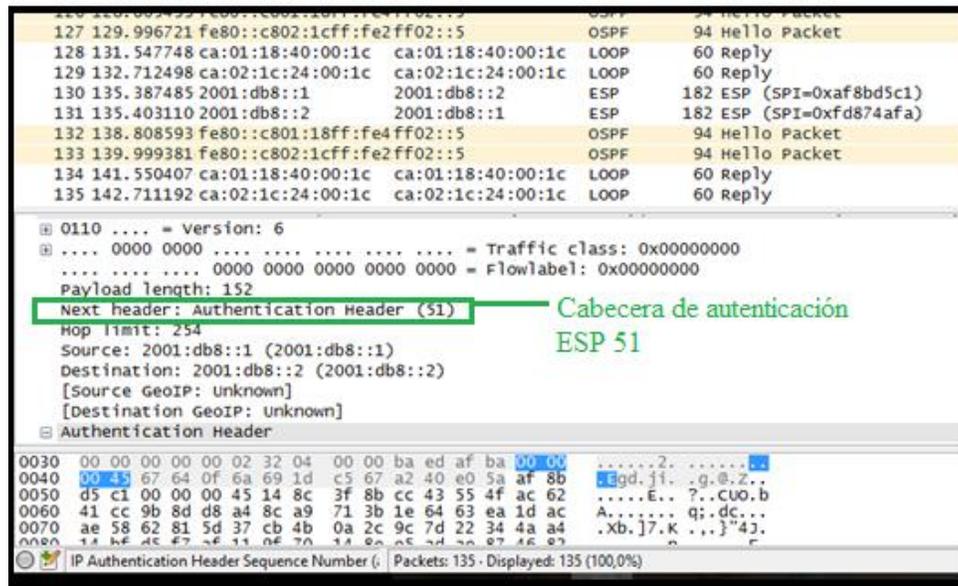


Figura 72. Cabecera ESP (51)

Fuente: Captura propia extraída de software Wireshark

Conclusiones de las pruebas de Funcionamiento

- En cuanto a la red Interna, se pudo verificar el acceso por parte de un usuario IPv4, IPv6 o con los dos direccionamientos al servidor WEB, que únicamente maneja IPv4. Es decir que para un usuario IPv6 acceda a este servicio, el servidor DNS64-NAT64, asigna una IPv6 para permitir el acceso a este usuario. Este proceso lo realiza de la siguiente manera:

Usuario → 2001:db8:20:8::5678

Aplicación → 172.16.8.6

Prefijo especial para mapear direcciones IPv4 a IPv6: 2001:db8:20:8:ffff::/96

IPv4 en binario → 10101100.00010000.00001000.00000110

IPv4 en hexadecimal → A C 1 0 0 8 0 6

Prefijo especial + IPv4 hexadecimal = IPv6 Asignada de aplicación

IPV6 Asignada de Aplicación → 2800:68:19:2408:ffff::AC10:0806

- Para un usuario externo, este método va a funcionar de la misma manera, con todas las reglas de acceso que se hayan configurado en el Firewall.

- El mecanismo implementado doble pila, funciona correctamente ya que permite a usuarios con IPv4, IPv6 o clientes dual Stack, acceder a los servicios. Este mecanismo es más fácil, sin embargo, no es la única solución si solo se apoya en este criterio, debido a que no todas las aplicaciones o servicios van a tener compatibilidad con IPv6, es ahí donde se utiliza el servidor DNS64-NAT64.
- El tener funcionando dos mecanismos de transición, demanda la utilización de más recursos de la red, lo que no es óptimo, pero mientras las redes se adecuen a utilizar IPv6, es una solución bastante fiable.
- En servidor de correo, accede a las aplicaciones IPv4, a pesar de que maneje solo IPv6, esto es debido al DNS64, que permite crear registros AAAA, para mantener la conexión a estas aplicaciones que en muchos casos no son compatibles con IPv6. Existirán algunas aplicaciones nuevas que manejen el nuevo protocolo, y esta es una solución que se podría utilizar en tanto se maneje como protocolo nativo IPv6.
- Los equipos de red, funcionan de manera mucho más rápida con IPv6, debido a que se analizó que realizan menor procesamiento porque la cabecera es mucho más eficiente, analizan menos campos en la misma, lo que permite que las comunicaciones sean más veloces.

3.3.3.5 Monitorización de la red con la implementación de IPv6. El monitoreo de la red es un tema relevante en las redes de hoy en día, pues se pueden analizar varios factores que determinen resultados que al administrador le pueden alertar de varios beneficios o problemas. En este caso, analizar el tráfico IPv4 o IPv6 de los diferentes servicios de red, se vuelve importante porque esto permite determinar el uso del protocolo con el que se está conectado a la Internet. (Acosta, 2014)

De la misma manera, permite de acuerdo a los resultados que evidencie este monitoreo, se va a poder determinar acciones para solucionar el problema y conformar planes de contingencia para que los servicios de la red funcionen correctamente y los usuarios no tengan inconvenientes al momento de acceder a cualquiera de ellos. (Acosta, 2014)

Por esta razón, se ha analizado si la red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, cuenta con alguna herramienta que permita analizar el tráfico de red y efectivamente existe implementada en la red la herramienta SNMP (Simple Network Management Protocol), que permite monitorear el tráfico que atraviesa por determinado dispositivo entre otras ventajas. Hay que tener en cuenta que el equipo que se monitorea es el que debe soportar SNMP para IPv6.

También, la herramienta Wireshark permite analizar con qué protocolos se está trabajando, que puede ser con IPv4 o IPv6, filtrado de paquetes entre otros. Existe la herramienta NetFlow que a diferencia de SNMP, permite obtener más información además de la carga de tráfico en la interfaz, por ejemplo, direcciones origen y destino o los protocolos de las capas superiores que atraviesan la interfaz. (Acosta, 2014)

Como se observa, existen muchas herramientas que pueden ser aprovechadas para el monitoreo de la red, cualquiera de ellas que se utilicen, permitirán analizar si la red, empieza ya a utilizar el protocolo IPv6 en sus servicios y si los usuarios hacen uso de la misma. Para esto, se ha realizado unas plantillas que permiten evidenciar los resultados de la monitorización que se haya realizado para conocer cuál es el estado de cada uno de los equipos, servicios o aplicaciones:

Este modelo fue desarrollado junto al Ingeniero Gabriel Bucheli, en el cual se van a detallar los equipos, servicios o aplicaciones que funcionen con IPv6, y con ayuda de cualquier herramienta que permita el análisis de tráfico para IPv4 o IPv6, se pueda determinar los respectivos resultados que permitan conocer si la red está manejando IPv6.

De la misma manera, es importante que los resultados con fecha y hora, se evidencien y se explique en qué periodo de tiempo estuvieron funcionando. Es sustancial que se realice este análisis porque va a permitir en caso de que no exista la disponibilidad del Administrador de la Red, que existan estos indicadores para diferentes factores que pueden ser clave para el buen desempeño de la red.

Estos modelos están diseñados para marcar resultados tanto en hardware como en software y en ellos se recopilarán los resultados del monitorio que se realice a la red.

Información para el seguimiento de Hardware			
Nombre del Responsable:		Ing. Gabriel Bucheli	
Cargo:		Administrador de la Red	
Área/Departamento		Dirección de Tecnologías Informáticas	
Fecha:		01/10/2016	
Resultado Obtenido	Estado	Última fecha de estado	Observaciones
Observaciones			


 Firma del Responsable

 
 Firma del Director de TICs

Información para el seguimiento de Software			
Nombre del Responsable:	Ing. Gabriel Bucheli		
Cargo:	Administrador de la Red		
Área/Departamento	Dirección de Tecnologías Informáticas		
Fecha:	01/10/2016		
Resultado Obtenido	Estado	Última fecha de estado	Observaciones
Observaciones			


 Firma del Responsable


 Firma del Director de TICs



3.3.3.6 Riesgos y plan de contingencia con IPv6. Sin duda que un proyecto tecnológico de este tipo, puede tener varios riesgos, es por eso que se van a explicar en la Tabla 15 los cuáles pueden ser:

Tabla 15: *Riesgos de Implementación de IPv6*

RIESGOS DE IMPLEMENTAR IPv6
Daño físico en el equipamiento de hardware
Pérdida de información
Incompatibilidad en hardware o software
Inestabilidad de las aplicaciones
Problemas con el funcionamiento del Sistema Operativo
Falta de compromiso por parte del personal del Departamento de Tecnologías Informáticas
Fallas de instalación y conexión de equipos
Falta de tiempo de adaptación al nuevo protocolo IPv6
Falta de capacitación al personal del Departamento de Tecnologías Informáticas

Fuente: Recuperado de http://www.magazcitur.com.mx/?p=568#.WB-xu_nhDIU

Así también, se van a analizar los riesgos de no implementar IPv6 en la Tabla 16:

Tabla 16: *Riesgos de no implementar IPv6.*

RIESGOS DE NO IMPLEMENTAR IPv6
Dificultad para el surgimiento de nuevas redes
Alargar el tiempo de proceso de inclusión digital o reducir la cantidad de nuevos usuarios
Dificultar el surgimiento de nuevas aplicaciones
El costo de no implementar IPv6 podrá ser mayor que el de no implementarlo
Limitación de los ISP's para innovar y ofrecer nuevos servicios a los clientes

Fuente: Recuperado de <http://www3.lacnic.net/eventos/lacnic23/miercoles/guillermo-cicileo-ipv6-para-tomadores-de-decisiones%20copia.pdf>

Por último, se va a analizar el plan de contingencia, para va a permitir prevenir los riesgos con el objetivo de garantizar el buen desempeño del proyecto que asegure un servicio eficiente. En la Tabla 17, se indican las acciones que se deben llevar a cabo para prevenir los riesgos descritos anteriormente.

Tabla 17. *Plan de contingencia*

Plan de contingencia
Respalda toda la información en dispositivos de almacenamiento como discos duros, memorias USB, entre otros.
Revisar los manuales para la manipulación de los equipos de comunicación.
Realizar el mantenimiento y revisión del equipamiento de comunicación.
Supervisar las aplicaciones que se hayan implementado con IPv6.
Revisar las configuraciones y pruebas de funcionamiento.
Realizar las actualizaciones de los sistemas operativos continuamente.
Ejecutar planes de capacitación continua al personal de TIC's
Elaborar un cronograma de trabajo que permita supervisar cada una de las actividades a cada miembro de TIC's.
Evaluar al personal de TIC's con la finalidad de reforzar conocimientos para la adopción de IPv6.

Fuente: Recuperado de <https://www.emaze.com/@AFRZQZOL/Plan-de-Transici%C3%B3n-IPv4-a-IPv6>

Capítulo IV

4. Análisis Costo-Beneficio

En este capítulo se va a analizar el costo-beneficio del proyecto, que determine las ventajas de una posible implementación. Las entidades privadas se evalúan en términos de ganancia, en tanto que las públicas realizan la evaluación en términos de bienestar general. Es decir que el Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, al ser una entidad pública, los objetivos que persigue como institución gubernamental, se basa en el bienestar general social, en otras palabras, se debe buscar el beneficio social mejorando los aspectos: ambiental, cultural, tecnológico, entre otros. (Fabrycky, 2012)

4.1 Costo Social

En términos generales, el costo se refiere al precio que se debe pagar por un artículo. Sin embargo, el dinero proporcionado a las entidades públicas es por parte del Estado, entonces la obligación moral de las entidades públicas es invertir productivamente este dinero. Puesto el análisis que se pretende representar, se va a considerar como un costo social. El costo social, es el que debe pagar la sociedad cuando ocurre un acto de utilizar un recurso, y este costo puede estar ya incluido en los impuestos que los ciudadanos pagan al Estado. (Miller, 2010)

Para el análisis de los costos se van a considerar los siguientes aspectos:

4.2 Recurso Humano/Tecnológico

Son las personas que van a llevar a cabo la implementación de este proyecto. El personal del Departamento de Tecnologías de la Información, debe ser capacitado debido a que no se conoce mucho del tema y es necesario que se preparen en cuanto dure este proceso.

4.2.1 Costo de capacitación e implementación. Para realizar la estimación del costo que incluya la capacitación a todo el equipo que participará en el proyecto y la implementación para el protocolo IPv6, se ha tomado en cuenta una proforma que se pidió a la empresa Imbatec, debido a su pronta respuesta. Es una empresa que presta los servicios tecnológicos requeridos para este proceso ya que cuenta con ingenieros con certificación Cisco. De la misma manera tomando en cuenta los cursos que LACNIC ofertan para el conocimiento sugerido para este proceso que se encuentra en <http://www.lacnic.net/web/anuncios/2015-cursos-ipv6>, se ha realizado el siguiente análisis que se presenta en la Tabla 18.

Tabla 18: *Presupuesto de Capacitación e Implementación.*

PRESUPUESTO DE CAPACITACIÓN E IMPLEMENTACIÓN			
Descripción	Cantidad	Valor Unitario	Valor total
Recurso Humano: 5 personas para capacitación	140 horas	\$30	\$4200
Implementación del Proyecto (Configuraciones en todo el equipamiento de red)	80 Horas	\$30	\$2400
Total:			\$6600

Fuente: Proforma Imbatec, Cursos LACNIC.

4.3 Hardware.

Una vez que se ha analizado el equipamiento de red, se pudo identificar que existen algunos equipos que deben ser sustituidos por otros que tengan las condiciones óptimas para poder funcionar adecuadamente, debido a que estos equipos tienen ya 10 años trabajando, y según el análisis realizado en el inventario de hardware se deben realizar estos cambios. Y con respecto al soporte IPv6, los demás equipos, están listos para ser configurados.

4.3.1 Costos de Hardware. Como se analizó en el inventario de hardware, existen equipos que deben ser sustituidos para la adopción del nuevo protocolo. En la Tabla 19, se describen los equipos que deben ser sustituidos y el respectivo costo de cada uno de ellos.

Tabla 19: *Presupuesto de Hardware.*

PRESUPUESTO DE HARDWARE			
Unidad	Descripción	Valor Unitario (USD)	Valor Total (USD)
2	Switch de Acceso 4250T	1000	2000
2	Switch de Distribución 4250T	925	1850
1	Switch de Acceso 5500G/52	1046	1046
2	Switch de Distribución 4500	1139	2278
TOTAL			7174

Fuente: Anexo F.

4.4 Software

El Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, utiliza en la mayoría de sus sistemas operativos software libre. Para realizar la simulación de este proyecto se hizo uso del mismo y se utilizaron los siguientes:

- Centos versión 6 (Sistema Operativo)
- GNS3 versión 1.3.11 (simulador de red)
- VMWare 11.1 (Plataforma para máquina virtual)
- Wireshark 2.0.3 (Analizador de red)

En el caso de GNS3, VMWare y Wireshark son versiones de software que ya se encuentran liberadas.

4.4.1 Costo de Software. El software libre no es sinónimo de software gratuito, libre quiere decir que son aquellos que su uso, modificación y distribución son permitidos a todos. Sin embargo, para la instalación en un equipo se requiere de unidades de almacenamiento en la que se encuentre el software. (Debian, 2016)

En la Tabla 20 se indican los costos del software utilizado para la instalación en los respectivos equipos.

Tabla 20: *Presupuesto de Software*

PRESUPUESTO DE SOFTWARE	
Descripción	Valor (USD)
4 DVD's S.O Debian	12
4 DVD's Centos 6.5	12
TOTAL	24

Fuente: Recuperado de <https://www.debian.org/intro/about.es.html>

4.5 Costo total del proyecto

En la Tabla 21 se colocan los costos de capacitación e implementación, hardware y software que se necesitan para la puesta en marcha de este proyecto. También es importante que se considere un 10% adicional en caso de que se requiera contratar asesoramiento adicional en algunas configuraciones que pueden considerarse complejas. (Diaz, 2008)

Tabla 21: *Presupuesto Total del proyecto*

PRESUPUESTO TOTAL	
Descripción	Valor (USD)
Presupuesto de Capacitación e Implementación	6600
Presupuesto de Hardware	7174
Presupuesto de Software	24
Imprevistos (10%)	1379.80
TOTAL	15.177,80

Fuente: Elaboración propia

En la actualidad, las redes están ya implementando el protocolo IPv6, pero lo están realizando a paso lento, por este motivo es importante que se trate de incentivar a las grandes y medianas empresas a que lo incorporen en sus redes para poder beneficiarse de las ventajas que la tecnología que hoy en día avanza de manera impresionante.

Así mismo con la expansión de la red, se dará pie para el surgimiento de nuevos negocios, el uso de nuevos dispositivos, que contribuirán sin duda al desarrollo empresarial y laboral del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra.

Razón Beneficio Costo

Para realizar este análisis, es importante considerar que, para esta entidad gubernamental, no se puede medir las ganancias en valores monetarios, más bien estas ganancias se transforman en beneficios que van a entregar a los usuarios internos como externos. También los beneficios que serán directamente para la red de datos del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra. Para ello, se van a describir estos beneficios en base a indicadores IPv4/IPv6 que se han realizado a lo largo de este estudio.

Autoconfiguración de dispositivos

- La característica plug and play, mecanismo que facilita a los usuarios en este caso a los internos la conexión automática a la red. Esto permite facilitar el proceso de administración de la red, ya que se asignará a cada usuario automáticamente una o varias direcciones IPv6.

Calidad de servicio a aplicaciones o servicios

- En el aspecto medioambiental, se pueden reducir costos, por ejemplo, si algún funcionario de la entidad tiene que viajar a una reunión importante en otro sitio, puede realizar desde la empresa una videoconferencia, aprovechando la mejora en cuanto a calidad de servicio.
- Lo que facilita la conexión extremo a extremo, que permite ampliar las ideas y dar mayor flexibilidad a desarrolladores, que de la misma manera reduce los costos de la técnica mencionada anteriormente.
- Con la mejora en la cabecera de IPv6 de etiqueta de flujo, permite que las características de calidad de servicio que existen en IPv4, sean mejoradas en IPv6, garantizando que las aplicaciones en tiempo real como videoconferencias o VoIP que pueden ser ofrecidas al usuario final mejoren de esta manera.

Implementación de máquinas inteligentes

- Cuando la implementación de IPv6 concluya, la mayor parte de tráfico en las redes de comunicación consistirá en transacciones entre máquinas sin la intervención por parte de los humanos. Esta evolución representará un cambio importante en el sector de las comunicaciones.
- La calidad de la experiencia para el usuario, puede mejorarse integrando la automatización de procesos en la entidad con la ayuda de objetos inteligentes conectados con direcciones IPv6 únicas.

Creación de Redes de Sensores

- Las redes de sensores que consisten en sensores autónomos que colaboran en la supervisión de condiciones físicas y medioambientales concretas. Permitirán que se controle varios parámetros como calor, temperatura, presión, sonido, vibración, entre otros. Pueden integrarse a sistemas inteligentes que permitan ser monitoreados cada uno, esto permitirá que la ciudad se vaya convirtiendo en una Smart City que beneficiará a los seres vivos de la ciudad de Ibarra.

Proyectos ambientalistas

- Pueden crearse algunos, por ejemplo, el control de velocidad de los vehículos públicos, que permitirá contribuir a mejorar la seguridad en el transporte para la ciudadanía.
- Beneficios de ahorro eléctrico, se pueden crear una red eléctrica inteligente que tenga por objetivo modernizar el sistema eléctrico con comunicaciones bilaterales para supervisar y gestionar la producción, transmisión y distribución de energía eléctrica conjuntamente con la empresa Emelnorte, que contribuye al beneficio para los ciudadanos. Esto con el despliegue de IPv6 que se vea implementado en el Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra.

Seguridad

- La seguridad es un aspecto importante en cualquier red, es por ello que el protocolo IPv6 incluye este parámetro y puede proporcionar encriptación, autenticidad e integridad de la información.

Acceso a aplicaciones o servicios

- Los servicios o aplicaciones que manejen Dual Stack, permitirá que usuarios tanto IPv4 como IPv6 puedan acceder a ellos, debido a que todas las peticiones que se realizan a las aplicaciones desde un host IPv4 se responden desde los servidores IPv4, de igual manera las peticiones de un host IPv6 serán contestadas desde servidores IPv6.
- Al utilizar el mecanismo NAT64-DNS64, los usuarios nativos IPv6 acceden directamente a internet o a la nube de aplicaciones IPv6, pero cuando se necesita ir desde un usuario nativo IPv6 hacia la nube de aplicaciones IPv4, Nat64 realiza el mapeo que se necesita para comunicar a estos usuarios.
- IoT (Internet de las cosas), es uno de los aspectos más sobresalientes con IPv6, que será la red que interconecta objetos comunes equipados con módulos de inteligencia miniaturizados, que dará pie al desarrollo de grandes proyectos tecnológicos dedicados a mejorar la calidad de vida de los ciudadanos de la ciudad de Ibarra.

CONCLUSIONES

- El desarrollo de la propuesta de transición de servicios de IPv4 a IPv6 para el Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, permitió desarrollar un modelo que vaya de la mano con el plan de acción propuesto por el MINTEL, permitiendo una transición ordenada y eficaz para la coexistencia de los dos protocolos.
- El estudio del protocolo IPv6, permitió analizar las ventajas que tiene sobre IPv4, por ejemplo, la autoconfiguración de los hosts, mayor utilización de IP's, mejor procesamiento de la información, movilidad IP, incremento de seguridad aprovechando el protocolo IPsec.
- El equipamiento de red del GAD-I, en algunos equipos, se requiere la actualización de los IOS en específico en todas las versiones anteriores a la 12.0()T, en otros casos es necesario realizar el requerimiento de nuevos equipos debido a su tiempo de vida útil en el que se recomienda que los equipos no superen los diez años de uso.
- En cuanto a actualizaciones de software, en los sistemas operativos que manejan software libre, el kernel requerido para funcionar con IPv6 se tiene a partir de la versión 2.4 en adelante, se cumple con este objetivo y de la misma manera todos ellos tienen el soporte para IPv6.
- Es necesario que se analice el servidor de base de datos, debido a que las aplicaciones Web como correo necesitan de la información albergada en el mismo, por lo tanto, se debe analizar cuidadosamente cuales deben ser los servicios que necesiten mayor prioridad de transición.
- La elección del mecanismo de transición que se ha decidido utilizar es doble pila o dual Stack, que permite mantener la red funcionando tanto en IPv4 como en IPv6, teniendo como ventaja manejar los dos protocolos y tener coexistencia con los mismos. Si se llegara a dejar de utilizar la red IPv4, la red IPv6 estará disponible, permitiendo que la red siga estando disponible para todos los usuarios.
- Para mantener conectividad a usuarios que solo utilicen IPv6 y deban acceder a aplicaciones que se encuentren solamente utilizando IPv4, se hace necesaria la implementación de un

traductor DNS64 y NAT64, el cual asignará una IPv6 a la aplicación IPv4 mediante una traducción que se consigue mapeando una dirección IPv4 a una IPv6.

- En cuanto a seguridad, se ha decidido aprovechar el protocolo IPsec, ya que su uso es imprescindible por ejemplo en el servidor WEB, debido a que se maneja información delicada, por tanto, se ha implementado en dispositivos de gateway de seguridad o llamados también como intermedios utilizando el modo túnel con encapsulación ESP, el cual proporciona autenticación, integridad y confidencialidad en los paquetes transmitidos.
- Al realizar el análisis en cuanto a costos y beneficios, se determinó que el GAD-I, al ser una entidad gubernamental, cuando genera un proyecto, no se espera que se generen ganancias económicas y que se recupere el dinero invertido en un periodo de tiempo, más bien se traduce a beneficios sociales que permitan obtener satisfacción a los usuarios.
- Con el protocolo IPv6, se tiene capacidad para más usuarios, más redes, esta ventaja de IPv6 puede ser aprovechada para la implementación de proyectos tecnológicos que tengan relación con el tema IoT, que el GAD-I, puede aprovechar y trabajar en conjunto para lograr encaminar a la ciudad de Ibarra para ser una Smart City.
- Este proyecto, es realizado con la finalidad de que las empresas públicas o privadas de la ciudad de Ibarra, se motiven para empezar a desplegar IPv6 en las redes, de modo que se aprovechen todos los beneficios que se tiene al utilizar el protocolo de nueva generación.
- IPv6 presenta significativas oportunidades para crear modelos empresariales innovadores, esto debido a que se pueden asignar direcciones únicas a dispositivos cotidianos conectados lo que permitirá la generación de aplicaciones y servicios tecnológicos que permitirá la automatización, productividad y eficiencia de la empresa que maneje su red con el nuevo protocolo.

RECOMENDACIONES

- Es importante que, a partir de este estudio, se realicen nuevas investigaciones que permitan implementar en todos los servidores y equipos el soporte del protocolo IPv6 que permitirá que los servicios sigan subsistiendo, en caso de que el protocolo IPv4 deje de ser utilizado, y de la misma manera, que siga siendo visto por cualquier usuario, especialmente el que utilice IPv6 de forma nativa.
- Es importante que exista la motivación por parte del Departamento de Gestión de Tecnologías e Información para empezar a utilizar IPv6, como ya se ha mencionado, por todas las ventajas que se tiene al manejar este protocolo y al existir el desarrollo de la tecnología permitirá sin duda la creación de muchas más redes que se vean implementadas en proyectos del futuro como es IoT.
- Las configuraciones en cada uno de los equipos para la implementación del mecanismo de transición elegido, debe realizarse con el personal capacitado para evitar cualquier falla de operación en la red.
- Se recomienda que cada uno de los servidores que se han mencionado WEB. Correo Electrónico y el DNS64-NAT64, se encuentren funcionando en equipos diferentes, ya que tienden a ser utilizados con frecuencia, así el proceso de peticiones por parte de los usuarios permitirá respuestas más rápidas.
- En cuanto al costo de implementación y capacitación del proyecto presente, se podría llegar a un convenio con la Universidad Técnica del Norte con el Gobierno Autónomo Descentralizado de la ciudad de Ibarra, que permita a los estudiantes de la carrera de Ingeniería en Electrónica y Redes de Comunicación aplicar sus conocimientos en cuanto al tema propuesto, enriqueciendo sus conocimientos y al mismo tiempo al Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra permitiendo que se mantenga a la vanguardia de las nuevas tecnologías.

- Para la demostración de los servidores WEB y Correo Electrónico se utilizó el sistema operativo Centos, ya que permite un buen desempeño en cuanto a este tipo de configuraciones y de la misma forma el simulador GNS3 para implementar los servicios y realizar las pruebas de funcionamiento.
- Tomar en cuenta la vida útil de los equipos, para que de esta manera, los equipos que tienen un tiempo de uso que sobrepasa los diez años, sean reemplazados por equipos con nuevas actualizaciones para un buen desempeño de la red.

GLOSARIO DE TÉRMINOS

TÉRMINO	DESCRIPCIÓN
3DES	En criptografía, Triple DES (Data Encryption Standard - Algoritmo de Encriptación Estándar), se le llama al algoritmo que hace triple cifrado del DES. También es conocido como TDES o 3DES, fue desarrollado por IBM en 1998 y es utilizado para la seguridad en redes informáticas.
A	Registro de dominio IPv4 para un host IPv4.
AAAA	Registro de dominio IPv6 para un host IPv6.
ARIN	Registro Regional de Internet para América.
AS	Sistema Autónomo que realiza su propia gestión del tráfico que fluye entre él y los restantes Sistemas Autónomos que forman Internet.
BGP	Border Gateway Protocol, protocolo de enrutamiento dinámico.
CIDR	Classless Interdomain Routing (enrutamiento entre dominios sin clases).
CNAME	Canonical Name, utilizado en servidores DNS. Los registros CNAME se suelen utilizar para asignar un subdominio, como www o mail al dominio que aloja el contenido de dicho subdominio.
DES	Data Encryption Standard (algoritmo de cifrado), utilizado en seguridad de la información.
DHCP	Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Host).
DNS64	Domine Name System 64 (Sistema de nombres de dominio 64).
DS-lite	Dual stack lite (doble pila), mecanismo de transición.
EIA	Electronics Industry Association (Alianza de Industrias Electrónicas). Desarrolla normas y publicaciones sobre las principales áreas técnicas: los componentes electrónicos, electrónica del consumidor, información electrónica, y telecomunicaciones.
EIGRP	(Protocolo de enrutamiento de gateway interior mejorado).

ESP	Encapsulated Security Payload (Carga de seguridad encapsulada), seguridad de la información.
FTP	File Transfer Protocol (Protocolo de Transferencia de Archivos).
Gbps	Gigabit por segundo, medida utilizada para velocidad de la información.
GNS3	Programa que funciona como simulador de red.
HTTP	Hypertext Transfer Protocol (en español protocolo de transferencia de hipertexto).
HTTPS	Hypertext Transfer Protocol Secure (Protocolo seguro de transferencia de hipertexto).
IANA	Internet Assigned Numbers Authority (Autoridad de Asignación de Números de Internet).
ICMP	Protocolo de Mensajes de Control de Internet.
ICMPv6	Protocolo de Mensajes de Control de Internet versión 6.
ID	Identificador utilizado en algunos casos para las redes de información.
IETF	Internet Engineering Task Force (Grupo de Trabajo de Ingeniería de Internet).
IGP	Interior Gateway Protocol (Protocolo de pasarela Interno).
IKE	Internet Key Exchange (Intercambio de clave de Internet).
IOS	Sistema operativo de simulación equipos CISCO.
IoT	Internet de las cosas.
IPSec	Internet Protocol Security, utilizado en seguridad de la información.
IPv4	Protocolo de Internet versión 4 (Internet protocol versión 4).
IPv6	Protocolo de Internet versión 6 (Internet protocol versión 6).
ISAKMP	Internet Security Association and Key Management Protocol, seguridad de la información.
ISO 9001	Norma de sistemas de gestión de la calidad (SGC) reconocida internacionalmente.
ISO/IEC 11801	Especifica sistemas de cableado para telecomunicación de cableado estructurado.
ISP	Internet Service Provider (proveedor de servicios de Internet).

kernel	Núcleo del sistema operativo.
LACNIC	Latin America & Caribbean Network Information Centre (Registros de Direcciones IPv4/IPv6).
LAN	Local Area Network (red de área local).
LSA	link-state advertisement (estado de una red o de un router).
MAC	Media Access Control o control de acceso al medio
Mbps	Megabits por segundo, unidad de medida para la velocidad de la información
MD5	Message-Digest Algorithm 5 (Algoritmo de Resumen del Mensaje 5), utilizado para la seguridad de la información.
MDF	Medium Density Fibreboard (elaborado con fibras de madera).
MLD	Descubrimiento de escucha multidifusión, utilizado en la transferencia de la información.
MTU	Maximum Transmission Unit (Unidad Maxima de Transferencia), de la información.
NAT	Network Address Translation (traducción de direcciones de red).
ND	Neighbor Discovery (Descubrimiento de vecinos), utilizado en las redes para la transferencia de la información.
NIC	Network Interface Card (Tarjeta de Interfaz de Red).
NS	Name Server, utilizado en servidores DNS.
NTP	Network Time Protocol, utilizado para ciertos protocolos de red.
OSPF	Open Shortest Path First (protocolo de direccionamiento de tipo enlace-estado).
PAT	Port Address Translation (traducción de dirección de red).
PDU	Unidades de datos de protocolo.
PTR	Apuntador, registro inverso, utilizado en servidores DNS.
QoS	Calidad de servicio, entendida como satisfacción de las necesidades y expectativas del cliente
RFC	Request for Comments, memorando que ingenieros o expertos en la materia han hecho llegar al IETF, el consorcio de colaboración técnica más importante en Internet, para que éste sea valorado por el resto de la comunidad.

RIP	Routing Information Protocol (protocolo de información de encaminamiento).
RIR's	Registros Regionales, es una organización que supervisa la asignación y el registro de recursos de números de Internet dentro de una región particular del mundo. Los recursos incluyen direcciones IP (tanto IPv4 como IPv6) y números de sistemas autónomos (para su uso en encaminamiento BGP).
RJ-45	interfaz física comúnmente utilizada para conectar redes de computadoras, con cableado estructurado.
RSA	Rivest, Shamir y Adleman (sistema criptográfico de clave pública), seguridad de la información.
SA	Asociación de seguridad, utilizado en la seguridad de la información.
SDF	Bloque secundario de fibra óptica.
SHA	(Secure Hash Algorithm, Algoritmo de Hash Seguro), utilizado en la seguridad de la información.
SIP	Session Initiation Protocol (SIP o Protocolo de Inicio de Sesiones).
SSH	Secure Shell (Intérprete de órdenes seguro), es un cifrado de protocolo de red para servicios de red de operación segura a través de una red no segura. La aplicación de ejemplo más conocido es el de control remoto de acceso a los sistemas informáticos de los usuarios.
TCP	Transmission Control Protocol (Protocolo de Control de Transmisión).
TIA-942	Norma de infraestructura de telecomunicaciones para centros de datos.
ToS	Tipo de Servicio, servicio diferenciado. Método de definición de precedencia para un tipo particular de tráfico para fines de calidad del servicio.
Transición	Paso o cambio de un estado
UDP	User Datagram Protocol (Protocolo de datagrama de usuario)
UTP	Unshielded twisted pair o par trenzado sin blindaje
VoIP	Voice Over Internet Protocol (Voz sobre protocolo de internet)
WEB	Conjunto de información que se encuentra en una dirección determinada de internet.

BIBLIOGRAFÍA

- 6SOS. (5 de Enero de 2004). *IPv6 Servicio de Información y Soporte* . Obtenido de El protocolo IPv6: http://www.6sos.org/documentos/6SOS_El_Protocolo_IPv6_v4_0.pdf
- Acosta, A. y. (2014). *IPv6 para operadores de Red*. (Ebook, Editor) Obtenido de http://portalipv6.lacnic.net/wp-content/uploads/2014/12/ipv6_operadores_red.pdf
- Alonso, J. C. (2001). *Neighbor Discovery*. Obtenido de http://www.labs.lacnic.net/site/sites/default/files/ES-Neighbor_y_MTU-Discovery.pdf
- Amelines, J. (2012). *IPv4toIPv6*.
- APR. (2016). *Qué es un servidor y cuáles son los principales tipos de servidores (proxy,dns, web,ftp,pop3 y smtp, dhcp...)*. Obtenido de http://aprenderaprogramar.com/index.php?option=com_content&view=article&id=542:que-es-un-servidor-y-cuales-son-los-principales-tipos-de-servidores-proxydns-webftppop3-y-smtp-dhcp&catid=57:herramientas-informaticas&Itemid=179
- Ariganello, E. (16 de Noviembre de 2012). *Aprende Redes*. Obtenido de INTRODUCCIÓN AL GNS3: <http://aprenderedes.com/2012/11/introduccion-al-gns3/>
- Carlos, J. C. (s.f.). *Direccionamiento IPv6*. Obtenido de <http://www.labs.lacnic.net/site/sites/default/files/001-Direccionamiento%20y%20Protocolo%20IPv6.pdf>
- Cedeño., J. C. (Febrero de 4 de 2013). *Propuesta de transición de IPv4 a IPv6*. Obtenido de Tunel 6to4: <http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf>
- CHECKPOINT. (5 de septiembre de 2015). *Check Point 4600 Appliance | Ficha de datos*. Obtenido de CHECK POINT 4600 APARATO: <https://www.checkpoint.com/downloads/product-related/datasheets/4600-appliance-datasheet.pdf>

Cicileo, G. R. (2009). *IPv6 para todos*. (E-Books, Ed.) Buenos Aires, Argentina.

CISCO. (2013). *Entendimiento IPv6, Subredes y Direccionamiento*.

CISCO. (17 de Octubre de 2016). *Túnel IPv6 a través de una Red IPv4*. Obtenido de http://www.cisco.com/cisco/web/support/LA/102/1027/1027026_ipv6tunnel.pdf

CISCO Academy Network. (2009). *EIGRP*. Obtenido de http://giret.ufps.edu.co/cisco/descargas/tutoriales_docentes/ITN_PT_ILM-Docs%20Simulaciones.pdf

CISCO Systems. (s.f.). *OPSFv3 para IPv6*. Obtenido de http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15-sy/iro-15-sy-book/ip6-route-ospfv3.html

Corporación Digital Colombia. (2016). *Colombia Digital*. Obtenido de <https://colombiadigital.net/actualidad/articulos-informativos/conceptos-tic.html>

De la Luz, S. (4 de Noviembre de 2010). *Criptografía : Algoritmos de cifrado de clave simétrica*. Obtenido de <http://www.redeszone.net/2010/11/04/criptografia-algoritmos-de-cifrado-de-clave-simetrica/>

Debian. (5 de Julio de 2016). Obtenido de <https://www.debian.org/intro/about.es.html>

Deering, S. (11 de Agosto de 2011). *ICMPv6 para IPv6*. Obtenido de www.ietf.org/rfc/rfc2463.txt

Diaz, J. (Mayo de 2008). *Formulación y evaluación de proyectos*. Obtenido de <http://www.eumed.net/ce/2008a/>

Fabrycky, W. (2012). *Decisiones Económicas, Análisis y Proyectos*. Ed. Prentice Hall.

Fundamentos de Redes. (2013). Obtenido de <https://sites.google.com/site/fundamentosderedesuteztic1h/home>

Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra. (12 de Abril de 2015). *Ibarra, ciudad a la que siempre se vuelve*. Obtenido de <http://ibarra.gob.ec/web/index.php/informativo/ibarra1234/informacion-general>

- Herramientas WEB. (2013). *El protocolo Http*. Obtenido de <http://neo.lcc.uma.es/evirtual/cdd/tutorial/Indice.html>
- Ibarra, G. A. (2015). *Servidores virtuales*. Ibarra.
- Iglesias, S. (Noviembre de 2011). Análisis del protocolo IPsec. 51-63. Obtenido de Telefónica Investigación y Desarrollo.
- INSAT. (s.f.). *La electrónica*. Obtenido de Sistema Hexadecimal: http://www.ite.educacion.es/formacion/materiales/47/cd/mod1b/1bb_4.htm
- Internet Society. (2016). *Breve historia del Internet*. Recuperado el 25 de Abril de 2016, de <http://www.internetsociety.org/es/breve-historia-de-internet>
- Kent, a. R. (1998). *Protocol Encapsulating Security Payload (ESP)*. New York.
- LACNIC. (2012). *No hay más direcciones IPv4 en América Latina y Caribe*. Obtenido de <http://www.lacnic.net/web/anuncios/2014-no-hay-mas-direcciones-ipv4-en-lac>
- Lujan, P. (4 de Junio de 2015). *Error capa 8*. Obtenido de ¿Porqué se llama IPv4 e IPv6?: <https://errorcapa8.wordpress.com/2015/06/04/por-que-se-llaman-ipv4-e-ipv6/>
- MacDonald, M. A. (2008). *Aspectos básicos de networking*. Madrid, España: Pearson.
- Microsoft. (Enero de 2005). *Descubrimiento de escucha de multidifusión (MLD)*. Obtenido de [https://msdn.microsoft.com/es-es/library/cc776494\(v=ws.10\).aspx](https://msdn.microsoft.com/es-es/library/cc776494(v=ws.10).aspx)
- Miller, R. L. (2010). *Microeconomía Moderna*. Harla.
- Ministerio de Industria, energía y turismo de España. (2013). *IP.v6 protocolo de internet versión 6*. Obtenido de Características de IPv6: <http://www.ipv6.es/es-ES/Faqs/Paginas/tecnicas.aspx>
- Ministerio de Telecomunicaciones y Sociedad de la Información. (2012). Obtenido de <http://www.telecomunicaciones.gob.ec/ecuador-lidera-el-cambio-a-la-ipv6-que-es-por-que-el-cambio-en-que-nos-beneficia/>

- Moya, F. A. (Septiembre de 2009). *Rediseño de la Red ISP READYNET CIA. LTDA., PROCEDIMIENTO PARA CONVERTIR AL ISP EN UN SISTEMA AUTÓNOMO*. Obtenido de <http://bibdigital.epn.edu.ec/bitstream/15000/1819/1/CD-2405.pdf>
- Network Information Center México S.C. (2010). *IPv6 Mx*.
- Núñez, D. (2009). *Estudio de migración de IPv4 a IPv6 para la empresa proveedora de Internet Milltec S.A. Quito*.
- Palet, J. (Abril de 2007). *The Choice: IPv4 Exhaustion or Transition to IPv6*.
- Pérez, S. (2001). *Análisis del protocolo IPSec: el estándar*. Obtenido de <https://www.movistar.es/on/es/micro/seguridad/IPSec.pdf>
- Tanenbaum, A. S. (2011). *Redes de computadoras* (Vol. V). México: Pearson.
- TRIPOD. (2016). *Protocolos de Enrutamiento*. Obtenido de RIPng: <http://andersonramirez.tripod.com/protocolo.htm>
- Universidad de San Carlos de Guatemala. (Agosto de 2009). *MIGRACIÓN DEL PROTOCOLO IPv4 A IPv6 EN UNA RED, LOS BENEFICIOS Y SEGURIDAD QUE CONLLEVA ESTE CAMBIO*. Obtenido de Identificación de Direcciones IPv6: http://biblioteca.usac.edu.gt/tesis/08/08_0246_EO.pdf
- Universidad Técnica Particular de Loja. (16 de Julio de 2010). *Propiedad planta y equipo*. Obtenido de <http://elizaherrera3/propiedad-planta-yequipo>

ANEXOS

ANEXO A: Especificaciones técnicas de switches del Cuarto de Equipos del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra

En el Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra se tienen dos clases de Switches 3COM y CISCO y se van a detallar cada uno de los modelos, para verificar el soporte para IPv6.

Switch CISCO CATALYST 4503-E

Este Switch se lo denomina también núcleo, porque permite la conexión entre dependencias externas e internas mediante fibra óptica y UTP del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra. Proporciona un alto rendimiento de aplicaciones, video y ahorro de energía con la infraestructura de apoyo a la resistencia, virtualización y automatización. Además, escalabilidad y servicios con menor costo. En la tabla 1 se proporcionan las principales características para conocer si tiene soporte para IPv6.



Figura A- 1. *Switch Core 4503*

Fuente: <http://www.cisco.com/c/en/us/support/switches/catalyst-4503-e-switch/model.html>

Tabla A. 1 Descripción Switch Core 4503

CARACTERÍSTICAS	
Descripción de capas	Conmutador de capas 2, 3 y 4. Encapsulación IEEE 802.1Q VLAN, 802.1s, 802.1w, 802.3ad, 802.1x, entre otros. 2.048 VLANs activas y 4.096 IDs de VLAN por switch (CoS) para tráfico, direccionamiento IP estático Protocolo de información de enrutamiento (RIP) y RIP2 ICMP, QoS, ACL, SNMP 1, SNMP 2, SNMP 3.
Dimensiones (H x W x D)	12.25 x 17.31 x 12.50 pulg. (31.12 x 43.97 x 31.70 cm)
Fuente de alimentación	1000W AC
Memoria	RAM: 256MB FLASH: 32MB
Procesador	CPU: 266 MHz
Puertos	48 Gigabit Ethernet 10/100/1000 Mbps 8 puertos SPF 1000BASE-T
Soporte IPv6	IPv6 en el hardware, proporcionando reenvío a velocidad de cable para redes IPv6 y soporte para doble pila con el uso innovador de recursos

Fuente: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-series-switches/data_sheet_c78-686325.html&prev=search

✚ Switch CISCO CATALYST 2960 (24/48 PUERTOS)

Interconectar los segmentos de red del edificio principal del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra. Además, son el borde de ataque de nivel 2, proporcionando una mayor facilidad de uso, las operaciones comerciales de alta seguridad, mejora de la sostenibilidad, y una experiencia de red sin fronteras. El Cisco Catalyst 2960-S y la serie 2960 son switches de acceso de configuración fija diseñada para las empresas, medianas, y las redes de sucursales para ofrecer un menor coste total de propiedad.



Figura A- 2. Switch CISCO 2960

Fuente: <http://www.secureitstore.com/C2960-24TC-L.asp>

Tabla A. 2. Descripción Switch CISCO 2960

CARACTERÍSTICAS	
Descripción de capas	Conmutador de capa 2 Encapsulación IEEE 802.1Q VLAN, IEEE 802.1p, IEEE 802.1w, IEEE 802.1x, IEEE 802.3ab Soporta QoS Protocolos de gestión: Telnet, RMON 2, RMON 1, SNMP 1, SNMP 3, SNMP 2c, TFTP, SSH Protocolos de red admitidos: ACL, ARP, DiffServ, IGMP, IP, RADIUS, SSH, TCP, UDP, DHCP, TFTP
Dimensiones	Ancho 44.5 cm x Profundidad 23.6 cm x Altura 4.4 cm
Fuente de alimentación	Interruptor de alimentación: 464W
Memoria	RAM: 64 MB FLASH: 32MB
Procesador	Single core
Puertos	Fast Ethernet 24/48 -10/100 Mbps Gigabit Ethernet: 2- 10/100/1000 Mbps
Soporte IPv6	RFC 1981 - Unidad de transmisión máxima (MTU) el descubrimiento de ruta IPv6

Fuente: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-series-switches/product_data_sheet0900aecd80322c0c.html

Switch 3COM 4500 G

En el Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, este switch permite la conexión de los servidores del cuarto de equipos, tiene como características avanzadas de voz optimizados tales como alimentación a través de Ethernet (PoE) y VLAN de voz automática y QoS. Es ideal para empresas y medianas empresas que desean construir una red convergente segura.



Figura A- 3. Switch 3COM 4500G

Fuente: <http://articulo.mercadolibre.com.mx/MLM-550822109-switch-3com-4500-g-pwr-24-puertos- JM>

Tabla A. 3. Descripción Switch 3COM 4500G

CARACTERÍSTICAS	
Descripción de capas	Conmutador Capas 2, 3 Capa 2: IEEE 802.Q VLANs, 802.3ad, control de flujo 802.3x full-duplex, STP 802.1D, RSTP 802.1w, multicast IGMP v1/v2. Capa 3: Routing basado en hardware, ECMP, ARP, interfaces virtuales, routing estático/dinámico, RIPv1/v2, OSPF, Soporta QoS.
Dimensiones	Alto: 43,6 mm; ancho: 440 mm, fondo: 450 mm
Fuente de alimentación	Voltaje de entrada: 90-240 VAC
Memoria	FLASH: 128MB
Procesador	CPU: 264MHz
Puertos	24 Gigabit Ethernet 10BASE-T/100BASE-TX/1000BASE-T 4 puertos de uso dual 10/100/1000 ó SPF
Soporte IPv6	Filtrado de 128 grupos de multidifusión Hardware preparado para IPv6

Fuente: [https://www.thomas-](https://www.thomas-krenn.com/redx/tools/mb_download.php/mid.101112078065055104101048043079052061/Datenblatt_Switch_3com_4500G_Englisch_1.pdf)

[krenn.com/redx/tools/mb_download.php/mid.101112078065055104101048043079052061/Datenblatt_Switch_3com_4500G_Englisch_1.pdf](https://www.thomas-krenn.com/redx/tools/mb_download.php/mid.101112078065055104101048043079052061/Datenblatt_Switch_3com_4500G_Englisch_1.pdf)

Switch 3COM 5500 SI

Se lo utiliza para interconectar los segmentos de red del edificio principal. El 3Com Switch 5500 son una solución de última generación para la entrega de los niveles de primas de rendimiento, seguridad y fiabilidad. Sus globales basadas en estándares características ayudan a crear un futuro a prueba. Proporciona a la red de la empresa que proporciona más seguridad y convergencia



Figura A- 4. Switch 3COM 5500

Fuente: <http://www.line1partners.com/catalog/3comswitches.htm>

Tabla A. 4. Descripción Switch 3COM 5500

CARACTERÍSTICAS	
Descripción de capas	Conmutador Capas 2, 3 Capa 2: IEEE 802.Q VLANs, 802.3ad, control de flujo 802.3x full-duplex, STP 802.1D, RSTP 802.1w, Capa 3: Enrutamiento estático/dinámico, RIPv1/v2, OSPF, ARP, interfaces virtuales.
Dimensiones	Altura: 43,6 mm; anchura: 440 mm; fondo: 270 mm
Fuente de alimentación	Soporta múltiples modos de alimentación: sólo AC, AC y DC, y sólo DC
Memoria	RAM:256 MB FLASH: 32MB
Procesador	Cache 2.80ghz 800mhz
Puertos	48 Fast Ethernet - 10/100 Mbps BASE T/TX 4 Gigabit Ethernet - 1000 Mbps BASE-X SPF
Soporte IPv6	Commutación basada en estándares (incluyendo IPv6 filtrado de tráfico y clasificación), una solución flexible de enlace ascendente / ranura del módulo y avanzado funciones de gestión de redes proporcionan una solución que maximiza la inversión existente y compatible con los estándares emergentes.

Fuente: http://www.pco2.com/v/vspfiles/downloadables/switch_5500g_family.pdf

✚ Switch 3COM 4500

También se lo utiliza para interconectar los segmentos de red del edificio principal. Este dispositivo de red, proporciona una conectividad de LAN segura y flexible para las redes empresariales y de sucursales. La serie 4500 ofrece switching de Capa 2 y routing dinámico de Capa 3, así como robustas funcionalidades de seguridad, calidad de servicio (QoS) y administración para proporcionar una conectividad de extremo inteligente para las aplicaciones empresariales esenciales.



Figura A- 5. Switch 3COM 4500

Fuente: http://produto.mercadolivre.com.br/MLB-758748752-switch-3com-4500-26-porta-_JM

Tabla A. 5. Descripción Switch 3COM 4500

CARACTERÍSTICAS	
Descripción de capas	Conmutador Capas 2, 3 Soporta 802.1x, Clase de Servicio / Calidad de Servicio (CoS/QoS) 802.1p, ACL, VLAN Enrutamiento dinámico con RIP. Los switches detectan y ajustan las conexiones de cables cruzados o directos mediante la funcionalidad "Auto MDI/MDIX".
Dimensiones	26.92 x 43.94 x 4.32 cm
Fuente de alimentación	Tensión de entrada: 90-240 VAC
Memoria	SDRAM: 64 MB FLASH: 8 MB
Procesador	Cache 2.80ghz 800mhz
Puertos	26 puertos Capacidad de switching de hasta 8,8 Gbps Velocidad de transmisión de hasta 6,5 Mbps 8.000 direcciones MAC soportadas 50 puertos Capacidad de switching de hasta 13,6 Gbps Velocidad de transmisión de hasta 10,1 Mbps 8.000 direcciones MAC soportadas
Soporte IPv6	Soporta IPv6, además del ya mencionado IPv4.

Fuente: http://www.tarconis.com/documentos/3COM_4500ds.pdf

Switch 3COM 4250T

Se lo Utiliza para interconectar los segmentos de red del edificio principal del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra. Tiene como principales características de conmutación de Capa 2 a un precio increíble, así como prestaciones sin bloqueo en todos los puertos, y sencilla instalación "Plug and Play".

Las funciones de robusta disponibilidad incluyen agregación de enlaces, soporte para Rapid Spanning Tree, opción de fuente de alimentación redundante, que aseguran el máximo rendimiento en las aplicaciones críticas.



Figura A- 6. Switch 3COM 4250T

Fuente: <http://www.abox.com/productos.asp?pid=622>

Tabla A. 6. Descripción Switch 4250T

CARACTERÍSTICAS	
Descripción de capas	Conmutador de capa 2 Control de flujo, conmutador MDI/MDI-X, soporte VLAN, apilable Cumplimiento de normas IEEE 802.1Q, IEEE 802.1P, IEEE 802.1w. Administración: configuración basada en web, SNMP 1. O a través de 3Com Network Supervisor, 3Com Network Director, 3Com Enterprise Management Suite.
Dimensiones	Ancho 44 cm x Altura 27.4 cm x Profundidad 4.4 cm
Fuente de alimentación	90-240 V CA
Memoria	-
Procesador	-
Puertos	48 x 10/100 + 2 x 10/100/1000
Soporte IPv6	Soporta IPv6

Fuente: <http://www.zdtronic.com/NETWORKING/3COM-NETWORKING/3COM-3C17302-10-100-1000-48-PORTS-SUPERSTACK-3-SWITCH-4250T-SWITCH.html>

FIREWALL CHECKPOINT

Este dispositivo se encuentra entre el proveedor y el core del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra. Cumple como función brindar seguridad a la red. El Check Point 4600 Appliance ofrece todo lo necesario para garantizar su red de la empresa en un solo aparato. El 4600 combina las tecnologías de redes rápidas con capacidades de multi-core de alto rendimiento - proporcionan el más alto nivel de seguridad sin comprometer la velocidad de la red para mantener sus datos, la red y los empleados seguro.



Figura A- 7. Firewall Checkpoint 4610

Fuente: <http://www.checkfirewalls.com/4600.asp>

Tabla A. 7. Descripción Firewall Checkpoint

CARACTERÍSTICAS	
Dimensiones	Estándar (W x D x H): 17,25 x 12,56 x 1,73 pulg.
Fuente de alimentación	Voltaje de entrada AC: 100 - 240V
Rendimiento	405 SecurityPower 3.4 Gbps de rendimiento de firewall 630 Mbps servidor de seguridad y el rendimiento IPS
Puertos	8 x puertos 10/100 / 1000BASE-T RJ45 Unidad de disco duro de 250 GB Una fuente de alimentación de CA. Montaje en rack estándar
Soporte IPv6	IPv4 e IPv6 <ul style="list-style-type: none"> • 1024 interfaces o VLAN por sistema • 4096 interfaces de por sistema (en el modo Virtual System) • agregación de enlaces 802.3ad pasiva y activa • Capa 2 (transparente) y el modo de capa 3 (routing)

Fuente: https://www.checkpoint.com/downloads/product-related/datasheets/4600-appliance-datasheet.pdf&usg=ALkJrhjeh0kdoZLrYEW__m4zPmh1N7skJg

ANEXO B: Creación de la máquina virtual en VMWare e instalación de Centos 6

1. Dirigirse a VMWare y crear una nueva máquina virtual

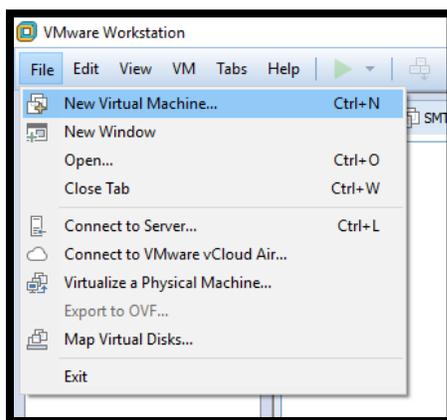


Figura B- 1. *Creación de nueva máquina virtual*

Fuente: Captura propia extraída de software VMWare

2. Se elige la creación de una máquina personalizada y click en Next (siguiente)

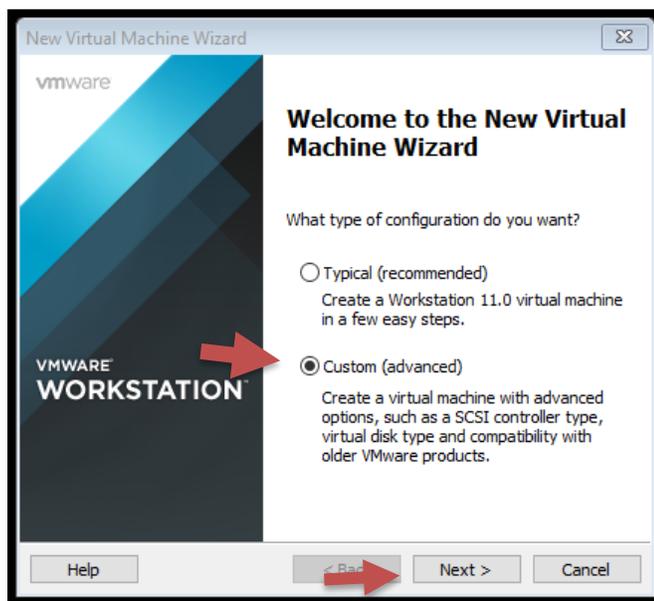


Figura B- 2. *Instalación personalizada de VMWare*

Fuente: Captura propia extraída de software VMWare

3. Se elige la compatibilidad de la máquina, en este caso se deja por defecto la que aparece y click en Next.

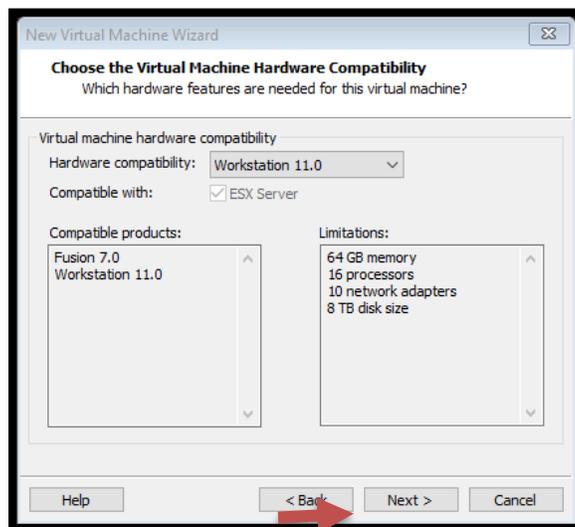


Figura B- 3. *Compatibilidad de máquinas virtuales*

Fuente: Captura propia extraída de software VMWare

4. Se elige la ubicación del archivo.iso que en este caso es el sistema operativo y Next

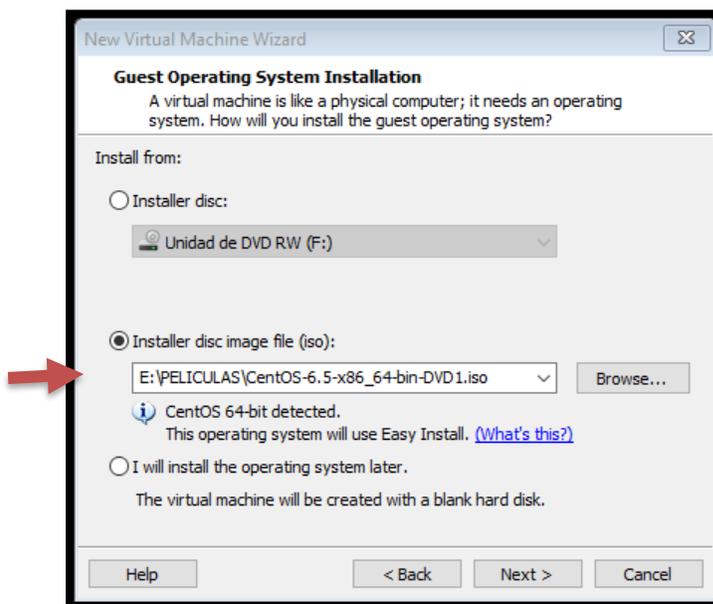


Figura B- 4. *Selección de Imagen.iso*

Fuente: Captura propia extraída de software VMWare

5. Se coloca la cuenta de la persona que se requiere tenga acceso al servidor y click en Next



Figura B- 5. Acceso y contraseñas de usuario

Fuente: Captura propia extraída de software VMWare

6. Se coloca el nombre de la máquina virtual deseado y click en Next

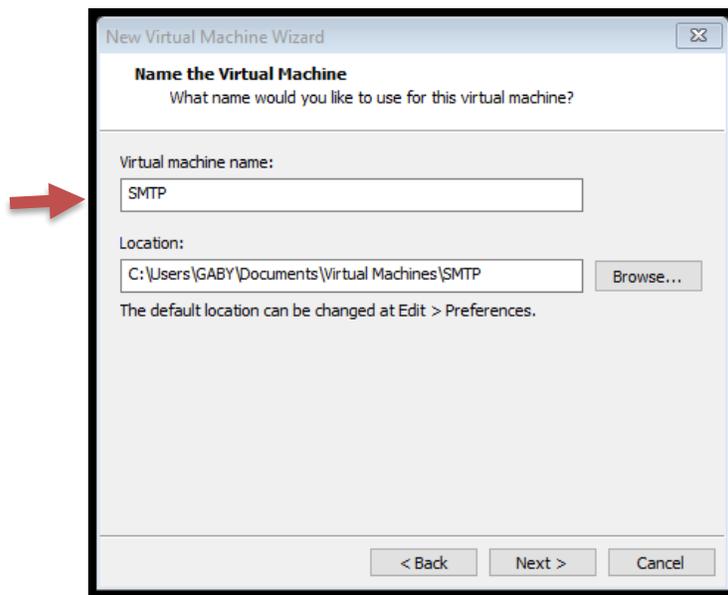


Figura B- 6.Nombre de la máquina

Fuente: Captura propia extraída de software VMWare

7. Se colocan los procesadores a utilizar, en este caso es recomendable dejarlo por defecto

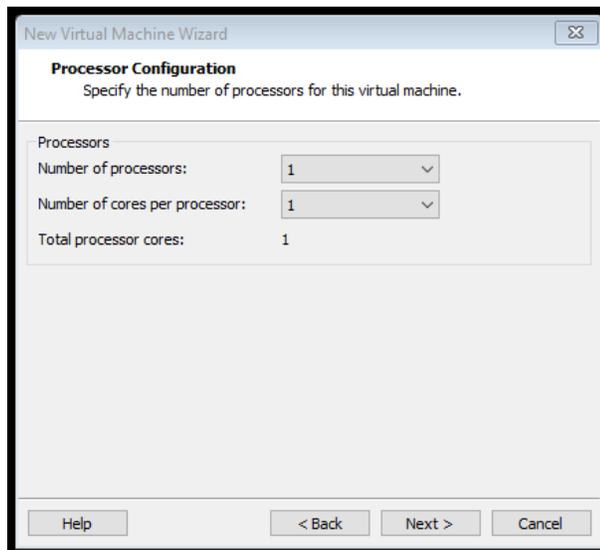


Figura B- 7. Selección de procesadores de Sistema
Fuente: Captura propia extraída de software VMWare

8. Se coloca la RAM que se vaya a requerir y Next

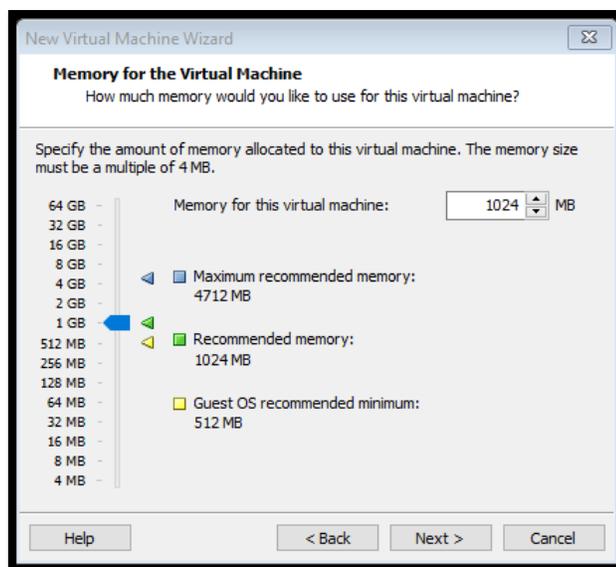


Figura B- 8. Memoria RAM de la máquina virtual

Fuente: Captura propia extraída de software VMWare

9. Se recomienda colocar en modo bridge para utilizar interfaces reales

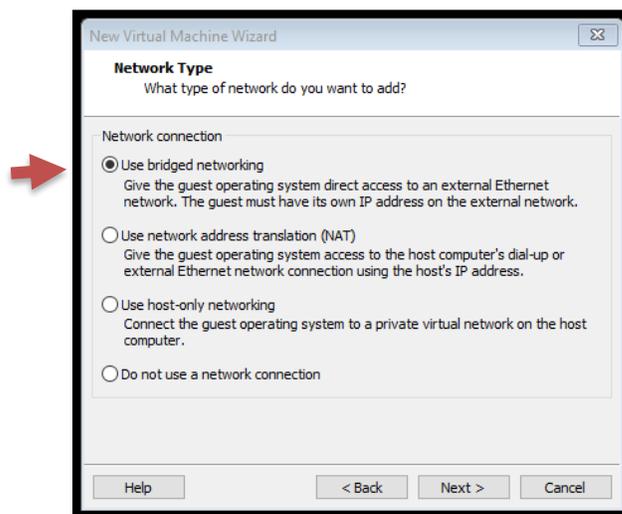


Figura B- 9. Selección tipo de adaptador de red

Fuente: Captura propia extraída de software VMWare

10. En los controladores de entrada o salida se recomienda dejarlo por defecto y Next

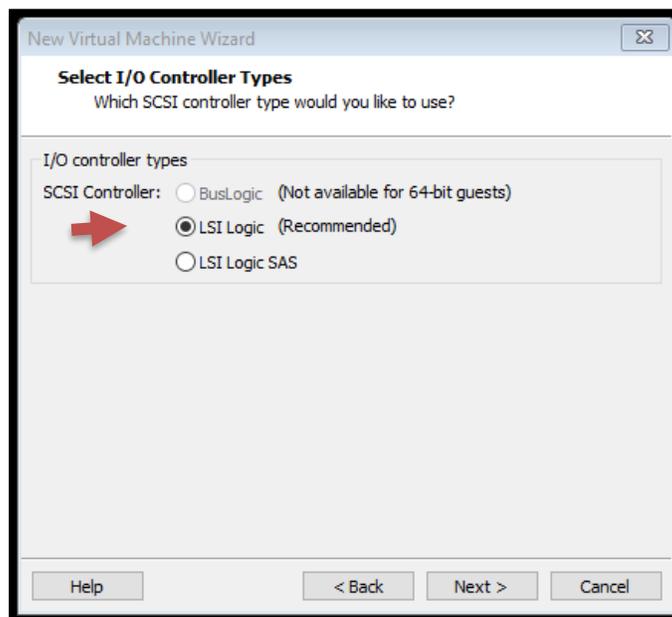


Figura B- 10. Selección de los controladores de entrada/salida

Fuente: Captura propia extraída de software VMWare

11. Para la elección del disco virtual se recomienda dejarlo de igual modo recomendado

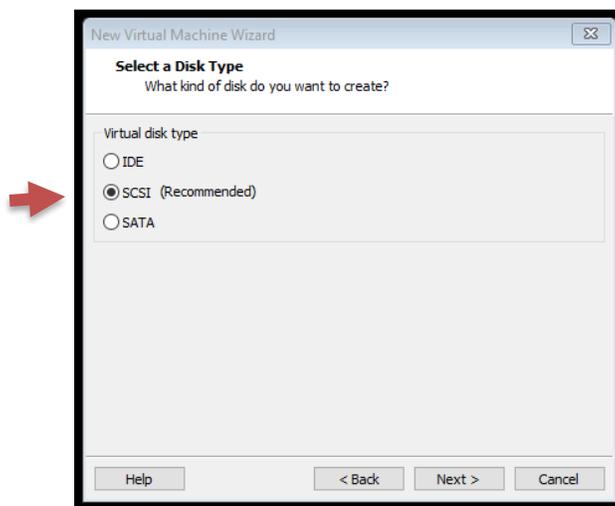


Figura B- 11. *Disco a utilizar*

Fuente: Captura propia extraída de software VMWare

12. Se crea un nuevo disco virtual y Next

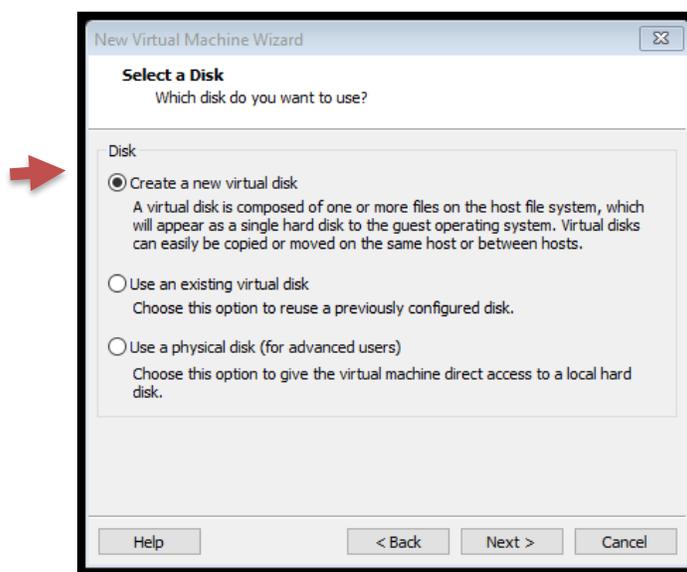


Figura B- 12. *Seleccionar un disco virtual nuevo*

Fuente: Captura propia extraída de software VMWare

13. Se coloca la memoria que tendrá el tamaño del disco y click en Next

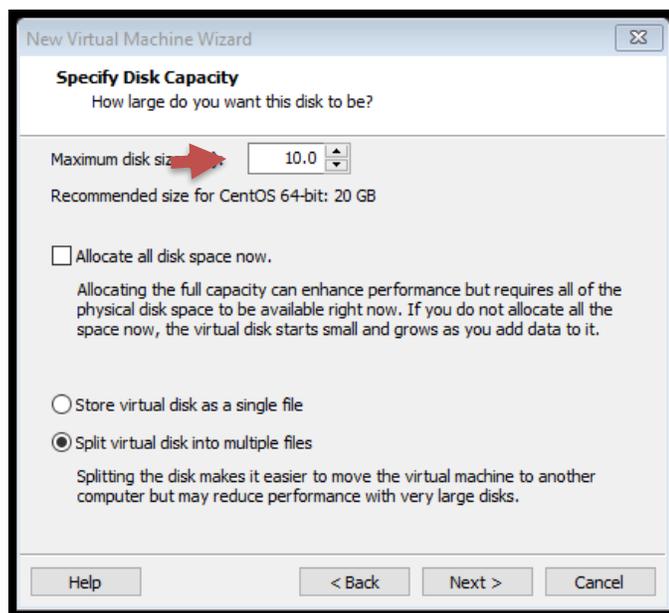


Figura B- 13. *Espacio de disco duro*

Fuente: Captura propia extraída de software VMWare

14. Se especifica el nombre del disco virtual

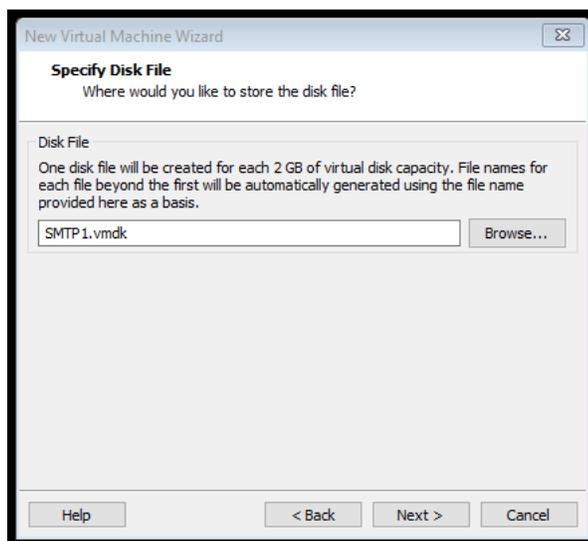


Figura B- 14. *Archivo de ubicación del disco virtual*

Fuente: Captura propia extraída de software VMWare

15. Y finalizamos la creación de la máquina observando los parámetros que se han configurado

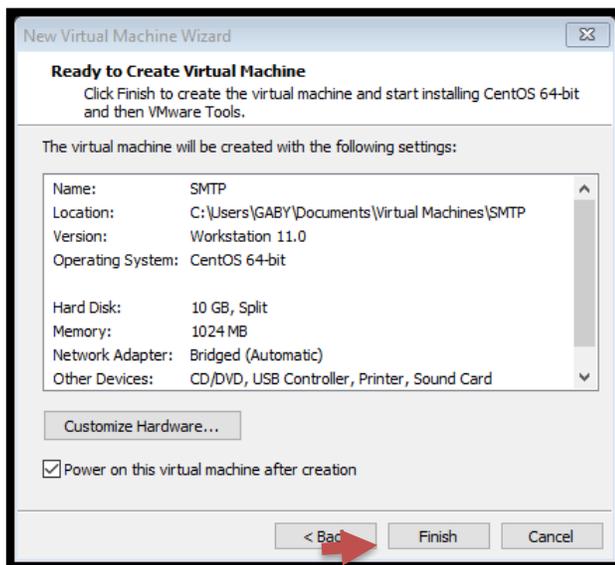


Figura B- 15. *Finalización de la Instalación*

Fuente: Captura propia extraída de software VMWare

16. Ahora se iniciará la máquina y se procede a instalar el sistema operativo, el cual tiene como primera pantalla la Figura y se escoge la primera opción



Figura B- 16. Pantalla de inicio de Instalación Centos

Fuente: Captura propia extraída de software Centos 6

17. Se coloca skip, para continuar con la instalación



Figura B- 17. Continuar con la instalación

Fuente: Captura propia extraída de software Centos 6

18. Aparecerá la pantalla de Centos 6 y click en Next

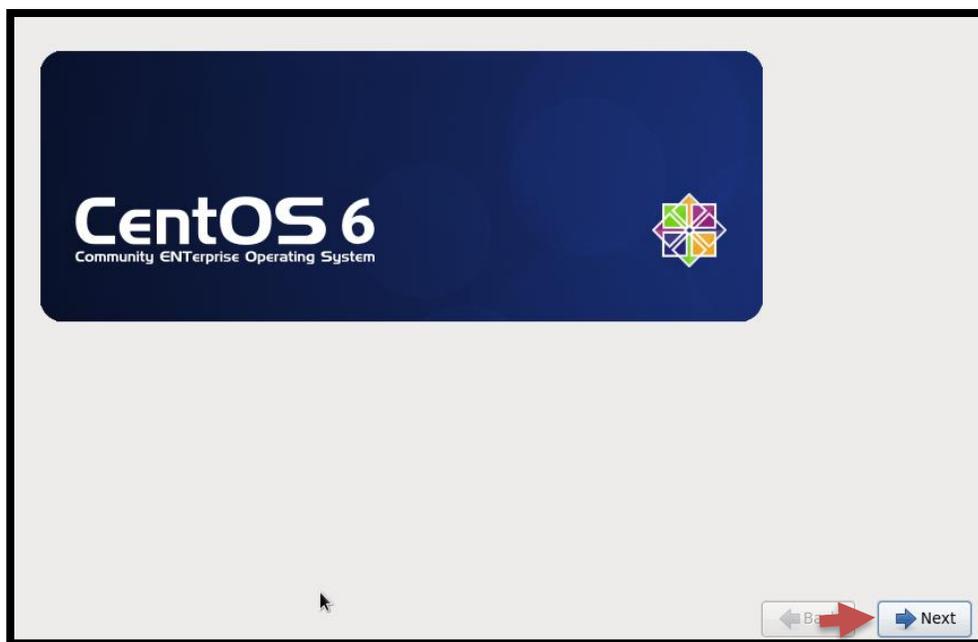


Figura B- 18. Continuar con la instalación 2

Fuente: Captura propia extraída de software Centos 6

19. Se elige el idioma que se desee utilizar, en este caso English debido a los comandos que se utilizan son mejor combinados para mejor configuración y Next

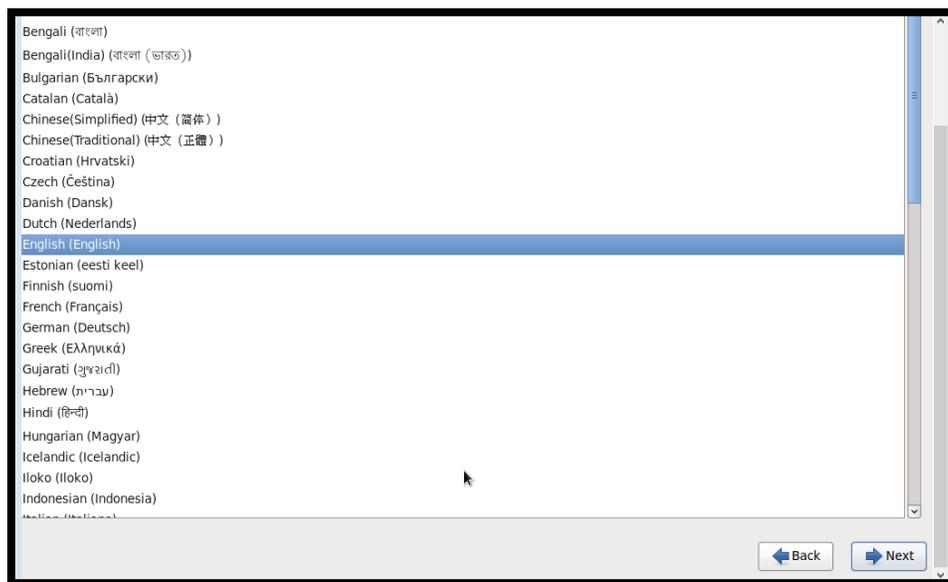


Figura B- 19. Selección del idioma del sistema operativo

Fuente: Captura propia extraída de software Centos 6

20. Se escoge la opción de dispositivos de almacenamiento básico y Next

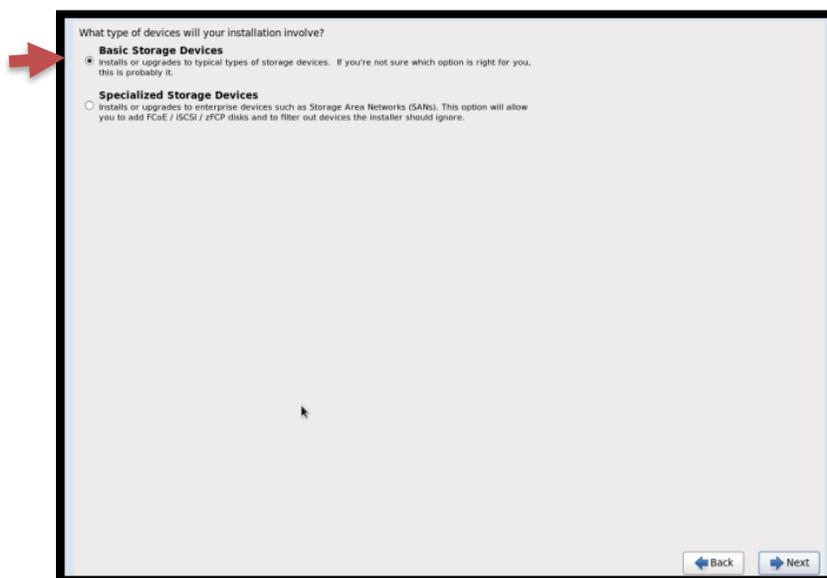


Figura B- 20. *Instalación Básica*

Fuente: Captura propia extraída de software Centos 6

21. Se deja por defecto la configuración del local host y click en siguiente

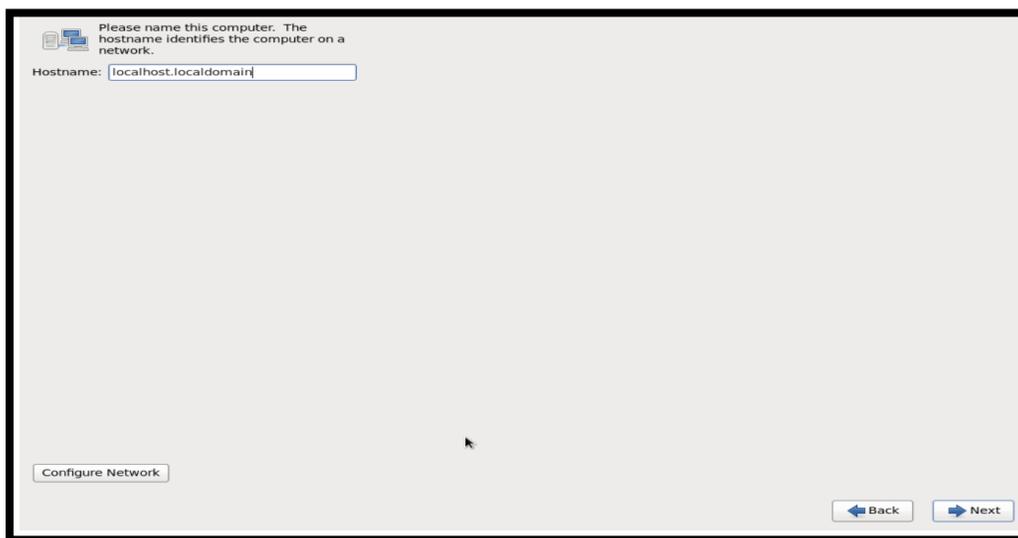


Figura B- 21. *Nombre del equipo en la red*

Fuente: Captura propia extraída de software Centos 6

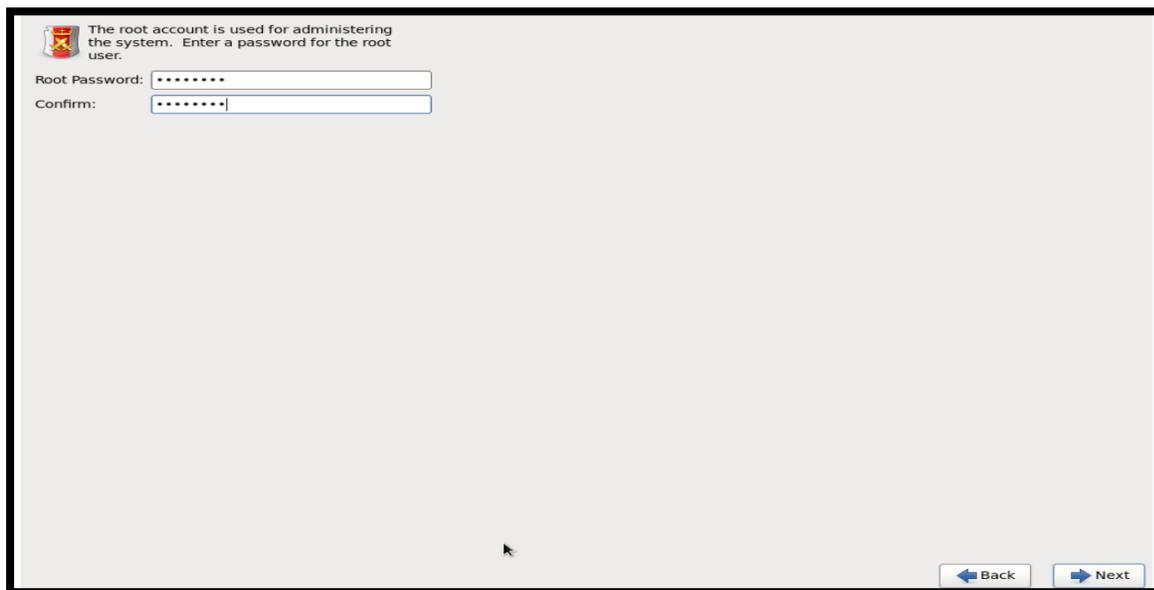
22. Seleccionar la ubicación



Figura B- 22. *Ubicación del servidor/máquina*

Fuente: Captura propia extraída de software Centos 6

23. Se coloca una contraseña para el super usuario root y su correspondiente contraseña



The screenshot shows a terminal window with the following text and input fields:

 The root account is used for administering the system. Enter a password for the root user.

Root Password:

Confirm:

At the bottom right, there are two buttons: "Back" (with a left arrow) and "Next" (with a right arrow).

Figura B- 23. *Claves de acceso*

Fuente: Captura propia extraída de software Centos 6

24. Se procede a dejar esta opción por defecto que es reemplazar cualquier sistema existente y click en next

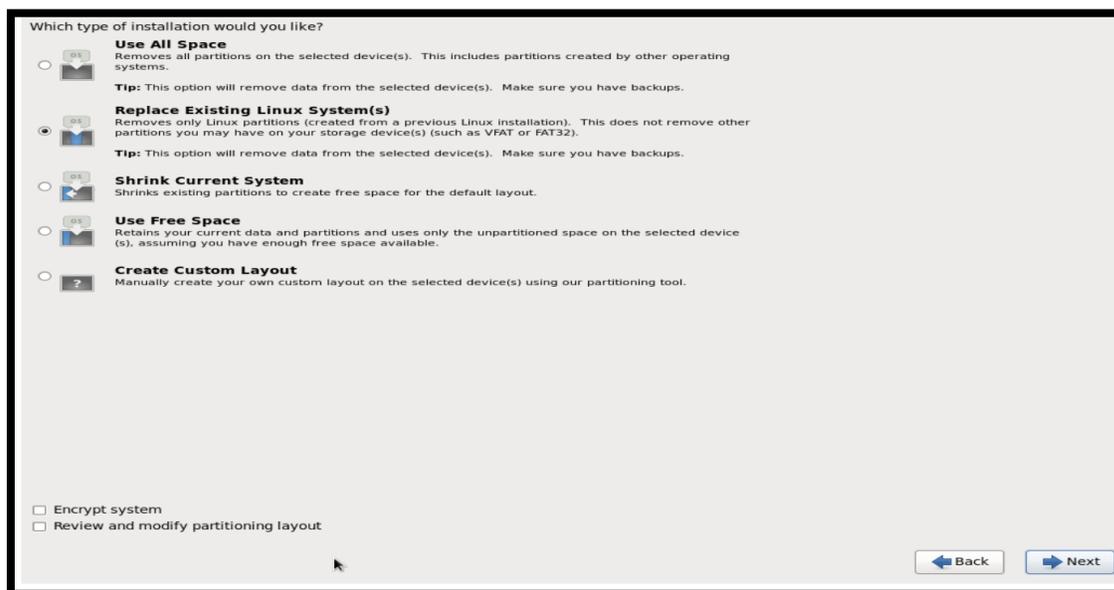


Figura B- 24. *Espacio en el disco*

Fuente: Captura propia extraída de software Centos 6

25. Se coloca escribir las configuraciones realizadas

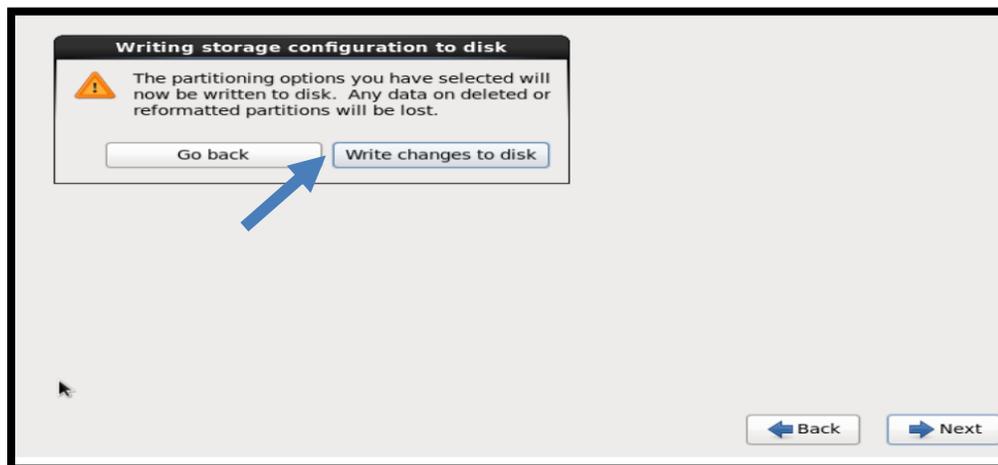


Figura B- 25. Escribir en los discos los cambios realizados

Fuente: Captura propia extraída de software Centos 6

26. Se escoge la opción de desktop o escritorio y click en next

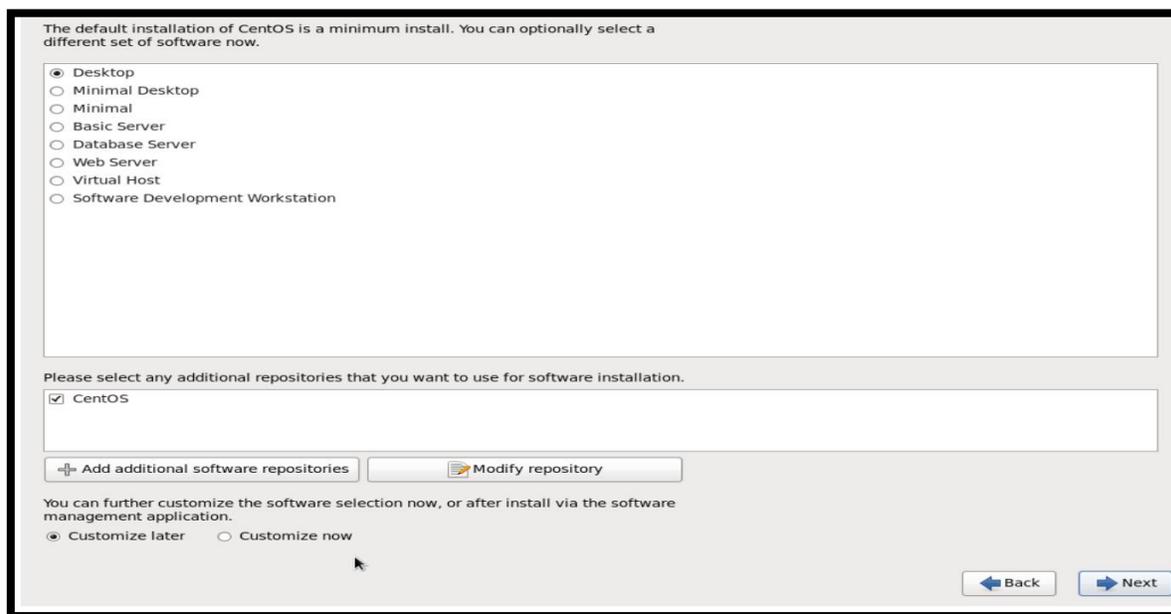


Figura B- 26. Instalación de complementos de escritorio

Fuente: Captura propia extraída de software Centos 6

27. Se esperará un tiempo hasta que se realice la instalación de los paquetes

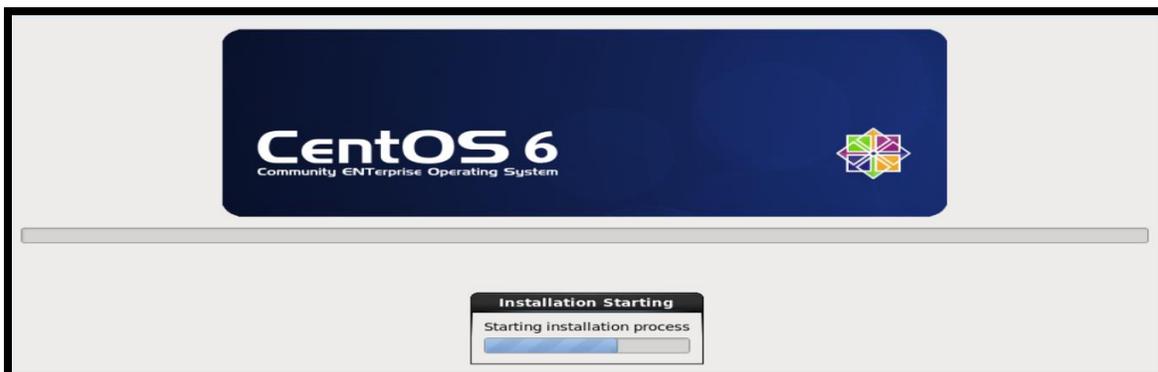


Figura B- 27. Proceso de Instalación Centos

Fuente: Captura propia extraída de software Centos 6

28. Al finalizar la instalación se procederá a reiniciar el sistema

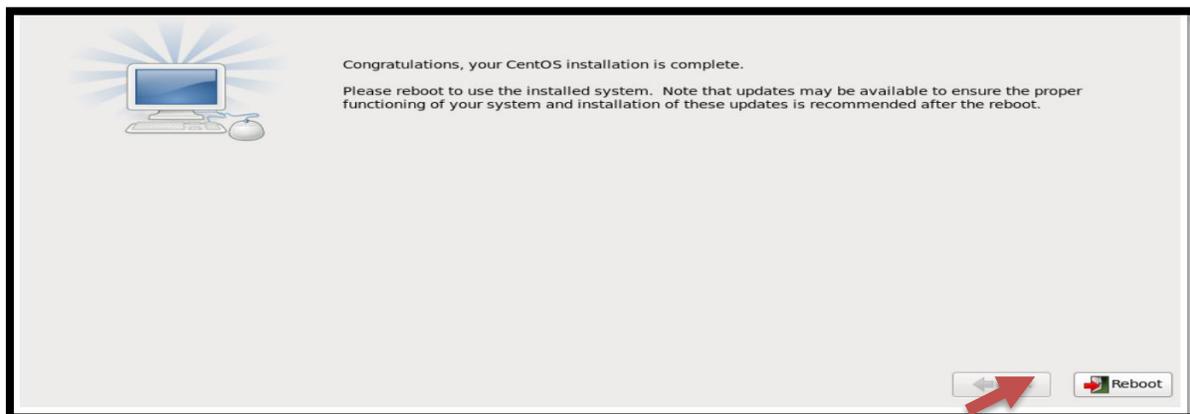


Figura B- 28. *Finalización de Instalación*

Fuente: Captura propia extraída de software Centos 6

29. Se observará después del reinicio la pantalla de bienvenida y se coloca forward

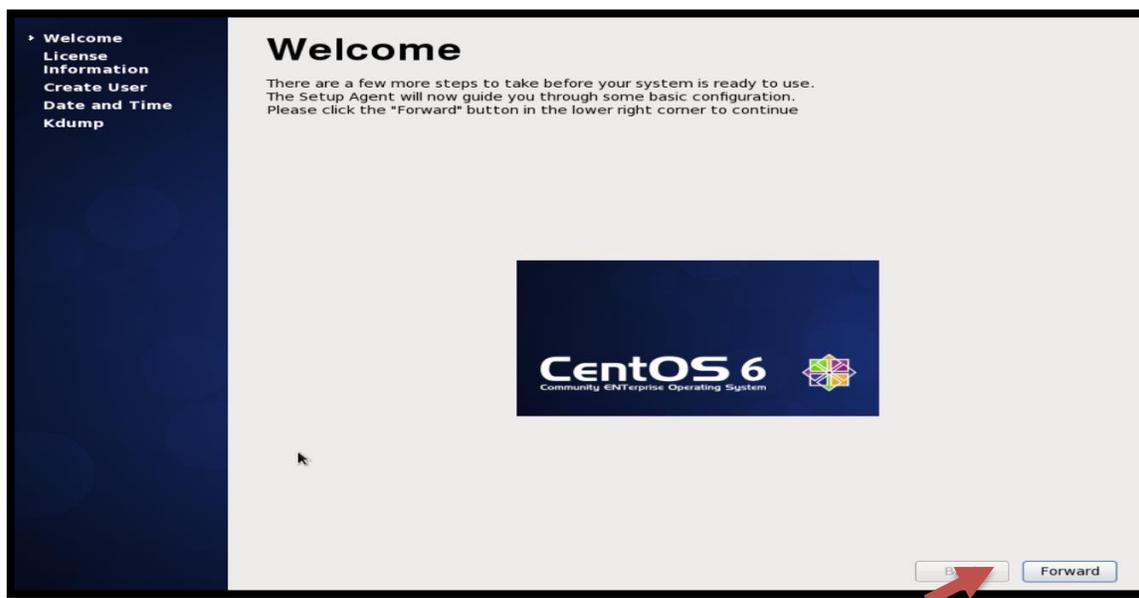


Figura B- 29. *Pantalla de bienvenida de Centos*

Fuente: Captura propia extraída de software Centos 6

30. Se acepta el contrato de licencia y forward

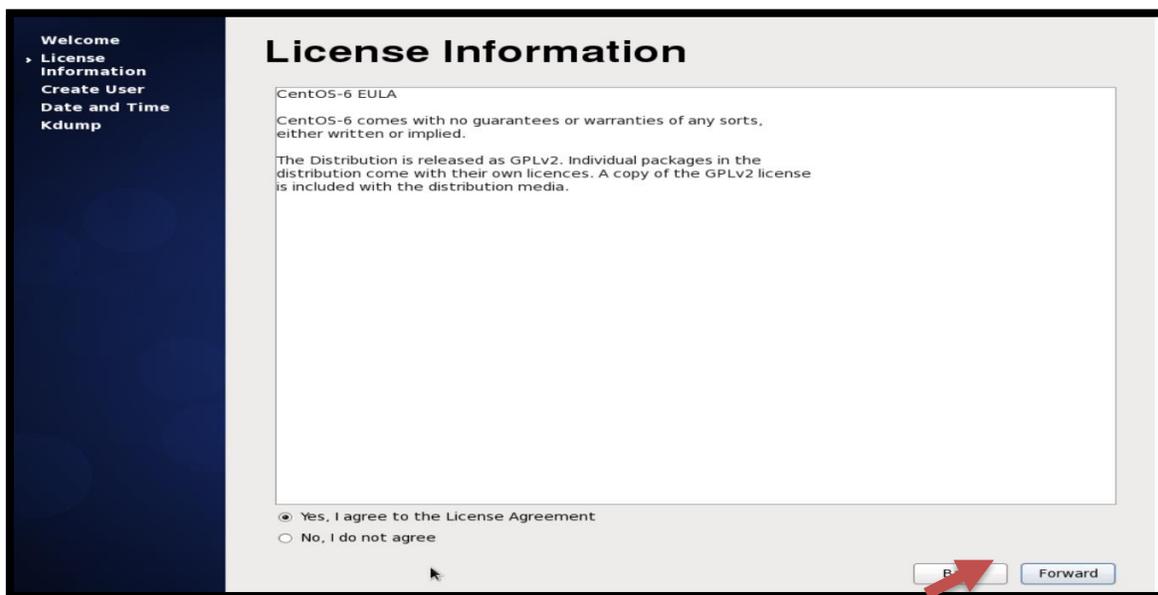


Figura B- 30. *Aceptar contrato de licencia*

Fuente: Captura propia extraída de software Centos 6

31. Si se desea crear un usuario se lo puede realizar

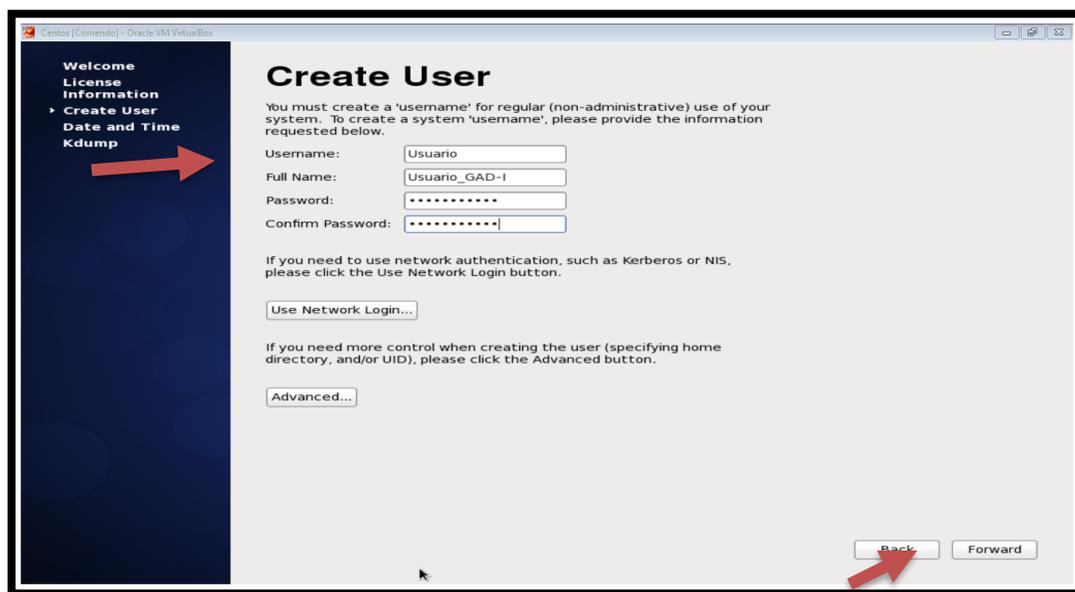


Figura B- 31. *Creación de Usuarios*

Fuente: Captura propia extraída de software Centos 6

32. Configurar la hora y fecha del sistema

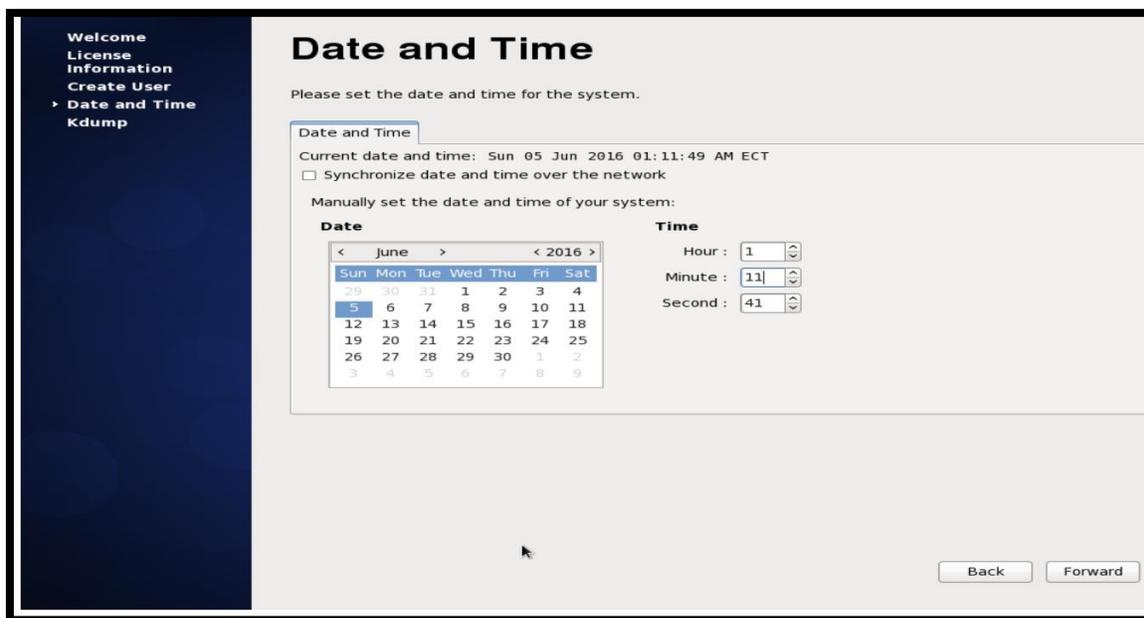


Figura B- 32. Configuración de fecha y hora

Fuente: Captura propia extraída de software Centos 6

33. Y a continuación se inicia sesión

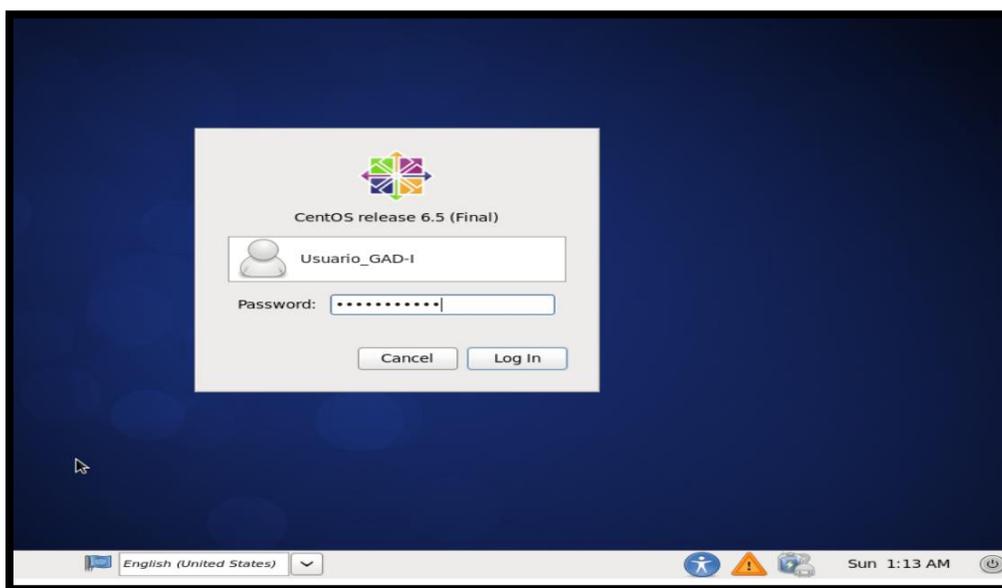
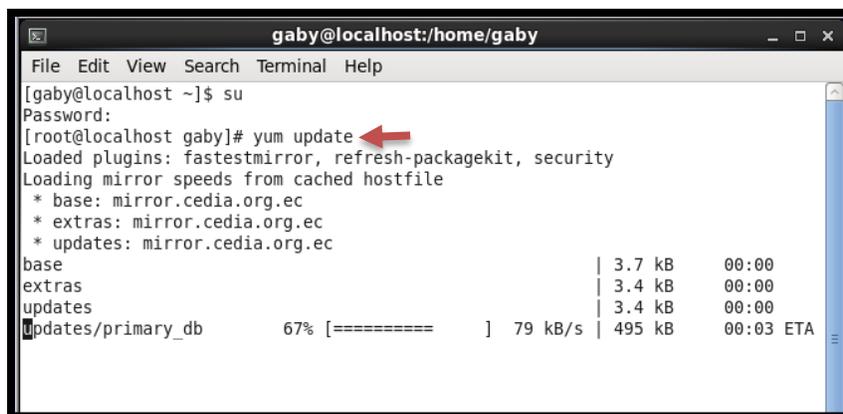


Figura B- 33. Ingreso al sistema

Fuente: Captura propia extraída de software Centos 6

ANEXO C: Manual de Administrador para la instalación del Servidor de Correo Electrónico, servidor WEB, servidor DNS64NAT64 y configuración de doble pila

Para que los servidores puedan ser levantados y funcionen correctamente, es necesario que se actualicen los repositorios del sistema, para lo cual se utiliza el comando `#yum update` y para ello se debe tener acceso a internet para su correcta instalación

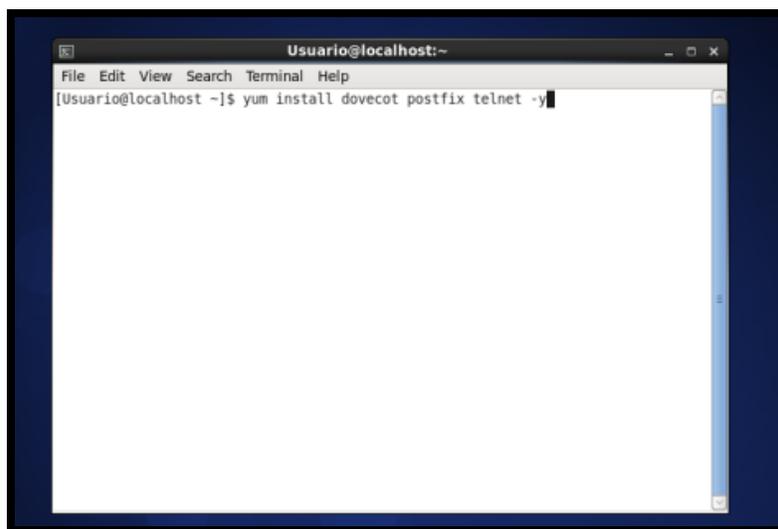


```
gaby@localhost:/home/gaby
File Edit View Search Terminal Help
[gaby@localhost ~]$ su
Password:
[root@localhost gaby]# yum update
Loaded plugins: fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * base: mirror.cedia.org.ec
 * extras: mirror.cedia.org.ec
 * updates: mirror.cedia.org.ec
base | 3.7 kB | 00:00
extras | 3.4 kB | 00:00
updates | 3.4 kB | 00:00
updates/primary_db 67% [===== ] 79 kB/s | 495 kB | 00:03 ETA
```

Figura C-1. Actualización de repositorios S.O Centos 6

Fuente: Captura propia extraída de software Centos 6

1. Se abre un terminal y se procede a instalar los paquetes dovecot, postfix y telnet



```
Usuario@localhost:~
File Edit View Search Terminal Help
[Usuario@localhost ~]$ yum install dovecot postfix telnet -y
```

Figura C- 2. Instalación de paquetes de correo electrónico

Fuente: Captura propia extraída de software Centos 6

2. Se va a editar el fichero main.cf en postfix para comenzar a configurar el servidor

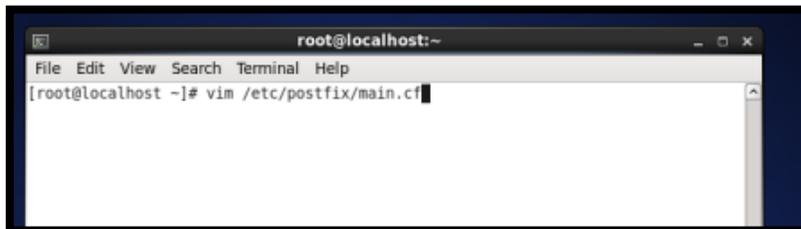


Figura C- 3. Fichero /etc/postfix/main.cf

Fuente: Captura propia extraída de software Centos 6

3. Se descomenta la línea marcada y colocamos el dominio que se ha escogido en este caso gad-i.gob.ec

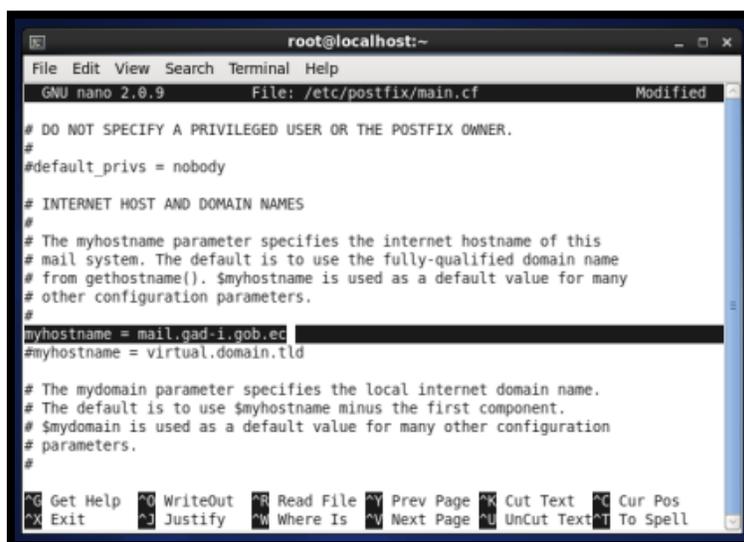


Figura C- 4. Fichero /etc/postfix/main.cf

Fuente: Captura propia extraída de software Centos 6

4. Y de igual manera la línea mydomain se descomenta y se coloca el dominio ya especificado

```

root@localhost:~
File Edit View Search Terminal Help
GNU nano 2.0.9 File: /etc/postfix/main.cf Modified
# other configuration parameters.
#
myhostname = mail.gad-i.gob.ec
#myhostname = virtual.domain.tld

# The mydomain parameter specifies the local internet domain name.
# The default is to use $myhostname minus the first component.
# $mydomain is used as a default value for many other configuration
# parameters.
#
#mydomain = gad-i.gob.ec

# SENDING MAIL
#
# The myorigin parameter specifies the domain that locally-posted
# mail appears to come from. The default is to append $myhostname,
# which is fine for small sites. If you run a domain with multiple
# machines, you should (1) change this to $mydomain and (2) set up
# a domain-wide alias database that aliases each user to
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell

```

Figura C- 5. Fichero /etc/postfix/main.cf

Fuente: Captura propia extraída de software Centos 6

- De la misma manera, descomentar la línea inet interfaces = all

```

root@localhost:~
File Edit View Search Terminal Help
GNU nano 2.0.9 File: /etc/postfix/main.cf Modified
# RECEIVING MAIL
#
# The inet_interfaces parameter specifies the network interface
# addresses that this mail system receives mail on. By default,
# the software claims all active interfaces on the machine. The
# parameter also controls delivery of mail to user@[ip.address].
#
# See also the proxy_interfaces parameter, for network addresses that
# are forwarded to us via a proxy or network address translator.
#
# Note: you need to stop/start Postfix when this parameter changes.
#
inet_interfaces = all
#inet_interfaces = $myhostname
#inet_interfaces = $myhostname, localhost
inet_interfaces = localhost
inet_protocols = ipv4
inet_protocols = ipv4, ipv6

```

Figura C- 6.Fichero /etc/postfix/main.cf

Fuente: Captura propia extraída de software Centos 6

6. Se comenta la primera línea marcada en negrilla y la segunda se descomenta

```

root@localhost:~
File Edit View Search Terminal Help
GNU nano 2.0.9 File: /etc/postfix/main.cf Modified
#
# The local machine is always the final destination for mail addressed
# to user@[the.net.work.address] of an interface that the mail system
# receives mail on (see the inet_interfaces parameter).
#
# Specify a list of host or domain names, /file/name or type:table
# patterns, separated by commas and/or whitespace. A /file/name
# pattern is replaced by its contents; a type:table is matched when
# a name matches a lookup key (the right-hand side is ignored).
# Continue long lines by starting the next line with whitespace.
#
# See also below, section "REJECTING MAIL FOR UNKNOWN LOCAL USERS".
#
#mydestination = $myhostname, $mydomain, localhost.$mydomain, localhost
#mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
#mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain,
# mail.$mydomain, www.$mydomain, ftp.$mydomain
#
# REJECTING MAIL FOR UNKNOWN LOCAL USERS
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell

```

Figura C- 7.Fichero /etc/postfix/main.cf

Fuente: Captura propia extraída de software Centos 6

7. Se descomenta la primera línea en negrilla y se coloca la dirección del servidor con la que se va a trabajar

```

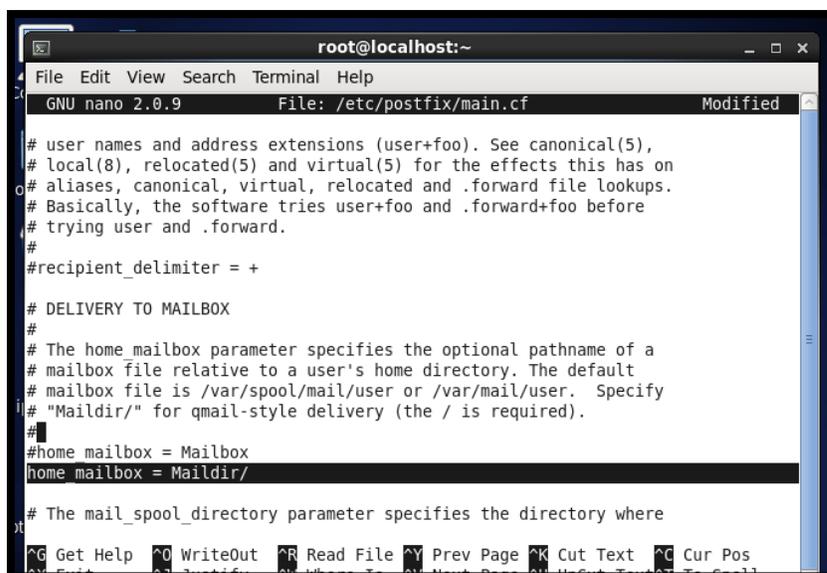
*main.cf (/etc/postfix) - gedit
File Edit View Search Tools Documents Help
#
# You can also specify the absolute pathname of a pattern file instead
# of listing the patterns here. Specify type:table for table-based lookups
# (the value on the table right-hand side is not used).
#
#mynetworks = 172.16.8.5/28, 127.0.0.0/8, [::1]/128, [2001:db8:20:8::]/92
#mynetworks = $config_directory/mynetworks
#mynetworks = hash:/etc/postfix/network_table
#
# The relay_domains parameter restricts what destinations this system will
# relay mail to. See the smtpd_recipient_restrictions description in
# postconf(5) for detailed information.
#
# By default, Postfix relays mail
# - from "trusted" clients (IP address matches $mynetworks) to any
# destination,
# - from "untrusted" clients to destinations that match $relay_domains or
# subdomains thereof, except addresses with sender-specified routing.
# The default relay_domains value is $mydestination.
#
Plain Text Tab Width: 8 Ln 267, Col 74 INS

```

Figura C- 8.Fichero /etc/postfix/main.cf

Fuente: Captura propia extraída de software Centos 6

8. Se descomenta también la línea marcada en negrilla y se guardan los cambios



```
root@localhost:~
File Edit View Search Terminal Help
GNU nano 2.0.9 File: /etc/postfix/main.cf Modified

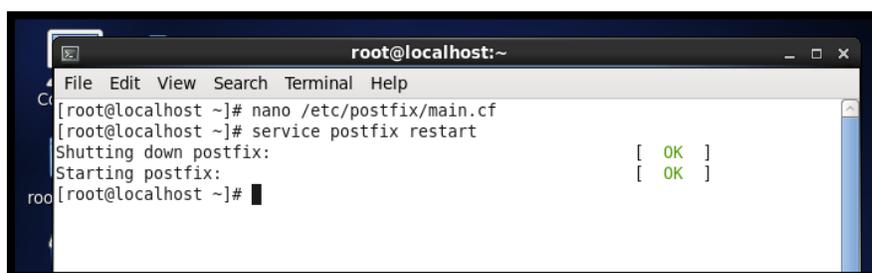
# user names and address extensions (user+foo). See canonical(5),
# local(8), relocated(5) and virtual(5) for the effects this has on
# aliases, canonical, virtual, relocated and .forward file lookups.
# Basically, the software tries user+foo and .forward+foo before
# trying user and .forward.
#
#recipient_delimiter = +
#
# DELIVERY TO MAILBOX
#
# The home_mailbox parameter specifies the optional pathname of a
# mailbox file relative to a user's home directory. The default
# mailbox file is /var/spool/mail/user or /var/mail/user. Specify
# "Maildir/" for qmail-style delivery (the / is required).
#
#home_mailbox = Mailbox
home_mailbox = Maildir/

# The mail_spool_directory parameter specifies the directory where
```

Figura C- 9. Fichero /etc/postfix/main.cf

Fuente: Captura propia extraída de software Centos 6

9. Ahora se reinicia el servicio de postfix

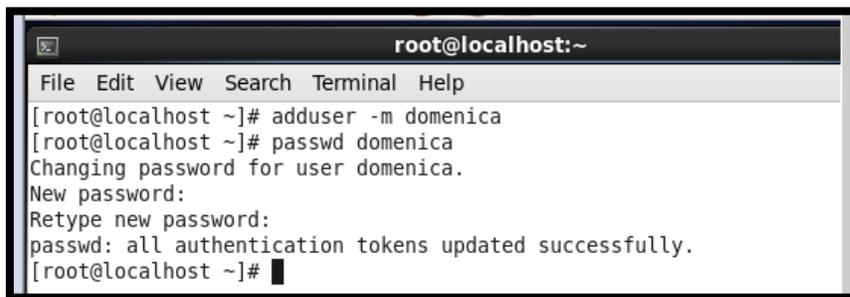


```
root@localhost:~
File Edit View Search Terminal Help
[root@localhost ~]# nano /etc/postfix/main.cf
[root@localhost ~]# service postfix restart
Shutting down postfix: [ OK ]
Starting postfix: [ OK ]
root@localhost ~]#
```

Figura C- 10. Reinicio servicio Postfix

Fuente: Captura propia extraída de software Centos 6

10. Ahora se añaden los usuarios

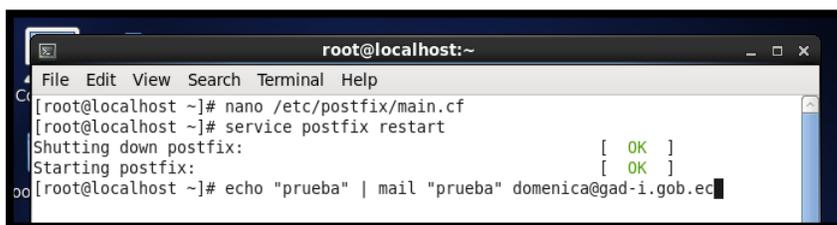
A terminal window titled 'root@localhost:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
[root@localhost ~]# adduser -m dominica
[root@localhost ~]# passwd dominica
Changing password for user dominica.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]#
```

Figura C- 11. Adición de usuarios

Fuente: Captura propia extraída de software Centos 6

11. Ahora se va a enviar un correo de prueba al usuario que se ha creado anteriormente

A terminal window titled 'root@localhost:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
[root@localhost ~]# nano /etc/postfix/main.cf
[root@localhost ~]# service postfix restart
Shutting down postfix: [ OK ]
Starting postfix: [ OK ]
[root@localhost ~]# echo "prueba" | mail "prueba" dominica@gad-i.gob.ec
```

Figura C- 12. Envío de correo a un usuario

Fuente: Captura propia extraída de software Centos 6

12. Ingresar al usuario dominica con el comando `su - dominica` y ahí entrar a la carpeta Maildir donde se reciben los correos y verificar que el correo haya sido enviado por el usuario root y recibido por el usuario dominica

```

[root@localhost ~]# echo "prueba" | mail "prueba" domenica@gad-i.gob.ec
[root@localhost ~]# su
[root@localhost ~]# su - domenica
[domenica@localhost ~]$ cat Maildir/new/1465322063.Vfd00I21195M48512.localhost
Return-Path: <root@gad-i.gob.ec>
X-Original-To: domenica@gad-i.gob.ec
Delivered-To: domenica@gad-i.gob.ec
Received: by mail.gad-i.gob.ec (Postfix, from userid 0)
        id C34306298A; Tue, 7 Jun 2016 12:54:22 -0500 (ECT)
Date: Tue, 07 Jun 2016 12:54:22 -0500
To: domenica@gad-i.gob.ec, prueba@gad-i.gob.ec
User-Agent: Heirloom mailx 12.4 7/29/08
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-Id: <20160607175422.C34306298A@mail.gad-i.gob.ec>
From: root@gad-i.gob.ec (root)

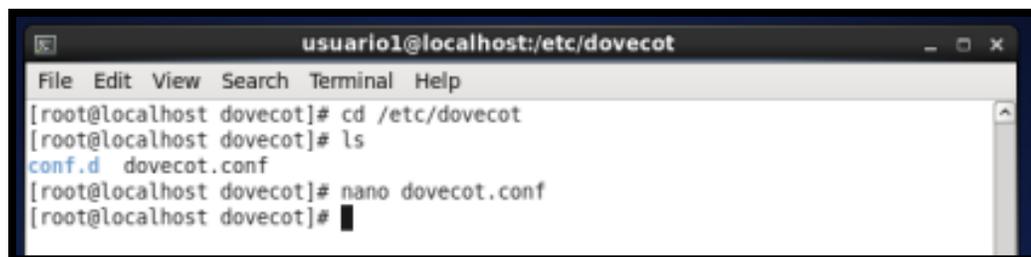
prueba
[domenica@localhost ~]$ █

```

Figura C- 13. Verificación de recepción de correo a usuario

Fuente: Captura propia extraída de software Centos 6

13. Ahora se va a proceder a configurar el fichero dovecot



```

usuario1@localhost:/etc/dovecot
File Edit View Search Terminal Help
[root@localhost dovecot]# cd /etc/dovecot
[root@localhost dovecot]# ls
conf.d dovecot.conf
[root@localhost dovecot]# nano dovecot.conf
[root@localhost dovecot]# █

```

Figura C- 14. Configuración Fichero Dovecot

Fuente: Captura propia extraída de software Centos 6

14. Descomentar la línea en negrita

```

usuario1@localhost:/etc/dovecot
File Edit View Search Terminal Help
GNU nano 2.0.9 File: dovecot.conf Modified
# Protocols we want to be serving.
protocols = imap pop3 lmt
# A comma separated list of IPs or hosts where to listen in for connections.
# "*" listens in all IPv4 interfaces, "::" listens in all IPv6 interfaces

```

Figura C- 15. Fichero /etc/dovecot.conf

Fuente: Captura propia extraída de software Centos 6

15. Ahora, dirigirse a la carpeta conf.d, ahí se va a editar el fichero 10-mail.conf

```

conf.d dovecot.conf
[root@localhost dovecot]# nano dovecot.conf
[root@localhost dovecot]# cd conf.d/
[root@localhost conf.d]# ls
10-auth.conf      20-lmt.conf      auth-master.conf.ext
10-director.conf  20-pop3.conf     auth-passwdfile.conf.ext
10-logging.conf   90-acl.conf      auth-sql.conf.ext
10-mail.conf      90-plugin.conf   auth-static.conf.ext
10-master.conf    90-quota.conf    auth-system.conf.ext
10-ssl.conf       auth-checkpassword.conf.ext auth-vpopmail.conf.ext
15-lda.conf       auth-deny.conf.ext
20-imap.conf      auth-ldap.conf.ext
[root@localhost conf.d]# nano 10-mail.conf

```

Figura C- 16.Fichero /etc/dovecot.conf/10-mail.conf

Fuente: Captura propia extraída de software Centos 6

16. Una vez en el fichero, descomentar las líneas en negrita y colocar vmail y guardar esta configuración

```

root@localhost:/etc/dovecot/conf.d
File Edit View Search Terminal Help
GNU nano 2.0.9 File: 10-mail.conf
#subscriptions = no
# List the shared/ namespace only if there are visible shared mailboxes.
#list = children
#}
# System user and group used to access mails. If you use multiple, userdb
# can override these by returning uid or gid fields. You can use either numbers
# or names. <doc/wiki/UserIds.txt>
mail_uid = vmail
mail_gid = vmail
# Group to enable temporarily for privileged operations. Currently this is
# used only with INBOX when either its initial creation or dotlocking fails.
# Typically this is set to "mail" to give access to /var/mail.
#mail_privileged_group =
# Grant access to these supplementary groups for mail processes. Typically
# these are used to set up access to shared mailboxes. Note that it may be
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^N Next Page ^U UnCut Text ^T To Spell

```

Figura C- 17. Fichero 10-mail.conf

Fuente: Captura propia extraída de software Centos 6

17. Ahora dirigirse al fichero 20-pop3.conf

```

10-master.conf 90-quota.conf auth-system.conf.ext
10-ssl.conf auth-checkpassword.conf.ext auth-vpopmail.conf.ext
15-lda.conf auth-denial.conf.ext
20-imap.conf auth-ldap.conf.ext
[root@localhost conf.d]# nano 10-mail.conf
[root@localhost conf.d]# nano 20-pop3.conf

```

Figura C- 18. Fichero /etc/Dovecot/20-pop3.conf

Fuente: Captura propia extraída de software Centos 6

18. Se descomenta la primera línea en negrilla y se coloca la segunda línea para poder acceder a Outlook de la misma manera y se guardan los cambios

```

root # Dovecot's default, so if you're building a new server it would be a good
# idea to change this. %08Xu%08Xv should be pretty fail-safe.
#
pop3_uidl_format = %08Xu%08Xv
pop3_client_workarounds = outlook-no-nuls
# Permanently save UIDLs sent to POP3 clients, so pop3_uidl_format changes
# won't change those UIDLs. Currently this works only with Maildir.
#pop3_save_uidl = no

```

Figura C- 19. Fichero /etc/Dovecot/20-pop3.conf

Fuente: Captura propia extraída de software Centos 6

19. Ahora se reinicia el servicio de dovecot

```
[root@localhost conf.d]# nano 20-pop3.conf
[root@localhost conf.d]# service dovecot restart
Stopping Dovecot Imap:           [ OK ]
Starting Dovecot Imap:          [ OK ]
[root@localhost conf.d]# █
```

Figura C- 20. Reinicio servicio Dovecot

Fuente: Captura propia extraída de software Centos 6

20. Se procede a realizar la prueba de telnet y verificar que el usuario esté registrado y que haya recibido el correo

```
root@localhost:/etc/dovecot/conf.d
File Edit View Search Terminal Help
[root@localhost conf.d]# telnet 127.0.0.1 pop3
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^'.
+OK Dovecot ready.
user dominica
+OK
pass dominica1234
+OK Logged in.
list
+OK 1 messages:
1 546
```

Figura C- 21. Prueba de Telnet

Fuente: Captura propia extraída de software Centos 6

21. Con retr 1, se puede visualizar el correo que se ha recibido

```
retr 1
+OK 546 octets
Return-Path: <root@gad-i.gob.ec>
X-Original-To: dominica@gad-i.gob.ec
Delivered-To: dominica@gad-i.gob.ec
Received: by mail.gad-i.gob.ec (Postfix, from userid 0)
        id C34306298A; Tue, 7 Jun 2016 12:54:22 -0500 (ECT)
Date: Tue, 07 Jun 2016 12:54:22 -0500
To: dominica@gad-i.gob.ec, prueba@gad-i.gob.ec
User-Agent: Heirloom mailx 12.4 7/29/08
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-Id: <20160607175422.C34306298A@mail.gad-i.gob.ec>
From: root@gad-i.gob.ec (root)

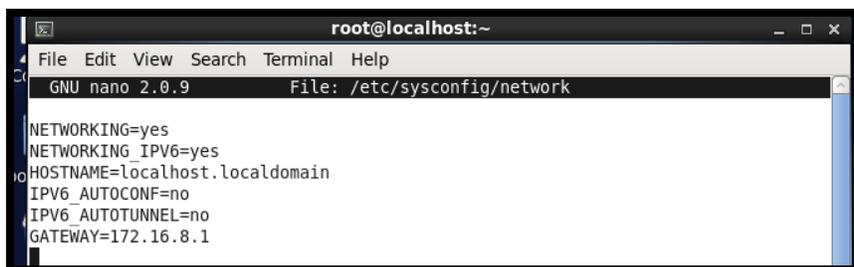
prueba
.
```

Figura C- 22. Mail recibido prueba

Fuente: Captura propia extraída de software Centos 6

Para demostrar el funcionamiento del servidor de correo electrónico que está configurado como IPv4/IPv6 se utilizará software libre con el sistema operativo Centos 6 versión 7 y está funcionando en una máquina virtual montando en VMWare, el proceso de creación de la máquina virtual y la instalación del servidor de correo electrónico, se encuentran en el Anexo B.

1. Se activa a la red para que funcione con IPv6

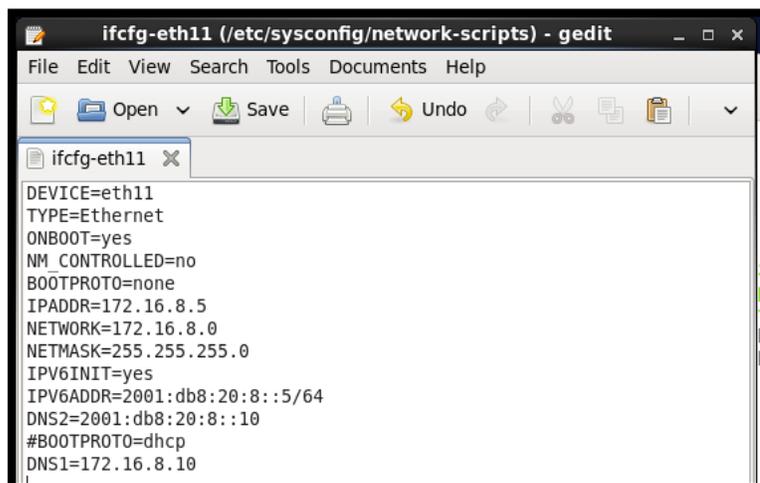


```
root@localhost:~  
File Edit View Search Terminal Help  
GNU nano 2.0.9 File: /etc/sysconfig/network  
NETWORKING=yes  
NETWORKING_IPV6=yes  
HOSTNAME=localhost.localdomain  
IPV6_AUTOCONF=no  
IPV6_AUTOTUNNEL=no  
GATEWAY=172.16.8.1
```

Figura C-25. Activación de Red para soporte IPv6

Fuente: Captura propia extraída de software Centos 6

2. Se comienza configurando la tarjeta de red con el comando que ya se ha señalado anteriormente y se configuran las IP's o la doble pila



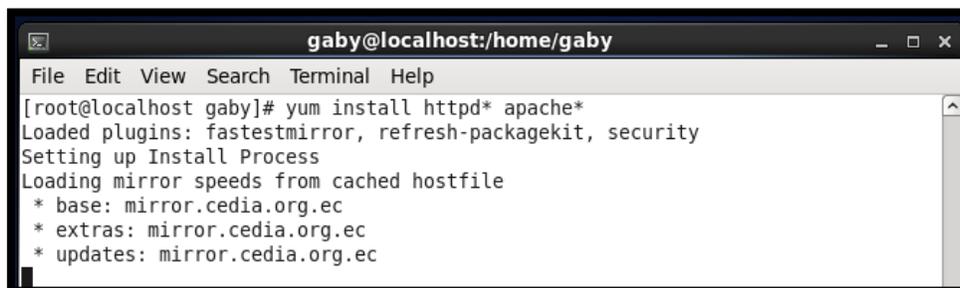
```
ifcfg-eth11 (/etc/sysconfig/network-scripts) - gedit  
File Edit View Search Tools Documents Help  
Open Save Undo  
ifcfg-eth11  
DEVICE=eth11  
TYPE=Ethernet  
ONBOOT=yes  
NM_CONTROLLED=no  
BOOTPROTO=none  
IPADDR=172.16.8.5  
NETWORK=172.16.8.0  
NETMASK=255.255.255.0  
IPV6INIT=yes  
IPV6ADDR=2001:db8:20:8::5/64  
DNS2=2001:db8:20:8::10  
#BOOTPROTO=dhcp  
DNS1=172.16.8.10
```

Figura C-26. Configuración doble pila

Fuente: Captura propia extraída de software Centos 6

Servidor WEB en Centos 6.5 en VMware

1. Se instala el paquete httpd y apache



```

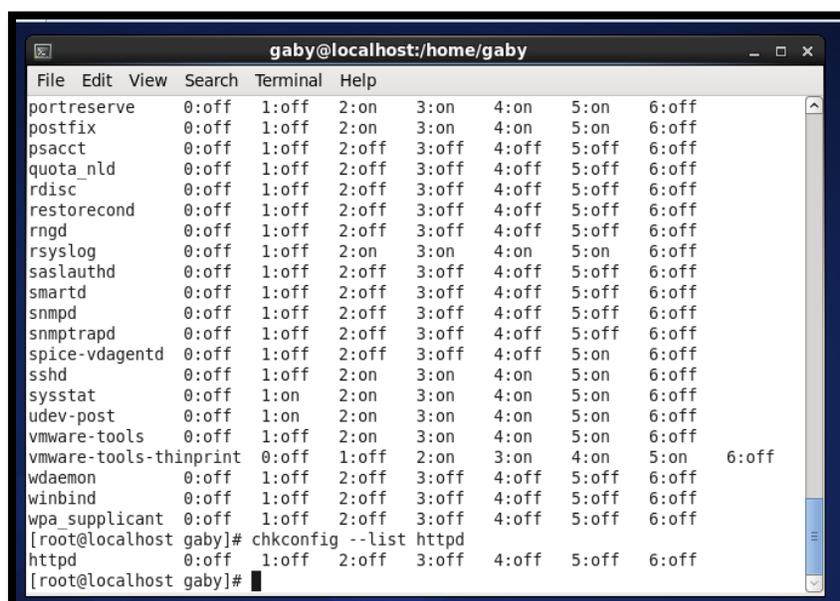
gaby@localhost:/home/gaby
File Edit View Search Terminal Help
[root@localhost gaby]# yum install httpd* apache*
Loaded plugins: fastestmirror, refresh-packagekit, security
Setting up Install Process
Loading mirror speeds from cached hostfile
* base: mirror.cedia.org.ec
* extras: mirror.cedia.org.ec
* updates: mirror.cedia.org.ec

```

Figura D- 1. *Instalación paquetes http y apache*

Fuente: Captura propia extraída de software Centos 6

2. Se verifica el estado del httpd y se observa que está apagado



```

gaby@localhost:/home/gaby
File Edit View Search Terminal Help
portreserve 0:off 1:off 2:on 3:on 4:on 5:on 6:off
postfix 0:off 1:off 2:on 3:on 4:on 5:on 6:off
psacct 0:off 1:off 2:off 3:off 4:off 5:off 6:off
quota_nld 0:off 1:off 2:off 3:off 4:off 5:off 6:off
rdisc 0:off 1:off 2:off 3:off 4:off 5:off 6:off
restorecond 0:off 1:off 2:off 3:off 4:off 5:off 6:off
rngd 0:off 1:off 2:off 3:off 4:off 5:off 6:off
rsyslog 0:off 1:off 2:on 3:on 4:on 5:on 6:off
saslauthd 0:off 1:off 2:off 3:off 4:off 5:off 6:off
smartd 0:off 1:off 2:off 3:off 4:off 5:off 6:off
snmpd 0:off 1:off 2:off 3:off 4:off 5:off 6:off
snmptrapd 0:off 1:off 2:off 3:off 4:off 5:off 6:off
spice-vdagentd 0:off 1:off 2:off 3:off 4:off 5:on 6:off
sshd 0:off 1:off 2:on 3:on 4:on 5:on 6:off
sysstat 0:off 1:on 2:on 3:on 4:on 5:on 6:off
udev-post 0:off 1:on 2:on 3:on 4:on 5:on 6:off
vmware-tools 0:off 1:off 2:on 3:on 4:on 5:on 6:off
vmware-tools-thinprint 0:off 1:off 2:on 3:on 4:on 5:on 6:off
wdaemon 0:off 1:off 2:off 3:off 4:off 5:off 6:off
winbind 0:off 1:off 2:off 3:off 4:off 5:off 6:off
wpa_supplicant 0:off 1:off 2:off 3:off 4:off 5:off 6:off
[root@localhost gaby]# chkconfig --list httpd
httpd 0:off 1:off 2:off 3:off 4:off 5:off 6:off
[root@localhost gaby]#

```

Figura D- 2. *Estado de puertos http*

Fuente: Captura propia extraída de software Centos 6

3. Colocar el comando `chkconfig httpd on` para que funcione

```

winbind      0:off  1:off  2:off  3:off  4:off  5:off  6:off
wpa_supplicant 0:off  1:off  2:off  3:off  4:off  5:off  6:off
[root@localhost gaby]# chkconfig --list httpd
httpd        0:off  1:off  2:off  3:off  4:off  5:off  6:off
[root@localhost gaby]# chkconfig httpd on
[root@localhost gaby]# service httpd status

```

Figura D- 3. Encender puertos y habilitación al inicio del servicio http

Fuente: Captura propia extraída de software Centos 6

4. En el navegador colocar localhost y verificar que apache 2 está trabajando.

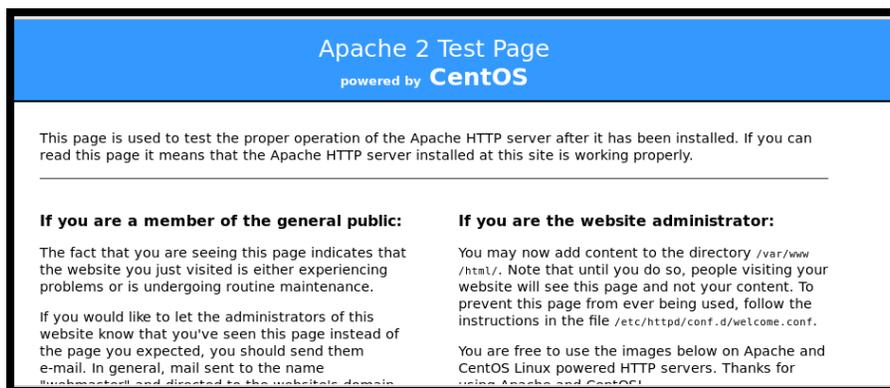


Figura D- 4. Verificación de estado de apache

Fuente: Captura propia extraída de software Centos 6

5. Acceder al fichero html y colocamos el título de la página WEB del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra y de la misma manera se le da permisos de escritura y lectura con el comando `chmod 664` a la carpeta del `index.html` que es donde se edita la página.

```

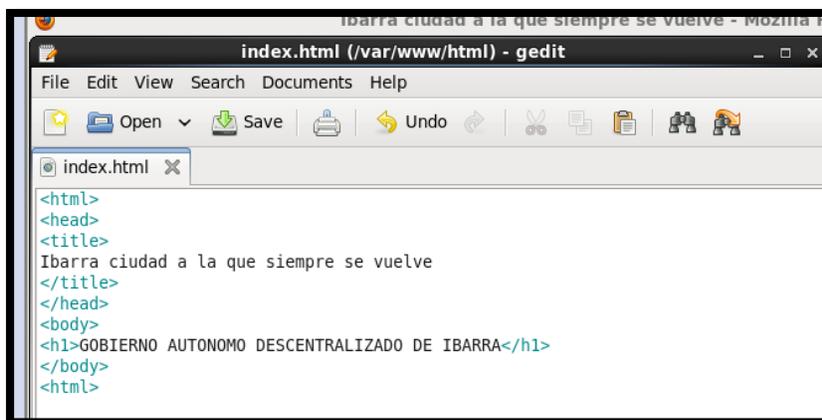
gaby@localhost:~/var/www/html
File Edit View Search Terminal Help
[root@localhost gaby]# cd /var/www/html
[root@localhost html]# ls
[root@localhost html]# echo "GOBIERNO AUTONOMO DESCENTRALIZADO DE IBARRA">>index.html
[root@localhost html]# chmod 644 index.html
[root@localhost html]#

```

Figura D- 5. Edición de la página del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra

Fuente: Captura propia extraída de software Centos 6

6. Con el comando `gedit index.html` se edita para configurar la página con el formato de su preferencia



```
<html>
<head>
<title>
Ibarra ciudad a la que siempre se vuelve
</title>
</head>
<body>
<h1>GOBIERNO AUTONOMO DESCENTRALIZADO DE IBARRA</h1>
</body>
</html>
```

Figura D- 6. Archivo *index.html*

Fuente: Captura propia extraída de software Centos 6

7. Se guardan las configuraciones y se procede a acceder nuevamente en el navegador localhost y se observa la creación de la página WEB de prueba para el Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra



Figura D- 7. *Página del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, prueba de funcionamiento, creada por la Autora*

Fuente: Captura propia extraída de software Centos 6



Figura D- 8. *Prueba de página en IPv6*

Fuente: Captura propia extraída de software Centos 6

Para demostrar el funcionamiento del servidor WEB configurado como IPv4/Ipv6 se utilizará el sistema operativo Centos 6 versión 7 y está funcionando en una máquina virtual montando en VMWare, el proceso de instalación del servidor WEB, se encuentran en el Anexo C.

3. Para configurar la red IPv4/Ipv6 se ingresa a un terminal:

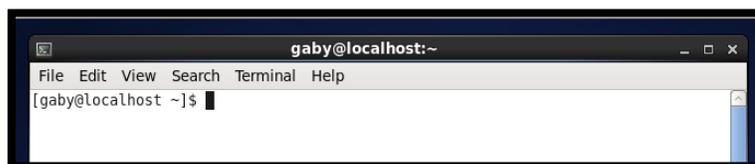


Figura D-9. Acceso a un terminal en Centos

Fuente: Captura propia extraída de software Centos 6

- Para configurar la interfaz de red, se edita con el siguiente comando:

```
#gedit /etc/sysconfig/network-scripts/ifcfg-eth0
```

Nota: en este caso la interfaz tiene especificada la eth0

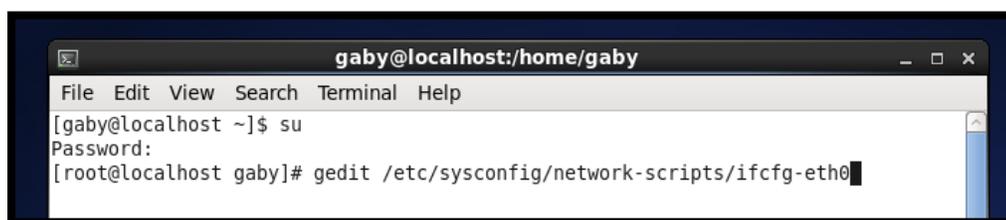


Figura D-10. Configuración de Interfaz

Fuente: Captura propia extraída de software Centos 6

- Se configuran las interfaces tanto en IPv4 como en Ipv6, estableciendo además el DNS, que de acuerdo a cuál se escoja como principal DNS1, será el primario, mientras que el secundario será el DNS2

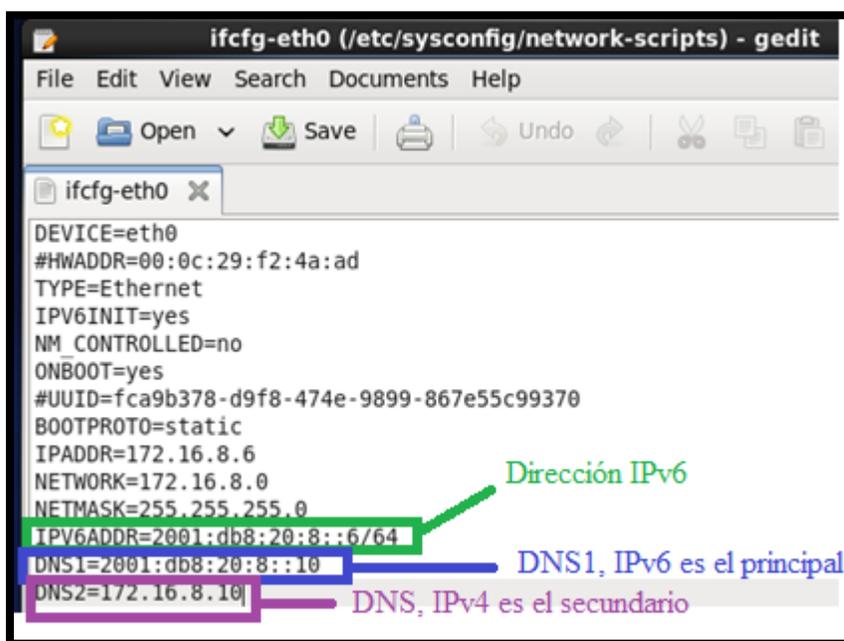


Figura D-11. Configuración de Interfaz de Red

Fuente: Captura propia extraída de software Centos 6

- Para habilitar el protocolo en la red y evitar que la dirección IPv6 sea asignada por RA se debe modificar el fichero #gedit /etc/sysconfig/network

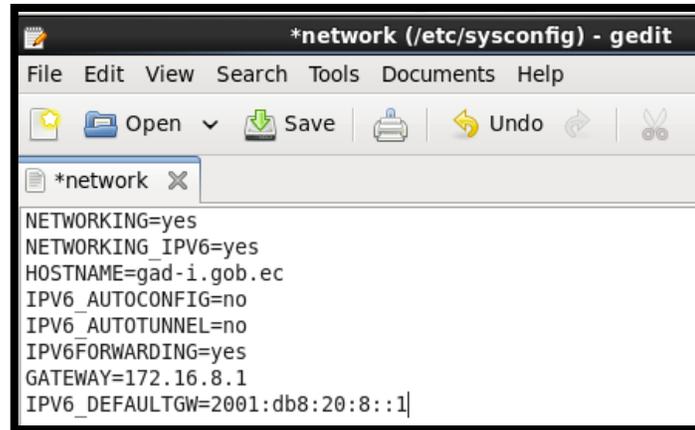


Figura D-12. Ingreso a fichero de configuración de red

Fuente: Captura propia extraída de software Centos 6

- Se guardan todos los cambios y reiniciamos el servicio de red

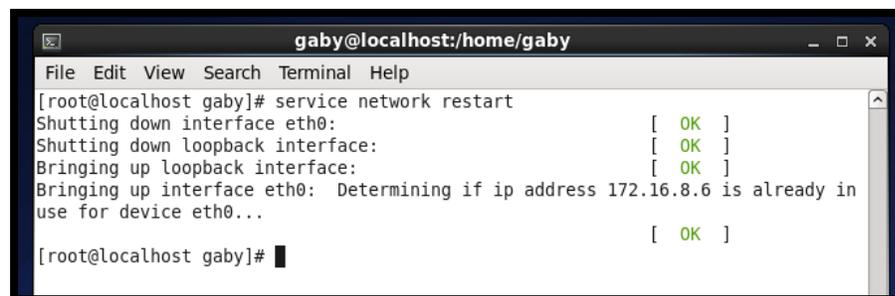


Figura D-13. Reinicio del servicio de red

Fuente: Captura propia extraída de software Centos 6

- Para verificar que se haya configurado la red se realiza un ping con el comando:

```
Ifconfig eth0 && ping6 2001:db8:20:8::6
```

```
[root@localhost ~]# ifconfig eth11 && ping6 2001:db8:20:8::6
eth11  Link encap:Ethernet  HWaddr 00:0C:29:C7:C8:BE
       inet addr:172.16.8.6  Bcast:172.16.8.255  Mask:255.255.255.0
       inet6 addr: 2001:db8:20:8::6/64 Scope:Global
       inet6 addr: fe80::20c:29ff:fec7:c8be/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:100 errors:0 dropped:0 overruns:0 frame:0
       TX packets:429 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:12375 (12.0 KiB)  TX bytes:31462 (30.7 KiB)
       Interrupt:19 Base address:0x2080

PING 2001:db8:20:8::6(2001:db8:20:8::6) 56 data bytes
64 bytes from 2001:db8:20:8::6: icmp_seq=1 ttl=64 time=0.029 ms
64 bytes from 2001:db8:20:8::6: icmp_seq=2 ttl=64 time=0.069 ms
64 bytes from 2001:db8:20:8::6: icmp_seq=3 ttl=64 time=0.070 ms
64 bytes from 2001:db8:20:8::6: icmp_seq=4 ttl=64 time=0.069 ms
64 bytes from 2001:db8:20:8::6: icmp_seq=5 ttl=64 time=0.069 ms
```

Figura D-14. Verificación de configuración IPv6

Fuente: Captura propia extraída de software Centos 6

9. Verificación del servicio IPv4



Figura D-15. Servidor Correo IPv4

Fuente: Captura propia extraída de software Centos 6

10. Comprobar el funcionamiento del servidor WEB con la dirección IPv6

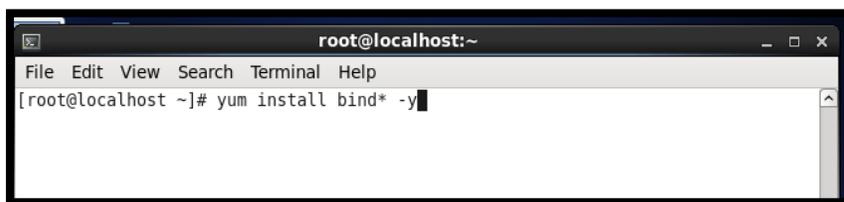


Figura D-16. Servidor WEB IPv6

Fuente: Captura propia extraída de software Centos 6

La configuración de este servidor es con la finalidad de realizar traducciones para que se conecten los dispositivos que trabajan con uno solo protocolo y puedan tener conectividad entre ambos a través de él. Para el funcionamiento de DNS64, se va a proseguir con los siguientes pasos de instalación.

1. Se instala el paquete BIND (Berkeley Internet Name Domain), siendo una herramienta muy utilizada caracterizada por ser robusta y estable por ello se utilizará en este servidor.

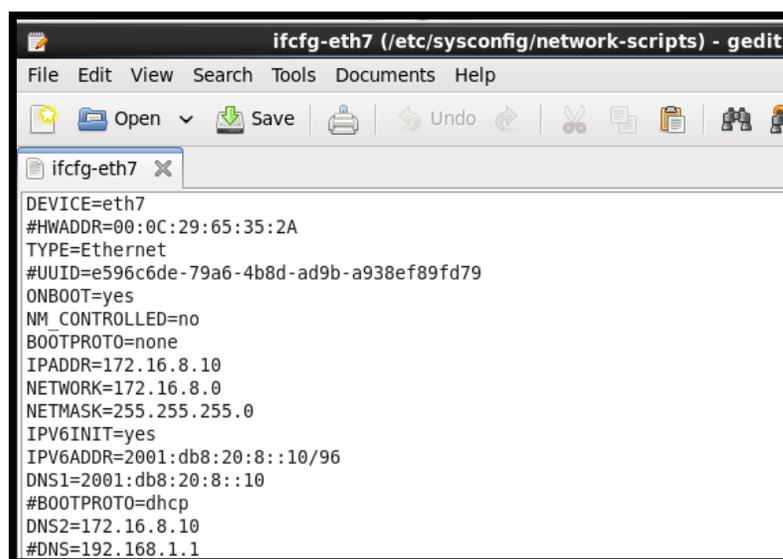


```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# yum install bind* -y
```

Figura E-1. Instalación del paquete Bind

Fuente: Captura propia extraída de software Centos 6

2. Se va configurar las interfaces para que pueda funcionar tanto en IPv4 como en Ipv6 editando el fichero ya conocido:



```
ifcfg-eth7 (/etc/sysconfig/network-scripts) - gedit  
File Edit View Search Tools Documents Help  
Open Save Undo  
ifcfg-eth7  
DEVICE=eth7  
#HWADDR=00:0C:29:65:35:2A  
TYPE=Ethernet  
#UUID=e596c6de-79a6-4b8d-ad9b-a938ef89fd79  
ONBOOT=yes  
NM_CONTROLLED=no  
BOOTPROTO=none  
IPADDR=172.16.8.10  
NETWORK=172.16.8.0  
NETMASK=255.255.255.0  
IPV6INIT=yes  
IPV6ADDR=2001:db8:20:8::10/96  
DNS1=2001:db8:20:8::10  
#BOOTPROTO=dhcp  
DNS2=172.16.8.10  
#DNS=192.168.1.1
```

Figura E-2. Configuración de las tarjetas de red

Fuente: Captura propia extraída de software Centos 6

3. Ahora, para el inicio de la configuración del servidor DNS64 se debe editar el fichero named.conf, utilizando el comando `#gedit /etc/named.conf`, Este archivo contiene los parámetros de configuración que el servidor necesita para poder funcionar. Utiliza el puerto 53 y aquí se editan las direcciones que va a escuchar, que serán traducidas y enviadas a su destino

```

File Edit View Search Terminal Help
[root@localhost ~]# gedit /etc/n
named/          named.root.key    nfsmount.conf
named.conf      nanorc            nsswitch.conf
named.iscdlv.key netconfig         ntp/
named.rfc1912.zones networks          ntp.conf
[root@localhost ~]# gedit /etc/named.conf

```

Figura E-3. Ingreso al archivo de Configuración del Fichero DNS

Fuente: Captura propia extraída de software Centos 6

- Se realiza el direccionamiento del puerto, en el campo options, se colocan las direcciones IPv4 e IPv6 respectivamente que el servidor va a tener. De igual manera asignar los forwarders o reenviadores de Internet que son los que redireccionan las peticiones a los DNS externos.

```

named.conf (/etc) - gedit
File Edit View Search Tools Documents Help
named.conf
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
options {
    listen-on port 53 { 127.0.0.1; 172.16.8.10; };
    listen-on-v6 port 53 { ::1; 2001:db8:20:8::10; };
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    forward first;
    forwarders {
        8.8.8.8;
        8.8.4.4;
        172.16.8.10;
        2001:db8:20:8::10;
    };
    allow-query { any; localhost; 172.16.8.0/24; 2001:db8:20:8::/64; };
    recursion yes;
    dns64 2001:db8:20:8:ffff::/96 {
    clients { any; };
};

```

Puertos DNS

Direcciones IPv4/IPv6

Busca primero en zonas directas, Servidores DNS que van a enrutar las peticiones del servidor de dominios

Redes de quien se escuchan peticiones DNS

Figura E-4. Configuración del Fichero DNS

Fuente: Captura propia extraída de software Centos 6

- Ahora se van a crear las zonas, en ellas se encuentran los registros que se van a traducir, por lo tanto, se crea una zona de reenvío por cada dominio que se tenga autoridad y una zona inversa por cada red que de igual forma se tenga control total, éstas se crean con el objetivo de resolver el dominio.

Zona Directa

Esta zona se configura en el mismo fichero /etc/named.conf, se puede definir si será primaria (máster) o secundaria (slave). Esto quiere decir que, si es primario, podrá transferir de las zonas de otros servidores DNS, en cambio, si es secundario se utiliza para tener más direcciones de un dominio.

```

zone "gad-i.gob.ec" IN {
    type master;
    file "forward.gad-i.gob.ec";
    allow-update { none; };
};

```

Annotations in the image:

- Zona de dominio**: points to "gad-i.gob.ec"
- Tipo primario**: points to "type master;"
- Archivo de zona directa**: points to "file 'forward.gad-i.gob.ec';"
- Host autorizados para enviar actualizaciones dinámicas**: points to "allow-update { none; };"

Figura E-5. Configuración Zona Directa

Fuente: Captura propia extraída de software Centos 6

Se guarda el contenido en el fichero named.conf y ahora se confirma que en la carpeta named se encuentre creado el archivo forward.gad-i.gob.ec.

```

$TTL 86400
@ IN SOA dns.gad-i.gob.ec. root.gad-i.gob.ec. (
    2016071022 ;Serial
    3600 ;Refresh
    1800 ;Retry
    604800 ;Expire
    86400 ;Minimun TTL
)
@ IN NS dns.gad-i.gob.ec.
@ IN A 172.16.8.10
@ IN AAAA 2001:db8:20:8::10
@ IN MX 10 mail
@ IN TXT "v=spr1 a mx -all"
dns IN A 172.16.8.10
6dns IN AAAA 2001:db8:20:8::10
www IN A 172.16.8.6
www IN AAAA 2001:db8:20:8::6
mail IN A 172.16.8.5
mail IN AAAA 2001:db8:20:8::5

```

Annotations in the image:

- Registros IPv4=A, Registros IPv6=AAAA**: points to the SOA and NS records.
- Registro para Mail**: points to the MX record.
- Direcciones DNS**: points to the dns A record.
- Direcciones WEB**: points to the www A and AAAA records.
- Direcciones MAIL**: points to the mail A and AAAA records.

Figura E-6. Archivo definido en zona directa

Fuente: Captura propia extraída de software Centos 6

Zona Inversa

6. Igual que las zonas directas se deben definir las zonas inversas en el mismo archivo /etc/named.conf

```

);
zone "gad-i.gob.ec" IN {
    type master;
    file "forward.gad-i.gob.ec";
    allow-update { none; };
};
zone "8.0.0.0.0.2.0.0.8.b.d.0.0.8.2.ip6.arpa." IN {
    file "reverse6.gad-i.gob.ec";
    allow-update { none; };
};
zone "8.16.172.in-addr.arpa" IN {
    type master;
    file "reverse.gad-i.gob.ec";
    allow-update { none; };
};
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

```

Figura E-7. Configuración del Fichero DNS

Fuente: Captura propia extraída de software Centos 6

7. Se guardan las configuraciones y se configuran las zonas inversas, primero se configura la zona inversa para ipv4 en el fichero #gedit /var/named/reverse.gad-i.gob.ec

```

$TTL 86400
@ IN SOA dns.gad-i.gob.ec. root.gad-i.gob.ec. (
    2016071022 ;Serial
    3600 ;Refresh
    1800 ;Retry
    604800 ;Expire
    86400 ;Minimum TTL
)
@ IN NS dns.gad-i.gob.ec.
@ IN PTR 172.16.8.10
10 IN PTR dns.gad-i.gob.ec.
6 IN PTR www.gad-i.gob.ec.
5 IN PTR mail.gad-i.gob.ec.

```

Figura E-8. Zona Inversa IPv4

Para registros A #dig any gad-i.gob.ec y para y para registros aaaa #dig aaaa any gad-i.gob.ec

```

root@localhost:/
File Edit View Search Terminal Help
[root@localhost /]# dig any gad-i.gob.ec

; <<> DiG 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.5 <<> any gad-i.gob.ec
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 3832
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 3

;; QUESTION SECTION:
;gad-i.gob.ec.                IN      ANY

;; ANSWER SECTION:
gad-i.gob.ec.                86400  IN      SOA     dns.gad-i.gob.ec. root.gad-i.gob
.ec. 2016071022 3600 1800 604800 86400
gad-i.gob.ec.                86400  IN      NS      dns.gad-i.gob.ec.
gad-i.gob.ec.                86400  IN      A       172.16.8.10
gad-i.gob.ec.                86400  IN      AAAA   2001:db8:20:8::10
gad-i.gob.ec.                86400  IN      MX     10 mail.gad-i.gob.ec.
gad-i.gob.ec.                86400  IN      TXT    "v=spf1 a mx -all"

;; ADDITIONAL SECTION:
dns.gad-i.gob.ec.           86400  IN      A       172.16.8.10
mail.gad-i.gob.ec.         86400  IN      A       172.16.8.5
mail.gad-i.gob.ec.         86400  IN      AAAA   2001:db8:20:8::5

;; Query time: 0 msec

```

Figura E-11. Comprobación de DNS con IPv4

Fuente: Captura propia extraída de software Centos 6

```

root@localhost:/
File Edit View Search Terminal Help
[root@localhost /]# dig aaaa any gad-i.gob.ec
;; Warning, extra type option

; <<> DiG 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.5 <<> aaaa any gad-i.gob.ec
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 18369
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 3

;; QUESTION SECTION:
;gad-i.gob.ec.                IN      ANY

;; ANSWER SECTION:
gad-i.gob.ec.                86400  IN      SOA     dns.gad-i.gob.ec. root.gad-i.gob.
ec. 2016071022 3600 1800 604800 86400
gad-i.gob.ec.                86400  IN      NS      dns.gad-i.gob.ec.
gad-i.gob.ec.                86400  IN      A       172.16.8.10
gad-i.gob.ec.                86400  IN      AAAA   2001:db8:20:8::10
gad-i.gob.ec.                86400  IN      MX     10 mail.gad-i.gob.ec.
gad-i.gob.ec.                86400  IN      TXT    "v=spf1 a mx -all"

;; ADDITIONAL SECTION:
dns.gad-i.gob.ec.           86400  IN      A       172.16.8.10
mail.gad-i.gob.ec.         86400  IN      A       172.16.8.5
mail.gad-i.gob.ec.         86400  IN      AAAA   2001:db8:20:8::5

```

Figura E-12. Comprobación de DNS con IPv6

Fuente: Captura propia extraída de software Centos 6

11. Con el comando `#nslookup gad-i.gob.ec` se puede realizar consultas dinámicamente al DNS que permite conocer el nombre o traducir el dominio sabiendo la IP.



```

root@localh
File Edit View Search Terminal Help
[root@localhost /]# nslookup gad-i.gob.ec
Server:          2001:db8:20:8::10
Address:         2001:db8:20:8::10#53

Name:   gad-i.gob.ec
Address: 172.16.8.10

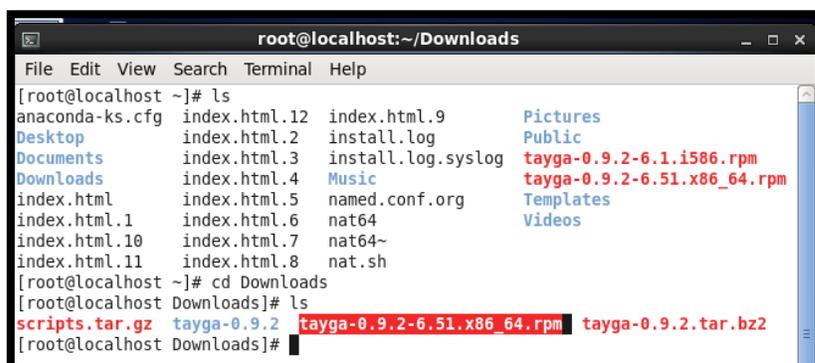
[root@localhost /]# █

```

Figura E-13. Prueba del nslookup

Fuente: Captura propia extraída de software Centos 6

12. Para el funcionamiento del NAT64, se debe instalar un paquete de traducción de red que se llama tayga, se descarga. A continuación, se descomprime y se instala el programa



```

root@localhost: ~/Downloads
File Edit View Search Terminal Help
[root@localhost ~]# ls
anaconda-ks.cfg  index.html.12  index.html.9      Pictures
Desktop         index.html.2   install.log       Public
Documents       index.html.3   install.log.syslog  tayga-0.9.2-6.1.i586.rpm
Downloads       index.html.4   Music            tayga-0.9.2-6.51.x86_64.rpm
index.html      index.html.5   named.conf.org    Templates
index.html.1    index.html.6   nat64             Videos
index.html.10   index.html.7   nat64~
index.html.11   index.html.8   nat.sh
[root@localhost ~]# cd Downloads
[root@localhost Downloads]# ls
scripts.tar.gz  tayga-0.9.2  tayga-0.9.2-6.51.x86_64.rpm  tayga-0.9.2.tar.bz2
[root@localhost Downloads]# █

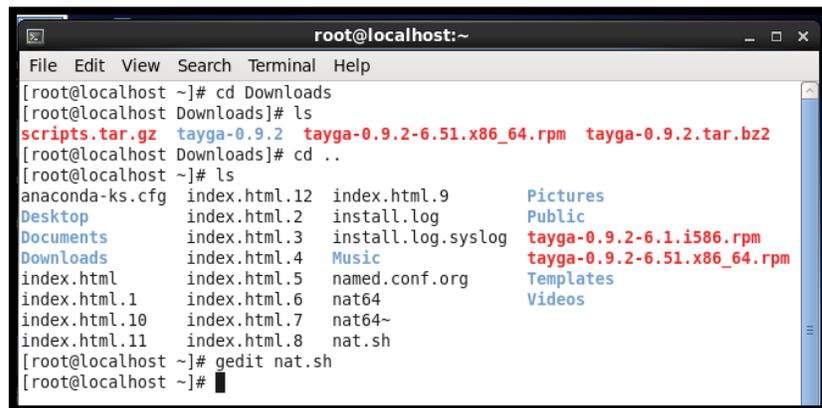
```

Figura E-14. Instalación de tayga

Fuente: Captura propia extraída de software Centos 6

Estos comandos crean la interfaz nat64 con las direcciones IP, (172.16.8.10) IPv4 y (2001:db8:20:8::10) 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



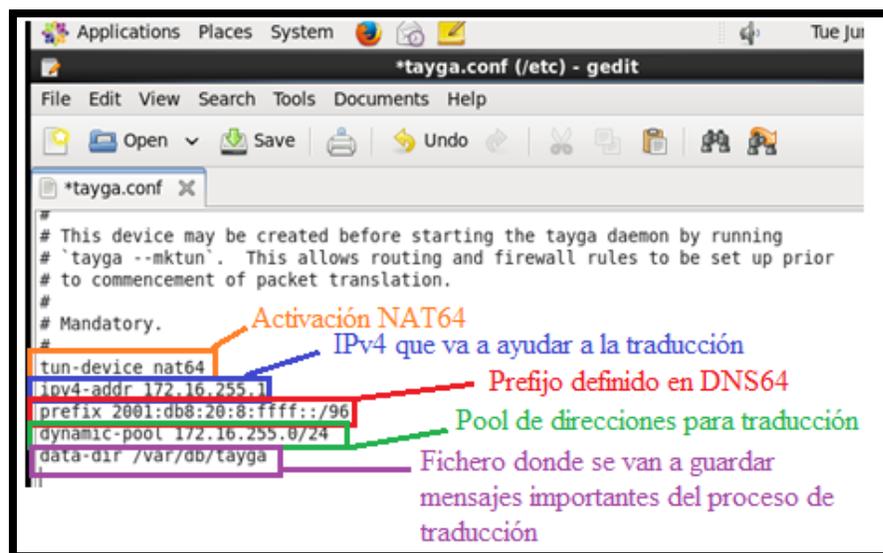
```

root@localhost:~
File Edit View Search Terminal Help
[root@localhost ~]# cd Downloads
[root@localhost Downloads]# ls
scripts.tar.gz tayga-0.9.2 tayga-0.9.2-6.51.x86_64.rpm tayga-0.9.2.tar.bz2
[root@localhost Downloads]# cd ..
[root@localhost ~]# ls
anaconda-ks.cfg index.html.12 index.html.9 Pictures
Desktop index.html.2 install.log Public
Documents index.html.3 install.log.syslog tayga-0.9.2-6.1.i586.rpm
Downloads index.html.4 Music tayga-0.9.2-6.51.x86_64.rpm
index.html index.html.5 named.conf.org Templates
index.html.1 index.html.6 nat64 Videos
index.html.10 index.html.7 nat64~
index.html.11 index.html.8 nat.sh
[root@localhost ~]# gedit nat.sh
[root@localhost ~]#
  
```

Figura E-15. Edición del Tayga

Fuente: Captura propia extraída de software Centos 6

Luego se configura el fichero tayga.conf, y se asigna los valores de NAT y rangos con los que va a traducir las direcciones de IPv4 a IPv6.



```

Applications Places System Tue Jul
*tayga.conf (/etc) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
*tayga.conf X
#
# This device may be created before starting the tayga daemon by running
# `tayga --mktun`. This allows routing and firewall rules to be set up prior
# to commencement of packet translation.
#
# Mandatory.
#
tun-device nat64
ipv4-addr 172.16.255.1
prefix 2001:db8:20:8::ffff::/96
dynamic-pool 1/2.16.255.0/24
data-dir /var/db/tayga
  
```

Activación NAT64

IPv4 que va a ayudar a la traducción

Prefijo definido en DNS64

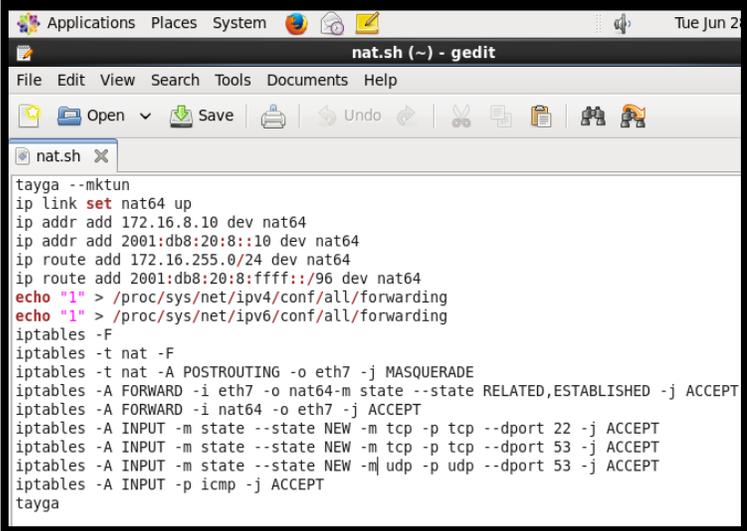
Pool de direcciones para traducción

Fichero donde se van a guardar mensajes importantes del proceso de traducción

Figura E-16. Configuración del NAT64

Fuente: Captura propia extraída de software Centos 6

De la misma forma se deben agregar las reglas de nat y dar los permisos de tráfico en el firewall del servidor, como se muestra en la Figura 49.



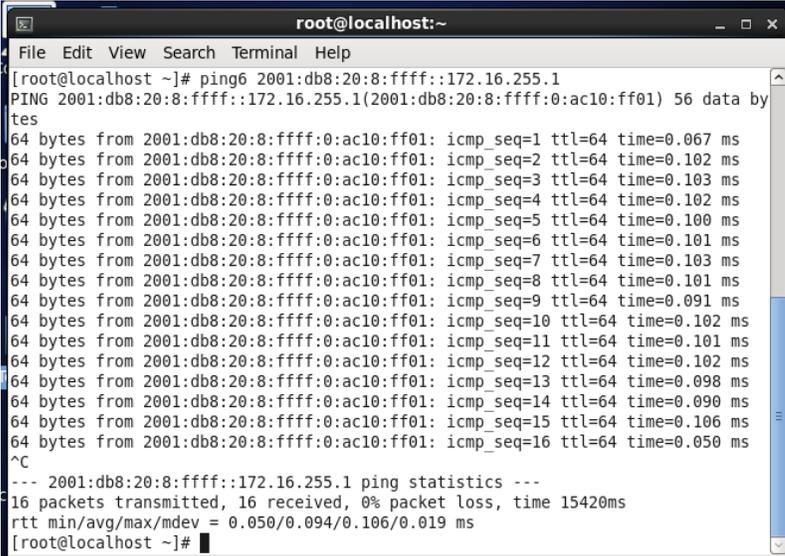
```

tayga --mktun
ip link set nat64 up
ip addr add 172.16.8.10 dev nat64
ip addr add 2001:db8:20:8::10 dev nat64
ip route add 172.16.255.0/24 dev nat64
ip route add 2001:db8:20:8:ffff::/96 dev nat64
echo "1" > /proc/sys/net/ipv4/conf/all/forwarding
echo "1" > /proc/sys/net/ipv6/conf/all/forwarding
iptables -F
iptables -t nat -F
iptables -t nat -A POSTROUTING -o eth7 -j MASQUERADE
iptables -A FORWARD -i eth7 -o nat64 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i nat64 -o eth7 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 53 -j ACCEPT
iptables -A INPUT -m state --state NEW -m udp -p udp --dport 53 -j ACCEPT
iptables -A INPUT -p icmp -j ACCEPT
tayga
  
```

Figura E-17. Configuración de permisos de enrutamiento en el ejecutable nat64.sh

Fuente: Captura propia extraída de software Centos 6

13. Para conocer si la traducción de IP's se ha configurado correctamente, se debe hacer ping IPv6 con su respectiva dirección IPv4, como se muestra en la Figura 50



```

root@localhost:~# ping6 2001:db8:20:8:ffff::172.16.255.1
PING 2001:db8:20:8:ffff::172.16.255.1(2001:db8:20:8:ffff:0:ac10:ff01) 56 data by
tes
64 bytes from 2001:db8:20:8:ffff:0:ac10:ff01: icmp_seq=1 ttl=64 time=0.067 ms
64 bytes from 2001:db8:20:8:ffff:0:ac10:ff01: icmp_seq=2 ttl=64 time=0.102 ms
64 bytes from 2001:db8:20:8:ffff:0:ac10:ff01: icmp_seq=3 ttl=64 time=0.103 ms
64 bytes from 2001:db8:20:8:ffff:0:ac10:ff01: icmp_seq=4 ttl=64 time=0.102 ms
64 bytes from 2001:db8:20:8:ffff:0:ac10:ff01: icmp_seq=5 ttl=64 time=0.100 ms
64 bytes from 2001:db8:20:8:ffff:0:ac10:ff01: icmp_seq=6 ttl=64 time=0.101 ms
64 bytes from 2001:db8:20:8:ffff:0:ac10:ff01: icmp_seq=7 ttl=64 time=0.103 ms
64 bytes from 2001:db8:20:8:ffff:0:ac10:ff01: icmp_seq=8 ttl=64 time=0.101 ms
64 bytes from 2001:db8:20:8:ffff:0:ac10:ff01: icmp_seq=9 ttl=64 time=0.091 ms
64 bytes from 2001:db8:20:8:ffff:0:ac10:ff01: icmp_seq=10 ttl=64 time=0.102 ms
64 bytes from 2001:db8:20:8:ffff:0:ac10:ff01: icmp_seq=11 ttl=64 time=0.101 ms
64 bytes from 2001:db8:20:8:ffff:0:ac10:ff01: icmp_seq=12 ttl=64 time=0.102 ms
64 bytes from 2001:db8:20:8:ffff:0:ac10:ff01: icmp_seq=13 ttl=64 time=0.098 ms
64 bytes from 2001:db8:20:8:ffff:0:ac10:ff01: icmp_seq=14 ttl=64 time=0.090 ms
64 bytes from 2001:db8:20:8:ffff:0:ac10:ff01: icmp_seq=15 ttl=64 time=0.106 ms
64 bytes from 2001:db8:20:8:ffff:0:ac10:ff01: icmp_seq=16 ttl=64 time=0.050 ms
^C
--- 2001:db8:20:8:ffff::172.16.255.1 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15420ms
rtt min/avg/max/mdev = 0.050/0.094/0.106/0.019 ms
root@localhost ~]#
  
```

Figura E-18. Verificación de la interfaz nat64 funcionando

Fuente: Captura propia extraída de software Centos 6

ANEXO D: Instalación de GNS3

Para simular la topología de red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, se va a utilizar este simulador de red, que es compatible con la mayoría de dispositivos de la red, y además de ello nos permite añadir los servicios configurados mediante las máquinas virtuales que son el CORREO, WEB, DNS64 y NAT64.

1. Se va a descargar la versión 1.13.13 de la página de GNS3

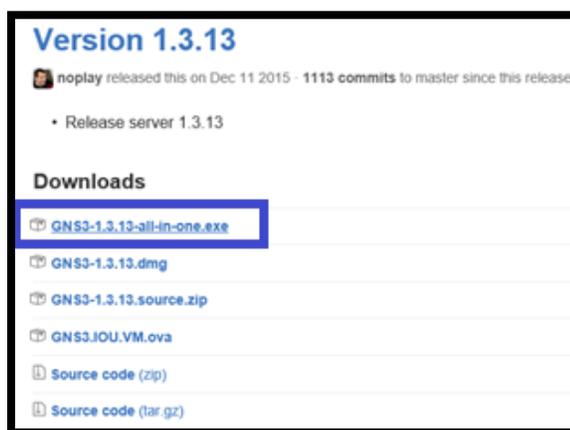


Figura F- 1. Descarga de GNS3

Fuente: <https://www.gns3.com/>

2. Una vez descargado, se hace doble click y aparecerá la pantalla siguiente:

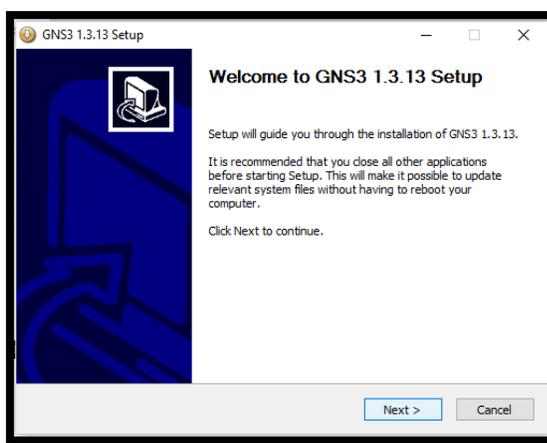
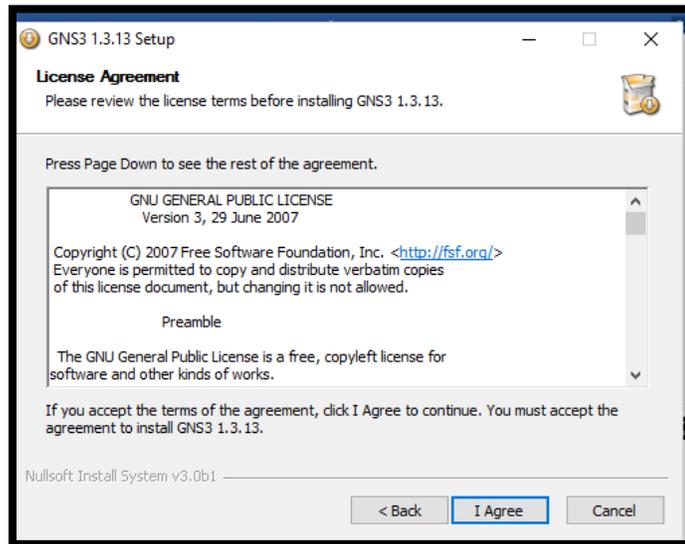


Figura F - 2. *Bienvenida de Instalación GNS3*

Fuente: Captura propia extraída de software GNS3

3. Se acepta la licencia, haciendo click en I Agree

Figura F - 3. *Contrato de Licencia*

Fuente: Captura propia extraída de software GNS3

4. Se escoge el nombre de la carpeta

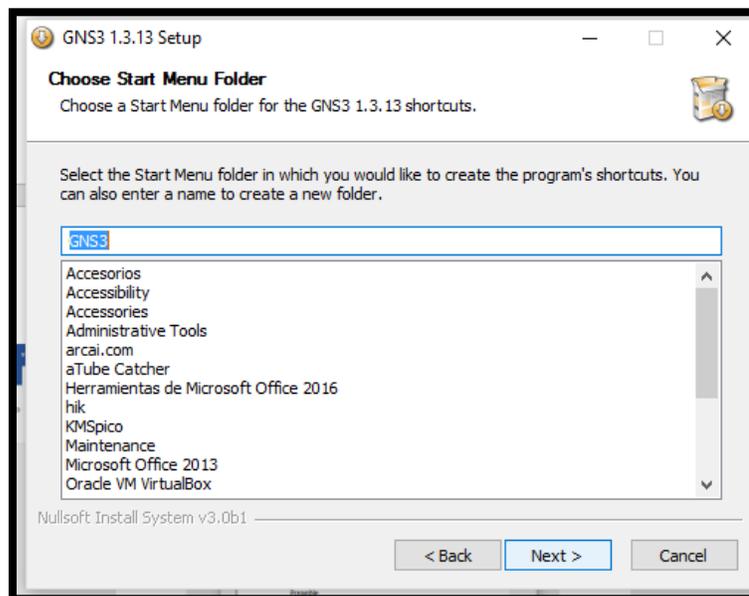


Figura F - 4. Archivo de Inicio de GNS3

Fuente: Captura propia extraída de software GNS3

5. Se acepta la instalación de todos los programas

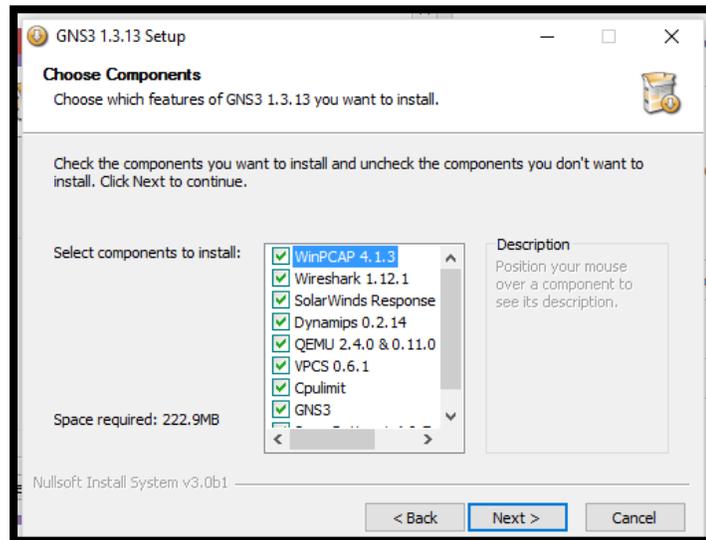


Figura F - 5. Componentes de funcionalidad de GNS3

Fuente: Captura propia extraída de software GNS3

6. Seleccionar en dónde se van a localizar los archivos

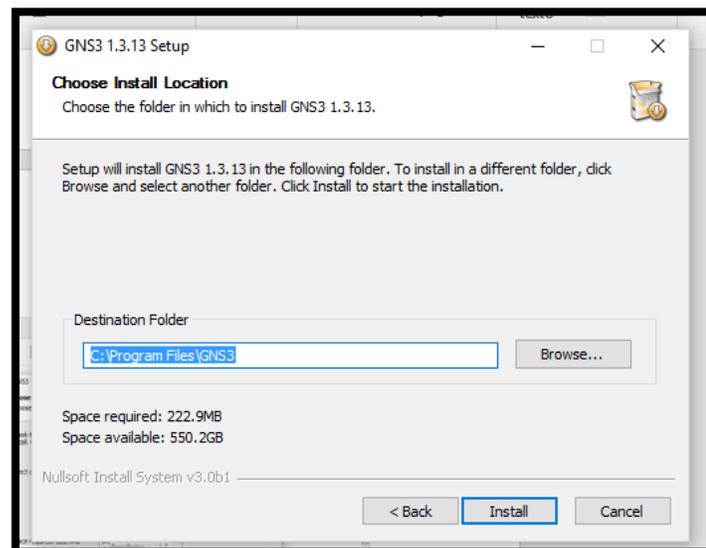


Figura F - 6. Localización del programa GNS3

Fuente: Captura propia extraída de software GNS3

7. Ahora instalado, se ingresa al programa

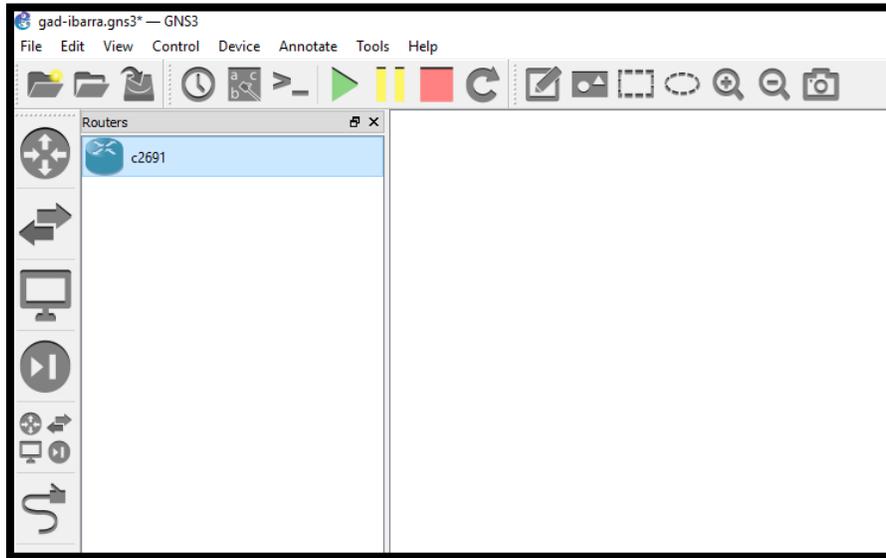


Figura F - 7. Interfaz gráfica de GNS3

Fuente: Captura propia extraída de software GNS3

8. Para agregar los dispositivos, se deben descargar los IOS o imágenes de los dispositivos, por ejemplo, una página que facilita este proceso es: <http://www.networkvn.net/2014/06/cisco-ios-image-for-gns3.html>

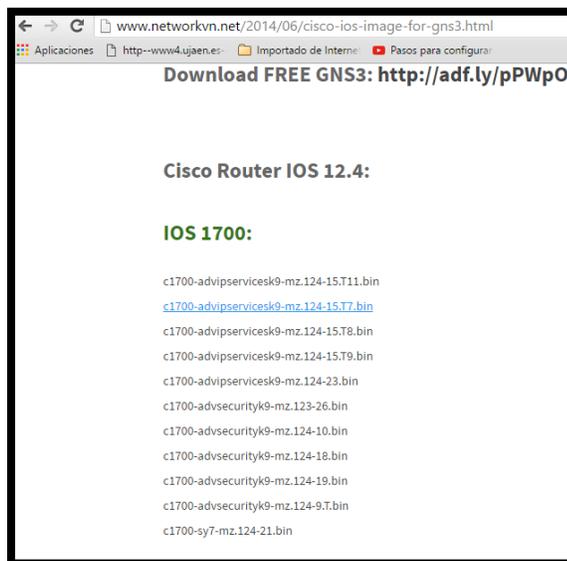


Figura F - 8. Descarga de IOS

Fuente: Captura propia extraída de software GNS3

9. Una vez descargada la imagen, se debe agregar a GNS3, para ello, se dirige a:

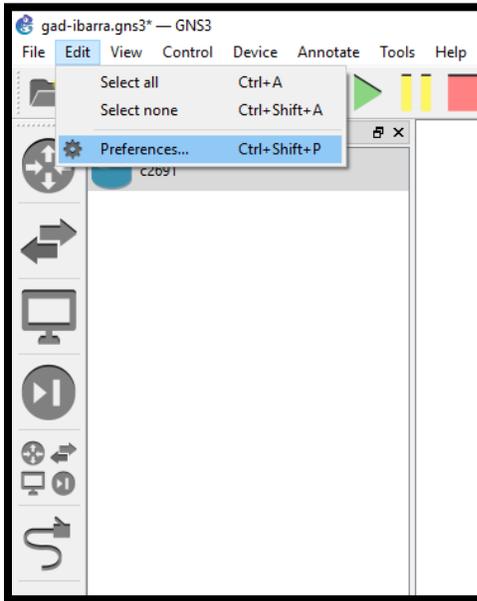


Figura F - 9. *Preferencias del GNS3*

Fuente: Captura propia extraída de software GNS3

10. Se dirige a Dynamips y se escoge IOS routers y se coloca new

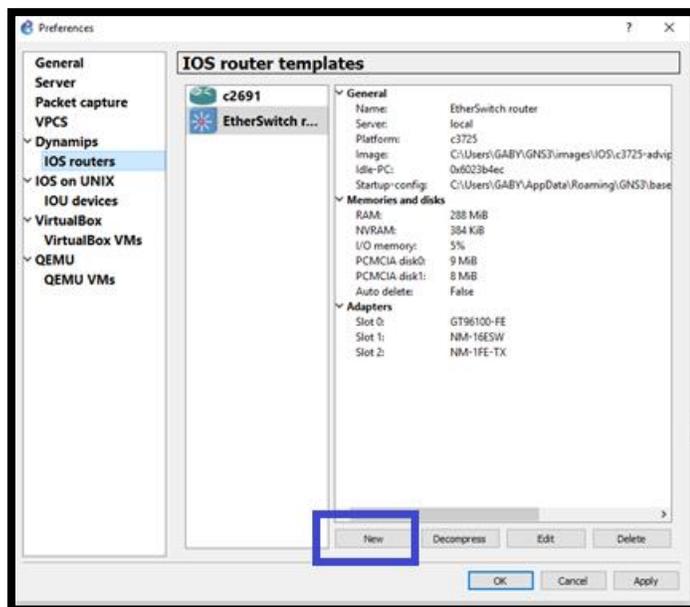


Figura F - 10. *Instalación GNS3*

Fuente: Captura propia extraída de software GNS3

11. Se busca la imagen del IOS, y una vez encontrado, se coloca Next

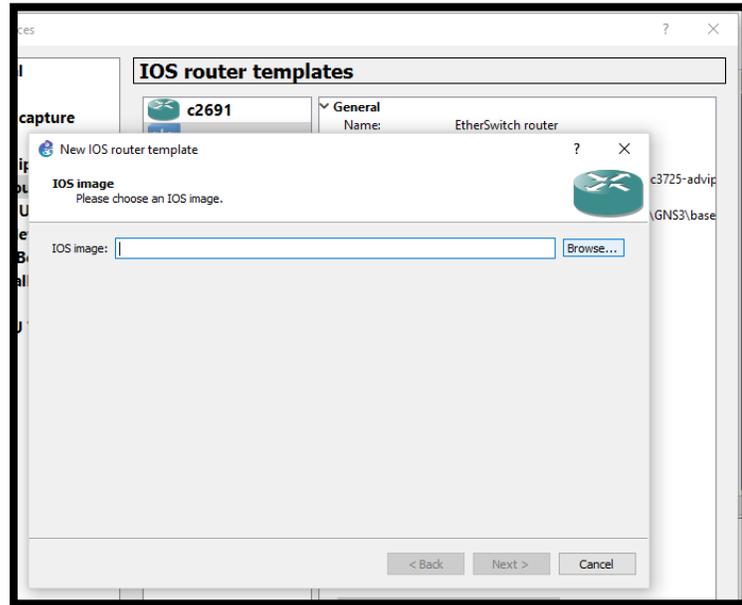


Figura F - 11. Elección de la imagen del equipo IOS

Fuente: Captura propia extraída de software GNS3

12. De igual forma se coloca Next

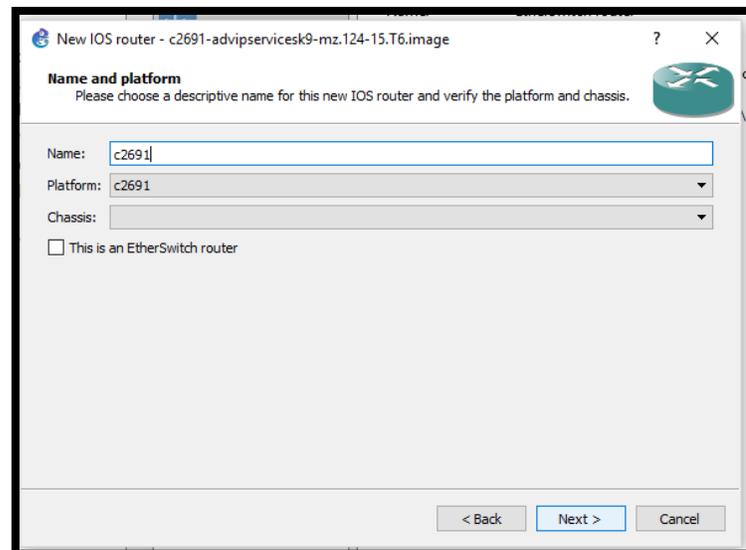


Figura F - 12. Elección del nombre del IOS

Fuente: Captura propia extraída de software GNS3

13. Seleccionar la memoria RAM para poder trabajar y se coloca Next

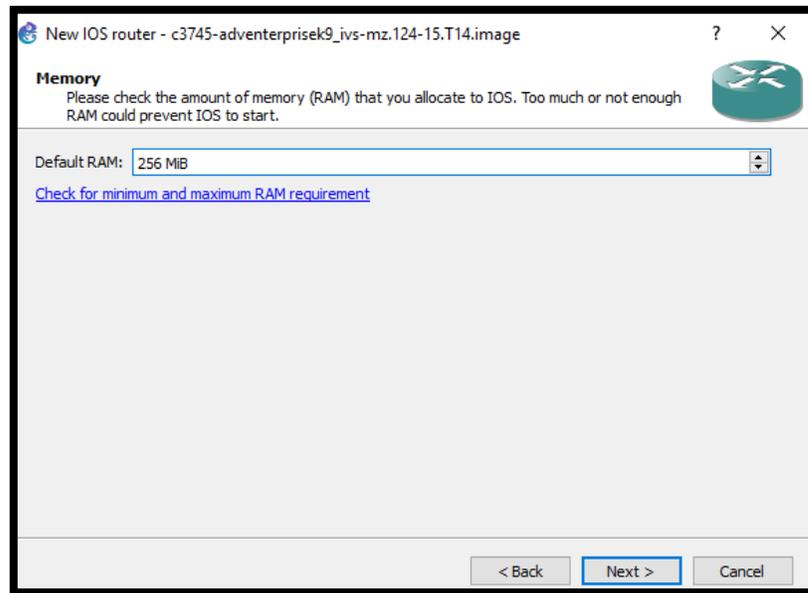


Figura F - 13. Memoria RAM para equipo

Fuente: Captura propia extraída de software GNS3

14. Seleccionar los adaptadores de red

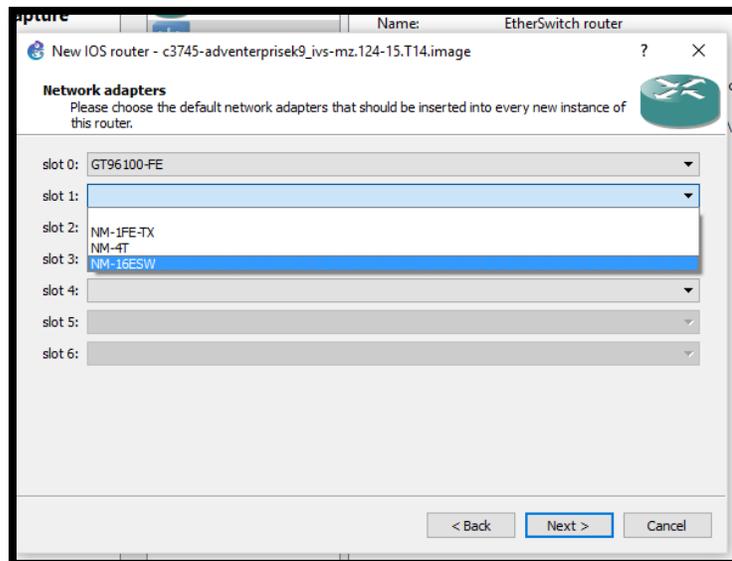


Figura F - 14. Elección de Interfaces

Fuente: Captura propia extraída de software GNS3

15. Y finalmente se coloca finish, con este proceso se puede ya empezar a trabajar con los equipos.

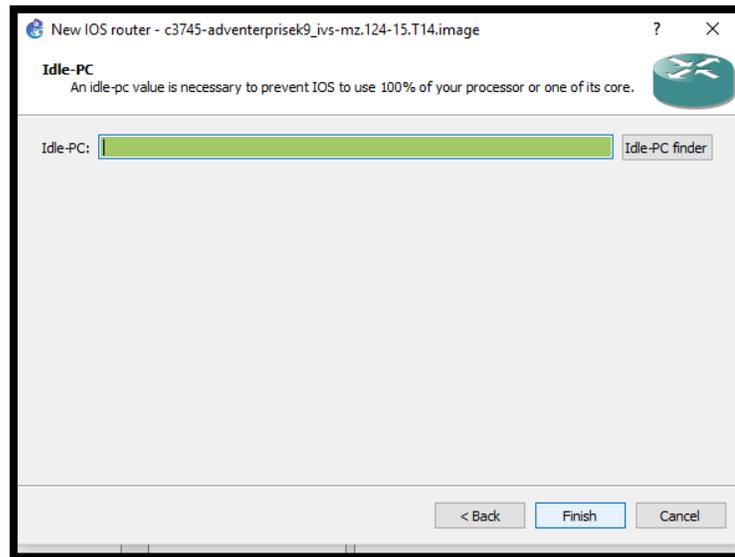


Figura F - 15. Finalización de configuración de equipo

Fuente: Captura propia extraída de software GNS3

Configuración en los equipos:

En este switch se configuran las VLANS de la red local y de la misma manera la comunicación hacia el firewall Checkpoint, de esta forma se muestra la configuración de una de ellas y el proceso va a ser el mismo para todas las demás VLANS.

Para la comprensión de la configuración de estos equipos CISCO, se va a utilizar el programa GNS3, que permite diseñar y simular topologías de redes simples o complejas. Permite ejecutar imágenes IOS de Cisco Systems. (Ariganello, 2012)

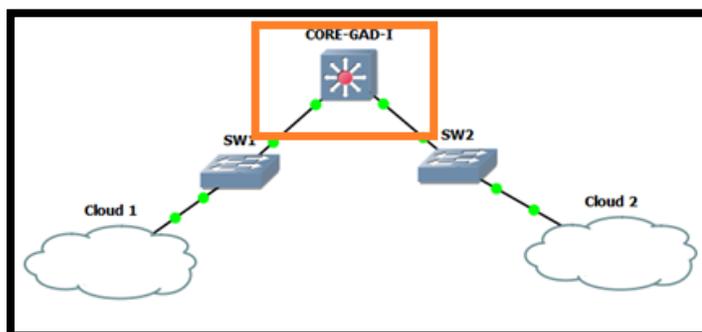


Figura F-16. *Simulación de Red*

Fuente: Captura propia extraída de software GNS3

Se hace doble click en el ethernet switch seleccionado en este caso, se ha escogido uno que soporte IPv6, 3725-advipservicesk9-mz124-25b.bin, y se selecciona start

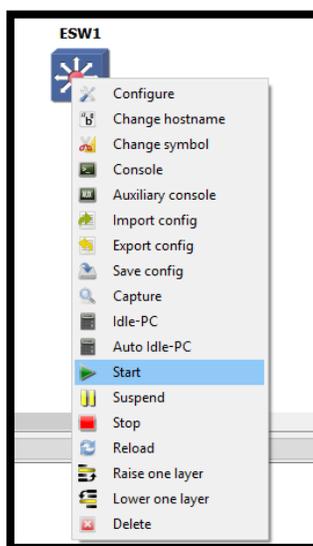


Figura F-17. *Poner en marcha el simulador del equipo*

Fuente: Captura propia extraída de software GNS3

El dispositivo va a empezar a inicializarse y entonces se va a empezar con la correspondiente simulación.

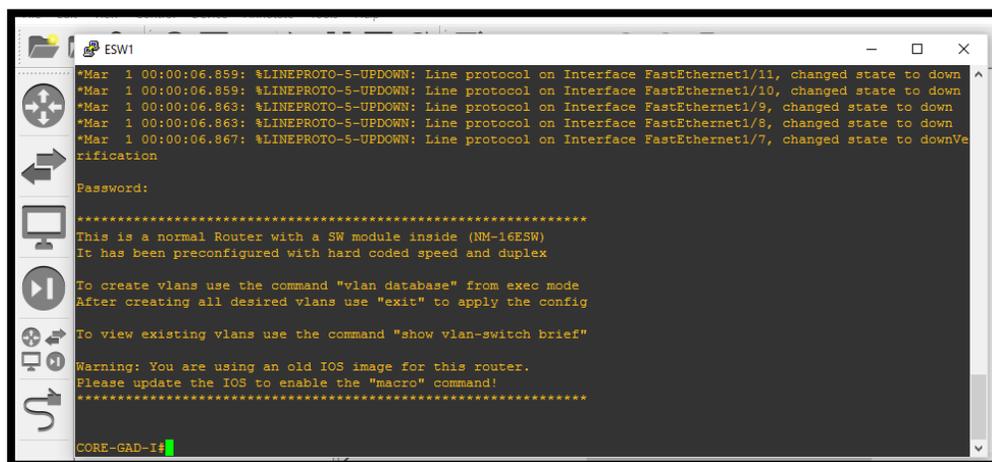


Figura F-18. Inicialización del equipo

Fuente: Captura propia extraída de software GNS3

Se ha configurado previamente, el nombre y acceso al mismo, por lo tanto, se va a proceder a configurar las respectivas VLANS con los comandos:

```
CORE-GAD-I# vlan database
```

```
CORE-GAD-I(vlan)# vlan <número de la vlan> name <nombre de la vlan>
```

Por lo tanto, para la configuración de este proyecto sería:

```
CORE-GAD-I# vlan database
```

```
CORE-GAD-I(vlan)# vlan 2 name SERVIDORES
```

Así para todas las VLANS del GAD-I

```

*****
This is a normal Router with a SW module inside (NM-16ESW)
It has been preconfigured with hard coded speed and duplex

To create vlans use the command "vlan database" from exec mode
After creating all desired vlans use "exit" to apply the config

To view existing vlans use the command "show vlan-switch brief"

Warning: You are using an old IOS image for this router.
Please update the IOS to enable the "macro" command!
*****

CORE-GAD-I#vlan database
CORE-GAD-I(vlan)#vlan 2 name SERVIDORES
VLAN 2 modified:
  Name: SERVIDORES
-----

```

Figura F-19. Configuración de VLAN's

Fuente: Captura propia extraída de software GNS3

Ya asignadas las VLAN's, para que se propaguen por el resto de la red, se debe habilitar vtp server, lo que resulta eficiente para reducir la configuración de la misma VLAN en todos los switches de la red. Para ello se utilizan los siguientes comandos:

```
CORE-GAD-I(vlan)# vtp server
```

```
CORE-GAD-I(vlan)# vtp domain <nombre de dominio>
```

```
CORE-GAD-I(vlan)# vtp password <asignar una contraseña>
```

```

CORE-GAD-I#vlan database
CORE-GAD-I(vlan)#vlan 2 name SERVIDORES
VLAN 2 modified:
  Name: SERVIDORES
CORE-GAD-I(vlan)#vtp server
Device mode already VTP SERVER.
CORE-GAD-I(vlan)#vtp domain gad-i.gob.ec
Domain name already set to gad-i.gob.ec .
CORE-GAD-I(vlan)#vtp password ibarra
Password already set to ibarra.
CORE-GAD-I(vlan)#

```

Figura F-20. Configuración de VTP Server

Fuente: Captura propia extraída de software GNS3

Para verificar que se han configurado las VLANS se ejecuta el comando show vlan-switch.

```

ESW1
CORE-GAD-I#
CORE-GAD-I#show vlan-s
CORE-GAD-I#show vlan-switch

```

VLAN	Name	Status	Ports
1	default	active	Fa1/0, Fa1/1, Fa1/2, Fa1/3 Fa1/4, Fa1/5, Fa1/6, Fa1/7 Fa1/8, Fa1/9, Fa1/10, Fa1/11 Fa1/12, Fa1/13, Fa1/14, Fa1/15
2	SERVIDORES	active	
3	ADMIN_EQUIPOS	active	
4	DIRECCION_INFORMATICA	active	
5	ALCALDIA	active	
6	AUDITORIA_INTERNA	active	
7	PROCURADURIA	active	
8	PLANIFICACION	active	
9	COMUNICACION	active	
10	SECRETARIA_GENERAL	active	
11	FINANZAS	active	
15	RECURSOS_HUMANOS	active	
18	AVALUOS	active	
20	ADMINISTRACION	active	
21	OBRAS_PUBLICAS	active	

Figura F-21. Visualización de VLAN's creadas

Fuente: Captura propia extraída de software GNS3

Ahora se ejecutan los comandos para que se pueda trabajar en los dos protocolos:

CORE-GAD-I# configure terminal

CORE-GAD-I(config)# interface vlan <número de la vlan>

CORE-GAD-I(config-if)# ip address <direccion IP> < mascara de subred>

CORE-GAD-I(config-if)# ipv6 address <direccion IPv6>/<prefijo>

CORE-GAD-I(config-if)# ipv6 enable

CORE-GAD-I(config-if)# no shutdown

```

ESW1
33  enet  100033  1500  -  -  -  -  -  0  0
34  enet  100034  1500  -  -  -  -  -  0  0
35  enet  100035  1500  -  -  -  -  -  0  0
36  enet  100036  1500  -  -  -  -  -  0  0
37  enet  100037  1500  -  -  -  -  -  0  0
38  enet  100038  1500  -  -  -  -  -  0  0
39  enet  100039  1500  -  -  -  -  -  0  0
40  enet  100040  1500  -  -  -  -  -  0  0
1002 fddi  101002  1500  -  -  -  -  -  1  1003
1003 tr   101003  1500  1005  0  -  -  srb  1  1002
1004 fdnet 101004  1500  -  -  1  -  ibm  -  0  0
1005 trnet 101005  1500  -  -  1  -  ibm  -  0  0
CORE-GAD-I#
CORE-GAD-I#
CORE-GAD-I#
CORE-GAD-I#
CORE-GAD-I#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CORE-GAD-I(config)#int vlan 2
CORE-GAD-I(config-if)#ip add 172.16.8.1 255.255.255.0
CORE-GAD-I(config-if)#ipv6 add 2800:0db8:20:8::1/64
CORE-GAD-I(config-if)#ipv6 enable
CORE-GAD-I(config-if)#no shut
CORE-GAD-I(config-if)#

```

Figura F-22. Configuración de Ip's de VLAN's

Fuente: Captura propia extraída de software GNS3

Se debe habilitar IPv6 en todos los switches de la red

```

CORE-GAD-I (config-if)#exit
CORE-GAD-I (config)#ipv6 unicast
CORE-GAD-I (config)#ipv6 unicast-routing
CORE-GAD-I (config)#

```

Figura F-23. *Habilitación de Ruteo en IPv6*

Fuente: Captura propia extraída de software GNS3

Para colocar en modo acceso al puerto o interfaz de la VLAN se deben escribir los siguientes comandos.

```

CORE-GAD-I #configure terminal
CORE-GAD-I (config)# interface fastEthernet 1/0
CORE-GAD-I (config-if)# switchport mode access
CORE-GAD-I (config-if)# switchport access vlan 2
CORE-GAD-I (config-if)# no shutdown

```

```
CORE-GAD-I(config)#ipv6 unicast
CORE-GAD-I(config)#ipv6 unicast-routing
CORE-GAD-I(config)#int fa1/0
CORE-GAD-I(config-if)#sw
CORE-GAD-I(config-if)#switchport mo
CORE-GAD-I(config-if)#switchport mode a
CORE-GAD-I(config-if)#switchport mode access
CORE-GAD-I(config-if)#s
CORE-GAD-I(config-if)#sw
CORE-GAD-I(config-if)#switchport acc
CORE-GAD-I(config-if)#switchport access vlan 2
CORE-GAD-I(config-if)#no shut
CORE-GAD-I(config-if)#
```

Figura F-24. *Configuración de VLAN's modo acceso*

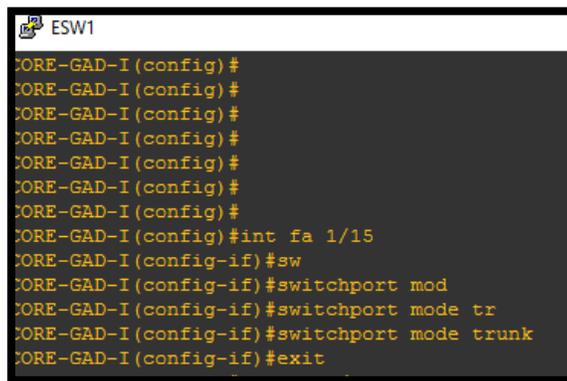
Fuente: Captura propia extraída de software GNS3

Nota: Verificar cuales de las interfaces permiten que se asignen VLANs.

Para que cualquier dispositivo de la red que esté conectado en otro switch, pueda comunicarse donde se hayan configurado las VLANs, debe configurarse el Trunk, que es un enlace entre dos switches que permite la afluencia de tráfico entre ellos.

El Trunk debe ser configurado en los dos extremos del enlace, en este caso, en los Switchs que están conectados directamente al CORE mediante los comandos,

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



```
ESW1
CORE-GAD-I (config) #
CORE-GAD-I (config) #int fa 1/15
CORE-GAD-I (config-if) #sw
CORE-GAD-I (config-if) #switchport mod
CORE-GAD-I (config-if) #switchport mode tr
CORE-GAD-I (config-if) #switchport mode trunk
CORE-GAD-I (config-if) #exit
```

Figura F-25. Configuración de interfaces modo troncal

Fuente: Captura propia extraída de software GNS3

Switch CISCO Catalyst 2960

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

En la topología de red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, se encuentra segmentada de acuerdo a la función de cada grupo de trabajo, es decir, la VLAN de Alcaldía sólo tendrá dispositivos asociados con la Alcaldía, en tanto que, en el departamento de Cultura la VLAN sólo tendrá dispositivos relacionados con Cultura. Con la habilitación de ruteo, los dispositivos de cada VLAN pueden comunicarse entre sí, a pesar de no encontrarse en el mismo dominio de colisión.

De acuerdo a esta explicación, para que las VLANS que se han configurado en el CORE se propaguen, se debe habilitar en cada uno de los Switches de la red como clientes VTP y el puerto en modo troncal para recibir las actualizaciones de cada una de las VLANS.

```
SW1(vlan)#vtp clien
Device mode already VTP CLIENT.
SW1(vlan)#vtp do
SW1(vlan)#vtp domain gad-i.gob.ec
Domain name already set to gad-i.gob.ec .
SW1(vlan)#vtp pas
SW1(vlan)#vtp password ibarra
Password already set to ibarra.
SW1(vlan)#
```

Figura F-26. Configuración VTP modo cliente

Fuente: Captura propia extraída de software GNS3

Como anteriormente, se ha configurado de modo trunk la interfaz que une al CORE con el Switch, de la misma manera se configura la interfaz del Switch que une al CORE, para que tengan comunicación. Esto se realizará para todos los switches que deseen conectarse al CORE, es decir que se tendrá que realizar el mismo procedimiento.

```
SW1(config)#int fa0/0
SW1(config-if)#sw
SW1(config-if)#switchport mo
SW1(config-if)#switchport mode tr
SW1(config-if)#switchport mode trunk
SW1(config-if)#
```

Figura F-27. Configuración de interfaces modo troncal

Fuente: Captura propia extraída de software GNS3

Ahora se verifica si las VLANS se han propagado, con el comando #show vlan-switch, en este caso para la simulación, para el caso de equipos reales solo con el comando #show vlan

```

SW1
SW1#show vl
SW1#show vlan-sw
SW1#show vlan-switch

VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15
2    SERVIDORES             active
3    ADMIN EQUIPOS          active
4    DIRECCION_INFORMATICA  active
5    ALCALDIA               active
6    AUDITORIA_INTERNA      active
7    PROCURADURIA           active
8    PLANIFICACION          active
9    COMUNICACION           active
10   SECRETARIA_GENERAL      active
11   FINANZAS               active
15   RECURSOS_HUMANOS       active
18   AVALUOS                active
20   ADMINISTRACION         active
21   OBRAS_PUBLICAS         active

```

Figura F-28. Verificación de propagación de VLAN's

Fuente: Captura propia extraída de software GNS3

Ahora, para poder habilitar un puerto del Switch en modo acceso para dar conectividad a la VLAN que se requiere, se debe colocar los siguientes comandos, los cuales se muestran en la siguiente Figura

```

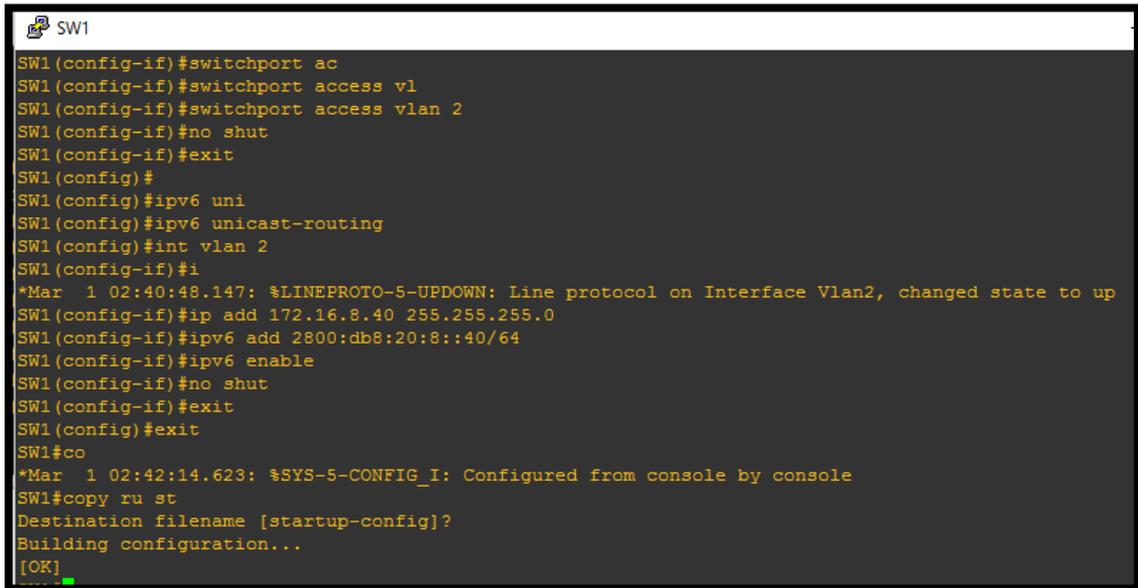
SW1(config)#int fa0/1
SW1(config-if)#sw
SW1(config-if)#switchport mo
SW1(config-if)#switchport mode a
SW1(config-if)#switchport mode access
SW1(config-if)#s
SW1(config-if)#sw
SW1(config-if)#switchport ac
SW1(config-if)#switchport access vl
SW1(config-if)#switchport access vlan 2
SW1(config-if)#no shut
SW1(config-if)#

```

Figura F-29. Configuración de VLAN modo acceso

Fuente: Captura propia extraída de software GNS3

En los Switches se coloca el comando `ipv6 unicast-routing`, para la habilitación del reenvío de paquetes IPv6. Y de la misma manera se añaden las direcciones IPv4 e IPv6 como se indica en la Figura, esto es para poder administrar los switches.



```
SW1
SW1(config-if)#switchport ac
SW1(config-if)#switchport access vl
SW1(config-if)#switchport access vlan 2
SW1(config-if)#no shut
SW1(config-if)#exit
SW1(config)#
SW1(config)#ipv6 uni
SW1(config)#ipv6 unicast-routing
SW1(config)#int vlan 2
SW1(config-if)#i
*Mar  1 02:40:48.147: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up
SW1(config-if)#ip add 172.16.8.40 255.255.255.0
SW1(config-if)#ipv6 add 2800:db8:20:8::40/64
SW1(config-if)#ipv6 enable
SW1(config-if)#no shut
SW1(config-if)#exit
SW1(config)#exit
SW1#co
*Mar  1 02:42:14.623: %SYS-5-CONFIG_I: Configured from console by console
SW1#copy ru st
Destination filename [startup-config]?
Building configuration...
[OK]
-----
```

Figura F-30. *Configuración de IP's a las VLAN's*

Fuente: Captura propia extraída de software GNS3

La misma configuración para otro Switch de la red

```

SW2
SW2 (config)#int fa0/1
SW2 (config-if)#swi
SW2 (config-if)#switchport mo
SW2 (config-if)#switchport mode c
SW2 (config-if)#switchport mode ac
SW2 (config-if)#switchport mode access
SW2 (config-if)#sw
SW2 (config-if)#switchport ac
SW2 (config-if)#switchport access vl
SW2 (config-if)#switchport access vlan 2
SW2 (config-if)#no shut
SW2 (config-if)#
SW2 (config-if)#exit
SW2 (config)#ipv6 uni
SW2 (config)#ipv6 unicast-routing
SW2 (config)#int vlan 2
SW2 (config-if)#ip a
*Mar 1 02:47:49.179: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up
SW2 (config-if)#ip add 172.16.8.50 255.255.255.0
SW2 (config-if)#ipv6 add 2800:db8:20:8::50/64
SW2 (config-if)#ipv6 en
SW2 (config-if)#ipv6 enable
SW2 (config-if)#no shut
SW2 (config-if)#

```

Figura F-31. Configuración de IP's a las VLAN's

Fuente: Captura propia extraída de software GNS3

Ahora se utiliza el comando ping para determinar si existe conectividad entre las VLANs, para ello se digita:

```
SW1#ping 172.16.8.50
```

```
SW1#ping ipv6 2800:db8:20:8::50
```

```

SW1
*Mar 1 02:42:14.623: %SYS-5-CONFIG_I: Configured from console by console
SW1#copy ru st
Destination filename [startup-config]?
Building configuration...
[OK]
SW1#ping 172.16.8.50

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.8.50, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 56/158/272 ms
SW1#ping 172.16.8.50

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.8.50, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/138/260 ms
SW1#ping ipv6 2800:db8:20:8::50

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:DB8:20:8::50, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/31/56 ms
SW1#

```

Figura F-32. Verificación de conectividad

Fuente: Captura propia extraída de software GNS3

ANEXO E: Instalación del Firewall Checkpoint en VMWare

La creación sobre este firewall Gaia R77 se realizó sobre esta imagen .iso debido a que se puede asemejar a las características de funcionamiento del Ccheckpoint 4610 que se tiene en el Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra.

Luego de la creación de los parámetros de la máquina virtual del checkpoint, iniciamos la máquina para su correspondiente instalación.

1. Al prender la máquina la pantalla de inicio es la siguiente y seleccionamos la primera opción de instalar el Gaia en el sistema y se presiona enter.

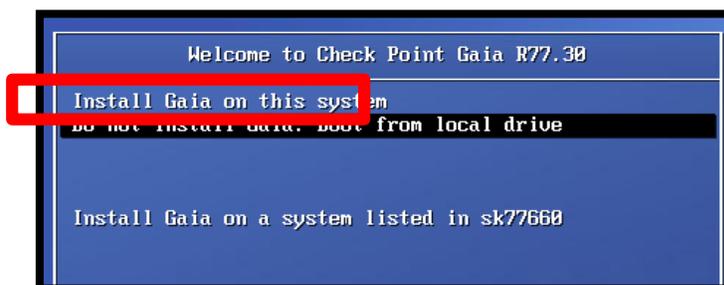


Figura G- 1. *Instalación del Firewall Gaia*

Fuente: Captura extraída de Firewall Checkpoint GAIA R77

2. Se coloca Ok para proceder con la instalación

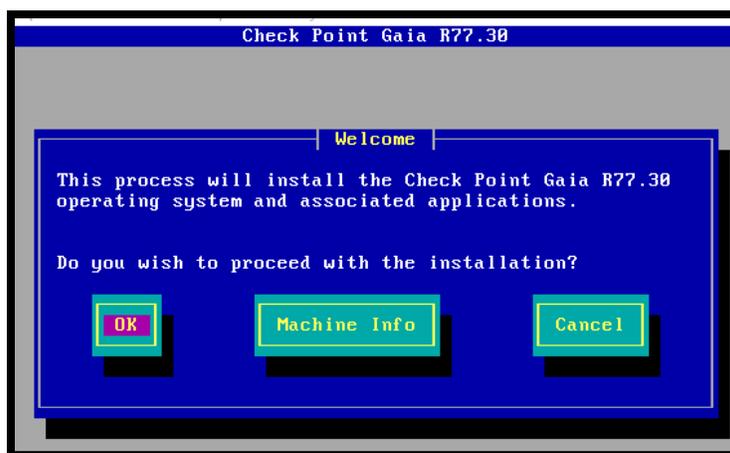


Figura G- 2. Pantalla de Bienvenida de instalación Checkpoint

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

3. Se configure la IP en versión cuatro y se la coloca la necesaria para poder trabajar en ella.
El gateway se lo deja vacío para posteriores configuraciones.

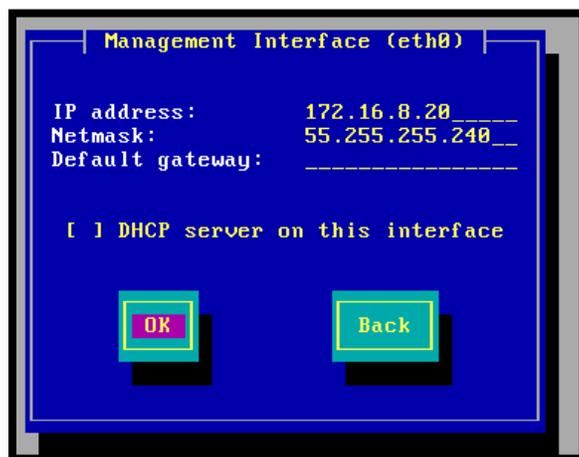


Figura G - 3. Configuración de Interfaz de red

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

4. Se continua con el proceso de instalación

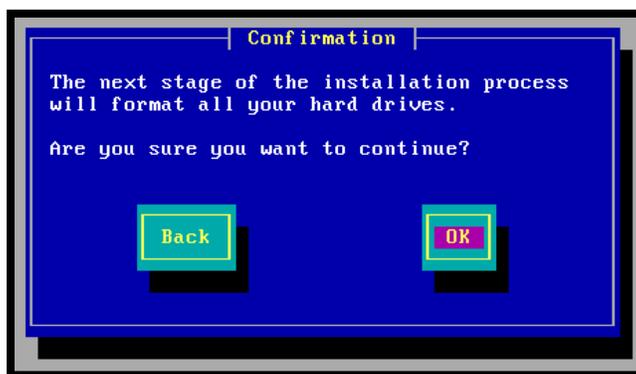


Figura G - 4. Confirmación de proceso de Instalación

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

5. Proceso de Instalación del sistema

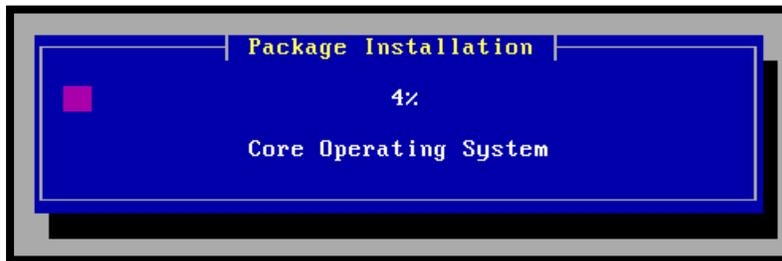


Figura G - 5. *Proceso de Instalación del Sistema*

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

6. Se tomará algún tiempo hasta que se instalen todos los paquetes.

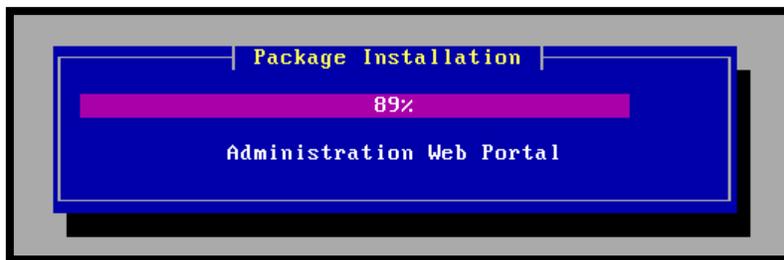


Figura G - 6. *Instalando todos los paquetes*

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

7. Al terminar el proceso de instalación se reinicia la máquina.

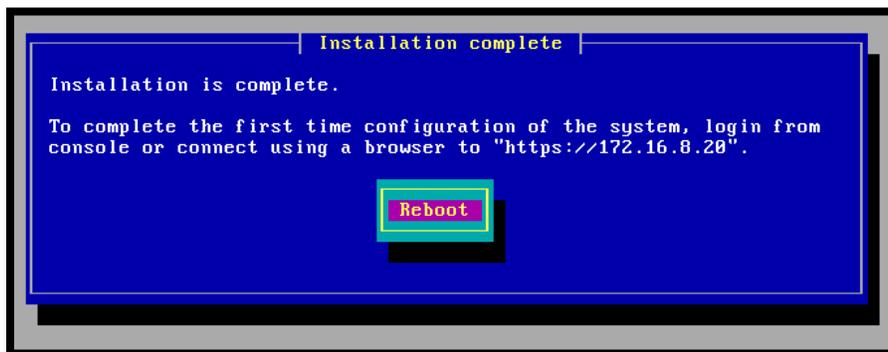


Figura G - 7. *Reinicio del Sistema*

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

8. Al reiniciar la máquina la pantalla de inicio será la siguiente, a continuación, se colocará la contraseña de Admin que se colocó al instalar el sistema operativo:

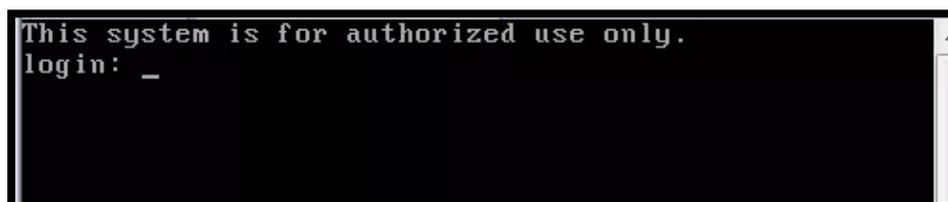


Figura G - 8. Inicio de Firewall Checkpoint

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

9. Ahora se apaga la máquina y se procede a configurar las interfaces de red. Para ello se va a la opción:

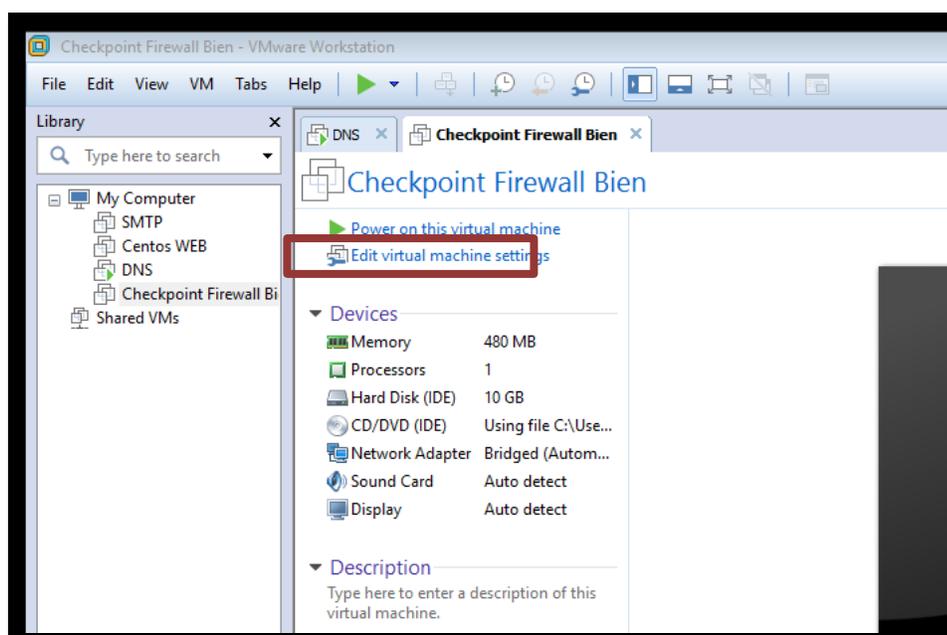


Figura G - 9. Editar las configuraciones de Checkpoint

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

10. Se configura el adaptador de red como puente para permitir una conexión directa y poder configurar el firewall desde la red, para ello vamos a tomar en cuenta la topología

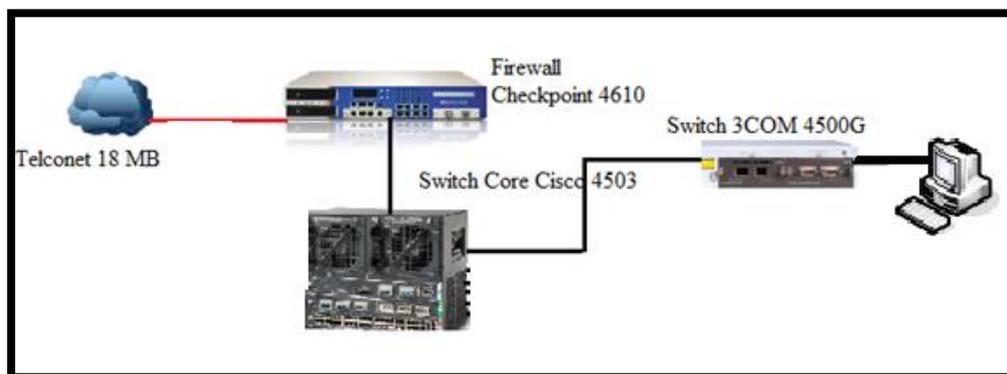


Figura G - 10. Determinar interfaces en la topología de red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra

Fuente: Captura propia extraída de software Paint Windows-10

11. Por lo tanto, se configurará una interfaz, por el momento, para la red local como se indica en la Figura

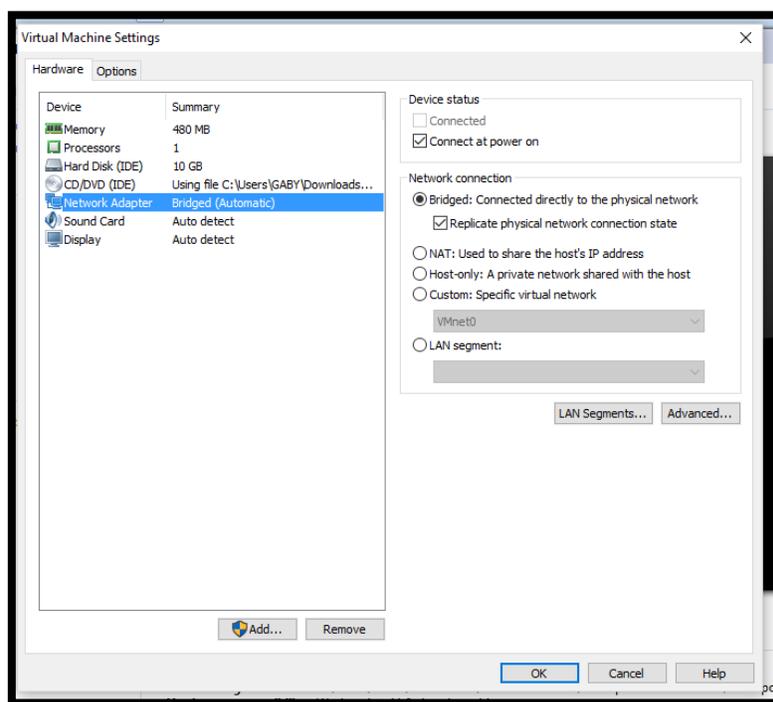


Figura G - 11. Configuración del adaptador de red en Bridge

Fuente: Captura propia extraída de software VMWare

12. Ahora se van a configurar las propiedades de la tarjeta y para ello se dirige a:

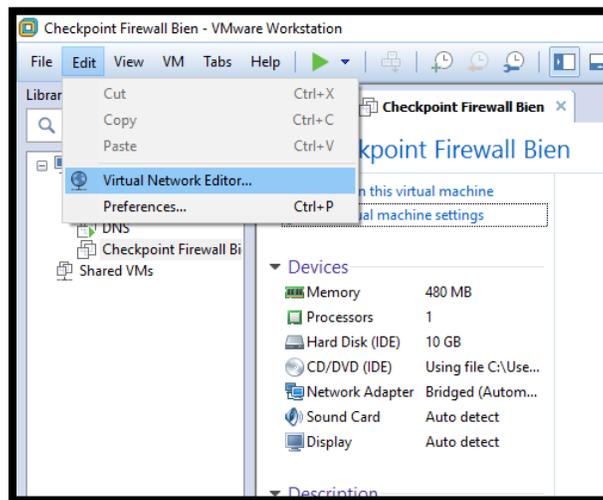


Figura G - 12. Edición de preferencias de la red

Fuente: Captura propia extraída de software VMWare

13. Y en la opción puente, escogemos una interfaz que permita la configuración hacia la red interna y aceptar

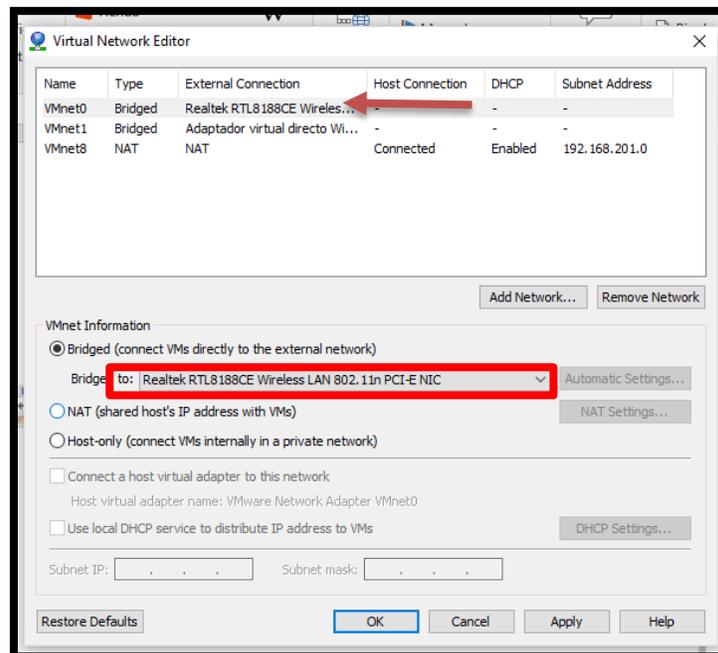


Figura G - 13. Elección de interfaz de red

Fuente: Captura propia extraída de software VMWare

14. Ahora se configura la tarjeta de red de la máquina para proceder a la configuración del firewall, que debe estar dentro de la misma red que se configuro el firewall

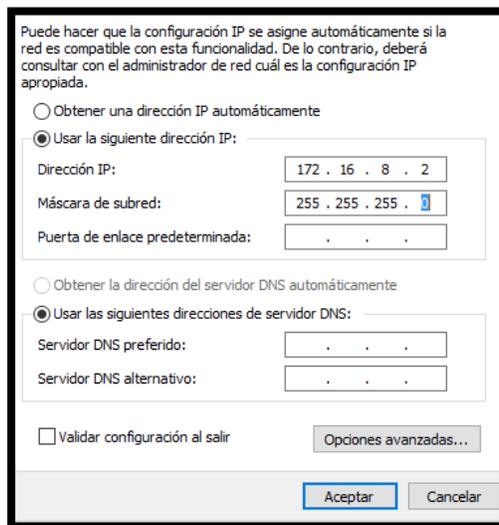


Figura G - 14. Configuración de tarjeta de red en un cliente Windows 10

Fuente: Captura propia extraída de sistema operativo windows 10

- Configuración del Firewall Checkpoint

La instalación del Checkpoint, se encuentra en el anexo F. Ahora se procederá a la configuración más importante como es la red IPv4/IPv6.

1. Con la Ip del firewall, que en este caso es la 172.16.8.3 se coloca en el navegador de la computadora conectada directamente

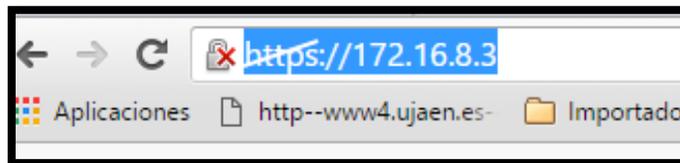


Figura G - 15. Configuración del Checkpoint modo gráfico

Fuente: Captura propia extraída de sistema operativo Windows 10

2. Ahora, se tendrá la página mostrada en la Figura y se coloca detalles avanzados y aparecerá una opción que dirá continuar a 172.16.8.3 y se la selecciona

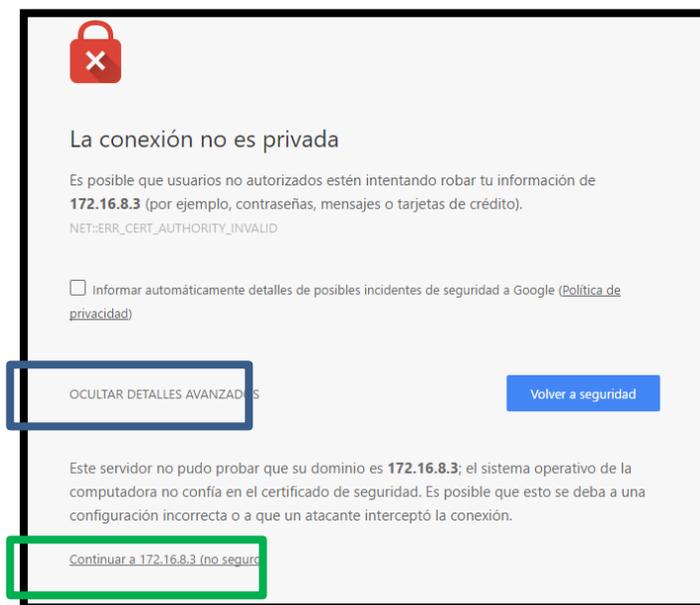


Figura G - 16. Acceso a conexión no privada

Fuente: Captura propia extraída de sistema operativo Windows 10

- Ahora se muestra la ventana de inicio del Gaia R77.30 colocamos el usuario y la clave, antes de ello verificar que el firewall checkpoint, esté encendido



Figura G - 17. Acceso a Gaia

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

4. Esta es la pantalla de Bienvenida que permitirá configurar al Firewall y se coloca next



Figura G - 18. *Conexión de VMware con Checkpoint*

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

5. Continuar con la instalación del Checkpoint

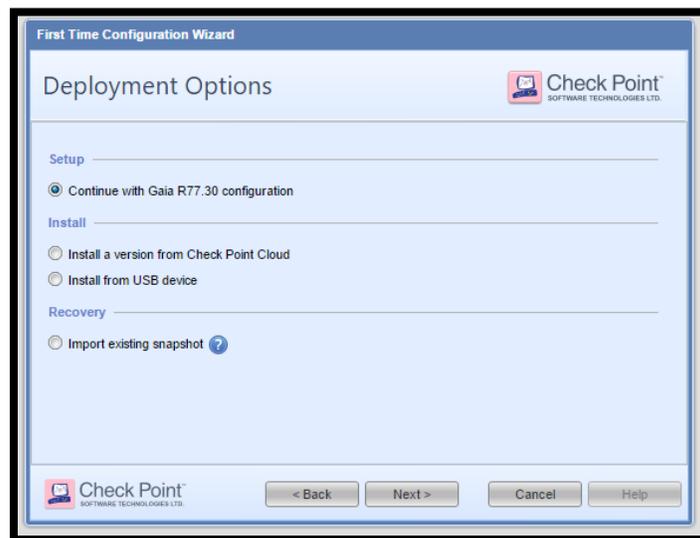
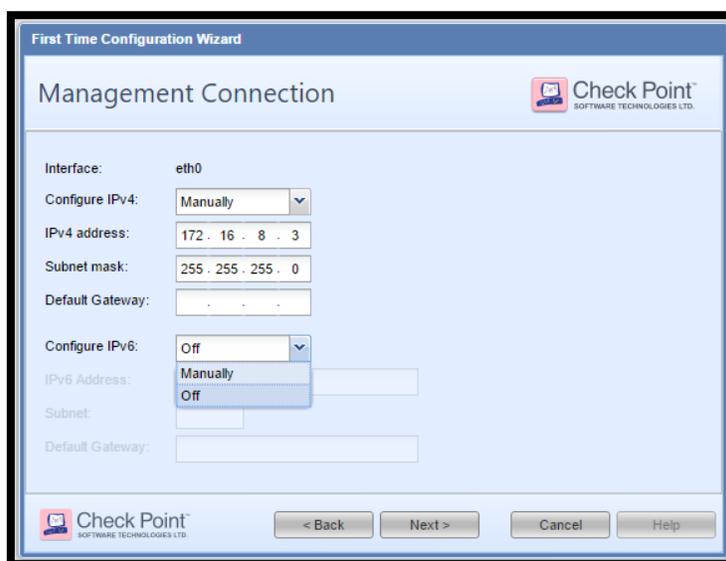


Figura G - 19. *Instalación de Checkpoint*

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

6. Se configura la red IPv4

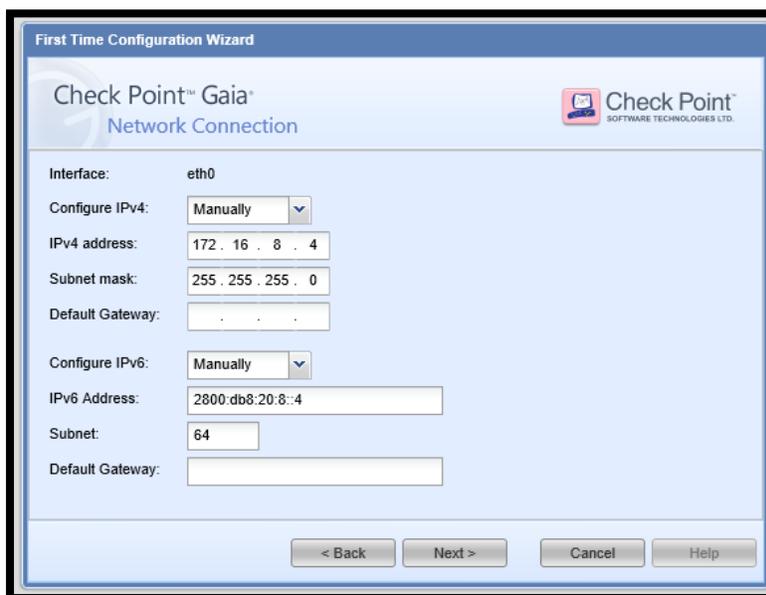


The screenshot shows the 'First Time Configuration Wizard' for 'Management Connection'. The interface is 'eth0'. The 'Configure IPv4' dropdown is set to 'Manually'. The IPv4 address is '172.16.8.3', the subnet mask is '255.255.255.0', and the default gateway is empty. The 'Configure IPv6' dropdown is set to 'Off', and its options are visible in a dropdown menu. The IPv6 address, subnet, and default gateway fields are empty. Navigation buttons at the bottom include '< Back', 'Next >', 'Cancel', and 'Help'.

Figura G - 20. Configuraciones de Red

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

7. Se configura la red IPv6

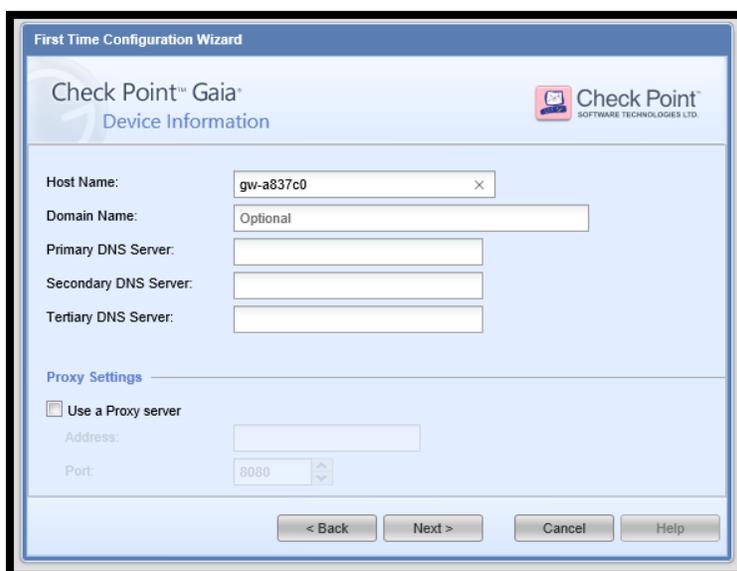


The screenshot shows the 'First Time Configuration Wizard' for 'Network Connection'. The interface is 'eth0'. The 'Configure IPv4' dropdown is set to 'Manually'. The IPv4 address is '172.16.8.4', the subnet mask is '255.255.255.0', and the default gateway is empty. The 'Configure IPv6' dropdown is set to 'Manually'. The IPv6 address is '2800:db8:20:8::4', the subnet is '64', and the default gateway is empty. Navigation buttons at the bottom include '< Back', 'Next >', 'Cancel', and 'Help'.

Figura G - 21. Configuraciones de Red

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

8. Configuraciones de DNS, se puede dejar en blanco o llenar el campo



First Time Configuration Wizard

Check Point™ Gaia®
Device Information

Host Name: gw-a837c0

Domain Name: Optional

Primary DNS Server:

Secondary DNS Server:

Tertiary DNS Server:

Proxy Settings

Use a Proxy server

Address:

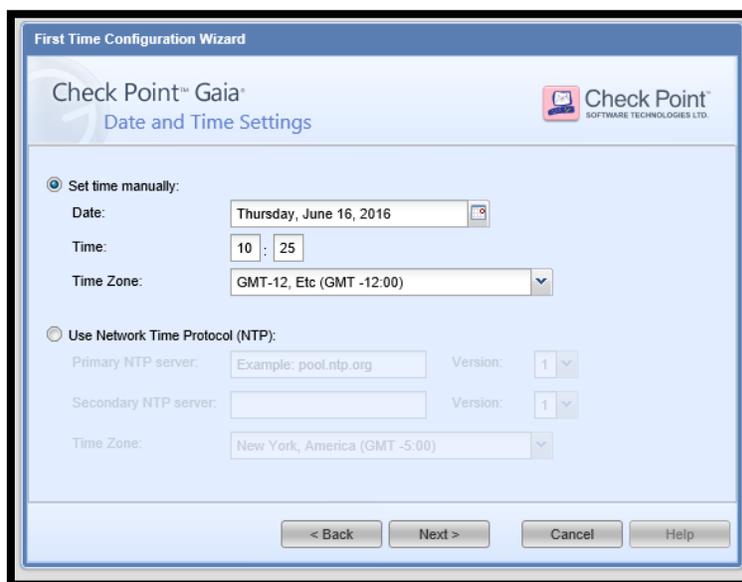
Port: 8080

< Back Next > Cancel Help

Figura G - 22. Configuración DNS

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

9. Se configura la fecha y la hora de acuerdo a las necesidades del usuario



First Time Configuration Wizard

Check Point™ Gaia®
Date and Time Settings

Set time manually:

Date: Thursday, June 16, 2016

Time: 10 : 25

Time Zone: GMT-12, Etc (GMT -12:00)

Use Network Time Protocol (NTP):

Primary NTP server: Example: pool.ntp.org Version: 1

Secondary NTP server: Version: 1

Time Zone: New York, America (GMT -5:00)

< Back Next > Cancel Help

Figura G - 23. Configuraciones de fecha y hora

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

10. Se selecciona el tipo de servicio que prestará el Checkpoint, en este caso será de Seguridad

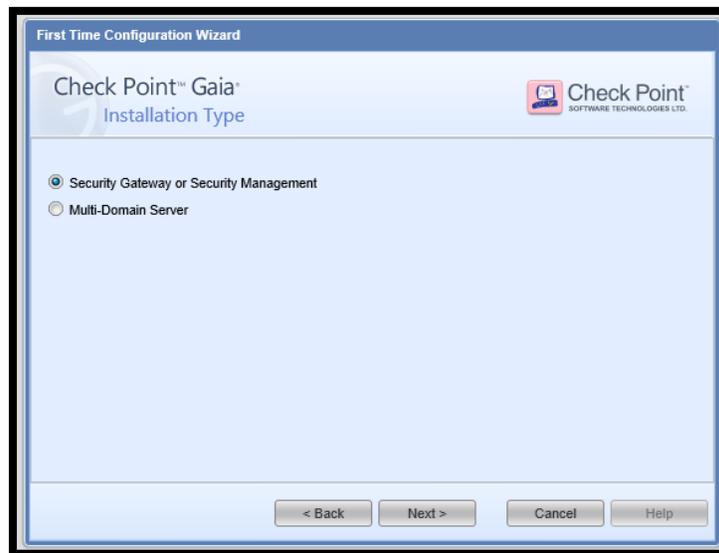


Figura G - 24. Selección tipo de servidor

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

11. Seleccionar las Características del servidor en este caso se eligen las marcadas en la Figura F-24.

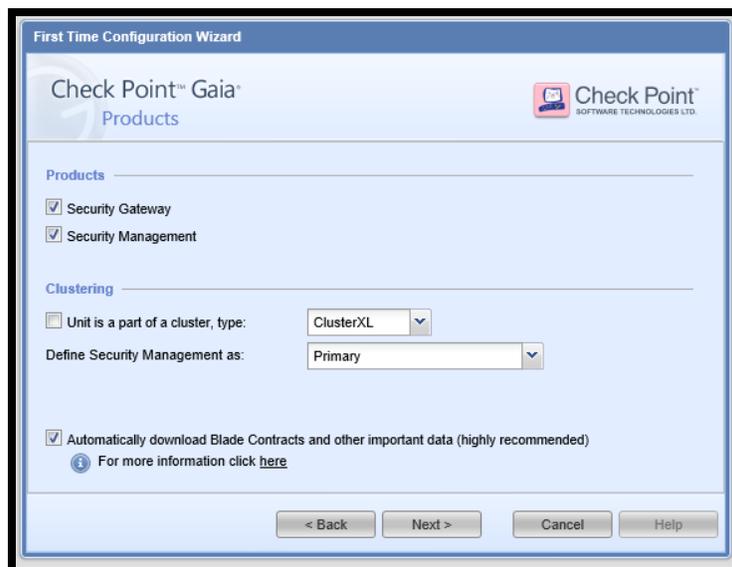
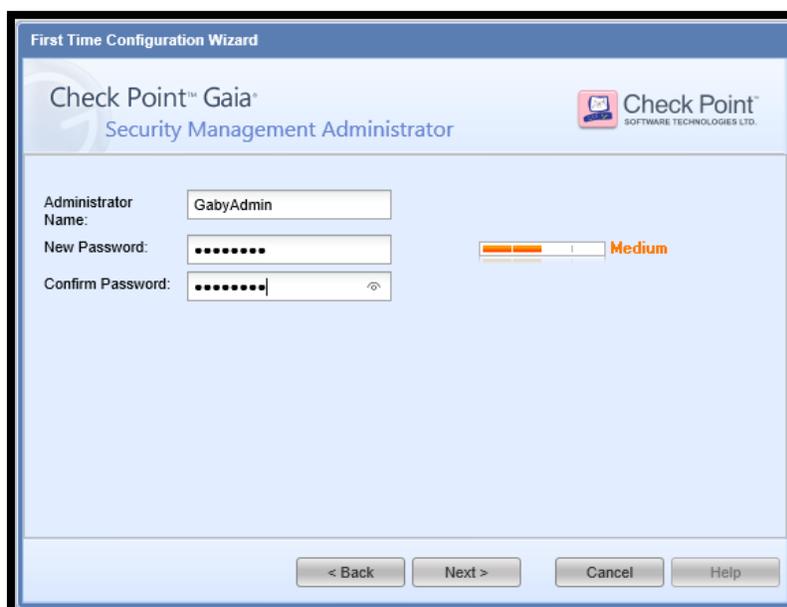


Figura G - 25. Características del servidor

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

12. Se colocan nombres con sus respectivas clases de acceso



First Time Configuration Wizard

Check Point™ Gaia®
Security Management Administrator

Administrator Name: GabbyAdmin

New Password: [Redacted]

Confirm Password: [Redacted]

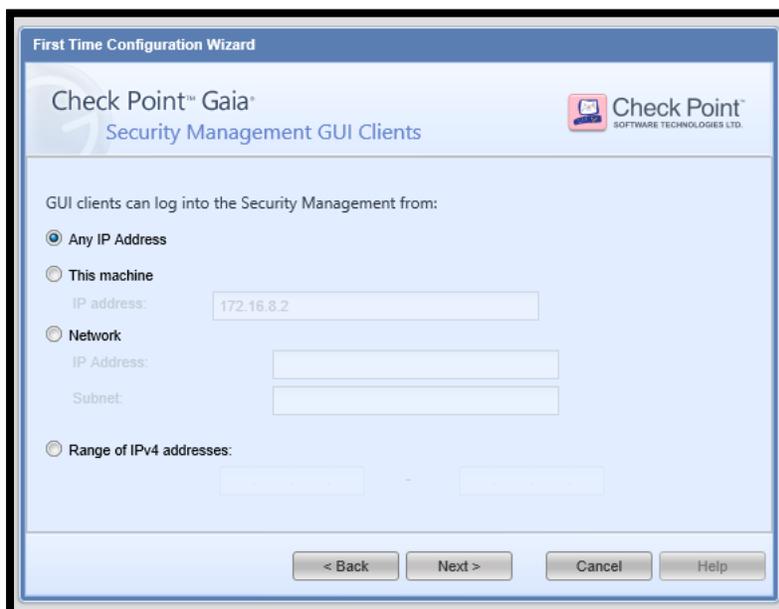
Medium

< Back Next > Cancel Help

Figura G - 26. Claves de acceso de administrador

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

13. Seleccionar cualquier ip para un cliente que quiera ingresar a este sistema



First Time Configuration Wizard

Check Point™ Gaia®
Security Management GUI Clients

GUI clients can log into the Security Management from:

Any IP Address

This machine
IP address: 172.16.8.2

Network
IP Address: [Redacted]
Subnet: [Redacted]

Range of IPv4 addresses:
[Redacted] - [Redacted]

< Back Next > Cancel Help

Figura G-27. Acceso a un cliente al servidor

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

14. Se completa con la instalación dando click el finalizar

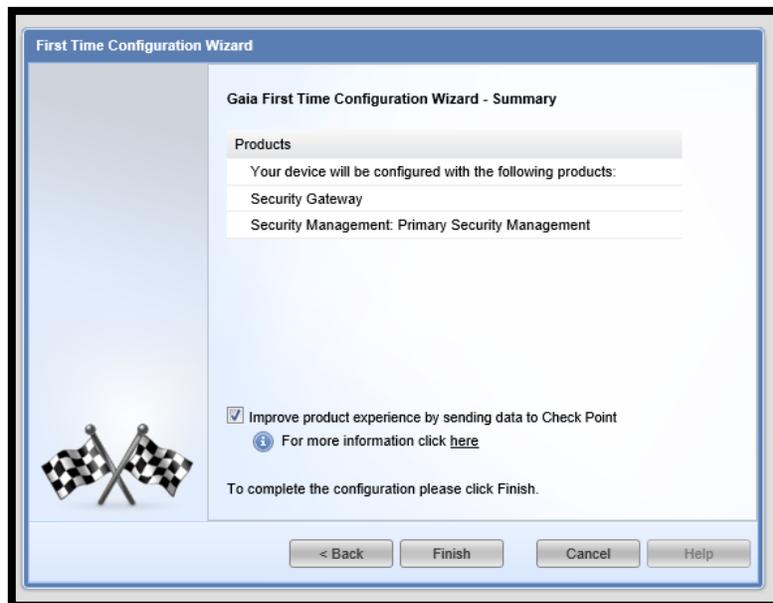


Figura G - 28. *Finalización de Instalación Checkpoint*

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

15. Esta pantalla va a permitir que se pueda configurar en modo gráfico el servidor

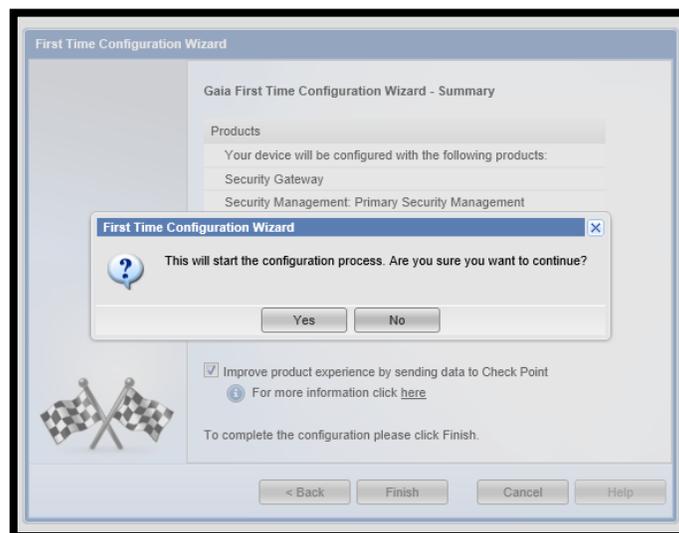


Figura G - 29. *Configurar gráficamente Checkpoint*

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

16. Comenzará el proceso de la instalación

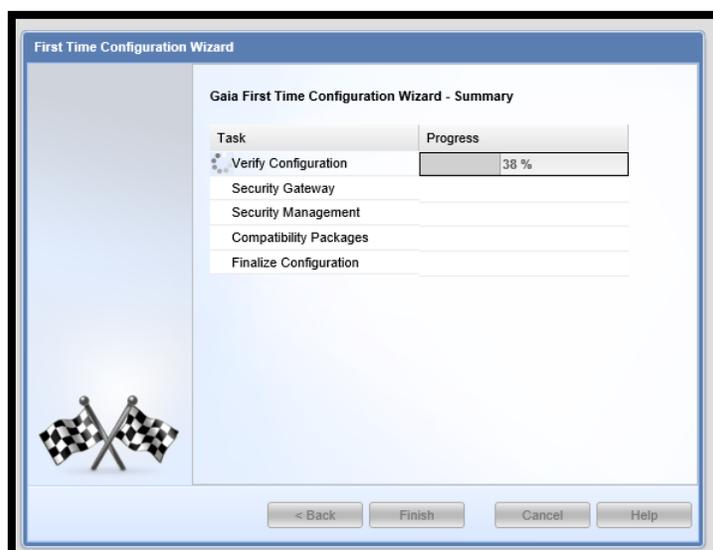


Figura G - 30. *Proceso de Instalación*

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

17. Se configurarán todos los complementos necesarios para la correcta funcionalidad.

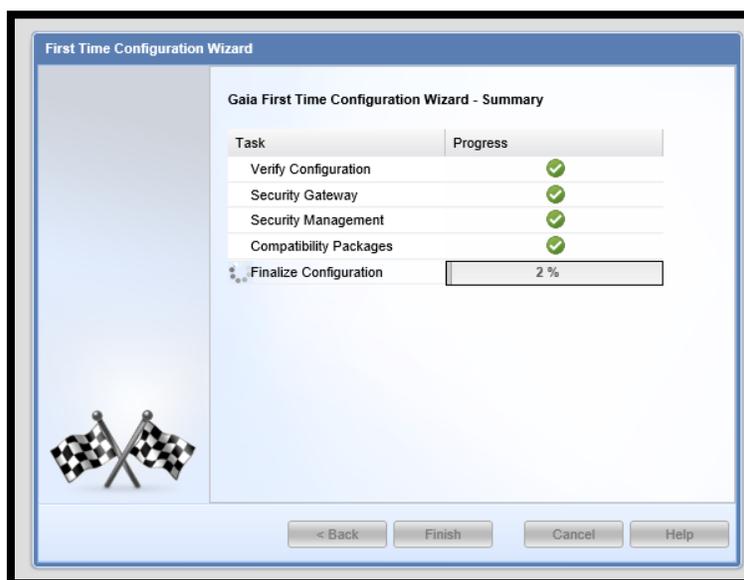


Figura G - 31. *Proceso de Instalación*

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

18. Una vez, terminado el proceso se reinicia el sistema

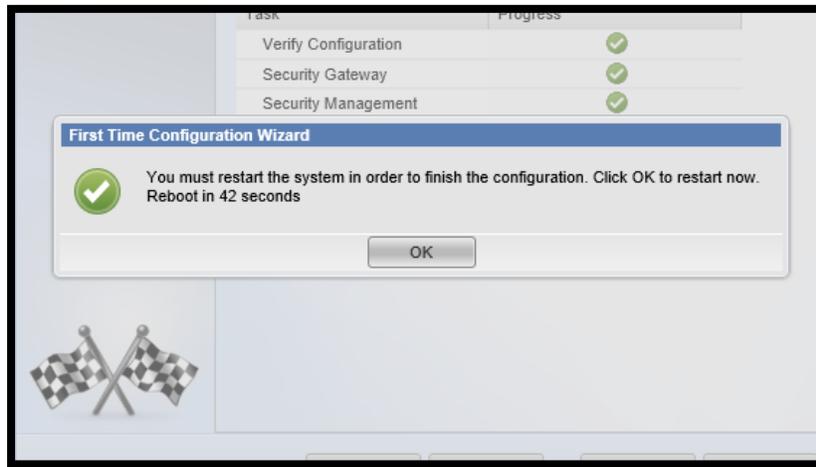


Figura G - 32. Reinicio de sistema

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

19. Y aparecerá este modo gráfico en el que es mucho más eficiente realizar cualquier configuración

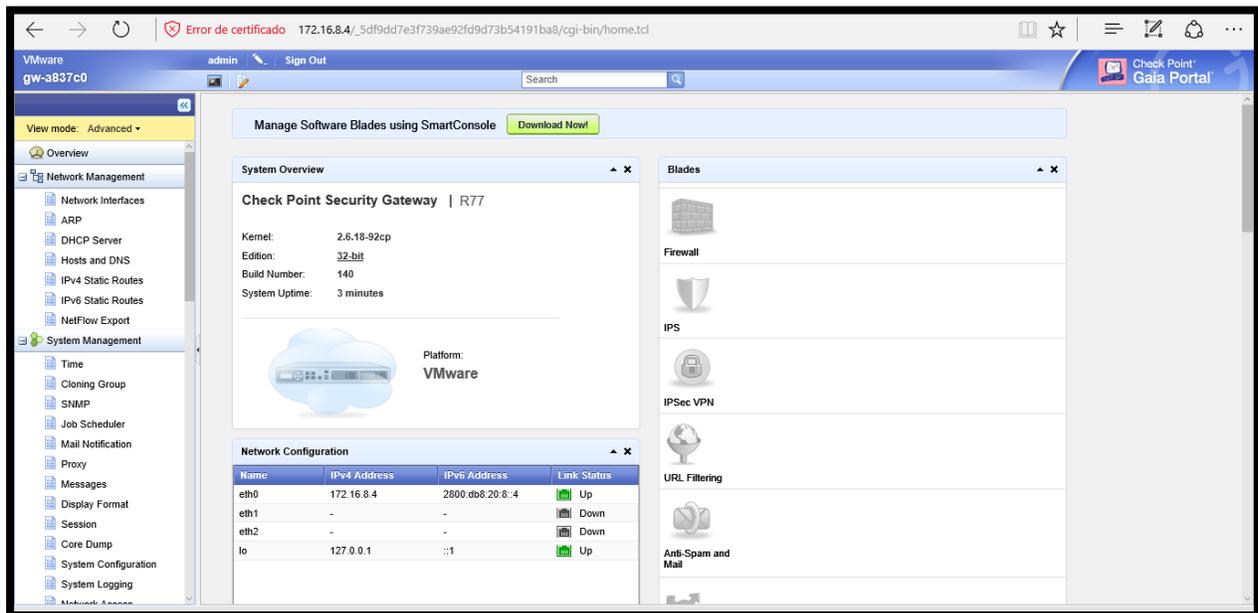


Figura G - 33. Modo gráfico de Firewall-Checkpoint

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

La configuración del Checkpoint consiste el control de tráfico que transita en la red y su correspondiente enrutamiento, es decir, se establecen las reglas de encaminamiento para la comunicación entre la red interna y la red externa.

El ingreso al firewall para la configuración se realiza por medio del software proporcionado por el mismo equipo, y se va a ingresar con la IP del equipo como se indica en la Figura 68.

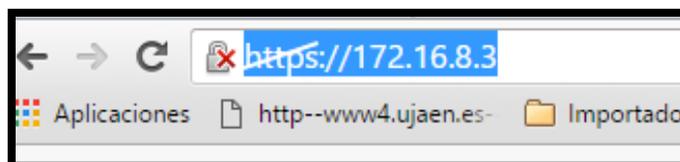


Figura G-34. *Ingreso a la interfaz de administración*

Fuente: Captura propia extraída de sistema operativo Linux, software Checkpoint.

En seguida, se solicita el usuario y contraseña para acceder a las configuraciones siguientes:

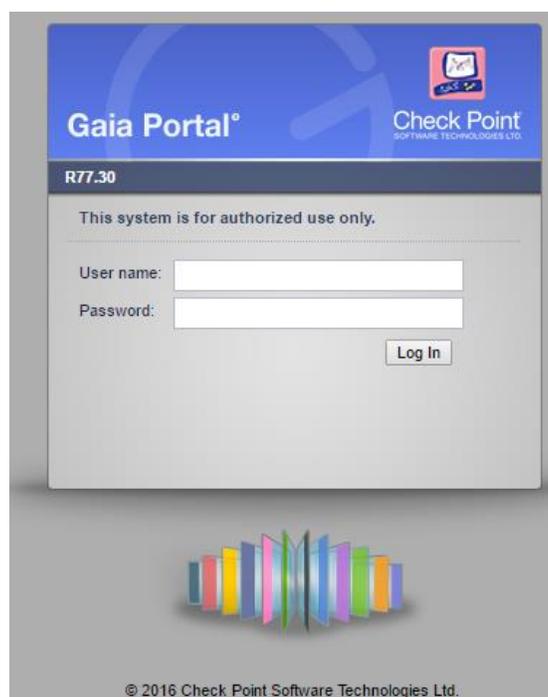


Figura G-35. *Ingreso a Firewall Checkpoint*

Fuente: Captura propia extraída de sistema operativo Linux, software Checkpoint.

1. Lo primero que se debe realizar es la configuración de las interfaces WAN y LAN, es decir eth1 y eth0 correspondientemente. El Firewall tiene la funcionalidad de implementar doble pila, por lo tanto, se pueden configurar las interfaces tanto en IPv4 como IPv6.

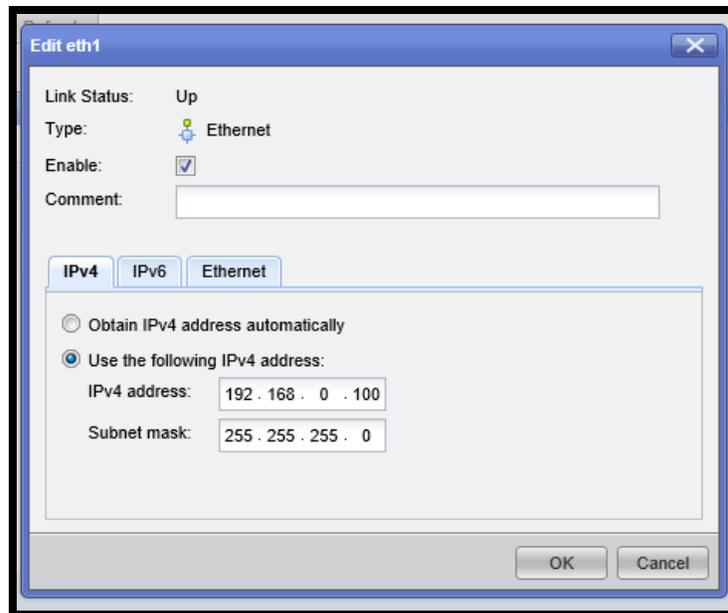
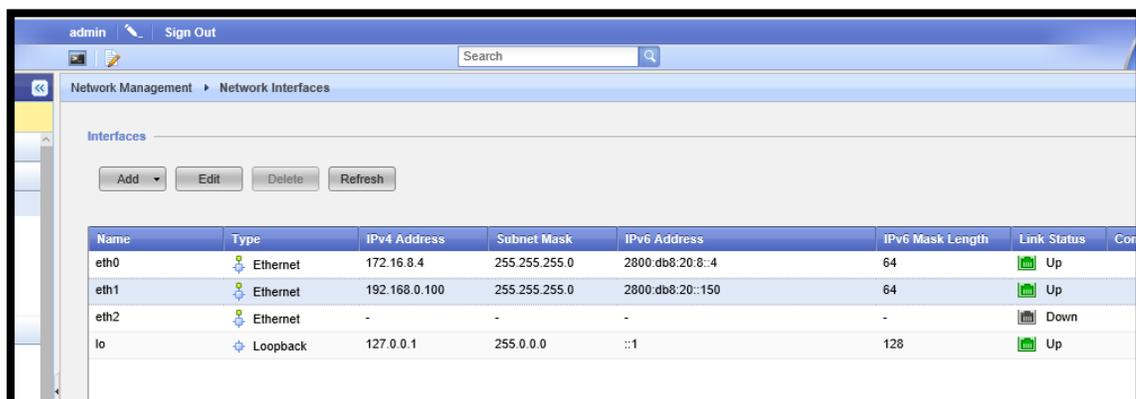


Figura G-36. *Configuración de Interfaces*

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

20. En la pestaña de interfaces, se puede observar el estado de cada una de ellas con las IP's asignadas



Name	Type	IPv4 Address	Subnet Mask	IPv6 Address	IPv6 Mask Length	Link Status	Color
eth0	Ethernet	172.16.8.4	255.255.255.0	2800:db8:20:8::4	64	Up	
eth1	Ethernet	192.168.0.100	255.255.255.0	2800:db8:20::150	64	Up	
eth2	Ethernet	-	-	-	-	Down	
lo	Loopback	127.0.0.1	255.0.0.0	::1	128	Up	

Figura G-37. Estado de Interfaces

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

21. Ahora se van a configurar las VLAN's en el Firewall para poder tener conectividad en la red con cada una de ellas.

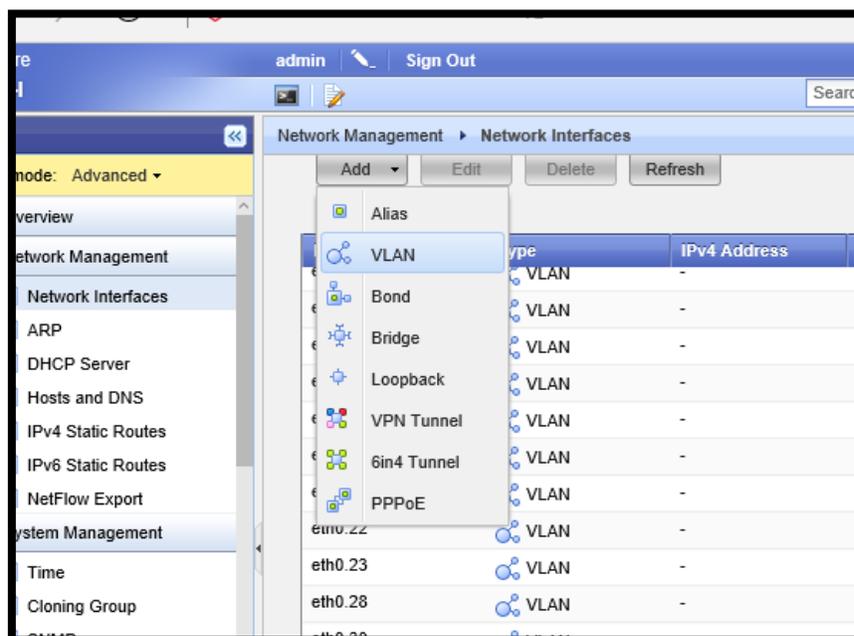


Figura G-38. Creación de Vlans

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

22. Se configura el nombre, y el ID de cada una de ellas.

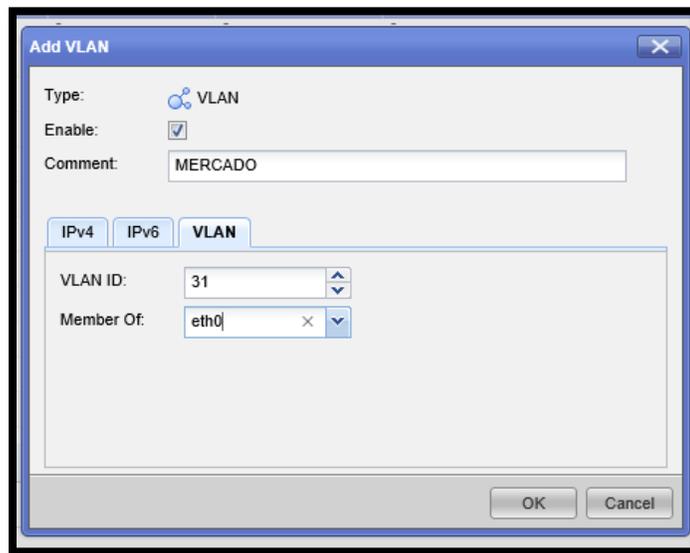


Figura G-39. Asignación de parámetros a Vlan

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

23. Asignación de IPv4 a la Vlan

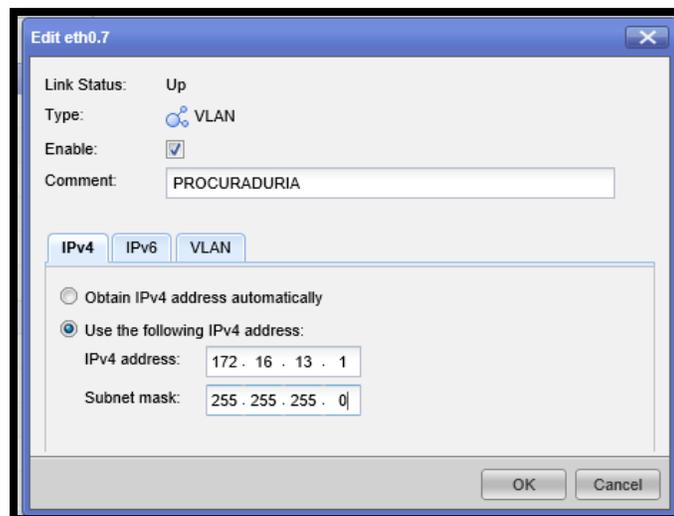


Figura G-40. IPv4 a la VLAN

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

24. Asignación de IPv6 a la Vlan

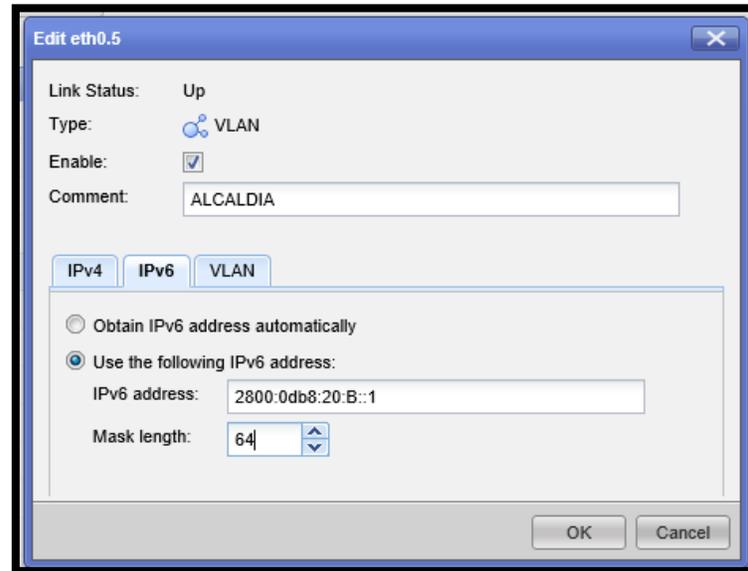


Figura G-41. IPv6 a la VLAN

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

25. Ahora se va a configurar el tipo de enrutamiento, en este caso rutas estáticas para poder llegar a los destinos correspondientes tanto en IPv4 como en IPv6.

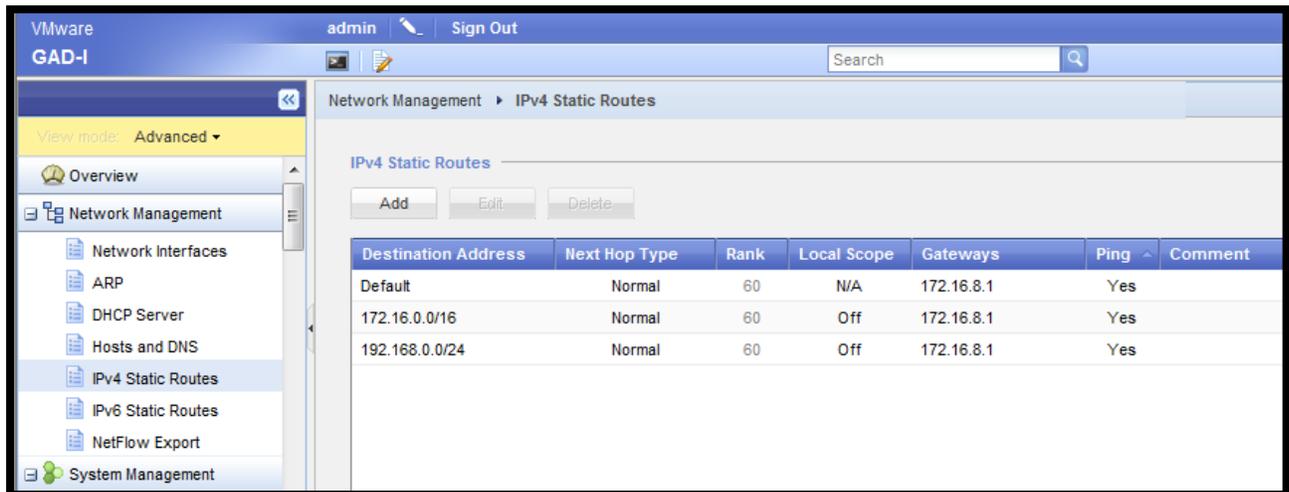


Figura G-42. Configuración de Rutas estáticas en IPv4

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

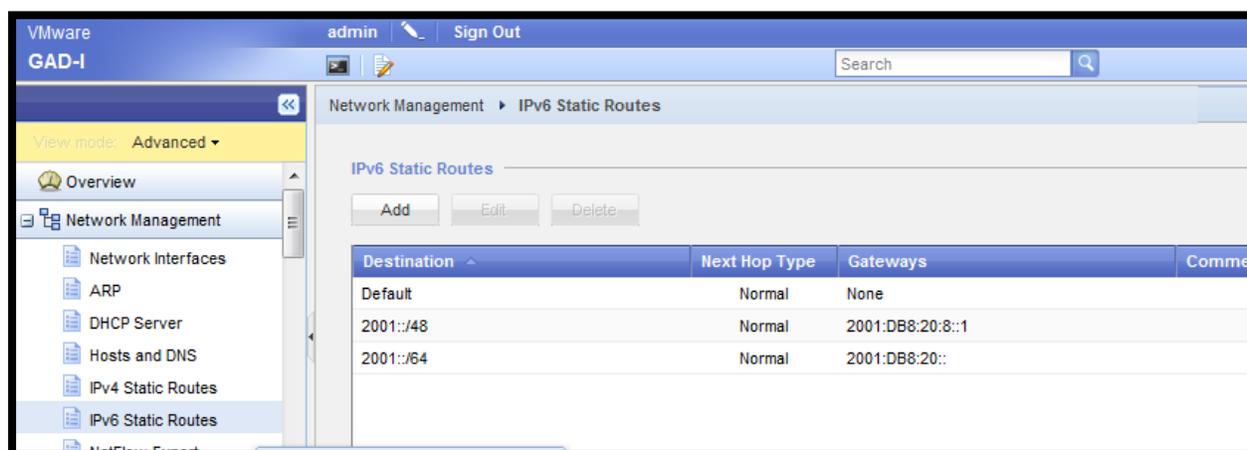


Figura G-43. Configuración de rutas estáticas en IPv6

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

26. De la misma forma se deben crear las políticas necesarias para permitir el tráfico de paquetes, en este caso se deben habilitar el tráfico IPv6. Para ello se debe dirigir a las políticas y agregar las necesarias. En este caso se debe habilitar el protocolo ICMPv6, HTTPv6 y SMTPv6.

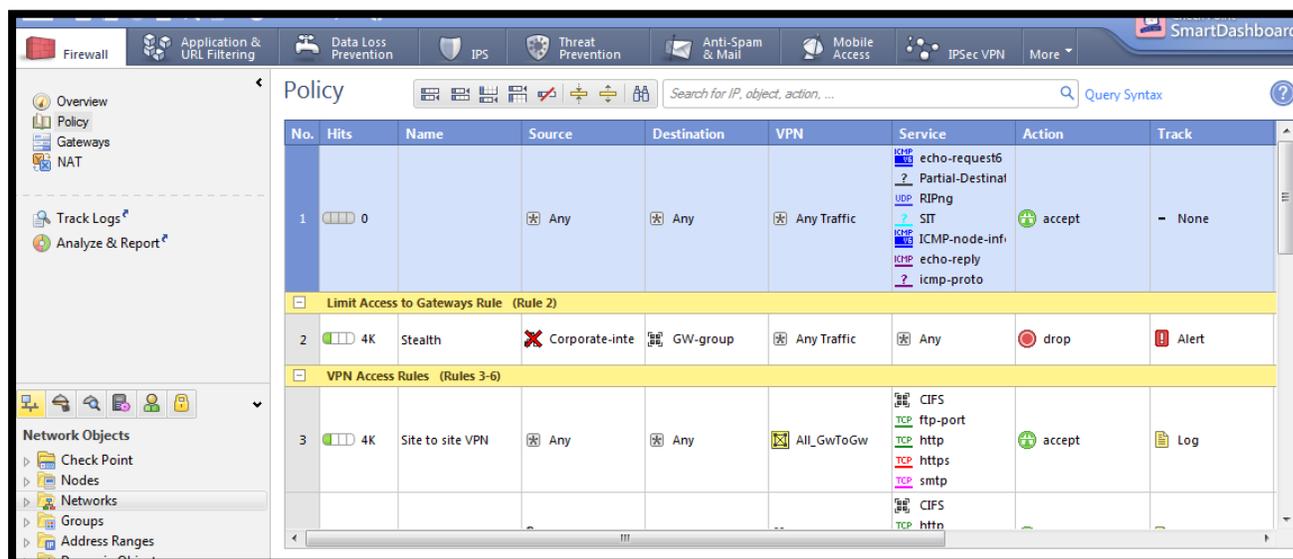


Figura G-44. Establecimiento de políticas o reglas de acceso o denegación

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

The screenshot displays the 'Policy' configuration page in the Checkpoint GAIA R77 interface. The left sidebar shows navigation options like Overview, Policy, Gateways, NAT, Track Logs, and Analyze & Report. The main area shows a table of rules under the heading 'Common Rules - All Sites (Rules 14-20)'. The table columns are No., Hits, Name, Source, Destination, VPN, Service, Action, and Track. The rules listed are:

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track
13	370K	Internet Access	Guests All_Domain_Us	inet_http_proxy	Any Traffic	TCP HTTP_and_HTTP	accept (display ca)	Log
Common Rules - All Sites (Rules 14-20)								
14	3M	Terminal server	Corporate-inte	Any	Any Traffic	Any	Session Auth	Log
15	218K	DNS server	Any	Corporate-dns	Any Traffic	UDP domain-udp	accept	None
16	76K	SOAP	Any	Corporate-WA	Any Traffic	http->SOAP-re	accept	Log
17	1M	Mail and Web servers	Any	Corporate-dmz	Any Traffic	TCP http TCP https TCP smtp	accept	Log
18	2M	SMTP	Corporate-mail	Internal-net-gr	Any Traffic	TCP smtp	accept	Log
19	9K	DMZ and Internet	Internal-net-gr	Any	Any Traffic	Any	accept	Log
20	682K	Clean up rule	Any	Any	Any Traffic	Any	drop	Log

Figura G-45. Reglas correspondientes a los servicios seleccionados

Fuente: Captura propia extraída de Firewall Checkpoint GAIA R77

ANEXO F: Precios de equipos

amazon.co.uk
Try Prime

Computers

Shop by Department
Your Amazon.co.uk Today's Deals Gift Cards Sell Help

Hello, Sign in
Your Account

Computers Best Sellers Deals Laptops Desktops Printers Tablets Tablet Accessories Monitors Computer Accessories Components Networking

Cisco Systems WS-C4503E-S7L+48V+
by Cisco
Be the first to review this item

Price: **£4,479.00**

Only 2 left in stock.

Estimated delivery 6 - 13 July to Ecuador when you choose Standard at checkout. Details

Dispatched from and sold by Cybertrading GmbH.

- WS-C4503E-S7L+48V+
- Cisco Systems
- 4503-E Chassis, One WS-X4648-RJ45V+E, Sup7L-E, LAN Base
- Cisco Catalyst 4500

See more product details

Roll over image to zoom in

Looking for Gaming Gear?
Check out our new PC Gaming store for the latest desktops, laptops, monitors, keyboards, mice, headsets and much more. [Learn more](#)

Figura G- 1. Precio del Switch CORE

Fuente: <https://www.amazon.co.uk/Cisco-WS-C4503E-S7L-48V-Systems/dp/B008S07WLO>

Check Point 4600 Appliance
Enterprise-grade security appliance (374 SPU/9Gbps)— fast networking and fiber and copper connectivity options

Check Point SOFTWARE TECHNOLOGIES LTD.

Check Point 4600 Series

Check Point 4600 Security Appliances

4600 Next Generation Firewall Appliance with 7 blades suite - Including Firewall, VPN, Advanced Networking & Clustering, Identity Awareness, Mobile Access for 5 concurrent users, IPS, and Application Control blades	#CPAP-SG4600-NGFW List Price: \$15,200.00 Our Price: \$12,236.00	<input type="button" value="Add to Cart"/>
4600 Next Generation Threat Prevention Appliance with 11 blades suite - Including Firewall, VPN, Advanced Networking & Clustering, Identity Awareness, Mobile Access for 5 concurrent users, IPS, Application Control blades, URL Filtering, Anti-Virus, Anti Bot and Anti-Spam blades	#CPAP-SG4600-NGTP List Price: \$18,500.00 Our Price: \$14,893.00	<input type="button" value="Add to Cart"/>

Figura G- 2. Precio Firewall Checkpoint

Fuente: <http://www.checkfirewalls.com/4600.asp>

mercado libre

Inscríbete Ingresar

Servidor Hp Proliant BL460c G6 Blade Nuevo! [Me gusta](#)

Nuevo

\$ 400.000

6 cuotas de \$ 66.667 sin interés con mercado pago

VISA

Más opciones

Entrega a acordar con el vendedor
Macul, RM (Metropolitana)
[Consultar costos](#)

¡Único disponible!

[Comprar](#)

Tu compra está protegida. [Ver condiciones](#)

Figura G- 3. Precio HP Proliant BLADE

Fuente: http://articulo.mercadolibre.cl/MLC-434062560-servidor-hp-proliant-bl460c-g6-blade-nuevo-_JM

24-port PoE Ethernet switches

Fancy using your network to supply power as well as data? IT Pro's Alan Stevens looks at six of the latest Power over Ethernet-enabled switches

3Com Switch 4500 PWR 26-Port

See all 2 pictures

Get the ITPro Newsletter

Get FREE weekly newsletters from ITPro - delivering the latest news, reviews, insight and case studies.

[Click here](#)

Advertisement

DOING I.T.PROPERLY

[CLICK FOR MORE](#)

FROM AROUND THE WEB Sponsored Links

Gamers around the world have been waiting for this game!

SHARE TWITTER LINKEDIN FACEBOOK GOOGLE+

WRITTEN BY
Alan Stevens, IT Pro

Price : £1,000

REVIEWS
6 Jun, 2006

Pros :
Plenty of power on tap, 24 PoE-enabled ports, optional redundant power supply

Figura G- 4. Precio 3COM 4500

Fuente: <http://www.itpro.co.uk/88231/3com-switch-4500-pwr-26-port>

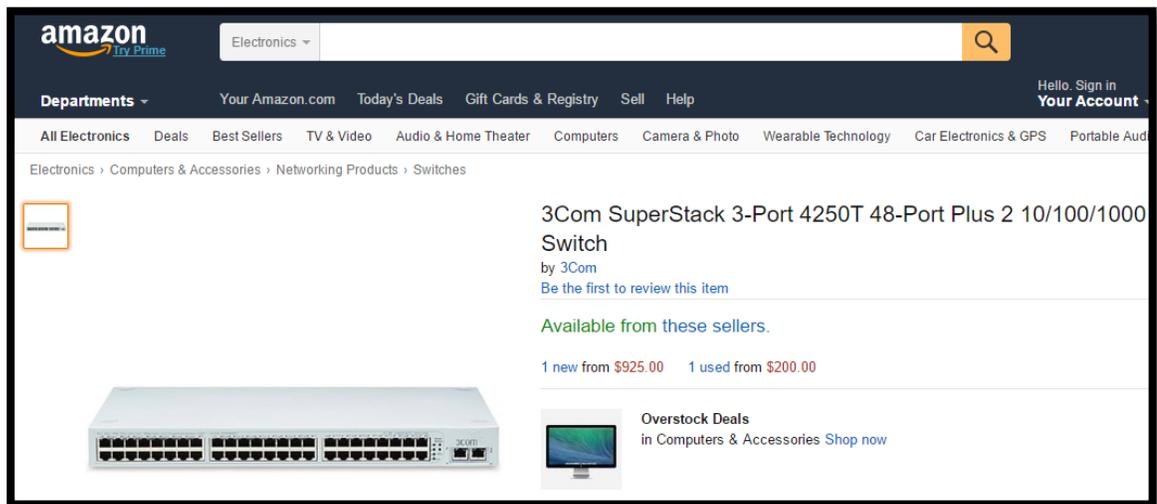


Figura G- 5. Precio 3COM 4250

Fuente: <https://www.amazon.com/3Com-SuperStack-3-Port-48-Port-Switch/dp/B00006HYA7g>



Figura G- 6. Precio Switch 3COM 5500G

Fuente: http://www.ciao.es/3Com_Switch_5500G_EI_24__643317



Figura G- 7. *Switch CISCO 2960*

Fuente: <http://articulo.mercadolibre.com.ec/MEC-409304937-switch-cisco-catalyst-ws-c2960-48tcs-admin-48-puertos-10100- JM>

ANEXO G: Proforma del proyecto



PROFORMA P-401

Ibarra, 1 de Julio del 2016

Srta. Gabriela Mera Terán

Nos es grato saludarle y a la vez presentarle el siguiente presupuesto en cuanto a la petición que nos ha hecho llegar, adjunto a Ud. el respectivo presupuesto de la propuesta de transición de servicios IPv4 a IPv6 para el Gobierno Autónomo Descentralizado de la ciudad de Ibarra. Tomando en cuenta los requerimientos de la red y previo análisis de los equipos a configurar.

DETALLES DEL PROYECTO

- Configuración e implementación de doble pila a switches y servidores WEB Y Correo Electrónico.
- Configuración e implementación de servidor NAT64/DNS64
- Configuración de IPv6 a usuarios finales
- Costo de capacitación al Gobierno Autónomo Descentralizado de la ciudad de Ibarra

PRESUPUESTO

INVERSIÓN TOTAL	\$6600
------------------------	---------------

La validez de esta proforma tiene una duración de siete días laborables y se deberá cancelar el valor del 40% al inicio y al terminar el 60%.

Atentamente:

Ing. Mauricio Cevallos E.
 Dirección: Brasil 4-36 y Panamá
 Celular: 0988998745
 Mail: gerencia@imbacorp.com

ANEXO H: Publicación de la página WEB del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra en la Internet, utilizando una red con mecanismo Doble Pila o Dual Stack

Para llevar a cabo esta actividad, se ha buscado un cliente corporativo que tenga direccionamiento tanto IPv4 como IPv6 o dual Stack, de esta manera se va a describir los pasos realizados:

Utilizando la red IPv4:

Se realizó el nateo respectivo en el firewall, es decir redireccionar la IP del servidor interna y asignarle una IP pública para que sea visible a través de la Internet. Como el cliente corporativo tiene publicada su página WEB, utilizando el puerto 8080, se hizo uso del puerto 8066 y se obtuvo el resultado de la página con direccionamiento IPv4.



Figura H-1: Acceso a la página del GAD-Ibarra con IPv4

Fuente: Captura propia desde teléfono celular

Para verificar la funcionalidad de la página en IPv4, se realizó el ingreso mediante un celular.

Utilizando la red IPv6

Este proceso es mucho más fácil utilizando el direccionamiento IPv6, debido a que el proveedor de Internet de este cliente corporativo, maneja IPv6. De esta manera se toma la dirección IPv6 del servidor en el cual se encuentra instalado el servicio WEB, de esta manera:

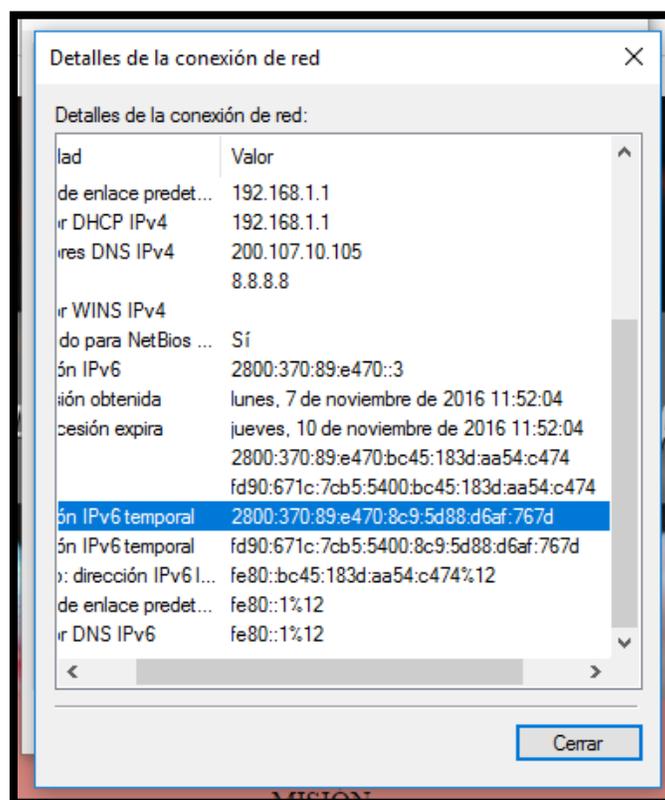


Figura H-2: Configuraciones IPv6

Fuente: Captura propia desde Windows



Figura H-3: Acceso a la página del GAD-Ibarra con IPv6

Fuente: Captura propia desde Windows

Con este análisis se puede concluir que manejar direccionamiento IPv6, es mucho más sencillo que hacerlo con IPv4, por el nateo que se debe realizar ya que con IPv6 se tiene suficientes direcciones públicas para hacer el proceso más directo con el usuario final.



**GOBIERNO AUTÓNOMO DESCENTRALIZADO
DE SAN MIGUEL DE IBARRA**



Ibarra, 22 de Septiembre del 2016

CERTIFICACIÓN

Señores:

UNIVERSIDAD TÉCNICA DEL NORTE

Presente.

De mis consideraciones. –

Siendo los auspiciantes del Proyecto de Tesis de la Sra. Gabriela Estefanía Mera Terán con CI. 100348746-7, quien desarrolló su trabajo con el tema “PROPUESTA DE TRANSICIÓN DE SERVICIOS DE IPv4 A IPv6 PARA LA RED DE DATOS CABLEADA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA CIUDAD DE IBARRA”, me es grato informar que se ha presentado la propuesta y el desarrollo del tema de tesis de forma virtualizada, con la respectiva revisión de cumplimiento de los requerimientos funcionales, por lo que se recibe el proyecto como culminado. Una vez recibida la documentación respectiva, nos comprometemos a utilizar la información en beneficio de nuestra entidad.

La Sra. Gabriela Estefanía Mera Terán, puede hacer uso de este documento para los fines pertinentes en la Universidad Técnica del Norte.

Atentamente,



**Ing. Carlos Gudino
DIRECTOR TICS**

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA