PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIONES

PERFIL DEL TRABAJO PREVIO LA OBTENCIÓN DEL TÍTULO DE:

MÁSTER EN REDES DE COMUNICACIÓN

TEMA:

"ESTUDIO PARA LA MIGRACION DEL PROTOCOLO iPV4 AL PROTOCOLO iPV6. CASO DE ESTUDIO PLENARIO DE LA ASAMBLEA NACIONAL."

Autor: Ing. Ulises A. Carofilis Moreira

Tutor: Ing. Damián A. Nicolalde Ramírez

Quito, Julio, 2017

Agradecimiento

Josue 1:9

Mira que te mando que te esfuerces y seas valiente; no temas ni desmayes, porque Jehová tu Dios estará contigo en donde quiera que vayas.

Padre Amado agradezco cada una de las pruebas académicas que has puesto en mi camino, y esta de una especial manera.

Rindo mi imperecedera gratitud a:

Cada una de las personas que de una u otra forma fueron parte de este proceso y etapa de mi vida.

A mi maravillosa familia, a mis invalorables amigos de quienes sentí un aliento en mis más grandes afanes.

Al personal de la PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR (PUCE), a Damián Nicolalde Tutor de mi trabajo de Tesis y a Gustavo Chafla Decano de la Facultad de Ingeniería y Corrector de la misma, por su capacidad y paciencia la cual me ayudó a plasmar el trabajo profesional en este proceso ya de 10 años al servicio de mi País y de mi querida Asamblea Nacional del Ecuador.

A esta amada tierra manabita de quien heredé el valiente e inclaudicable ADN que corre por las venas de todos mis coterráneos, caer es de todos, levantarse solo de pocos, levantarse es de valientes y de ganadores, te agradezco Manabí por las lecciones y testimonios de vida que día a día me enseñas desde aquel fatídico 16A del 2016.

Agradezco también a la institución educativa que me formó como ingeniero, la Universidad Laica Eloy Alfaro de Manabí (ULEAM), que me permitió aprender, aplicar y comprender que la verdadera capacidad educativa en un profesional no sólo se encuentra en el cerebro, si no también se aloja en el corazón.

Dedicatoria

I Samuel 16:7

Y Jehová respondió a Samuel: No mires a su parecer, ni a lo grande de su estatura, porque yo lo desecho; porque Jehová no mira lo que mira el hombre; pues el hombre mira lo que está delante de sus ojos, pero Jehová mira lo que hay en el corazón.

Dedico este trabajo de tesis de cuarto nivel a un gran ser humano y buen amigo: Justin Ulises Carofilis Lucas.

Porque siento y vivo tu vocación y talento por esta ciencia, hijo mío y porque estoy seguro que la ética y los valores con los que te estas formando, forjará al excelente profesional, cargado de humanidad y sencillez para recibir los galardones que la vida te depare.

Índice

Índice de Tablas 9

Capítulo I: Introducción 10

1.1 Antecedentes 12

1.2 Situación actual de la red 12

1.3 Situación problemática 14

1.4 Justificación 15

1.5 Objetivo General 16

1.6 Objetivos Específicos 16

1.7 Alcances de la investigación 17

Capítulo II: Marco Teórico 18

2.1 Marco Conceptual 18

2.1.1 Dirección IP 18

2.1.2 Clases de direcciones IP 18

2.2 Protocolo Ipv4 19

2.2.1 Desventajas 19

2.2.2 Formato de dirección 19

2.2.3 Protocolo Ipv4. Cabecera 20

2.4 Estudios similares 22

2.5 Descripción de IPv6 23

2.5.1 Cabecera Ipv6 23

2.6 Resolución de nombres IPv6 25

2.6.1 Tipos de registro 25

2.7 Protocolos fundamentales IPv6 26

2.7.1 Protocolo ICMPv6 26

2.7.2 ND 27

2.7.3 Protocolo MLD 28

2.8 Protocolos de enrutamiento 30

2.9 Direccionamiento IPv6 33

2.10 Enrutamiento IPv6 36
2.10.1 Tablas de ruteo 36
2.11 Cuadro comparativo entre ambos protocolos 37
2.12 Ventajas y desventajas de los protocolos 40
2.12.3 Ventajas de IPv6 41
2.12.4 Desventajas 42
2.13 Mejores prácticas Ipv6 43
2.14 Mecanismos para la transición de Ipv4 a Ipv6 43
2.14.1 Mecanismo Doble Pila (Dual stakc) 44
2.15 Túneles 46
2.15.1 Túneles configurados 46
2.15.2 Túneles automáticos 47
2.15.3 Traducción 49
2.16 Análisis comparativo entre los mecanismos de transición 53
2. 17 Mecanismo seleccionado para la transición 54
Capítulo III: Estructura de la red 55
3.1.1 Tráfico de red 57
3.1.2 Estructura del cableado 59
3.1.3 Dispositivo de trabajo 61
3.2 Diseño y obtención del diagrama Lógico 62
3.3 Diseño de las Vlans 64
3.3.1 Conectividad entre las Vlans 64
3.3.2 Direcciones Ipv4. Distribución 65
3.3.3 Tablas de enrutamiento 68
3.3.4 Características de los equipos de red 68
Capítulos IV: Resultado del estudio 75
4.1 Metodología de implementación de la red IPv6 75
4.2 Conexión a Internet con IPv6 76
4.2.1 Proveedor de servicios 76

4.2.2 Protocolos de enrutamiento 77
4.3 Transición a IPv6 81
4.3.1 Configuración para la primera opción de migración 82
4.3.2 Configuración de los dispositivos para la segunda opción 85
4.3.3 Configuración de ACLS en el firewall: 87
4.4 Diseño de la topología de red IPv6 revisa la sugerencia de la revisión anterior en este punto 88
4.5 Configuración de las VLANS en IPv6 89
4.5.1 Configuración de VLANS usando IPV6 89
4.5.2 Configurar ACLS en IPV6 90
4.6 Hardware 90
4.7 Software 91
4.7.1 Costos de Software 92
4.7.2 Costos en Hardware 93
4.7.3 Costos en RRHH 93
4.7.4 Costos en Capacitación 94
4.7.5 Inversión 94
Conclusiones 96
Recomendaciones 97
Bibliografía 98

Índice de Figuras

Figura 1: Formato de dirección Ipv4. ---- 20
Figura 2: Cabecera del protocolo Ipv4. ---- 20
Figura 3: Formato de la cabecera Ipv6. ---- 24
Figura 4: Sitio web asociado a diferentes tipos de registros. ---- 26
Figura 5: Registro PTR. ---- 26
Figura 6: Formato de un mensaje ICMPv6 ---- 27
Figura 7: Formato del protocolo MLD ---- 30
Figura 8: BGP ---- 32
Figura 9: Estructura direcciones locales de enlace ---- 34
Figura 10: Dirección anycast del router de la subred. ---- 34
Figura 11: Dirección multicast del router de la subred. ---- 35
Figura 12: Resolucion DNS ---- 45
Figura 13: Configuracion DNS. ---- 46
Figura 14:Túneles configurados ---- 47
Figura 15:Método 6to4 ---- 48
Figura 16: Método traducción ---- 49
Figura 17: Método NAT ---- 51
Figura 18:Método TRT ---- 53
Figura 19: Topología referencial del Plenario de la Asamblea Nacional ---- 55
Figura 20: Topología de la red del Plenario. ---- 63
Figura 21: Enrutamiento del router del Plenario ---- 68
Figura 22: Diagrama Físico del Plenario. ---- 71
Figura 23: Diagrama Físico del Plenario. ---- 76
Figura 24: Asignar nombre al router ---- 78
Figura 25: Enrutamiento de paquetes IPV6 ---- 79
Figura 26: Habilitar Ospf dentro de un router: ---- 80
Figura 27: Verificar las configuraciones ---- 81
Figura 28: verificar las configuraciones ---- 82
Figura 29: verificar las configuraciones ---- 84
Figura 30: Segunda opción de migración ---- 85
Figura 31: Configuración Ipv6 del router ---- 86
Figura 32: Configuración Ipv6 del router ---- 86
Figura 33: Topología de la red con Ipv6 ---- 89
Figura 34: Anexo 1 ---- 102
Figura 35: Anexo 2 ---- 103

Figura 36: Anexo 3 ---------- 103
Figura 37: Anexo 4 ---------- 104

Índice de Tablas

Tabla 1: Puertos de los Switch 13
Tabla 2: Distribución de subredes 13
Tabla 3: Cuadro comparativo de protocolos 37
Tabla 4: Cuadro comparativo de mecanismos de migración 53
Tabla 5: Función de los servidores 56
Tabla 6: Rack. Características. 60
Tabla 7: Patch Panel. Características 61
Tabla 8: Cable UTP. Características 61
Tabla 9: Patch Cord. Características 62
Tabla 10: Vlans 64
Tabla 11: Acceso entre Vlans 65
Tabla 12: Crecimiento futuro. Porcentaje 66
Tabla 13: Direcciones para cada subred 66
Tabla 14: Configuración entre las Vlans. 67
Tabla 15:Servidor de Correo. Características 68
Tabla 16:Servidor de aplicaciones. Características 69
Tabla 17:Servidor de BD. Características 69
Tabla 18:Servidor de Voto Electrónico. Características 70
Tabla 19: Prestaciones de ordenadores curules 71
Tabla 20: Prestaciones de ordenadores de la presidencia 72
Tabla 21: Prestaciones del firewall 72
Tabla 22: Prestaciones del router 73
Tabla 23: Prestaciones de los switch 73
Tabla 24: Prestaciones de los teléfonos IP 74
Tabla 25: Configuración de las Vlans con los dos protocolos 88
Tabla 26: Hardware del Plenario 90
Tabla 27: Software del Plenario 91
Tabla 28: Software de las PC´s 92
Tabla 29: Costos de Software 93
Tabla 30: Costos en Capacitación 94
Tabla 31: Costos del proyecto 94
Tabla 32: Riesgos del proyecto 95

Capítulo I: Introducción

En los últimos años se ha notado el avance que han tenido las Tecnologías de Información y Comunicaciones (TICs), las mismas han llegado a formar parte fundamental de la sociedad (Rivera L. , 2013). Hace algún tiempo, se han desarrollado diferentes tecnologías y servicios que facilitan la comunicación con personas que se encuentren a distancia. (Rivera L. , 2013)

Con el transcurso del tiempo, los medios de comunicación, tales como la mensajería, y la telefonía, se han orientado hacia el internet (Rivera J. , 2015). Este constituye la red de ordenadores más grande en todo el mundo. Dentro de ella existen disímiles subredes distribuidas por todo el mundo, así como usuarios que utilizan los ordenadores para conectarse. En tiempos de antaño la comunicación se lograba haciendo uso de una línea telefónica o de un puerto serie o paralelo, pero este sistema quedó en desuso luego del avance de las tecnologías. (Rivera J. , 2015)

Internet es una red integrada por miles de redes y computadoras interconectadas en todo el mundo mediante cables y señales de telecomunicaciones, que utilizan una tecnología común para la transferencia de datos. (Zamora, 2014)

Internet es también un sistema mundial de redes de computadora interconectadas. Las computadoras y las redes de computadoras intercambian información utilizando TCP/IP (Protocolo de Transmisiones/Protocolo de Internet) para comunicarse entre sí. Están conectadas vía las redes de comunicación e internet puede ser usado para enviar correos electrónicos, transferir archivos y accesar información de la Web. (Zamora, 2014)

Esta red tiene la estructura de una tela de arañas de ordenadores. Está compuesta por miles de redes y subredes que están ubicadas alrededor del mundo, haciendo participes de ella a un gran número de usuarios. La conexión inicial que se llevaba a cabo era partiendo de dos computadoras conectadas

a través de un puerto serie o paralelo, sin embargo, otras opciones surgieron a partir del gran auge y crecimiento de la red.

El Organismo Internacional para la Estandarización (ISO), realizó en el año 1984 algunas investigaciones sobre modelos de conexión de red TCP/IP, para poder solucionar los problemas de compatibilidad con las redes antiguas de las empresas. De esta forma surge el modelo de referencia de Interconexión de sistemas Abiertos (OSI). A partir de entonces Internet creció aceleradamente y pasó de ser una pequeña red a convertirse en una plataforma que brinda disímiles servicios de última tecnología.

En Julio de 1992, Ecuador estableció su primer enlace a Internet. El 1ro de febrero de 1991 fue registrado dentro del dominio nacional con Internet Assigned Numbers Authority (IANA). (Islas, 2012)

En el Ecuador, la primera institución en facilitar la apertura al Internet fue Ecuanex, el cual es un nodo de Internet creado por la Corporación Interinstitucional de Comunicación Electrónica, Intercom en 1991. Esta red integrala red mundial del Institute for Global Communications/Alliance for Progressive Communications (IGC/APC), que brinda este servicio a las organizaciones no gubernamentales y de desarrollo. (González, 2010)

La Corporación Ecuatoriana de Información, estableció en octubre de 1992 otro nodo, Ecuanet. una entidad sin fines de lucro patrocinado por el Banco del Pacífico, la ESPOL, la Universidad Católica Santiago de Guayaquil y otras entidades. Dicha red se conecta directamente al NSFNET, por medio del sistema de comunicaciones del Banco Pacífico. (González, 2010)

Uno de los protocolos para la conexión a internet es el protocolo de Internet versión 4 (Ipv4), el cual ha sido el utilizado hasta la actualidad. Sin embargo, la alta demanda de usuarios conectados a internet, ha hecho de este protocolo una opción limitada para llevar a cabo el proceso de conexión, por lo cual se han realizado cambios para suplir las necesidades de conexión de millones de usuarios. Claramente nunca se cuestionó la cantidad de usuarios que llegaría a tener internet algún día. (Salazar, 2013)

El desarrollo de esta investigación permitirá obtener resultados precisos que constituirán la base para la migración hacia el protocolo Ipv6 dentro de la Asamblea Nacional del Ecuador.

Para lograr los resultados deseados la investigación estará dividida en cuatro capítulos. El capítulo 1, presenta los objetivos generales y específicos del trabajo, la situación problemática, la cual conlleva a la realización del mismo, la justificación que constituye el sustento del proyecto y la situación actual de la red de la Asamblea Nacional.

El capítulo 2, permitirá desglosar el estudio realizado sobre las características de Ipv6, tales como sus protocolos fundamentales, los protocolos de enrutamiento, así como las ventajas y desventajas de Ipv4 e Ipv6.

En el acápite 3, se llevará a cabo el levantamiento de información de la red de la Asamblea, haciendo un estudio y exposición detallados de la estructura de la red actual, identificando la ubicación del cableado y describiendo el diagrama lógico.

En el capítulo 4, se llevará a cabo el diseño como solución Ipv6, para la red de la Asamblea Nacional. También se define la metodología para implementar este nuevo protocolo.

1.1 Antecedentes

La Asamblea Nacional del Ecuador, radica en Ave 6 de Diciembre y Piedrahita, frente al Hospital Eugenio Espejo, en el Palacio de la Asamblea Nacional. En ella trabajan un total de 142 personas. Esta institución está conformada por el Plenario y distintos locales de comisiones. Y cuenta además con un total de 137 ordenadores. A través de la presente investigación se propondrá una migración de protocolos de Ipv4 a Ipv6 para la red de la Asamblea.

1.2 Situación actual de la red

Dentro del pleno de la Asamblea Nacional, la red está compuesta por 9 switch de 48 puertos cada uno, todos de marca cisco modelo 3560X, de esos switch salen las conexiones a los 142 equipos de los asambleístas y los demás

dispositivos para la funcionalidad de todo el Sistema E-Curul y varios dispositivos. De los switch salen 4 AP que distribuyen red inalámbrica son los modelos cisco 3702. Estos salen conectados directamente al data center de forma redundate, y la conexión de los switch a los core es todo en fibra óptica, los core1 y core2 son cisco 6500 y manejan los siguientes puertos:

Tabla 1: Puertos de los Switch

Puertos que manejan los Switch	
Dispositivo	**Puertos**
Core1	32 puertos de 10GB y 96 puertos de 1000Mbps.
Core 2	32 puertos de 10GB y 48 puertos de 1000Mbps.

Elaborado por: el autor

También se cuenta con un Firewall IBM 3650 con su software Centos en IPtable. La conexión es en cobre, de ahí se sale a un router cnt. Cabe indicar además que los Ciscos 6500 son utilizados como data center. Los ordenadores que interactúan con el sistema E-Curul manejan IP fijas todas, y el DHCP solo se usa cuando se conecta algún equipo vía alámbrica o inalámbrica dentro de la infraestructura del pleno. Se cuenta con un servidor, donde se aloja el sistema de voto electrónico E-Curul, el mismo tiene una IP 10.15.38.245, perteneciente a la subred 10.15.38.0/23 y el Gateway 10.15.39.254. Unido a ello debe acotarse que en este lugar existen 7 Vlan, las cuales se describen a continuación en una tabla:

Tabla 2: Distribución de subredes

Distribución de Vlans	
Vlan	**Destino**
49	Servidor
1	Administración
52	Asambleístas

202	Comisiones
200	Móvil
201	Invitados
92	Presidencia
205	Funcionarios

Elaborado por: el autor

1.3 Situación problemática

La versión inicial comercial del Protocolo de Internet contaba con direcciones de 32 bits de longitud, o sea alrededor de 4.000 millones de direcciones. Analizando que actualmente cada una gran parte de las personas del planeta tiene varios dispositivos, es de entender que esta cantidad llegue a ser pequeña en algún momento. Actualmente la versión conocida y utilizada en todo el mundo es la 4, sin embargo, se ha desarrollado una versión nueva conocida como Ipv6. Dicha versión cuenta con 128 bits, o sea sextillones de direcciones, las cuales son suficientes para que casa persona utilice más direcciones que las direcciones que toda la internet actualmente. (Palet, 2012)

Para que internet crezca se necesita cambiar a IPv6. Con la implementación del nuevo protocolo se logrará que se conecten muchos usuarios a la red. Específicamente, para una empresa conectada a la red, es esencial estar preparada para la migración, ya que podría estar en riesgo de perder usuarios. La razón está dada porque algunos usuarios solo tendrán acceso a IPv6, entonces quedarán páginas que solo serán visibles con IPv4, dichos usuarios no podrán llegar a ellas.

Según un artículo publicado en el Sitio Web Ministerio de Industria Energía y Turismo (Ministerio de Industria, Energía y Turismo, 2015), desde el 3 de febrero del 2011 fueron entregadas las últimas direcciones IPv4 del registro central. Este factor influye sobre todos los países y claramente Ecuador está exento de ello. Para solucionar este problema se diseñó el protocolo IPv6, el

mismo tiene la característica de ser transparente para los usuarios, y en cuanto a la configuración de las redes tiene la característica de la ¨autoconfiguración¨ (Ministerio de Industria, Energía y Turismo, 2015). Este protocolo posee tantas direcciones que no necesita utilizar traductores de direcciones (NAT), y permite recuperar la conectividad extremo a extremo. IPv6 no es más seguro que IPv4, sin embargo, el estándar incorpora obligatoriamente el protocolo IPsec (seguridad IP), y al no necesitar NAT, se puede trabajar con IPsec extremo a extremo, lo cual puede contribuir al incremento de la seguridad en la Red (Ministerio de Industria, Energía y Turismo, 2015, p. 21).

Debido a que el número de direcciones que facilita el IPv6, se pueden tener millones de dispositivos y sensores conectados, esto se llama “Internet de las Cosas” (Ministerio de Industria, Energía y Turismo, 2015, p. 22). Este protocolo permite gestionar todo tipo de redes. Según estudios y publicaciones es difícil se agote en los próximos 480 años (Ministerio de Industria, Energía y Turismo, 2015, p. 22).

Por las razones antes mencionadas, el Ministro de Telecomunicaciones de Ecuador indicó que las instituciones públicas deberían iniciar la migración de protocolos IPv4 hacia IPv6, por las notables ventajas que esto traería para el buen funcionamiento de dichas instituciones.

1.4 Justificación

Migrar la red de la Asamblea a Ipv6 traería muchos beneficios, los cuales se listan a partir de las ventajas de este protocolo: Meisel (2016)

Direcciones más extensas. El tamaño nuevo de la dirección es lo más cambiante. IPv6 cuadriplica el tamaño de la dirección del IPv4 de 32 a 128bits. El espacio libre para una dirección IPv6 es tan inmenso que no podrá agotarse en un futuro visible.

Formatos de cabecera flexibles. IPv6 utiliza un nuevo formato de datagrama. A diferencia del IPv4, que utiliza una cabecera de datagrama de formato fijo, donde todos los campos, excepto la parte opcional, ocupan un número fijo de octetos, el IPv6 utiliza un conjunto opcional de cabeceras.

Soporte para reserva de recursos. IPv6 reemplaza la especificación del tipo de recursos del IPv4 con un mecanismo que permite la reserva con anterioridad de recursos de red. En particular, el nuevo mecanismo soporta aplicaciones como video en tiempo real, el cual necesita una garantía del ancho de banda retardado.

Suministro de extensiones al protocolo. Tal vez, el cambio más relevante en el Pv6 es la sustitución de un protocolo en el que estaban detallados totalmente todos los recursos a otro que permite más características. La capacidad de extensión tiene el potencial para permitir que el protocolo se adapte a cambios en el hardware de la red o a nuevas aplicaciones.

Número de saltos. Cuando el tiempo de vida en un paquete IPv4 se cambia por el número de saltos en IPv6 se mejora el hecho de que, si existe una acumulación en la red, este paquete no sea eliminado sin tener la opción de llegar hasta el nodo de destino. (Meisel, 2016)

1.5 Objetivo General

Realizar un estudio para el análisis y diseño del protocolo IPV6 en la Infraestructura de Red del Pleno de la Asamblea Nacional del Ecuador en el periodo legislativo 2013-2017.

1.6 Objetivos Específicos

1. Analizar la situación actual de la red de la Asamblea Nacional.
2. Realizar el análisis de los elementos de hardware, software y demás equipos de comunicaciones (infraestructura actual, compatibilidad de los mismos), para determinar el soporte de la implementación.
3. Analizar las metodologías existentes para la migración a IPv6.
4. Analizar las ventajas y desventajas de la migración hacia el nuevo protocolo.
5. Diseñar la solución del IPv6.
6. Realizar el análisis para la migración de forma tal que el Sistema E-Curul y el resto de los aplicativos utilizados en la Asamblea, continúen en marcha, sin dificultades.

1.7 Alcances de la investigación

El alcance investigativo, se refiere al resultado de lo que se obtendrá con su realización y condiciona el método que se seguirá para obtener dichos resultados, razón por la cual es muy importante identificar precisamente dicho alcance previo al comienzo de la investigación. (Carballo, 2013)

El alcance fundamental que tendrá la investigación será analizar y demostrar las ventajas que traerá para la Asamblea Nacional la migración de IPv4 a IPv6. Así como los aspectos administrativos, técnicos y económicos. También se realizará un vasto estudio que permitirá realizar la propuesta de la metodología para implementar la red haciendo uso de protocolo IPv6, en esta institución. Por consiguiente, el trabajo permitirá la conexión de los sistemas a través del protocolo IPv6, así como el acceso al conocido internet de las cosas. Además, facilitará la obtención de los costos que se necesitarán para llevar a cabo el cambio de protocolo.

Capítulo II: Marco Teórico

2.1 Marco Conceptual

2.1.1 Dirección IP

Es la sigla de Internet Protocolo, en español, Protocolo de Internet. Se trata de un estándar que se emplea para el envío y recepción de información mediante una red que reúne paquetes conmutados. (UNLAM, 2014, p. 10)

Las direcciones IP son números que identifican, jerárquica y lógicamente, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, smartphone) que trabaje con el protocolo IP (Internet Protocol), que forma parte del nivel de red del modelo TCP/IP. (UNLAM, 2014, p. 10)

2.1.2 Clases de direcciones IP

Cuando se asigna una dirección IP a una red, se tiene en cuenta el tamaño y las necesidades de éstas. Según Daniel Morató, estas se distinguen en 3 tipos principales de redes (y de direcciones IP):

Redes de clase A: son las redes que requieren de un gran número de direcciones IP, dado el número de host que comprenden. A este tipo de redes se les asigna un rango de direcciones IP, el cual se identifica por el primer octeto de la IP (Morató, 2013, p. 18), así que disponen de los otros 3 octetos que le siguen para asignar direcciones a sus hosts. Su primer byte tiene un valor estimado entre 1 y 126 (Morató, 2013, p. 18). El número de direcciones que se obtiene es muy elevado llegando a más de 16 millones, por lo que las redes de clase A corresponden fundamentalmente a organismos gubernamentales, grandes universidades, etc.

Redes de clase B: son redes que requieren de un número de direcciones IP intermedio para establecer la conexión de todos sus hosts con Internet (Morató, 2013, p. 18). A estas redes se les asigna un rango de direcciones IP que se identifica por los dos primeros octetos de la IP disponiendo de los otros 2 octetos siguientes para asignar direcciones a sus hosts (Morató, 2013, p. 18). Sus dos primeros bytes se encuentran entre 128.1 y 191.254, por lo que

el número de direcciones resultante es de 64.516. Las redes de clase B se utilizan generalmente en grandes empresas, universidades de tipo medio, y organizaciones gubernamentales etc.

Redes de clase C: son redes que necesitan un número de direcciones IP menos extenso para conectar sus hosts con Internet (Morató, 2013, p. 19). A estas de redes se les asigna un rango de direcciones IP identificado por los tres primeros octetos de la IP, por lo tanto, disponen de un sólo octeto para asignar direcciones a sus hosts (Morató, 2013, p. 19). Sus 3 primeros bytes deben estar comprendidos entre 192.1.1 y 223.254.254. La cantidad de direcciones obtenidas es de 256 para cada una de las redes, por lo que éstas corresponden principalmente a pequeñas empresas, organismos locales, etc. (Morató, 2013, p. 19)

2.2 Protocolo Ipv4

Este protocolo está pensado para los datos que son usados en la comunicación instalada entre redes mediante interrupciones (switches) de paquetes. (Rivera J. , 2015)

2.2.1 Desventajas

- Es un protocolo de un servicio de mensaje no fiable. (Rivera J. , 2015, p. 24)
- No proporciona garantía de entrega de datos. (Rivera J. , 2015, p. 24)
- No proporciona garantía sobre corrección de los datos. (Rivera J. , 2015, p. 24)
- Hace llegar paquetes duplicados. (Rivera J. , 2015, p. 24)
- Esta versión es capaz de generar aproximadamente 4.000 millones de combinaciones. (Rivera J. , 2015, p. 24)

2.2.2 Formato de dirección

Su dirección IP usa un tamaño de 32 bits y se divide en 4 grupos de 8 bits, divididos por puntos cuya representación es en números decimales. En el octeto cada bit tiene un peso binario (Rivera J. , 2015, p. 25). El valor mínimo

para un octeto es 0 y el valor mayor es 255. En gráfico que continúa se observa el formato básico de esta dirección IP con los 32 bits unidos en 4 octetos.

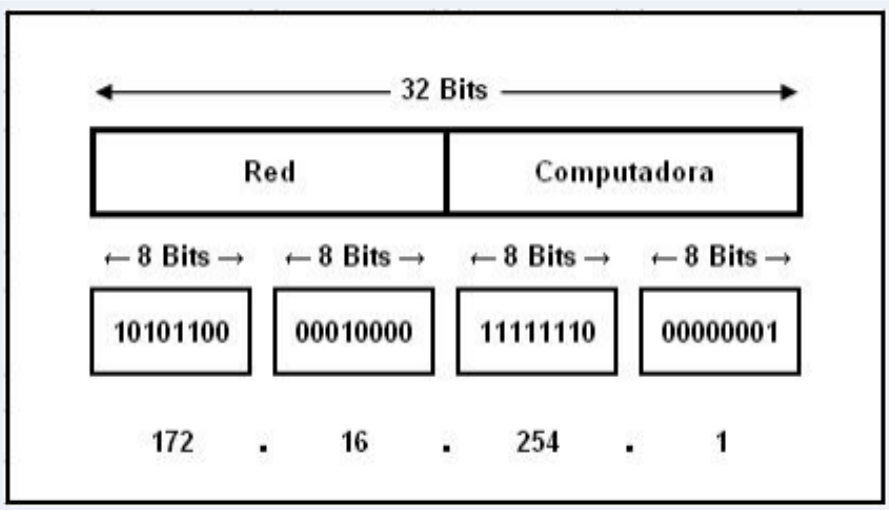


Figura 1: Formato de dirección Ipv4.
Fuente: (Rivera J. , 2015)

2.2.3 Protocolo Ipv4. Cabecera

La unidad menor de datos que se puede enrutar y transmitir mediante una red IP es conocida como paquete y está compuesto de una cabecera IP, y el contenido. Siendo la primera la parte más externa del paquete, llevando el código fuente y las direcciones IP de destino.

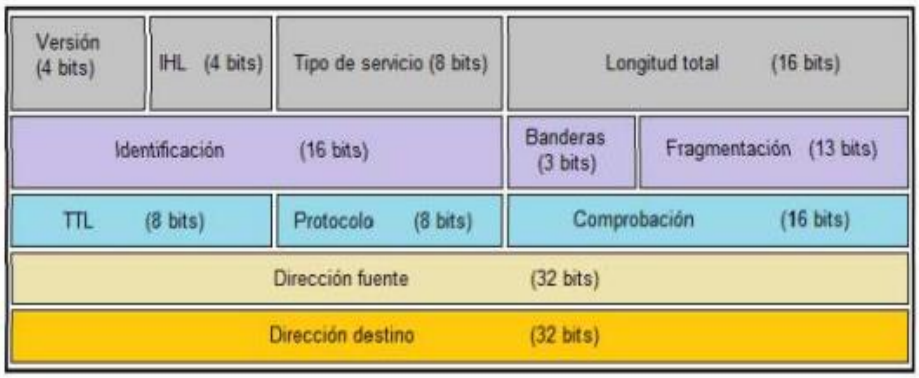


Figura 2: Cabecera del protocolo Ipv4.
Fuente: (Rivera J. , 2015, p. 12)

- El campo llamado versión significa un registro de la versión del protocolo de donde pertenece el datagrama.
- I.H.L. (Internet Header Length), especifica la longitud en palabras de 32 bits, el valor mínimo es de 5, cifra que se aplica cuando no hay opciones, el valor máximo de este campo de 4 bits es el 15.
- Tipo de servicio, contribuye a valorar cuán importantes son los datos enviados, determinando la forma en que se tratarán para transmitir 8 bits.
- La longitud total especifica la longitud completa en bytes del datagrama de 16 bits, conjuntamente con el encabezado y los datos. Por esta razón el datagrama es pequeño (16 bits) y teóricamente no sea mayor a 65.535 bytes.
- El campo identificación también tiene importancia ya que se encarga de ensamblar un datagrama cuando viaja, pues estos se transmiten fragmentados y cuando una parte llega al ordenador, tiene un valor en donde se indica el paquete al que pertenece.
- Banderas: es un identificador no utilizado en la fragmentación de 3 bits.
- Fragmentación: contribuye al ensamblaje de los datagramas fragmentados con previamente.
- El campo TTL (tiempo de vida) es un contador, el cual determina el tiempo de vida de un paquete, para que este no vague en la red.
- Si el paquete se ensambla totalmente, la computadora desconoce qué hacer con él, y luego entra el campo del protocolo, el cual es un número que orienta cómo entregar el paquete.
- Al inicio del viaje de los datagramas, el campo de comprobación verifica si estos tienen algún error, haciendo un cálculo de suma de verificación del encabezado.
- Los campos de dirección de destino y fuente son todos los que contienen la dirección IP de la computadora de destino y origen. (Rivera J. , 2015, p. 26)

2.4 Estudios similares

Actualmente, son varias las empresas e instituciones las que se han dedicado a realizar la configuración de sus dispositivos para lograr que la red soporte el protocolo IPv6. Ejemplo de ello es el proyecto realizado por Omar Llorente, titulado: “Transición a Ipv6 en un departamento universitario”. En este trabajo se analizaron los motivos que llevaron a la migración de protocolo en la institución. Sobre esto el autor considera que el departamento universitario se encuentra inmerso en tareas de investigación que conllevan al uso de tecnologías de última generación, así como la necesidad de manejar, experimentar y explorar los nuevos protocolos con el fin de estar un paso por delante de otros competidores. También existían factores externos e internos que ejercían presión para utilizar Ipv6. En este trabajo se analizaron los costes de la migración para poder implementar el proyecto y se trabaja de forma tal que los sistemas se vean afectados lo menos posible. Se utiliza el mecanismo dual stack para mantener la red Ipv4 y la red Ipv6 conviviendo al unísono.

Otro proyecto similar es la Propuesta de migración de Ipv4 a Ipv6 de la red de La Universidad Simón Bolívar por el ingeniero Wilfredo José Contramaestre Salazar. También se analiza la situación inicial de la red de la Universidad, así como los mecanismos que existen para la transición. Luego de implementar la migración inicial, se recomendó continuar con esta de forma paulatina para no afectar la conexión de los usuarios de la red universitaria.

En otro trabajo realizado por Edwin Felipe Morales Cal y titulado “Migración del Protocolo Ipv4 a Ipv6 en una red, los beneficios y seguridad que conlleva a este cambio” se analiza cuáles son los motivos para migrar a Ipv6, la cual se parten de la escases de direcciones IP con el protocolo Ipv4 e Ipv6 tiene la solución. Dentro del análisis realizado de las ventajas que se aprovecharán al utilizar IPv6 se encuentran las siguientes:

Mayores niveles de direccionamiento jerárquicos, lo cual provee una eficiente, jerárquica, e infraestructura de enrutamiento, o sea una mejor forma de agregación de rutas. (Morales, 2009, p. 102)

La arquitectura de direcciones fija y simple, lo que permite una sencilla planificación y con esto reducir el costo de manejo de las redes. En IPv6 son fijas las máscaras de subred y proveen una cantidad ilimitada virtual de nodos en un enlace. (Morales, 2009, p. 102)

Direcciones privadas, se conforman por bits específicos en la dirección para las redes que no se conectarán a la red. Dichas direcciones se diferencian de las redes privadas IPv4 del RFC1918, ya que en IPv6 estas direcciones se mantienen únicamente asignadas a una red o a un nodo, esto hace que la conectividad sea más fácil entre redes privadas. (Morales, 2009, p. 102)

2.5 Descripción de IPv6

Ipv6 es una nueva dirección del protocolo IP que ha sido diseñado por el IETF (Grupo Especial sobre Ingeniería de Internet) para sustituir paulatinamente a la versión actual de Ipv4.

El autor Fernández (2012) describe algunas de las características más importantes sobre el protocolo Ipv6, las cuales se muestran a continuación:

- Ofrece un espacio de direcciones mayor. El tamaño de las direcciones IP cambian de 32 bits a 128 bits, con el objetivo de soportar mayores niveles de jerarquía en el direccionamiento.
- Simplificación del formato de la cabecera Ipv4, debido a que algunos campos se quitan o se hacen opcionales.
- Permite concebir paquetes IP extensibles y eficientes.
- Paquetes con una carga de más de 65 335 bytes útil (datos).
- Clase de Servicios (CoS) y Calidad de servicio (QoS).
- Núcleo del protocolo (IPsec) seguro.
- Facilidad de etiquetas de flujo para ser usadas por un nodo origen y etiquetar paquetes que son parte de un flujo de tráfico particular. (p. 16)

2.5.1 Cabecera Ipv6

Las cabeceras de longitud fija brindan una facilidad para su procesamiento de los paquetes en los encaminadores. Si es fijo el tamaño de la cabecera,

entonces puede procesarse mediante hardware aumentando las prestaciones. Dado, que los campos estén alineados a 64 bits contribuye a que las nuevas generaciones de procesadores de 64 bits procesen con mayor eficacia las cabeceras IPv6. (Redes Locales y Globales, 2012)

El formato de la cabecera Ipv6 es el siguiente:

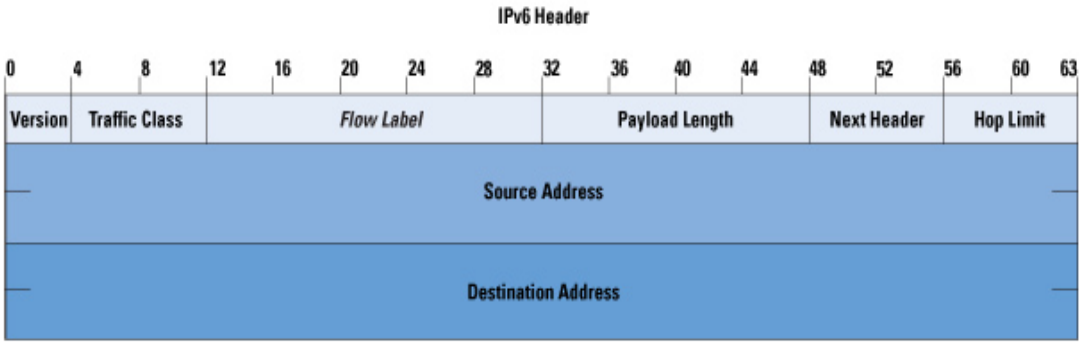


Figura 3: Formato de la cabecera Ipv6.
Fuente: (Redes Locales y Globales, 2012)

En la cabeceraIPv6 se han insertado dos campos que ayudan en la implementación de las nuevas características de IPv6, la Calidad de Servicio (QoS). Con dichos campos se puede controlar el flujo y la asignación de prioridades especificas según los tipos de servicios. Los campos son:

- Clase de Tráfico (Traffic Class), llamado Prioridad. El campo es similar al Tipo de Servicio (TOS) en IPv4. Mide 8 bits.
- Etiqueta de Flujo (Flow Label). Este campo se ha creado para dejar tráficos con requisitos de tiempo real y mide 20 bits de longitud.

Algunas de las funcionalidades de Ipv6 se listan seguidamente:

Aunque esta versión tiene las mismas características que Ipv4, informa sobre los errores en el procesamiento de paquetes, realizar diagnósticos y enviar mensajes de las características de la red.

El ICMPv6 recoge funciones de otros protocolos, que existen, pero independientemente en IPv4. Este cambio se ha diseñado con la misión de reducir los múltiples protocolos, que es perjudicial para mal consistencia y aumentar el tamaño de las implementaciones. Los protocolos utilizados en

IPv4, que ya no existe en IPv6 y sus características fueron anexadas a ICMPv6, son:

ARP (Address Resolution Protocol), cuyo objetivo es mapear las direcciones físicas de direcciones lógicas.

RARP (Reverse Address Resolution Protocol), que realiza la inversa de la ARP, el mapeo de direcciones lógicas a direcciones físicas.

- IGMP (Internet Group Protocolo de Gestión), que trabaja con los grupos de multidifusión de gestión de miembros. (Carabelli, 2011, p. 31)

2.6 Resolución de nombres IPv6

El Sistema de Nombres de Dominio (DNS), no puede ser extendido fácilmente, para ofrecer un soporte exitoso a las direcciones Ipv6, dado que las aplicaciones al ser consultadas solamente retornan direcciones Ipv4 de 32 bits. (Oicatá, 2014, p. 15)

Para soportar adecuadamente las direcciones Ipv6 se definen a continuación varios aspectos a tener en cuenta:

- Un registro nuevo para vincular una dirección Ipv6 con un nombre de dominio.
- Un nuevo dominio para dar soporte hacia las búsquedas basadas en Ipv6.

Definir otro tipo de registro ayuda a guardar la dirección Ipv6 de un host. En ocasiones un host tiene diversas direcciones Ipv6, por lo cual tendrá que contar con más de un registro similar. (Oicatá, 2014, p. 15)

2.6.1 Tipos de registro

Un nuevo tipo de recurso conocido como ¨AAAA¨, tiene el trabajo de almacenar una función Ipv6, su equivalente en Ipv4 es el registro ¨A¨. (Oicatá, 2014, p. 16)

Seguidamente se presenta un ejemplo de un sitio web con los dos tipos de registros:

Tipo de Registro	Formato
A	www.ups.edu.ec A 200.0.32.2
AAAA	www.ups.edu.ec AAAA 3FFE:YYYY:C18:1::2

Figura 4: Sitio web asociado a diferentes tipos de registros.
Fuente: (Oicatá, 2014)

La resolución inversa del nombre de dominio Ipv6 usa el tipo de registro de recurso ¨PTR¨, en Ipv4 es el mismo es el mismo equivalente.

Una dirección Ipv6 se representa partiendo de una secuencia de nibbles que se dividen por puntos con el sufijo ¨. Ipv6.INT¨. La secuencia de nibbles se codifica inversamente, o sea, primero el nibble de menor orden, seguido por el siguiente nibble de menor orden, etc. (Oicatá, 2014, p. 16)

Cada nibble queda representado por un dígito hexadecimal. Seguidamente se muestra un ejemplo:

Tipo de Registro	Formato
PTR	2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0. y.y.y.y.e.f.f.3.ip6.int PTR www.ups.edu.ec

Figura 5: Registro PTR.
Fuente: (Oicatá, 2014)

2.7 Protocolos fundamentales IPv6

2.7.1 Protocolo ICMPv6

El protocolo ICMPv6 se utiliza por los nodos Ipv6 con el fin de informar sobre los errores encontrados durante el procesamiento de los paquetes, además para realizar otras funciones relativas a la capa de internet como son los diagnósticos (¨ping¨). (Gil, 2012)

Los mensajes ICMPv6 se dividen en dos tipos: Gil (2012)

- **Mensajes de error:** se identifican con un 0 en su campo ¨Tipo de mensaje¨ y sus valores están entre 0 hasta 127.
- **Mensajes informativos:** sus valores están entre 128 y 255. (p. 40)

Mediante ICMPv6, los hosts y los enrutadores que se comunican mediante IPv6 pueden informar sobre los errores que se presentan y enviar mensajes de eco simples.

Seguidamente se observa el formato de un mensaje ICMPv6:

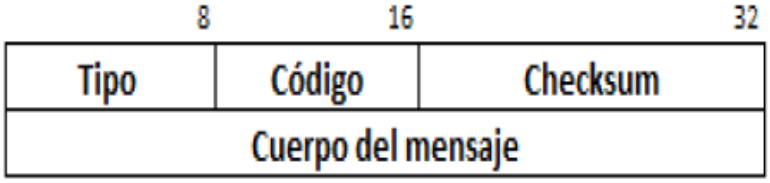


Figura 6: Formato de un mensaje ICMPv6
Fuente: (Gil, 2012)

2.7.2 ND

IPv6 aporta el protocolo ND (Neighbor Discovery, descubrimiento de vecinos), que utiliza la mensajería como vía para controlar la interacción entre nodos vecinos. Los nodos de IPv6, se entienden por nodos vecinos los que están en el mismo vínculo. Por ejemplo, al enviar mensajes referentes al descubrimiento de vecinos, un nodo puede grabar la dirección local de vínculo de un vecino. El protocolo ND controla las principales actividades seguidas del vínculo local de IPv6: (ORACLE, 2013)

- Descubrimiento de enrutadores: soporta los hosts para localizar enrutadores en el vínculo local.
- Configuración automática de direcciones: permite que un nodo configure direcciones IPv6 para sus interfaces automáticamente.
- Descubrimiento de prefijos: posibilita que los nodos detecten los prefijos de subred conocidos que han sido asignados a un vínculo. Los nodos utilizan prefijos para seleccionar los destinos que se encuentran en el vínculo local de los asequibles exclusivamente a través de un enrutador.

- Resolución de direcciones: permite que los nodos determinen la dirección local de vínculo de un vecino, pero solo a partir de la dirección IP de los destinos.
- Determinación de salto siguiente: utiliza un algoritmo para seleccionar la dirección IP de un cambio de destinatario de paquetes que está fuera del vínculo local. El siguiente salto puede ser el nodo de destino o un enrutador.
- Detección de inasequibilidad de vecinos: ayuda a los nodos a determinar el estado de asequibilidad de otros nodos. La resolución de direcciones puede repetirse tanto en enrutadores como en hosts.
- Detección de direcciones duplicadas: los nodos pueden identificar si se encuentran en uso o no otros nodos.
- Redirección: un enrutador indica a un host el mejor nodo de primer salto que puede ser utilizado para acceder a un determinado destino. (ORACLE, 2013, p. 6)

El protocolo ND emplea los tipos de mensajes ICMP siguientes para la comunicación entre los nodos de un vínculo:

- Solicitud de enrutador
- Anuncio de enrutador
- Solicitud de vecino
- Anuncio de vecino
- Redirección (ORACLE, 2013, p. 6)

2.7.3 Protocolo MLD

Multicast Listener Discovery (MLD) es el equivalente en IPv6 de la versión 2 del Protocolo de administración de grupos de Internet (IGMPv2) para IPv4. MLD es un grupo de mensajes que se mezclan enrutadores y nodos, que permite a los enrutadores descubrir el conjunto de direcciones de multidifusión para las que hay nodos escuchando en cada interfaz conectada. Al igual que IGMPv2, MLD sólo descubre la lista de direcciones de multidifusión para las que hay una escucha al menos, no la lista de escuchas de multidifusión para

cada dirección de multidifusión. En RFC 2710 se encuentra el descubrimiento de escucha de multidifusión (MLD) está documentado. (MEGS, 2013, p. 5)

A diferencia de IGMPv2, MLD utiliza mensajes ICMPv6 en vez de definir su propia estructura de mensajes. Todos los mensajes MLD son mensajes ICMPv6 de los tipos 130, 131 y 132. Los tres tipos de mensajes MLD son:

1. Multicast Listener Query (Consulta de escucha de multidifusión)

   Cada enrutador usa los mensajes Multicast Listener Query para comunicarse con las escuchas de multidifusión en un vínculo. Entre los dos tipos de mensajes se encuentran los siguientes: Multicast Listener Query: General Query (Consulta general) y Multicast-Address-Specific Query (Consulta específica de dirección de multidifusión). El mensaje General Query se usa para analizar desde las direcciones de multidifusión a escuchas de multidifusión. El mensaje Multicast-Address-Specific Query se utiliza para realizar las consultas escucha de multidifusión de una dirección de multidifusión específica. Las dos formas de mensajes se identifican mediante la dirección de destino de multidifusión en el encabezado IPv6 y una dirección de multidifusión en el mensaje Multicast Listener Query.

2. Multicast Listener Report (Informe de escucha de multidifusión)

   Una escucha de multidifusión utiliza Multicast Listener Report para informar del interés por recibir tráfico de multidifusión para una dirección de multidifusión determinada o para responder a un mensaje Multicast Listener Query.

3. Multicast Listener Done (Escucha de multidifusión terminada) (MEGS, 2013, p. 5)

Una escucha de multidifusión utiliza Multicast Listener Done para informar que ya no tiene interés en recibir tráfico de multidifusión para una dirección de multidifusión determinada. (MEGS, 2013, p. 6)

El paquete de un mensaje MLD consta de un encabezado IPv6, un encabezado de extensión Hop-by-Hop Options (Opciones de salto a salto) y el mensaje MLD. El encabezado de extensión Hop-by-Hop Options contiene la opción Router Alert (Alerta de enrutador) de IPv6 documentada en RFC 2711. Se utiliza para garantizar que los enrutadores procesan los mensajes MLD enviados a direcciones de multidifusión donde el enrutador no escucha. (MEGS, 2013, p. 6)

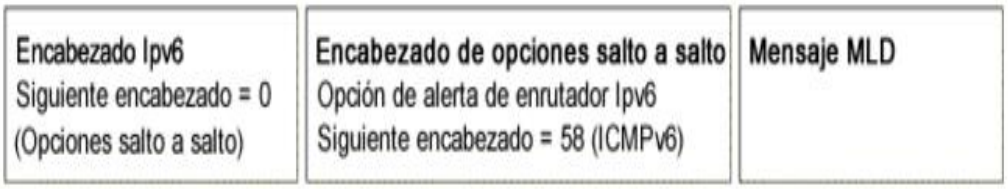


Figura 7: Formato del protocolo MLD
Fuente: (MEGS, 2013, p. 6)

2.8 Protocolos de enrutamiento

Actualmente Ipv6 adopta los mismos protocolos de enrutamiento que son utilizados en las redes Ipv4, los cuales se muestran seguidamente divididos en protocolos internos y externos:

Protocolos de enrutamiento interno:

Existen dos opciones fundamentales para trabajar con el enrutamiento interno: (OSPF, IS-IS), estos usan estructuras jerárquicas, tienen en cuenta la formación de estado y envían actualizaciones de manera optimizada. (Landy, 2013)

Otra opción es (RIP), el cual debe ser habilitado en las interfaces requeridas.

OSPFv3

- Open Shortest Path First version 3 (OSPFv3) . Protocolo IGP de tipo link-state.
- Los routers describen su estado actual durante el, AS enviando LSAs (flooding).

- Utiliza el algoritmo del camino de Dijkstra más corto.
- Agrupa los routers en áreas.
- Basado en el protocolo OSPFv2.
- Protocolo específico para IPv6. (Landy, 2013, p. 11)

RIPng

Está diseñado para que los routers intercambien información de rutas mediante una ruta de una red basada en Ipv6. (Landy, 2013, p. 11)

Es un protocolo de enrutamiento vector-distancia cuya finalidad es determinar mediante la métrica la ruta más óptima de forma automática y la dirección.

Cada router que implementa RIPin tiene una tabla de enrutamiento el cual posee una entrada para cada destino que se quiere alcanzar en todo el sistema de funcionamiento RIPng. (Landy, 2013, p. 12)

Cada entrada de la tabla de enrutamiento cuenta con la siguiente información:

- El prefijo Ipv6 de destino.
- Una métrica que identifica el número de saltos desde el router al destino.
- La dirección Ipv6 del siguiente router y la ruta hacia el destino.
- Una bandera para guiar el cambio de ruta.
- Varios contadores asociados con la ruta. (Landy, 2013, p. 12)

Protocolo de enrutamiento externo:

- El protocolo de enrutamiento externo, en la actualidad por defecto es Border Gateway Protocol versión 4 (BGP-4).
    - Protocolo de tipo path vector.
- Los routers BGP combinar información de enrutamiento entre ASs vecinos
    - Con esta información diseñan un grafo de conectividad entre los AS. (Landy, 2013, p. 12)

BGP

Puerto TCP 179.

Cuatro tipos de mensajes. (Nic, 2012)

- Open
- Update
- Keepalive
- Notification

Dos tipos de conexión

- eBGP
- iBGP

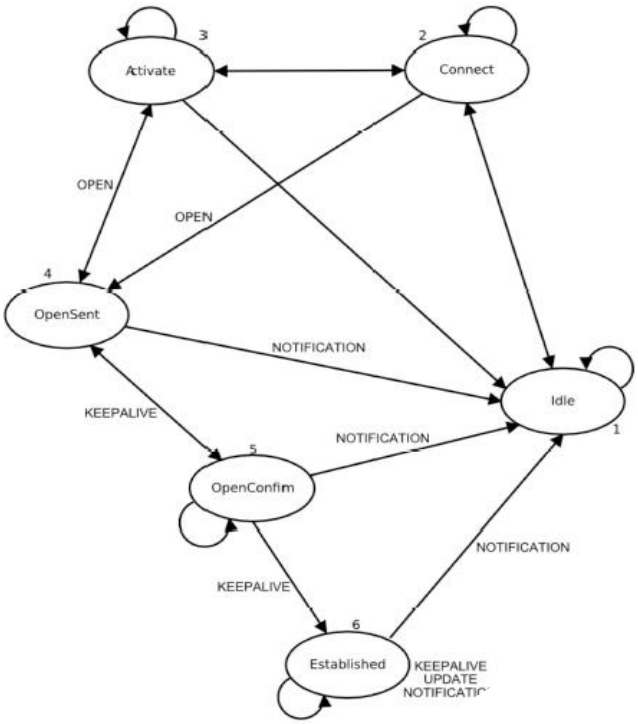


Figura 8: BGP
Fuente: (Nic, 2012, p. 20)

2.9 Direccionamiento IPv6

Las direcciones Ipv6 detectan las interfaces de red. A una misma interfaz de un nodo se le puede asignar múltiples direcciones Ipv6. Estas direcciones tienen tres clasificaciones: (Puerto, 2015)

1. Unicast: Identificador para interfaz única. Los paquetes enviados a una dirección unicast solo son entregados a la interfaz que se identifica con dicha dirección. Es el equivalente a las direcciones Ipv4 actuales.
2. Anycast: Identificador para un conjunto de interfaces (pertenecen a diferentes nodos). Un paquete enviado hacia una dirección anycast se entrega a una de las interfaces identificadas con esta dirección (la que esté más cerca). Permite crear ámbitos de redundancia de tal forma que varias máquinas se puedan ocupar del mismo tráfico dada una secuencia determinada.
3. Multicast: Identificador para un grupo de interfaces (pertenecientes a varios nodos generalmente). Un paquete enviado a una dirección multicast es entregado a cada una de las interfaces identificadaa por esta dirección. El objetivo de este tipo de paquetes es evidente: aplicaciones de transmisión múltiple(broadcast). (Puerto, 2015, pág. 29)

Direcciones Unicast:

Las direcciones locales de enlace se han diseñado para direccionar un único enlace para propósitos de auto-configuracion(mediante identificadores de interfaz), situaciones en las que no existen routers o descubrimiento del vecindario. Por cuanto, los encaminadores no pueden transmitir paquetes con las direcciones fuente o destino locales de enlace (su ambito esta restringido a la red local) Su formato es el siguiente: (Puerto, 2015, pág. 30)

10 bits	54 bits	64 bits
1111111010	0	Identificador de interfaz

Figura 9: Estructura direcciones locales de enlace
Fuente: (Puerto, 2015)

Direcciones Anycast Ipv6:

Una dirección anycast identifica múltiples interfaces. Con una topología de encaminadores eficiente. (Puerto, 2015)

Para que los paquetes sean entregados a la dirección anycast más cercana, el routing de la red debe conocer qué interfaz tiene asignada una dirección anycast y sus distancias.

Las direcciones anycast no tienen un espacio propio dentro del direccionamiento Ipv6, si no que utilizan un espacio común que las direcciones unicast (o sea que no se puede diferenciar entre las direcciones unicast y anycast). El ámbito de las direcciones se equipará con el unicast, así pueden existir direcciones anycast de ámbito de sitio de enlace global. Dichas direcciones solo pueden usarse como dirección de destino, nunca como fuente. (Puerto, 2015, pág. 31)

Existe una dirección anycast, que cada subred requiere, la cual se llama ¨dirección enycast del router de la subred¨. Su sintaxis es similar al prefijo que identifica el enlace de la dirección unicast, siendo el indicador de interfaz igual a cero:

N bits	128-n bits
Prefijo de subred	0

Figura 10: Dirección anycast del router de la subred.
Fuente: (Puerto, 2015)

Todos los routers deben soportar esta dirección para cada subred a la que se encuentran conectadas. Los paquetes enviados a la ¨dirección anycast del router de la subred¨ serán enviados a un router de la subred.

La utilidad de estas direcciones es para implementar los siguientes mecanismos:

Comunicación con el servidor más cercano. Estas direcciones contribuyen a que un cliente se pueda comunicar con un servidor de entre un grupo, y la red seleccionará el que sea más cercano. (Puerto, 2015, pág. 31)

Descubrimiento de servicios. Al configurar un nodo con Ipv6, no sería necesario especificarle la dirección del servidor DNS, Proxy, etc. Podría existir una dirección anycast que identifique esos servicios.

Movilidad. Nodos que tienen que comunicarse con un router del conjunto disponible de su red. (Puerto, 2015, pág. 31)

Direcciones multicast Ipv6

La dirección multicast en Ipv6 es el identificador de un conjunto de nodos. Un nodo puede encontrarse en uno o varios grupos multicast.

Las direcciones multicast tienen el siguiente formato:

Los primeros 8 bits indican que se trata de una dirección multicast, donde:

T: 0. Indica una dirección permanente, asignada por la autoridad de numeración global de internet.

T: 1. Indica una numeración temporal.

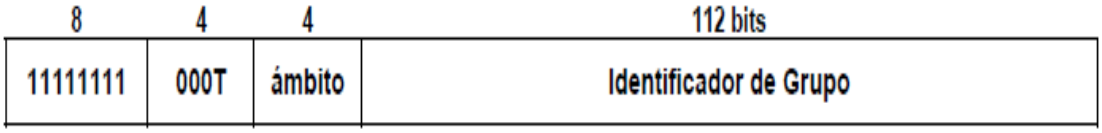


Figura 11: Dirección multicast del router de la subred.
Fuente: (Nic, 2012)

Una dirección IPv6 está formada por

128 bits. 2128 = 340.282.366.920.938.463.463.374.607.431.768.211.456

~ 5,6x1028 direcciones IP por cada ser humano.

~ 7,9x1028 de direcciones más que en IPv4.

La representación de las direcciones IPv6 divide la dirección en ocho grupos de 16 bits, separados mediante ":", representados con dígitos hexadecimales. 2001:0DB8:AD1F:25E2: CADE: CAFE: F0CA:84C1. (Martinez, 2014, p. 23)

En la representación de una dirección IPv6 está permitido:

- Utilizar caracteres en mayúscula o minúscula;
- Omitir los ceros a la izquierda;
- Representar los ceros seguidos":". Ejemplo: 2001:0DB8:0000:0000:130F: 0000:0000:140B 2001:db8:0:0:130f:140b

Formato no válido: 2001:db8::130f:140b (genera ambigüedad) (Martinez, 2014, p. 23)

2.10 Enrutamiento IPv6

El enrutamiento es la parte de Ipv6 que proporciona capacidades de reenvío entre host que se encuentran en segmentos independientes que pertenecen a una red mayor basada en Ipv6. (Fuentes, 2012)

El proceso de enrutamiento ocurre, en el lugar en el que los servicios de transporte del host crean los datos en forma de segmentos TCP o mensajes UDP al nivel Ipv6. Este nivel forma los paquetes con la información de las direcciones de origen y destino que se utiliza para el enrutamiento de los datos haciendo uso de la red. Por último, el nivel Ipv6 mueve los paquetes al nivel inferior del vínculo, donde los paquetes Ipv6 cambian en forma de tramas para su transmisión mediante los medios específicos de una red física. Este proceso ocurre en el orden contrario en el host de destino. (Fuentes, 2012)

2.10.1 Tablas de ruteo

Las tablas de enrutamiento Ipv6 se utilizan con el fin de mantener información y poder establecer una comunicación con redes y host remotos.

Previo a enviar un paquete Ipv6, el equipo inserta la dirección de Ipv6 de origen y la dirección Ipv6 de destino (para el destinatario) en el encabezado Ipv6. Después el equipo examina la dirección Ipv6 de destino, la compara con

una tabla de enrutamiento Ipv6 mantenida localmente y realiza la acción adecuada. (Fuentes, 2012, p. 8)

El equipo realiza una de las tres acciones siguientes:

- Traslada el paquete a un nivel de protocolo superior a Ipv6 en el host local.
- Vuelve a enviar el paquete por medio de una de las interfaces de red conectadas.
- No usa el paquete.

Por último, Ipv6 realiza una búsqueda en la tabla de enrutamiento para encontrar la ruta similar a la dirección Ipv6 de destino. (Fuentes, 2012, p. 9)

Según las investigaciones realizadas una tabla de enrutamiento en Ipv6 está formada por las entradas que se muestran a continuación:

- Prefijo de dirección.
- Interfaz mediante la cual se envían los paquetes.
- Dirección del siguiente salto.
- Valor de preferencia utilizado en la selección entre varias rutas que cuyos prefijos coincidadan.
- Duración de la ruta.
- Especificación cuando se publica la ruta.
- Especificación de vencimiento de la ruta.
- Tipo de ruta. (Fuentes, 2012, p. 9)

2.11 Cuadro comparativo entre ambos protocolos

Tabla 3: Cuadro comparativo de protocolos

Comparación entre ambos protocolos		
Descripción	Ipv4	Ipv6
Dirección IP	En este protocolo la dirección IP se representa mediante	Admite un sin número de direcciones. En esta versión una dirección

	un numero binario de 32 bits, ello proporciona una cantidad de direcciones IP que actualmente se encuentran agotadas.	IP se compone por ocho segmentos de 2 bytes cada uno, los cuales suman un total de 128 bites. Proporciona por su puesto mayor cantidad de direcciones IP.
Encabezados	En esta versión son desperdiciados los espacios en los campos de encabezados. Incluye una suma de comprobación.	Mayor simpleza en los encabezados de los datagramas. No incluye suma de comprobación.
Tráfico de paquetes	Poca seguridad.	Mayor seguridad para el tráfico de paquetes de datos en la red.
Ancho de banda	Desperdicio del ancho de banda.	Transferencia y conexiones de datos más eficaces dada la simplificación de la cabecera. El usuario puede entonces elegir el proceso que tendrá prioridad.
Direccionamiento	Unicast.	Multicast .
Autoconfiguración	No posee.	Los nodos Ipv6 pueden configurarse ellos mismos

		automáticamente una vez conectados a la red ruteada en Ipv6.
Ipsec	Compatibilidad opcional.	Compatibilidad obligatoria.
Identificación del número de los paquetes	No existe identificación de flujo de paquetes para que los enrutadores realicen su control.	Cuenta con identificación del flujo de paquetes haciendo uso del campo Flow Level.
Fragmentación	La realizan los enrutadores y el host que realiza el envío.	La realiza el host que efectúa el envío.
Administración de grupos locales de subred	Usa el protocolo de administración de grupos de internet (IGMP)	E sustituye el protocolo IGMP con los MLD (Mensajes de descubrimiento de escucha de multidifusión)
Direcciones de multidifusión	Son utilizadas para enviar el tráfico a cada nodo de una subred.	No existen direcciones de multidifusión Ipv6. Se utiliza de forma alternativa una dirección de multidifusión para cada nodo del ámbito local del vínculo.

Tamaño del paquete	Admite un tamaño de 576 bytes. (Fragmentado posiblemente)	Admite un tamaño de 1280 bytes sin ser fragmentado.
Selección de la mejor puerta de enlace predeterminada	Se usa el descubrimiento de enrutadores ICMP, de forma opcional.	Se sustituye el descubrimiento de enrutadores ICMP por la solicitud de enrutadores ICMPv6, además de los mensajes de anuncio de enrutador de forma obligatoria.

Elaborado por: el autor

2.12 Ventajas y desventajas de los protocolos

2.12.1 Ventajas Ipv4

1. Reduce los costos de operación a los proveedores de servicios de Internet (ISP).
2. Aminora la cantidad de IP asignadas (de forma fija) y no activas.
3. El usuario puede reiniciar el router para que le sea asignada otra IP y así evitar las restricciones que muchas webs ponen a sus servicios gratuitos de descarga o visionado multimedia online.
4. Capacidad de otorgar aproximadamente 4300 millones de direcciones. (Fuentes, 2012, p. 13)

2.12.2 Desventajas Ipv4

1. Obliga a depender de servicios que redirigen un host a una IP.
2. Es un protocolo usado paquetes conmutados de redes link Layer.

3. Utiliza registros de recursos (A) de dirección de host en el sistema de nombres de dominio (DNS) para correlacionar direcciones Ipv4 con nombres de host.
4. No hay ninguna identificación de flujos de paquetes para que los enrutadores guíen el QoS en el encabezado Ipv4.
5. Debe configurarse manualmente o a través de DHCP. (Fuentes, 2012, p. 13)

2.12.3 Ventajas de IPv6

- A través de IPv6 se genera un espacio de direcciones prácticamente infinita, con lo cual el sistema que corre en la infraestructura del Plenario de la Asamblea Nacional tendría la posibilidad de efectuar funciones con diferentes sistemas de votación en diferentes países.
- Ipv6 implementa otros protocolos como (IPsec)[1] para enviar paquetes de una forma más segura, de modo tal que se garantice la comunicación segura y fiable.
- Los protocolos AH[2] y ESP[3] brindan interoperabilidad, criptografía y alta calidad. Mejora el protocolo IP original facilitando autenticidad, confidencialidad, integridad y control de acceso a cada paquete IP.
- Sustituye ARP por el protocolo de detección de vecinos (ND). En IPv6 no hay necesidad de utilizar ARP, ya que el ID[4] de una dirección Ipv6 L3 se deriva directamente desde una dirección L2. Como resultado, los problemas de seguridad existentes con ARP, no aplican en Ipv6 utilizándose un nuevo protocolo llamado ND[5] definido como RFC 486111.
- Posee una mejor planificación de estructura de direccionamiento, por lo que los riesgos asociados a las nuevas IP se reducen. Permite simplificar a su vez las listas de control de acceso, las reglas de cortafuegos en operaciones de seguridad y también identificar la propiedad de sitios, enlaces e interfaces fácilmente.

[1] IP Security
[2] Encabezado de Autenticación
[3] Encapsulado de la Carga de Seguridad
[4] Identificador de Interfaz
[5] Descubrimiento de vecinos

- Cuenta con la dirección IEEE EUI-6412, la cual representa un nuevo estándar para el direccionamiento de la interfaz de red en Ipv6.
- El tiempo de procesamiento de los paquetes dentro de los routers es resuelto con la arquitectura jerárquica del protocolo IPv6, con esto se resuelve el problema generado por el protocolo IPv4 que consiste en el crecimiento exponencial de las tablas de ruteo dentro de los routers debido a su arquitectura plana, la cual genera un retardo en el proceso dentro del router para encontrar la ruta destino del paquete especifico.
- En el protocolo IPv6, se evita la configuración manual de los dispositivos antes de su conexión a la red, mediante mecanismos de autoconfiguración de direcciones, mientras que en el protocolo IPv4 la configuración debe realizarse manualmente. (Fernández F. , 2013)
- En IPv6 no hay direcciones broadcast. IPv6 codifica un alcance, estableciendo el dominio de alcance de un paquete multicast, algo que no es posible con el protocolo IPv4.
- En IPv6 la seguridad es un aspecto obligatorio y no adicional como en IPv4. En IPv6 se tienen una total integración de los mecanismos de seguridad, autenticación y confidencialidad, dentro del núcleo del protocolo.
- En IPv6 se introduce un mecanismo poderoso de control de flujo, asignación de prioridades diferenciadas según los tipos de servicios. En IPv4 dicha identificación de clase de servicio no es obligatoria. (Fernández F. , 2013)

2.12.4 Desventajas

- La necesidad de mantener un soporte permanente. Necesita algún tipo de NAT en los routers pasarela o una dirección Ipv4.
- En la actualidad una gran parte de las redes son Ipv4, por lo cual la implementación completa de Ipv6 costaría mucho y demoraría, mientras tanto se requieren la implementación de los mecanismos de transición para la interacción de las dos redes. (Fernández F. , 2013)

- No puede resolver todos los problemas de seguridad, sobre todo los ataques a capas, así como los ataques de fuerza bruta, ataques de adivinación de contraseñas en los módulos de autenticación, desbordamiento de búfer, virus y códigos maliciosos.
- Los ataques de denegación de servicio continúan presentes con Ipv6, así como los que se realizan a través de las técnicas de redes sociales como spamming de correo electrónico.

2.13 Mejores prácticas Ipv6

Seguidamente, se definen algunas prácticas recomendadas para referencia en la construcción y mantenimiento de IPv6 de forma segura:

- Utilizar direcciones estáticas no estándar para sistemas críticos.
- Asegurar una capacidad de filtrado adecuada para IPv6.
- Filtre las direcciones IPv6 de uso interno en los routers fronterizos.
- Bloquear todo el tráfico IPv6 en redes IPv4.
- Filtrar servicios innecesarios en el cortafuego.
- Desarrollar una política de filtrado granular ICMPv6 y filtrar todo el mensaje ICMP innecesario.
- Mantener la seguridad del host y de la aplicación con una política de seguridad coherente tanto para IPv4 e IPv6.
- Utilizar IPsec para autenticar y proporcionar confidencialidad a los activos.
- Documentar los procedimientos para el rastreo de último salto.

2.14 Mecanismos para la transición de Ipv4 a Ipv6

El proceso de transición de Ipv4 a Ipv6 no se podrá realizar de un día para el otro ya que las dos versiones de Ip deberán convivir durante algunos años. Es decir que el protocolo Ipv6, se puede implementar como una actualización de software en los nodos Ipv4 actuales, para esto, se define un tiempo de

transición con el objetivo de minimizar los costes de los nuevos equipos y cuidar las versiones realizadas en las empresas tecnológicas. (6SoS, 2015)

Es muy complejo saber cuándo las operadoras en Internet podrán migrar a la tecnología Ipv6 debido a que en la actualidad la mayoría de las operadoras utilizan nodos Ipv4 y con esta situación resulta difícil lograr una mayor motivación para el cambio.

Las características de configuración hacen que las redes Ipv6 sean más fáciles de configurar y mantener, todo esto puede resultar novedoso para las operadoras debido a que pueden realizar un despliegue de infraestructura muy rápido. (6SoS, 2015, p. 36)

Además, es muy crucial tomar en cuenta que para ayudar en la migración, las aplicaciones Ipv6 deben funcionar utilizando tanto Ipv4 como Ipv6, por ejemplo los navegadores de internet.

Los mecanismos de transición se clasifican en 3 grupos importantes que son:

- Dual Stack (Doble Pila).
- Túneles.
- Traducción. (6SoS, 2015, p. 36)

2.14.1 Mecanismo Doble Pila (Dual stakc)

Este es uno de los métodos más utilizados en los procesos de transición, debido a que utiliza un nodo de doble pila IPv6/IPv4, que puede llegar a comunicarse tanto como un nodo IPv4 ó como un nodo IPv6, para lograr este proceso cada nodo IPv6/IPv4 debe tener configurado los dos tipos de direcciones.

La implementación del método Dual Stack permite desactivar o activar una de las pilas, por esta razón un nodo puede tener 3 modos de funcionamiento:

- Cuando la pila IPV4 se activa y la pila IPV6 se desactiva, se comporta como un solo nodo IPV4.
- Cuando la pila IPV6 se activa y la pila IPV4 se desactiva, se

comporta como un único nodo IPV6.

- Cuando se encuentran disponibles las pilas IPV4 e IPV6, el nodo puede usar los dos protocolos. (6SoS, 2015, p. 38)

Un nodo IPv4/IPv6 utiliza una dirección para cada versión de protocolo.

Es muy importante mencionar que IPv4 utiliza mecanismos de configuración para direcciones IPV4 (configuración estática o DHCP) e IPv6 utiliza mecanismos de configuración para direcciones IPV6 (configuración estática o automática).

El DNS es utilizado por las dos versiones de protocolos para resolver los nombres y direcciones IP. Un nodo IPv6/IPv4 necesita una resolución DNS capaz de resolver los dos tipos de registros de direcciones DNS. (6SoS, 2015, p. 38)

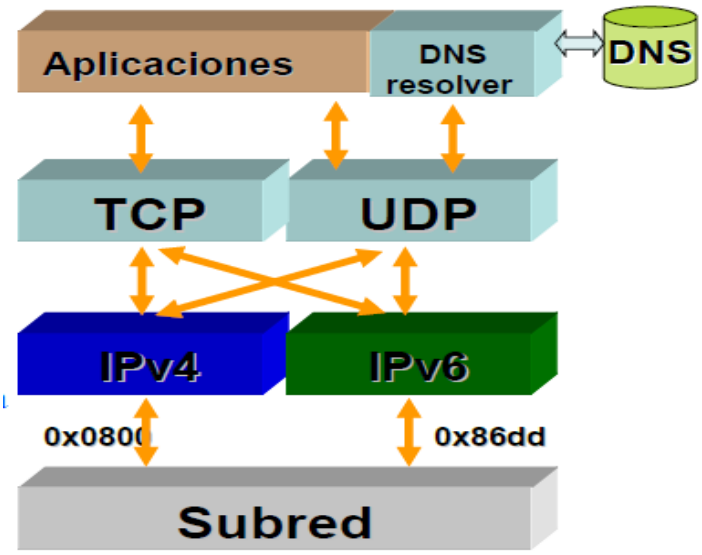


Figura 12: Resolucion DNS
Fuente: (6SoS, 2015, p. 39)

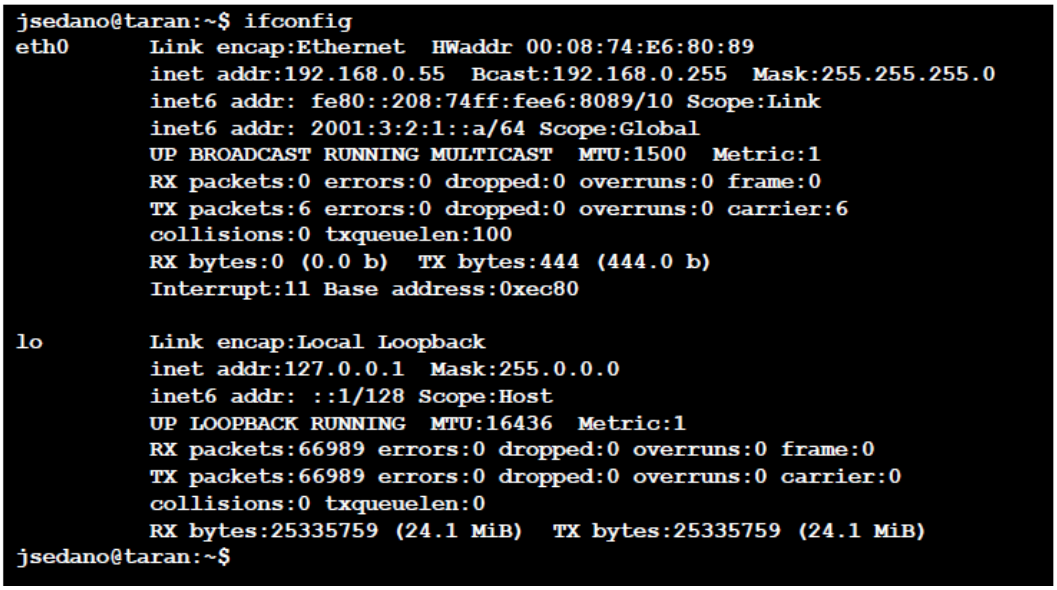


Figura 13: Configuracion DNS.
Fuente: (6SoS, 2015, p. 39)

2.15 Túneles

Este método permite transmitir paquetes IPv6 mediante una infraestructura IPv4, es decir se encapsula el contenido del paquete IPv6 en un paquete IPv4.

Ramón Millán (2001, parte II) se refiere a que el nodo IPv6 que está unido con el túnel, toma el paquete IPv6, y lo dispone en el campo de datos de un paquete IPv4. Este paquete IPv4 tiene como dirección de destino el nodo IPv6 en la parte final del túnel y es enviado al primer nodo IPv4 que es parte del túnel. Los nodos IPv4 del túnel orientan el paquete, sin tener certeza de que el paquete IPv4 que están manejando tiene un paquete IPv6. Por último, cuando el paquete llega al final del receptor IPv6 del túnel, este determina que el paquete IPv4 contiene un paquete IPv6 que debe ser extraído. (Perez, 2013, p. 18)

2.15.1 Túneles configurados

- Túneles usados extensivamente: mbone, multiprotocolo sobre IP, MIP.
- RFC 2893: Túneles Ipv6 en Ipv4.

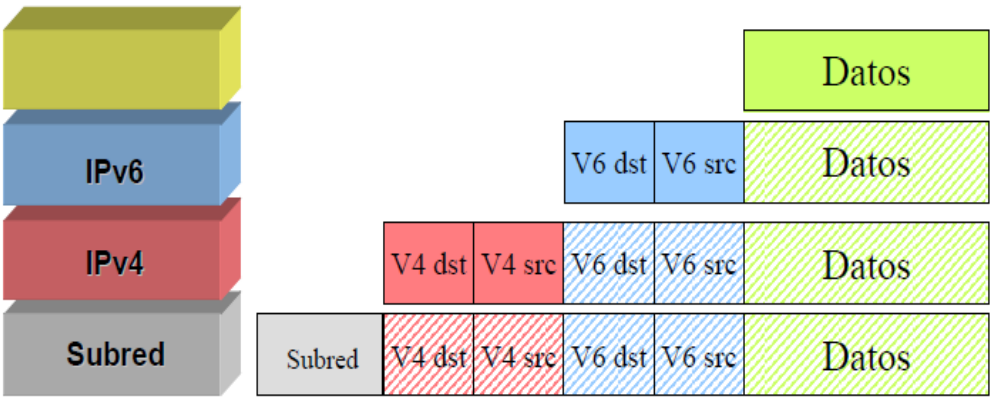


Figura 14:Túneles configurados
Fuente: (Perez, 2013, p. 20)

2.15.2 Túneles automáticos

Los nodos IPv6 pueden utilizar diferentes tipos de direcciones compatibles con IPv4, IPv6 ó 6to4, el túnel automático no es más que un túnel dinámico de paquetes IPv6 sobre una infraestructura de enrutamiento IPv4. La configuración de los túneles entre routers y host puede utilizarse de diferentes formas:

1. Router a Router: utiliza un mecanismo de túnel automático en donde los routers IPv6/IPv4 que están separados por una infraestructura IPv4 pueden encapsular paquetes IPv6 entre ellos mismos.

2. Host a Router: utiliza un mecanismo de túnel automático en el que un host IPv6/IPv4 encapsula paquetes IPv6 a un router intermedio IPv6/IPv4 que es accesible mediante una infraestructura de ruteo IPv4.

3. Host a Host: el mecanismo de túnel que utiliza es manual en donde los host IPv6/IPv4 que están interconectados por una infraestructura IPv4 pueden encapsular paquetes IPv6 entre ellos mismos.

4. Router a Host: utiliza un mecanismo de túnel manual en el cual los routers IPv6/IPv4 pueden encapsular paquetes IPv6 hacia su destino final. (Rivera J. , 2015)

2.15.2.1 Tunel 6to4

El método 6to4 define un mecanismo para que los sitios de IPv6 se puedan comunicar entre sí a través de la red IPv4 sin la necesidad de especificar una configuración explícita del túnel.

La red de área amplia IPv4 se trabaja como una capa de enlace punto a punto de unidifusión en la que los dominios de IPv6 se comunican por los routers 6to4 conocidos como puertas de enlace 6to4. Esto se realiza como un mecanismo de transición utilizado durante el período de coexistencia de IPv4 e IPv6. (Rivera J. , 2015)

"El método 6to4 utiliza el prefijo de dirección global:

2002:*WWXX*:*YYZZ*::/48

WWXX:YYZZ se refiere a la parte correspondiente al ID de agregación del siguiente nivel de una dirección global y la representación, en formato hexadecimal separado por dos puntos, de una dirección IPv4 pública (w.x.y.z) asignada al sitio o host. (Rivera J. , 2015)

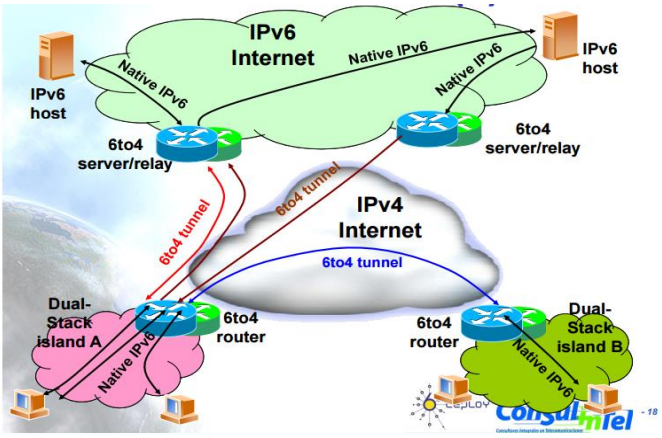


Figura 15:Método 6to4
Fuente: (Rivera J. , 2015)

2.15.3 Traducción

“Este método de traducción contribuye a un enrutamiento sencillo y claro de la comunicación entre varios nodos que sólo soportan a una versión del protocolo IP, o que utilizan Doble Pila. De igual modo, pueden operar de diversas formas o en capas distintas, traduciendo cabeceras IPv4 en cabeceras IPv6 y viceversa, actuando en el intercambio del tráfico TCP a UDP o realizando conversiones de direcciones”. (Rivera J. , 2015)

SIITIpv6 es evolución, no revolución:

- Misma filosofía.
- Muchos campos similares.

La traducción es posible y tiene sentido.

SIIT: Stateles IP/ICMP Translator, Traductor IP/ICMP sin estado.

- Marco de referencia para otros traductores. (Rivera J. , 2015)

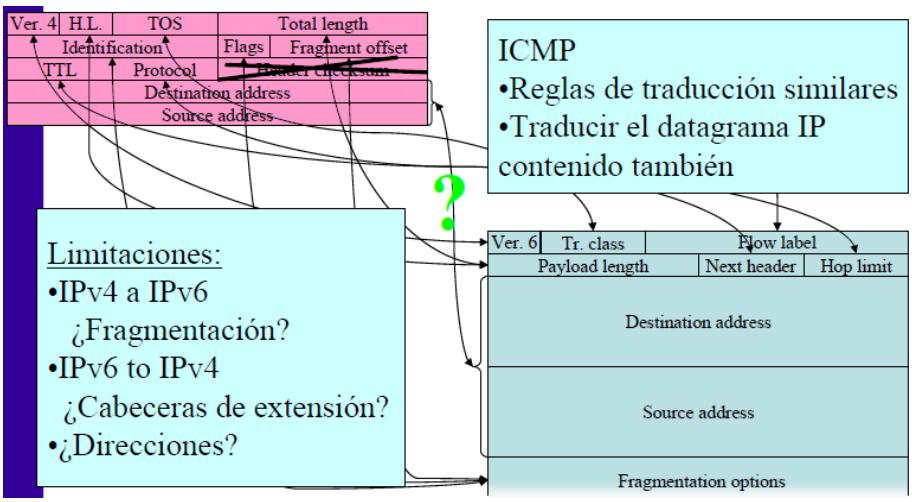


Figura 16: Método traducción

Fuente: (Rivera J. , 2015)

NAT-PT

NAT-PT RFC 2766 [Cn] (Network Address Translation – Protocol Translation /

Traducción de Direcciones de Red – Protocolo de Traducción) NAT-PT tiene la ventaja de no precisar cambios en los sistemas finales, pero es “con estado” por lo que es necesario el dispositivo NAT - PT para rastrear las sesiones activas. Todos los diagramas IP de entrada y salida en una sesión deberán ser encaminados a través del dispositivo NAT - PT. (Pérez, 2014, p. 31)

Además de la traducción de direcciones, el RFC define NAPT-PT (Network Address Port Translation - Protocol Translation / Traducción de Puertos en Direcciones de Red –Protocolo de Traducción), que permite la multiplexación de múltiples sesiones en una única dirección IPv4 mediante el uso del campo “port” en protocolos de capas superiores como TCP y UDP. Esto es igual a la multiplexación de puertos en entornos IPv4 (RFC 2663). (Pérez, 2014, p. 31)

El sistema de traducción NAT - PT. Asume lo siguiente:

- El sistema final IPv6 está en la misma subred que el dispositivo NAT - PT y usa una dirección de enlace local FECD:BA98::7654:3210 al comunicarse con el dispositivo NAT - PT.
- La sesión es establecida por el sistema final IPv6.
- El dispositivo NAT - PT tiene una colección de direcciones, incluida la subred 120.130.26.0/24, para asignar a las direcciones IPv6 de origen entrantes, en este caso, la dirección de enlace local anterior.
- El dominio IPv6 tiene asignado un PREFIJO: :/96, y el sistema final IPv6 usará este prefijo cuando se direccione el nodo IPv4 en un formato IPv6. Los paquetes IPv6 con dicho prefijo se encaminarán al dispositivo NAT - PT. La dirección de destino resultante es PREFIJO: v4, en donde v4 es la dirección IPV4 del sistema final IPv4. (Pérez, 2014, p. 32)

Cuando se establece una sesión desde un nodo “sólo IPv6” a un nodo “sólo IPv4”, el nodo IPv6 conocerá la dirección IPv4 del nodo de destino por medio de una consulta DNS. Este flujo de información se detalla en la figura (5.8). Cuando la sesión se inicia, el nodo IPv6 creará un paquete con lo siguiente:

- Dirección IPv6 de origen: FECD:BA98::7654:3210
- Dirección IPv6 de destino: PREFIJO: 132.146.243.30

En la recepción del paquete, el dispositivo NAT - PT asignará una de las direcciones IPv4 con que cuenta y esta dirección será utilizada como dirección origen cuando se encamine el paquete hacia el nodo IPv4. El paquete traducido resultante dispondrá de:

- Dirección IPv4 de origen: 120.130.26.10, asignada de la colección de direcciones IPv4.
- Dirección IPv4 de destino: 132.146.243.30, la dirección IPv4 del sistema final IPv4 (Pérez, 2014)

Esta correspondencia IPv6 a IPv4 existe mientras dura la sesión. Precisamente con base en que esta asociación de direcciones perdura, el tráfico de retorno será reconocido por el dispositivo NAT - PT en tanto pertenezca a la misma sesión. Como NAT - PT guarda el estado de la traducción, todas las sesiones se enrutarán a través del mismo dispositivo NAT -PT. (Pérez, 2014, p. 32)

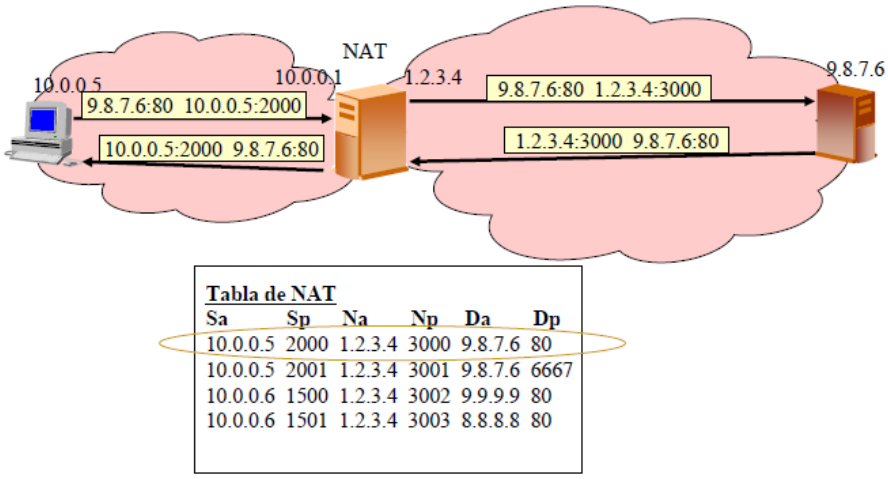


Figura 17: Método NAT
Fuente: (Pérez, 2014, p. 33)

TRT

Transport Relay Translation[6], es una de las varias técnicas de traducción que ayuda a que pueda haber comunicación entre los protocolos IPv4 con IPv6, TRT propone una traducción con una adaptación sencilla en comparación con

[6] Traductor de Transporte de Transmisión

los demás, esto se refleja en que no requiere demasiadas modificaciones en los nodos donde se implemente. (Pérez, 2014)

La técnica de transmisión de transporte no es nueva, se ha utilizado en varios sistemas relacionados con los firewalls, estos sistemas están diseñados para lograr lo siguiente:

- Prevenir el envío de ciertos paquetes IP a través del sistema.
- Ayudar el tráfico que va a través del sistema (Pérez, 2014)

112 A TRT se le ha reservado el prefijo IPv6 C6: /64, por lo que en la misma dirección IPv6 puede contener una dirección IPv4.

La información de encaminamiento debe ser configurada para que los paquetes C6: :/64 puedan ser enviados hacia el sistema TRT, además el prefijo fec0:0:0:1:/64 está reservado para mapeo de direcciones. Por ejemplo:

- Se considera un nodo destino IPv4 “exclusivo” y un nodo inicial IPv6 “exclusivo”.
- Cuando un nodo origen con una dirección IPv6 desea realizar una conexión con un nodo destino con una dirección IPv4, éste necesita realizar una conexión TCP/IPv6.
- Si la dirección de C6: :/64 es igual a fec0:0:0:1: :/64 y la dirección destino 10.1.1.1, la dirección destino que se usará es fec0:0:0:1::10.1.1.1.
- El paquete es enviado a través del sistema TRT, el sistema captura el paquete y obtiene la dirección destino verificando los primeros 32 bits de la dirección destino para obtener la dirección real IPv4, y el paquete se envía a su destino. (Pérez, 2014)

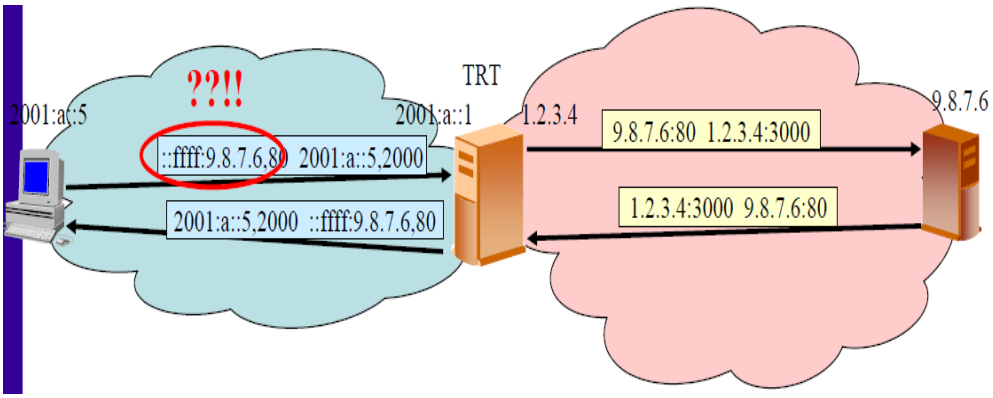


Figura 18:Método TRT
Fuente: (Pérez, 2014, p. 33)

2.16 Análisis comparativo entre los mecanismos de transición

Tabla 4: Cuadro comparativo de mecanismos de migración

Comparación entre mecanismos			
Descripción	**Dual Stack**	**Túnel**	**Traducción**
Implementación	Fácil de implementar, necesita que los hosts y los routers soporten las dos versiones de IP.	Más complejo	Más complejo
Aceptación	Máxima	Media	Media
Opciones	Obliga a cada ordenador a retener una dirección Ipv4.	Conecta nubes Ipv4 residuales a través de infraestructura Ipv6.	Requiere de ALG (Aplication Level Gateway) para convertir direcciones Ip Embebidas.

Escalabilidad	Alta	Media	Alta
Prestaciones	Alta	Media	Baja
Facilidad HA	Alta	Alta	Media
Impacto en Login	No	Si	No

Elaborado por: el autor

2. 17 Mecanismo seleccionado para la transición

Para realizar la migración del Plenario luego llevar a cabo un análisis de los distintos mecanismos existentes para la transición, se ha seleccionado el mecanismo Dual Stack, debido a que es muy utilizado por las bondades que brinda. Este mecanismo según lo analizado anteriormente brinda opciones de conexión exclusivamente con nodos Ipv4 al permitir la opción de desactivar el nodo Ipv6, algo que ocurre de forma similar con el protocolo Iv6 cuando se desactiva el nodo ipv4. También permite recibir y entender un datagrama Ipv6 o Ipv4 al poder activar los dos nodos a la vez. Por esta razón y dadas las características de la red del Plenario se selecciona este mecanismo como idóneo ya que brinda la opción de configurar la red del plenario posibilitando la comunicación independientemente de la configuración que tengan los demás nodos que estén conectados a la red.

Capítulo III: Estructura de la red

3.1 Identificación de la red

En esta etapa se realiza el diseño del diagrama de red del Plenario, el cual permite representar gráficamente los elementos que intervienen en la red de este lugar. El diagrama brindara la posibilidad de tomar decisiones respecto a la configuración de la red. La misma está constituida por la interconexión de datos de la Asamblea. En la siguiente figura se muestra la estructura que tiene este local.

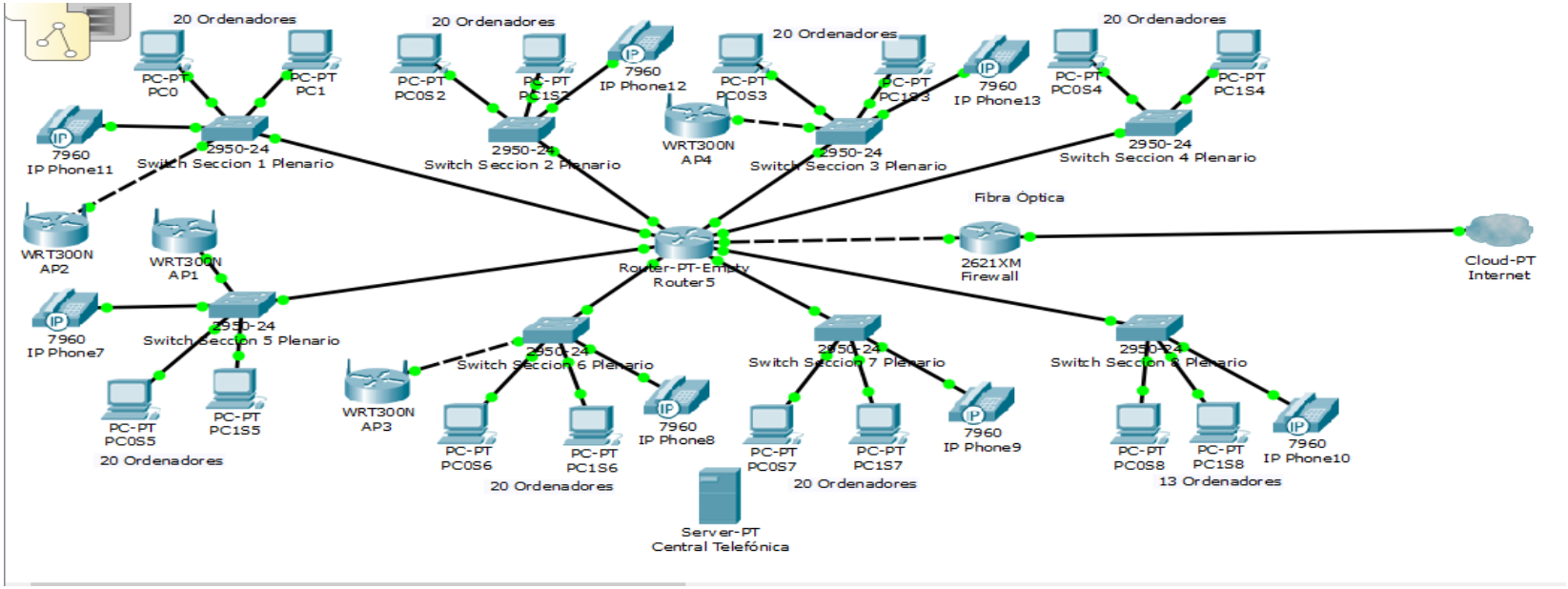


Figura 19: Topología referencial del Plenario de la Asamblea Nacional
Elaborado por: el autor

El enlace a internet del Plenario es otorgado por la Corporación Nacional de Telecomunicaciones (CNT) a una velocidad de 1GbPs.

La red del Plenario, permite la comunicación desde el switch principal hacia cada uno de los 8 switch que respaldan a los ordenadores. El router principal tiene la tarea de direccionar los mensajes según viajen a través de la red.

Los switch permiten interconectar la subred de Plenario con el resto de las subredes de la Asamblea Nacional y establecer una conexión con el switch principal de la institución.

De los nueve switch, ocho tienen 48 puertos y 1 cuenta con un total de 24.

Copio textualmente la sugerencia de la revisión anterior: “Aquí aumenta dos esquemas donde se pueda mirar el cableado horizontal y el vertical. Luego, aumenta un esquema por cada piso y finalmente, aumentas un esquema de la conexión hacia el Internet tomando en cuenta: el router, el firewall, servidor proxy, etc., etc.”

A continuación, se describen las funciones de los servidores:

Tabla 5: Función de los servidores

Servidor	**Actividad**
Correo	Permite recibir, enviar, almacenar y realizar otras operaciones referentes al email a los trabajadores del Plenario.
Aplicaciones	Permite el procesamiento de datos de un sistema a las computadoras cliente. También disminuye la complejidad del desarrollo de sistemas, debido a que las aplicaciones no necesariamente deben ser programadas, sino que son ensambladas desde los bloques que provee este servidor.

Base de Datos	Brinda los servicios de bases de datos a programas o computadoras.
Voto Electrónico (Jboss)	Brinda los servicios necesarios para el sistema de voto electrónico.

Elaborado por: el autor

Actualmente la estructura de la red en el protocolo Ipv4 del Plenario mantiene un funcionamiento correcto.

El enfoque de este análisis es mantener el diseño de la red del Plenario con Ipv4 y poder migrar a Ipv6, permitiendo la conexión de esta red hacía internet. Así la red del Plenario podrá contar con acceso a internet a través del protocolo Ipv6. De esta forma se dará el primer paso hacia la futura migración de la Asamblea Nacional.

En este punto, después de hacer el análisis de la red actual, deberías encontrar las desventajas encontradas en el capítulo 2, de la misma, de modo que se justifique la migración a IPv6.

También se debería encontrar el justificativo del porqué seleccionaste el método indicado en el capítulo 2 para migrar de ipv4 a ipv6

3.1.1 Tráfico de red

El servicio de análisis y diagnóstico de redes permite encontrar deficiencias en la red de datos y sus causas, u oportunidades de mejora y formular acciones correctivas y de mejoramiento. Este servicio se complementa con el de optimización de la red, en donde se implementan estas acciones mediante un plan acordado con el usuario final. (Bartolo, 2013)

La importancia de realizar el monitoreo de la red del Plenario es evaluar el consumo de tráfico y el rendimiento de cada componente, de esta forma detectar cuellos de botella que puedan surgir al aumentar la demanda de recursos. Algunos dispositivos fueron analizados para conocer si cuentan con la capacidad necesaria para soportar más carga de trabajo. Si se llega a saturar algún componente de la red, se puede producir un colapso de servicio y sufrir una disminución del desempeño.

El objetivo del análisis del tráfico para tu estudio no es el que indicas en la parte de arriba, el que debería ser es: demostrar que con ipv4 el consumo de la red aumenta Vs el uso de IPv6, justamente corroborando con lo que dice la teoría del ipv6.

El monitoreo de redes permite:

- Lograr una eficiencia mayor de la red sin tener que aumentar el ancho de banda.
- Analizar cuáles son las características de la res y avizorar un aumento de la capacidad en los equipos en caso de ser necesario.
- Obtener reportes sobre el estado de la res a través de las consolas.
- Controlar y administrar las redes remotas.
- Configurar los dispositivos locales y remotos.
- Solucionar los problemas que se puedan presentar en las redes locales y remotas.
- Analizar el tráfico de la red mediante en el tiempo.

Para realizar el monitoreo del Plenario el software seleccionado fue el Wireshark, el cual analiza los protocolos open source disponible para plataformas Windows y Unix. Hoy en día es una excelente herramienta para solucionar problemas de red.

Según Belda (2012) Wireshark implementa una amplia gama de filtros que facilitan la definición de criterios de búsqueda para los más de 1100 protocolos soportados actualmente (versión 1.4.3); y todo ello por medio de una interfaz sencilla e intuitiva que permite desglosar por capas cada uno de los paquetes capturados. Gracias a que Wireshark “entiende” la estructura de los protocolos, podemos visualizar los campos de cada una de las cabeceras y capas que componen los paquetes monitorizados, proporcionando un gran abanico de posibilidades al administrador de redes a la hora de abordar ciertas tareas en el análisis de tráfico. (p. 5)

En esta ocasión se realizó el monitoreo desde un ordenador conectado al switch # 1, vea figura (17) el mismo está conectado al router del plenario. Con ello se pudo analizar todo el tráfico de la red del plenario. El periodo de análisis estuvo comprendido ente el 10 y el 13 de Enero.

Para ver el análisis y la descripción de los gráficos observe el anexo # 1.

No veo un análisis del tráfico, lo que veo es una descripción de las gráficas, no considero necesario para nuestro estudio hacer el análisis de rendimiento de los equipos, los que deberías tratar de justificar en este anexo, es que con ipv4 el consumo de la red en mayor que con ipv6, para esto, puedes hacer el análisis de la red ipv4 que tienes funcionando, y para comparar con el consumo de ipv6, puedes hacerlo comparando con los resultados reportados en la literatura o creándote una red de pruebas ipv6.

3.1.2 Estructura del cableado

En este epígrafe se analizará la situación actual de la red Ipv4 para conocer la ubicación, los tipos de medio y las características de los equipos. Ello permitirá constatar si el Plenario cuenta con las instalaciones necesarias y los equipos adecuados para poder realizar la migración.

El cableado para las estaciones de trabajo se distribuye a través de canaletas Dexon Schneider Electric DXN11094 40x40. Se encuentran fijadas sobre la pared para separar el cableado de datos del cableado eléctrico.

3.1.2.1 Cableado Horizontal

El IDF[7] se encuentra ubicado en el cuarto de control del Voto Electrónico. El mismo cuenta con las siguientes características:

Características de los IDF:

- Los IDF tienen 2 m cuadrados (2m x 2m)

[7] Servicios de distribución intermedia

- pasantes circulares de 80 mm con flexiducto para permitir la pasada de los cables de las redes de datos y telefónica hacia el Plenario.
- Pintados internamente con pintura anti hongos.
- Las puertas de los IDF son laminas pintadas de negro No. 20.
- Llavines maestrados.
- tomacorrientes dobles polarizados debidamente y con conexión a la tierra del edificio.
- Temperatura ambiente promedio de 16˚ C.
- Una lámpara incandescente en cada uno.
- Los pisos tienen un acabado de baldosa, el cual evita que los equipos adquieran polvo.
- Las paredes son de cemento y cubiertas con pintura antinflama para evitar incendios que puedan ocurrir.

Los IDF se conforman de:

- Racks cerrados o abiertos.
- Patch Panel.
- Gabinetes.

Seguidamente se describen las características de gabinetes y racks ubicados en el IDF del Plenario:

Racks

Tabla 6: Rack. Características.

Cisco R42610	Estándar	Expansión
Dimensiones (A x L x P)	78.74 x 24 x 43.38 in. (/2000 x 610 x 1102 mm)	78.74 x 23.58 x 43.38 in. (/2000 x 599 x 1102 mm)
Dimensiones (H x L x P) con embalaje	89 x 33 x 47 in. (/2261 x 838 x 1194 mm)	89 x 33 x 47 in. (/2261 x 838 x 1194 mm)
Peso con embalaje	354 lb (/161 kg)	284 lb (/129 kg)

Paneles laterales incluidos	Yes	No
Capacidad de montaje del equipo	42RU	42RU
Capacidad de carga estática	2100 lb (/954 kg)	2100 lb (/954 kg)

Elaborado por: el autor

Patch

Tabla 7: Patch Panel. Características

Características	
Puertos	24
Altura	1U (44.4mm)
Incluye	24 Snap-In Tipo Cat 6 Keystone jacks, 24 Puertos Panel de Parche, Organizador Wire, Tie Wraps, Tornillos,
Ancho	19 pulgadas
Herramienta	Punzonado
Etiquetado	Campo de etiquetado claro

Elaborado por: el autor

3.1.3 Dispositivo de trabajo

Seguidamente se muestran las características fundamentales de los equipos y los elementos del área de trabajo.

Cable UTP

Tabla 8: Cable UTP. Características

Características

Características	Conductor de cobre sólido de 0.57 mm. Diámetro exterior 6.1 mm. Tipo de aislamiento: Polietileno Impedancia 100Ω
Aplicaciones	100 BASE VG ANYLAN, 1.2 Gbps ATM, 622 Mbps ATM, Video digital, 100 Base T, 100 Mbps TP-PMD, 1000 Base T, Video Banda Base y Banda Ancha.
Normas a aplicar	NMX-I-248-NYCE-2005, ANSI/TIA/EIA 568B.2-1, ANSI/ICEA S-102-700, NEMA WC66 ISO/IEC 11801 (2a edición, clase E), EN 50173-1, UL.

Elaborado por: el autor

Patch Cord

Tabla 9: Patch Cord. Características

Características
Conductor: 7 hilos de cobre de Ø0.20 mm. Aislamiento: polietileno fuertemente resistente Diámetro del conductor en el aislamiento: 0.98±0.05 mm Cantidad de pares: 4 Colores de los pares trenzados: azul-blanco/azul, naranja- blanco/naranja, verde-blanco/verde, marrón-blanco/marrón Forro: PVC Ø6.2±0.2 mm

Elaborado por: el autor

3.2 Diseño y obtención del diagrama Lógico

El diagrama lógico incluye la descripción entre la conexión de los equipos: switch, firewall, servidores, acces point, estaciones de trabajo y ruoters.

La topología de la red permite definir la estructura de la misma. La topología lógica está compuesta por la topología física que describe la posición de los medios y cables y por la parte lógica que describe como accede un host a los medios para enviar datos.

La topología de la red del Plenario tiene una estructura estrellada, ya que permite la conexión de los dispositivos individuales entre sí.

Para realizar el diseño de la topología de la red, así como el diagrama físico anteriormente mostrado se utilizó el software Pack Trace en su versión 6.3.0. El mismo permite crear topologías de red, insertar paquetes y configurar dispositivos y ayudar de esta forma a simular redes de manera interactiva.

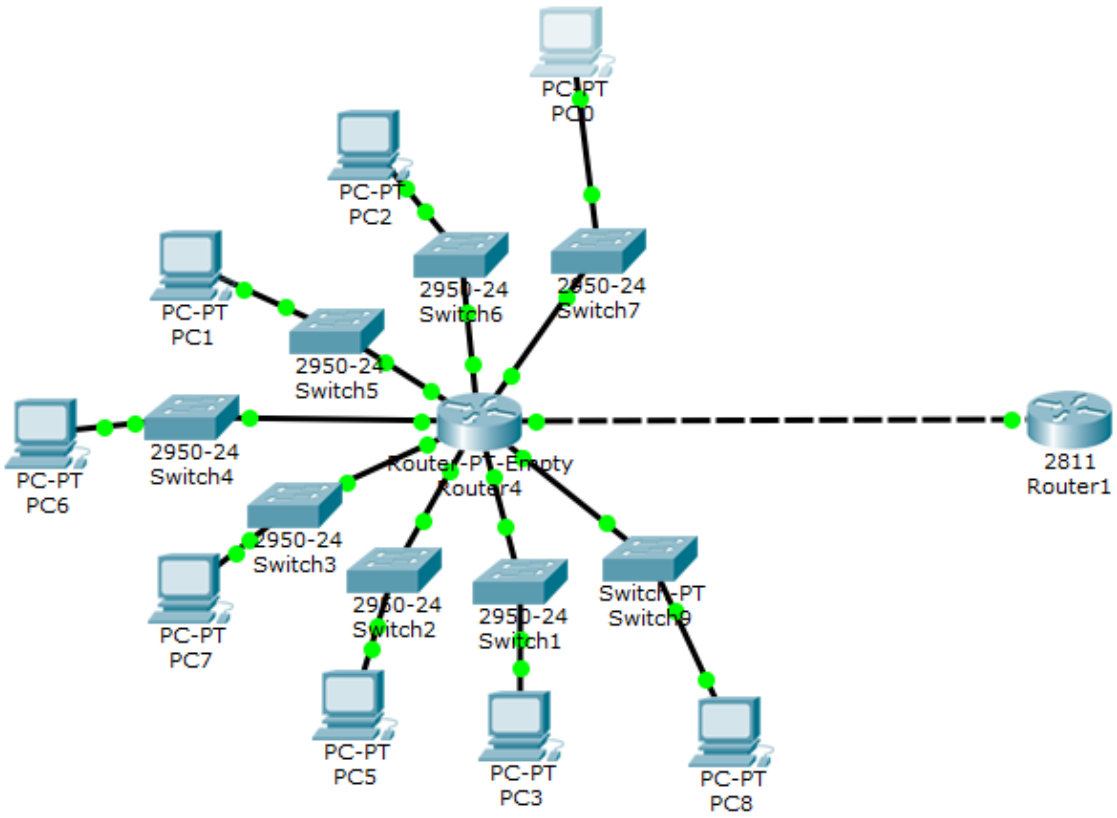


Figura 20: Topología de la red del Plenario.
Fuente: el autor

Este tipo de topología supone una ventaja para la red del Plenario, ya que, si algún dispositivo se ve afectado, el resto de los dispositivos no se verán en problemas, por el contrario, el resto de la red mantendrá la comunicación.

3.3 Diseño de las Vlans

Para lograr la eficiencia del ancho de banda, la seguridad de acceso a la red y la sencillez en la administración de dicha red se utiliza el diseño de las Vlans.

Se han diseñado 8 Vlans, las cuales contribuirán a obtener mayores beneficios dentro de la red del plenario. Las mismas han quedado distribuidas de la siguiente forma:

Tabla 10: Vlans

Detalles de las Vlans	
No. Vlan	**Nombre**
1	Servidores
2	Administración
3	Asambleístas
4	Comisión
5	Móvil
6	Invitados
7	Presidencia
8	Funcionarios

Elaborado por: el autor

3.3.1 Conectividad entre las Vlans

Se establecen las reglas de conectividad entre las Vlans con el objetivo de facilitar el acceso a algunos departamentos que manejan información similar y negarlo en caso de no ser así.

Seguidamente se presenta una tabla con un resumen de las reglas de acceso entre las Vlans configuradas.

Tabla 11: Acceso entre Vlans

Detalles de las Vlans	
Vlan	**Acceso**
1 Servidores	___
2 Administración	1,2,3,4,5,6,7,8
3 Asambleístas	4,6
4 Comisión	3
5 Móvil	___
6 Invitados	___
7 Presidencia	3,4,6,8
8 Funcionarios	___

Elaborado por: el autor

Como se puede observar las Vlans independiente manejan información única y están representadas con el signo ¨__¨.

Otras áreas manejan la información similar por lo que es importante estableces y mantener la comunicación entre ellas.

3.3.2 Direcciones Ipv4. Distribución

Las direcciones IP permiten identificar una computadora conectada a la red, a la par que la red de datos facilita la comunicación entre los dispositivos de red y los usuarios finales.

Generalmente las empresas cuentan con una dirección IP, la cual se calcula partiendo de la cantidad de ordenadores con los que se cuente y el posible crecimiento de la red.

Para el desarrollo del proyecto se tomará una dirección privada clase C: 192.30.0.0/16

Dirección IP en formato	192.168.0.0
Dirección IP en formato	10101100.10101000.00000000.0000
Mascara de red:	223.255.255.255

En la siguiente tabla se puede observar el número de ordenadores que posee cada dirección Ipv4 y compararlo con el total de ordenadores requeridos.

Seguidamente se muestra el porcentaje del posible crecimiento de la red del Plenario:

Tabla 12: Crecimiento futuro. Porcentaje

Detalles de las Vlans			
Subred	**PC**	**Crecimiento (%)**	**Total**
Administración	20	18	24
Asambleístas	23	10	25
Comisión	25	15	29
Móvil	20	20	24
Invitados	25	25	31
Presidencia	20	15	23
Funcionarios	20	10	22
Total	**153**	Total	**178**

Elaborado por: el autor

Seguidamente se muestran las direcciones Ipv4 para cada subred:

Tabla 13: Direcciones para cada subred

Detalles de las Vlans

Subred	Direcciones	Máscara
Administración	192.168.0.0/24	255.255.255.0
Asambleístas	192.168.1.0/24	255.255.0.0
Comisión	192.168.2.0/24	255.255.0.0
Móvil	192.168.3.0/24	255.255.0.0
Invitados	192.168.4.0/24	255.255.0.0
Presidencia	192.168.5.0/24	255.255.0.0
Funcionarios	192.168.6.0/24	255.255.0.0
Servidores	192.168.7.0/24	255.255.0.0

Elaborado por: el autor

En la siguiente tabla se podrá observar los datos del proceso de configuración entre las Vlans y el router principal.

Tabla 14: Configuración entre las Vlans.

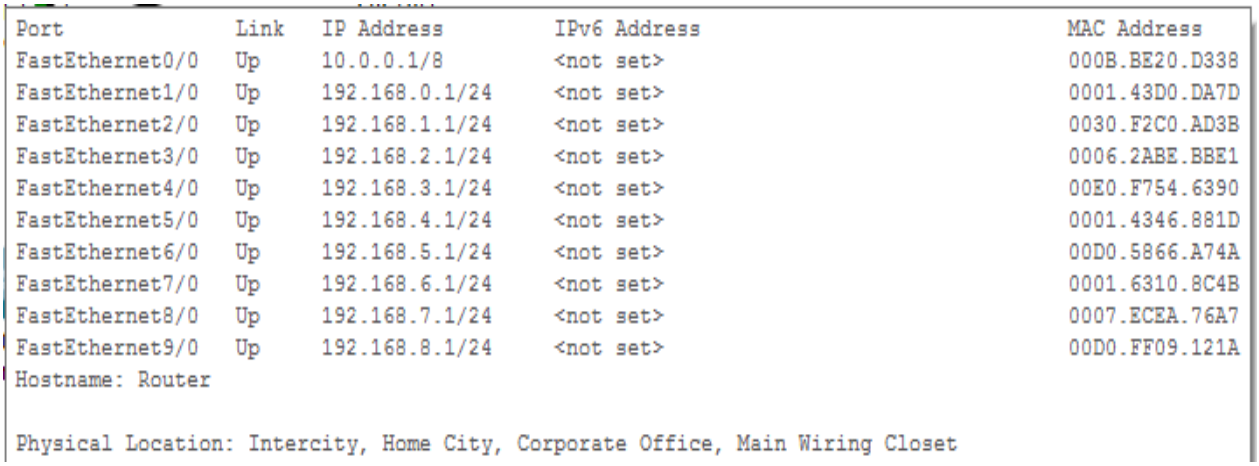
Detalles de las Vlans		
Vlan	**Interfaz**	**Dirección de la sub_interfaz**
Administración	fa1/0	192.168.1.1/24
Asambleístas	fa2/0	192.168.2.1/24
Comisión	fa3/0	192.168.3.1/24
Móvil	fa4/0	192.168.4.1/24
Invitados	fa5/0	192.168.5.1/24
Presidencia	fa6/0	192.168.6.1/24
Funcionarios	fa7/0	192.168.7.1/24
Servidores	Fa8/0	192.168.8.1/24

Elaborado por: el autor

3.3.3 Tablas de enrutamiento

El tipo de enrutamiento para la red del plenario es dinámico, por lo tanto, el administrador podrá configurar la información sobre las redes remotas en el router a través del nombre del host.

Seguidamente se muestra la tabla de enrutamiento del router del Plenario:



Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	10.0.0.1/8	<not set>	000B.BE20.D338
FastEthernet1/0	Up	192.168.0.1/24	<not set>	0001.43D0.DA7D
FastEthernet2/0	Up	192.168.1.1/24	<not set>	0030.F2C0.AD3B
FastEthernet3/0	Up	192.168.2.1/24	<not set>	0006.2ABE.BBE1
FastEthernet4/0	Up	192.168.3.1/24	<not set>	00E0.F754.6390
FastEthernet5/0	Up	192.168.4.1/24	<not set>	0001.4346.881D
FastEthernet6/0	Up	192.168.5.1/24	<not set>	00D0.5866.A74A
FastEthernet7/0	Up	192.168.6.1/24	<not set>	0001.6310.8C4B
FastEthernet8/0	Up	192.168.7.1/24	<not set>	0007.ECEA.76A7
FastEthernet9/0	Up	192.168.8.1/24	<not set>	00D0.FF09.121A

Hostname: Router

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

Figura 21: Enrutamiento del router del Plenario
Fuente: el autor

3.3.4 Características de los equipos de red

Servidores

Tabla 15: Servidor de Correo. Características

Correo	
Marca	IBM
Memoria	DDR3 - SDRAM - DIMM 240-pin - 1333
Procesador	Intel Xeon X3430 (2.4 Ghz/L3 8MB/1333 Mhz)
Modelo	System x3100 M4
Tarjeta de red	2 x Gigabit Ethernet.
Disco Duro	750 Gb

Puerto	Frontal: Usb2, Posterior: Seriales: 2, Paralelo: 1, RJ-45: 1, DB-15: 1, USB: 4.
Sistema Operativo	
Soporta Ipv6	S i

Elaborado por: el autor

Tabla 16: Servidor de aplicaciones. Características

Aplicaciones	
Marca	IBM
Memoria	DDR3 - SDRAM - DIMM 240-pin - 1333
Procesador	Intel Xeon X3430 (2.4 Ghz/L3 8MB/1333 Mhz)
Modelo	System x3100 M4
Tarjeta de red	2 x Gigabit Ethernet.
Disco Duro	1Tb
Puerto	Frontal: Usb2, Posterior: Seriales: 2, Paralelo: 1, RJ-45: 1, DB-15: 1, USB: 4.
Sistema Operativo	
Soporta Ipv6	S i

Elaborado por: el autor

Tabla 17: Servidor de BD. Características

Base de Datos	
Marca	IBM
Memoria	DDR3 - SDRAM - DIMM 240-pin - 1333

Procesador	Intel Xeon X3430 (2.4 Ghz/L3 8MB/1333 Mhz)
Modelo	System x3100 M4
Tarjeta de red	2 x Gigabit Ethernet.
Disco Duro	750 Gb
Puerto	Frontal: Usb2, Posterior: Seriales: 2, Paralelo: 1, RJ-45: 1, DB-15: 1, USB: 4.
Sistema Operativo	
Soporta Ipv6	S i

Elaborado por: el autor

Tabla 18: Servidor de Voto Electrónico. Características

Voto Electrónico	
Marca	IBM
Memoria	DDR3 - SDRAM - DIMM 240-pin - 1333
Procesador	Intel Xeon X3430 (2.4 Ghz/L3 8MB/1333 Mhz)
Modelo	System x3100 M4
Tarjeta de red	2 x Gigabit Ethernet.
Disco Duro	1TB Gb
Puerto	Frontal: Usb2, Posterior: Seriales: 2, Paralelo: 1, RJ-45: 1, DB-15: 1, USB: 4.
Sistema Operativo	
Soporta Ipv6	S i

Elaborado por: el autor

A continuación, se muestra el diseño del diagrama físico de la red del Plenario:

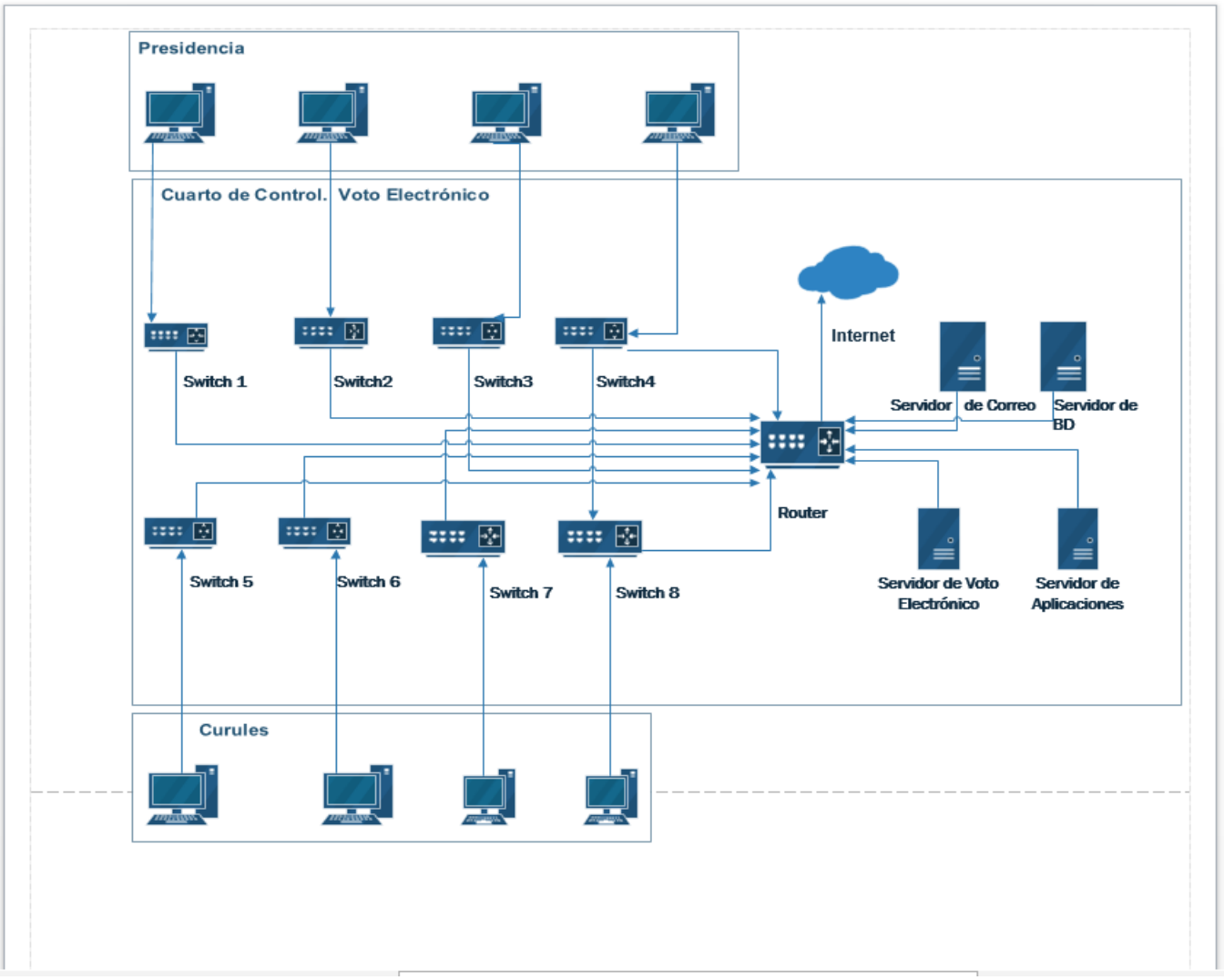


Figura 22: Diagrama Físico del Plenario.
Fuente: el autor

PC´s

Tabla 19: Prestaciones de ordenadores curules

Característica	Detalle
Marca	Pioneerpos Stealthtouch m5
Memoria	4GB
Procesador	Intel Core 2 Duo
Velocidad	2.5 GHZ
Tarjeta de red	10/100 Mbps

Disco Duro	320 GB
Sistema Operativo	Ubuntu 16.4
Soporta Ipv6	Si

Elaborado por: el autor

Tabla 20: Prestaciones de ordenadores de la presidencia

Característica	Detalle
Marca	Pioneerpos Stealthtouch m5
Memoria	8GB
Procesador	Intel Core 2 Duo
Velocidad	2.5 GHZ
Tarjeta de red	10/100 Mbps
Disco Duro	640 GB
Sistema Operativo	Ubuntu 16.4
Soporta Ipv6	Si

Elaborado por: el autor

Firewall

Tabla 21: Prestaciones del firewall

Característica	Detalle
Marca y Modelo	Cisco ASA 5500
Número de usuarios	Ilimitado
Conexiones por segundo	9000
E/S Integrada	FE de 5 puertos/ 10/100/1000 de 2 puertos, FE de 3 puertos

Fuentes de alimentación dobles	No disponibles
Capacidad de procesamiento con inspección de paquetes e información de estado	1 Gbps
Sesiones simultáneas	50 000 / 130 000

Elaborado por: el autor

Router

Tabla 22: Prestaciones del router

Característica	Detalle
Marca y Modelo	Cisco ASR 9922
Dimensiones	75.25 in. x 17.75 in. x 28.65 in.
Peso	12,4 Kg
Memoria Dram	75.25 in. x 17.75 in. x 28.65 in.
Protocolos de administración remota	SNMP3
Voltaje	AC 120/230 V (50/60 Hz)
Estándares	IEEE 802.3af

Elaborado por: el autor

Switch

Tabla 23: Prestaciones de los switch

Característica	Detalle
Modelo	Cisco 3702
Número de puertos	48 x 10/100 + 4 x SFP
Algoritmo de encriptación	SSL

Estándares	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1x, IEEE 802.1
Protocolo de enrutamiento	RIP-1, RIP-2, Enrutamiento Estático
Interfaces	48 x 100 Base-T/100 Base -TX-RJ-45
Voltaje	AC 120/230 V (50/60 Hz)
Dimensiones	42.8 cm x 28.2 cm
Software	4.2 Kg
Soporta Ipv6	Si

Elaborado por: el autor

Teléfonos IP

Tabla 24: Prestaciones de los teléfonos IP.

Característica	Detalle
Marca/Modelo	CISCO 7911G
Protocolos	SCCP
Visualizador	Pantalla de cristal líquido-monocromo
Cantidad de puertos de red	2 x Ethernet 10/100Base TX
Códec de voz	G.711, G.729
Dirección Ip. Asignación	DHCP
Propiedades de voz	Generación de ruido confortable (CNG), detección de actividad de voz (VAD)
Normas	EN55022, ICES-003, IEC 60950, EN 61000-3-3, CSA 22.2 No. 950, UL, VCCI, CISPR 22 Class B, EN 60950, EN 61000-3-2.
Peso	0.8 Kg
Dimensiones	16.4 cm x 14.8 cm x 19.8 cm

Elaborado por: el autor

Capítulos IV: Resultado del estudio

4.1 Metodología de implementación de la red IPv6

En este epígrafe se desarrollará una simulación de la red del Plenario haciendo uso del Pack Tracer con el objetivo de mostrar el mecanismo de transición de protocolo Dual Stack. Este método permite los routers y host se equipen con una pila para cada protocolo con el objetivo de poder recibir y enviar ambos tipos de paquetes (Ipv4 e Ipv6)

Haciendo uso de este método, se podrá obtener como resultado que, una vez que sea establecida la comunicación con un nodo Ipv6 el nodo Ipv6/Ipv4 funcionará como un solo nodo Ipv6. Por otro lado, cuando la comunicación sea establecida con un nodo Ipv4, este funcionará como un solo nodo Ipv4.

Todos los nodos Ipv6/Ipv4 deberán ser configurados con dos direcciones IP, usando diversos mecanismos. Para Ipv4 se utilizará el mecanismo DHCP el cual obtiene una dirección Ipv6, por su parte para Ipv6 el mecanismo DHCPv6, el cual logra obtener una dirección Ipv6.

Este método de transición llamado Dual Stack facilita la implementación y gestión del protocolo Ipv6, ya que se trabaja gradualmente, o sea permite configurar secciones pequeñas de la red. Esto permite solucionar la no existencia del protocolo Ipv4 3n un futuro ya que solo se deshabilitaría la pila de Ipv4 para cada nodo. Otra de las grandes ventajas que posee esta metodología es que facilita la reducción del impacto de funcionalidad de las aplicaciones, tiempo y costo.

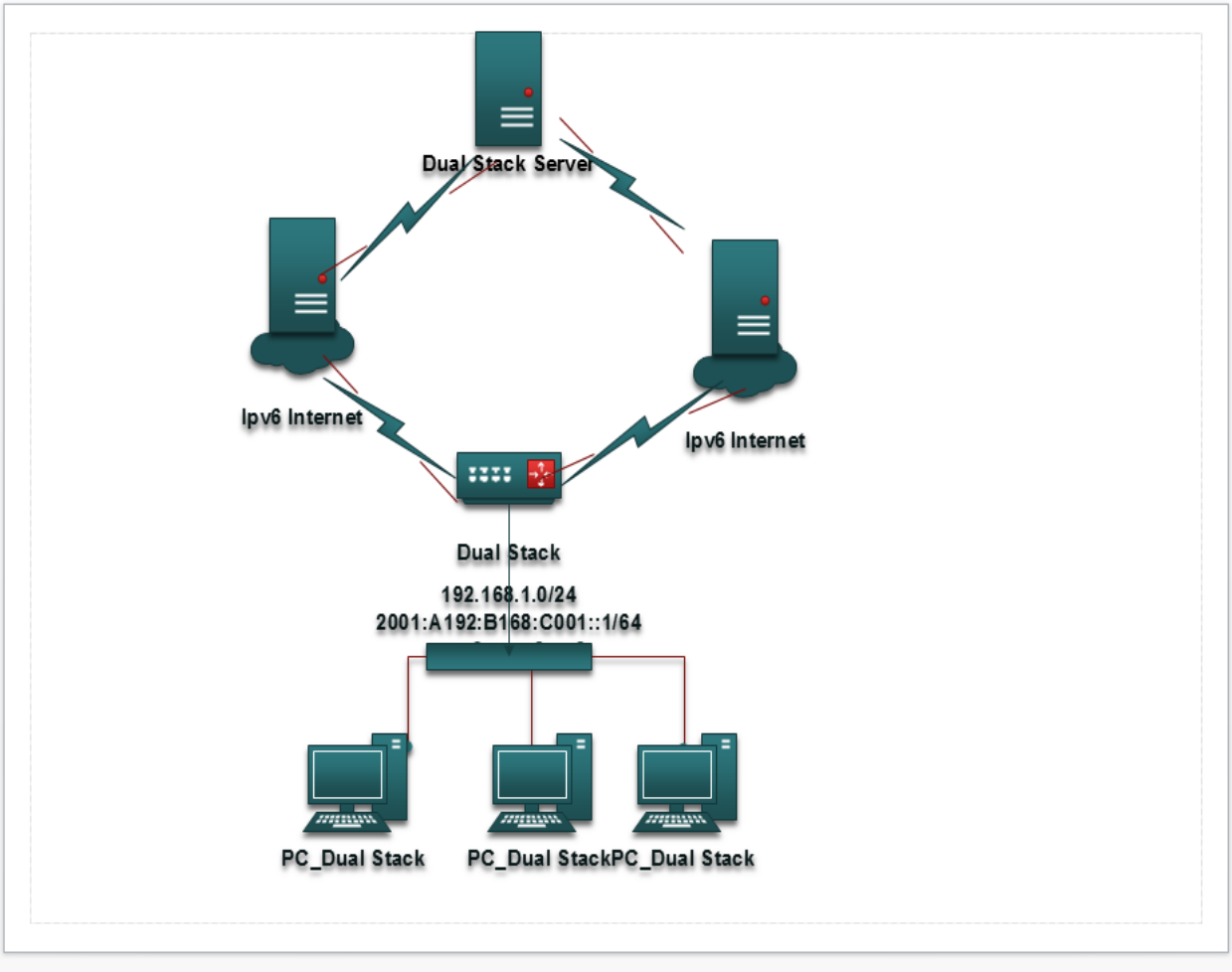


Figura 23: Diagrama Físico del Plenario.
Fuente: el autor

4.2 Conexión a Internet con IPv6

4.2.1 Proveedor de servicios

Actualmente la red del Plenario cuenta con un enlace a internet a través de Ipv4, otorgado por el proveedor CNT[8].

Esta empresa constituye un pilar importante en el país en cuanto prestación de servicios de internet se refiere. La misma brinda las siguientes opciones:

- Transmisión de datos
- Conexiones continuas a Internet.

[8] Corporación Nacional de Telecomunicaciones

- Paso al backbone de internet.
- Seguridad Lógica

Según estudios realizados, actualmente algunas ciudades del país soportan Ipv6. Ellas son:

Quito, Guayaquil, Ambato, Cuenca, Rio Bamba, Milagro, Loja y Guaranda.

Movistar una de las empresas de telefonía móvil en el Ecuador afirmó que ya está utilizando la nueva versión del protocolo IP, según Guillermo Miño experto en el área tecnológica de Movistar afirmó su trabajo con IPV6 desde el mes de Marzo de 2015, además señaló que la nueva tecnología se entrega a los clientes corporativos y desde este año se estaría brindando el soporte hacia los clientes individuales. (El Telégrafo., 2012, p. 14)

Dado lo antes mencionado, se determina que esta empresa es una de las que mayor red de fibra óptica brinda, por lo que se pueden interconectar con garantía redes de datos cercanas y distantes con una garantía sobre las rutas físicas independientes.

4.2.2 Protocolos de enrutamiento

Para la nueva estructura de la red y migración hacia el protocolo Ipv6, ha sido tenido en consideración el protocolo OSFP, debido a que este es uno de los protocolos de enrutamiento interno mejor implementados para redes corporativas grandes y medianas.

A continuación, se presenta un resumen de las características más importantes por las cuales se ha tomado en cuenta el protocolo OSPF para la migración a IPv6:

- Respuesta rápida y sin bucles ante cambios.
- Seguridad ante los cambios.
- Balanceo de carga en múltiples caminos.
- Escalabilidad en el crecimiento de rutas externas. (Polak, 2014)

4.2.2.1 Configuración del protocolo para Ipv6

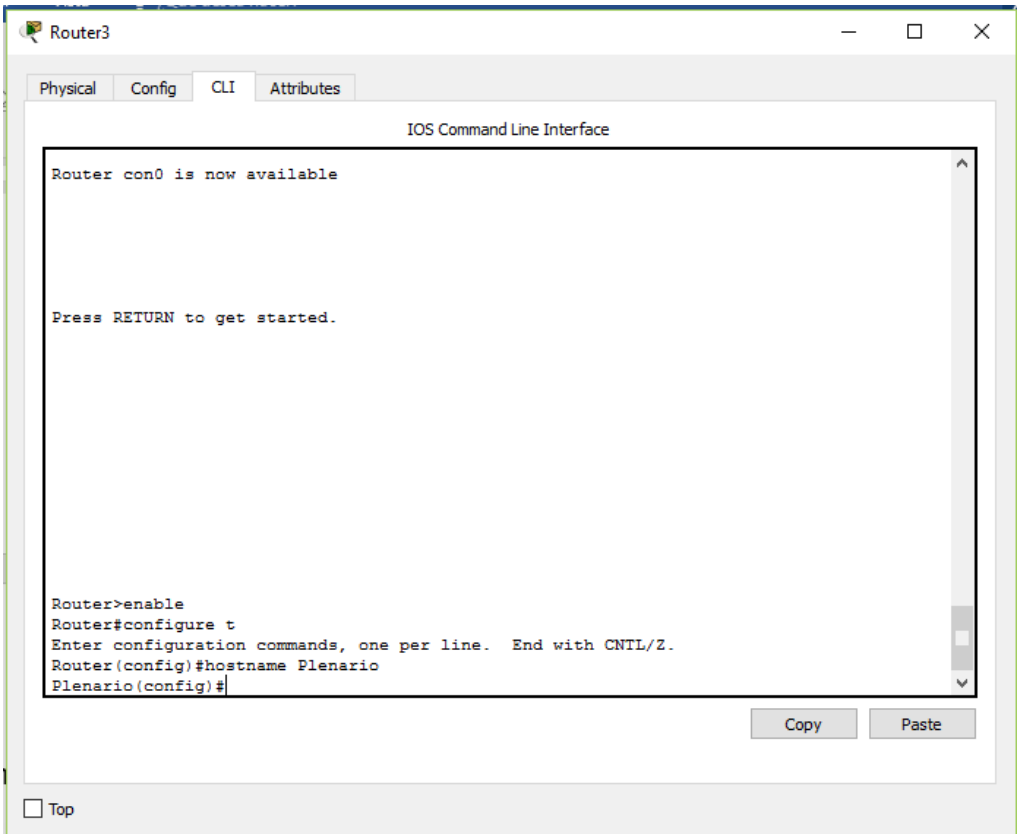


Figura 24: Asignar nombre al router
Fuente: el autor

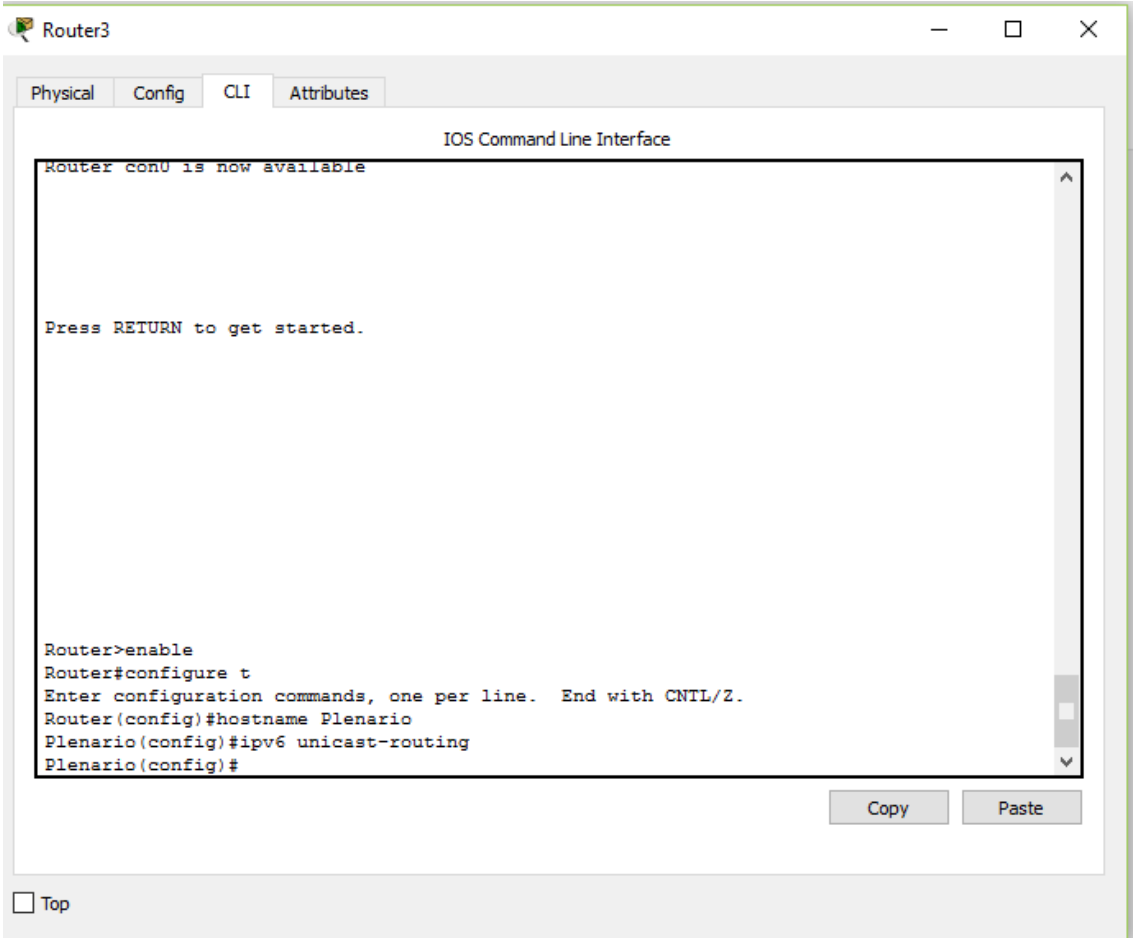


Figura 25: Enrutamiento de paquetes IPV6
Fuente: el autor

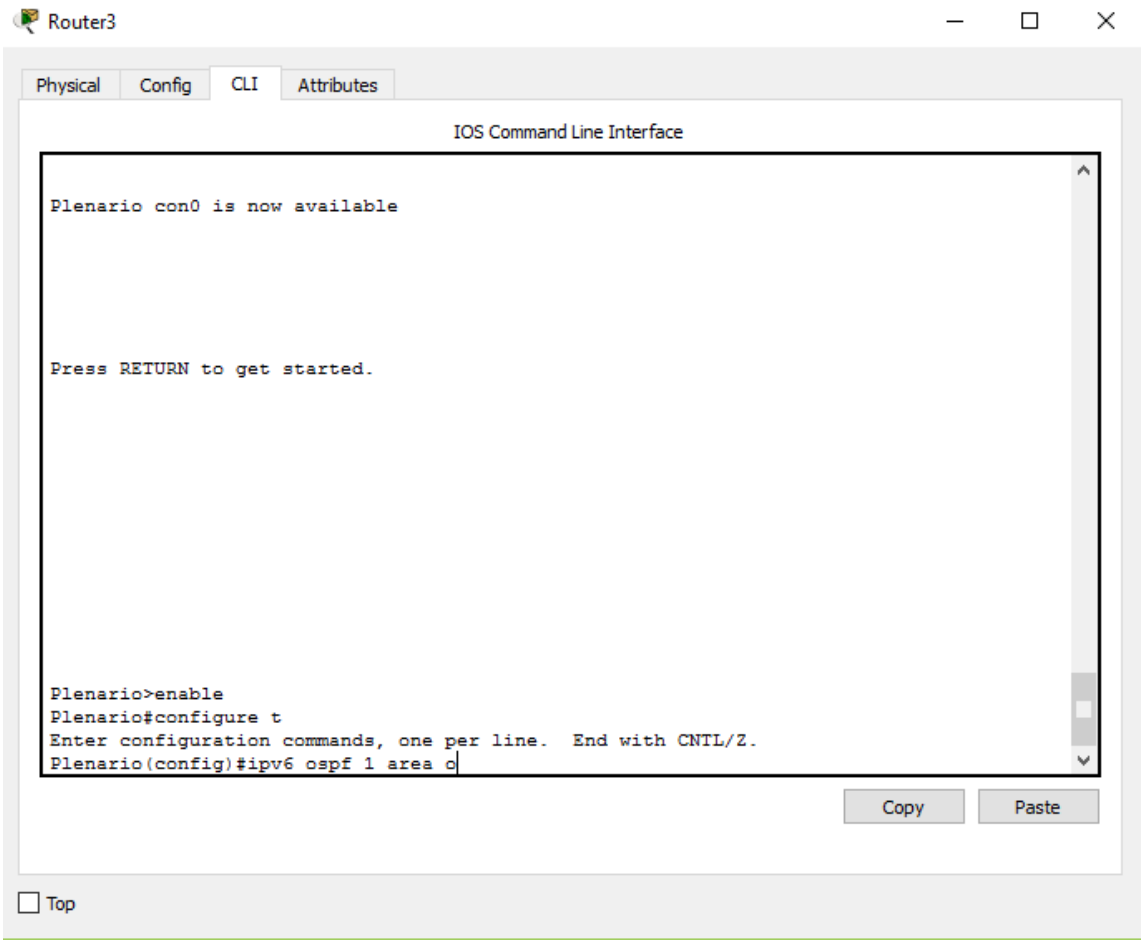


Figura 26: Habilitar Ospf dentro de un router:
Fuente: el autor

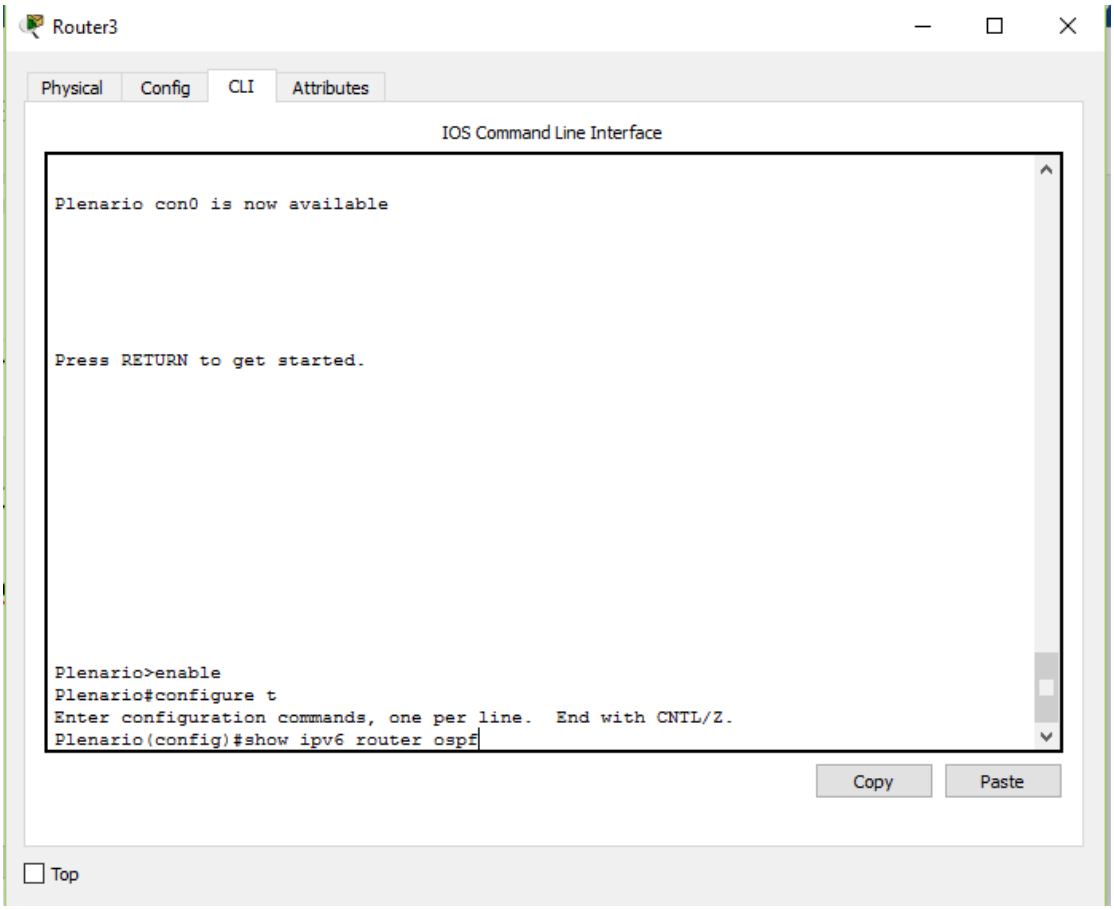


Figura 27: Verificar las configuraciones
Fuente: el autor

4.3 Transición a IPv6

La transición de Ipv4 a Ipv6 no es sencilla, ya que la comunicación entre la versión actual y el nuevo protocolo debe mantenerse, pues en algún momento se llevará a cabo una migración completa de Ipv4 a Ipv6, evitando afectar las aplicaciones y los servicios de la red actual del Plenario de la Asamblea.

Con la transición al nuevo protocolo IP, no se pretende remplazar los servicios Ipv4, si no buscar diferentes opciones para la migración, ya que el Plenario pertenece a una institución cuya tecnología es poco obsoleta, por lo tanto, es importante obtener mecanismos sólidos para transmitir los datos en ambos protocolos.

Seguidamente se detallan las opciones para la migración a Ipv6 dentro de la red del Plenario.

Permanecer con Ipv4 para el exterior y configurar en la red local Ipv6.

Para esta opción se desarrollará un esquema que permite la activación de la configuración Ipv6 de DHCP en los dispositivos de la red que están conectados al router principal hasta la conexión con el firewall.
La configuración del mecanismo Dual Stack será establecida dentro del firewall CISCO ASA 5510. Esto permitirá la comunicación de la red local de Ipv6 a Ipv4. Además, se llevará a cabo la configuración de NAT para facilitar la traducción de las direcciones Ipv4 a Ipv6.

Seguidamente se muestra el diagrama de la primera opción para la migración a Ipv6.

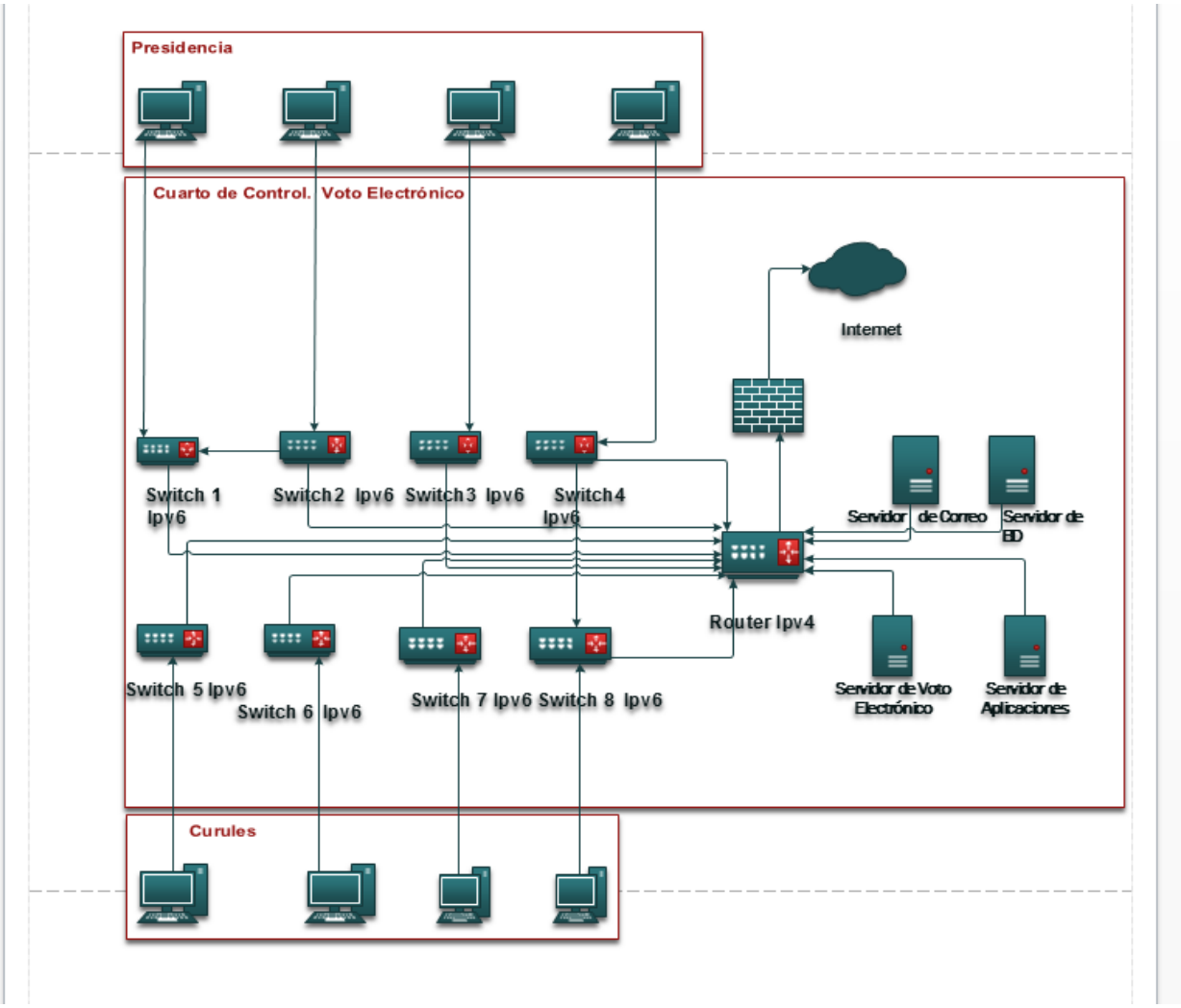


Figura 28: verificar las configuraciones

Fuente: el autor

4.3.1 Configuración para la primera opción de migración

La migración a Ipv6 se realizará de la forma más sencilla posible para que las nuevas IP queden organizadas de acuerdo a la configuración actual. Seguidamente se muestra un ejemplo para realizar la migración:

1- Se tiene la subred 192.168.170.0
2- Se organiza la subred asignándole a cada octeto de la IP letras del alfabeto. Para una mejor orientación observe el siguiente ejemplo:

   x x x - y y y - z z z

   1 9 2 - 1 6 8 - 1 7 0

   3- Se comienza a asignar la dirección ipv6 a partir de la 2001 o sea, 2001:axxx:byyy:czzz::/64

4- Posteriormente se sustituyen los valores correspondientes a las x, y, z respectivamente en la dirección ipv6 antes configurada, quedando de la siguiente forma; 2001:a192:b168:c170::/64 en donde la primera dirección ipv6 (2001:a192:b168:c170::1) será signada a la interfaz del Router perteneciente a dicha subred, y así sucesivamente con todas las subredes existentes.

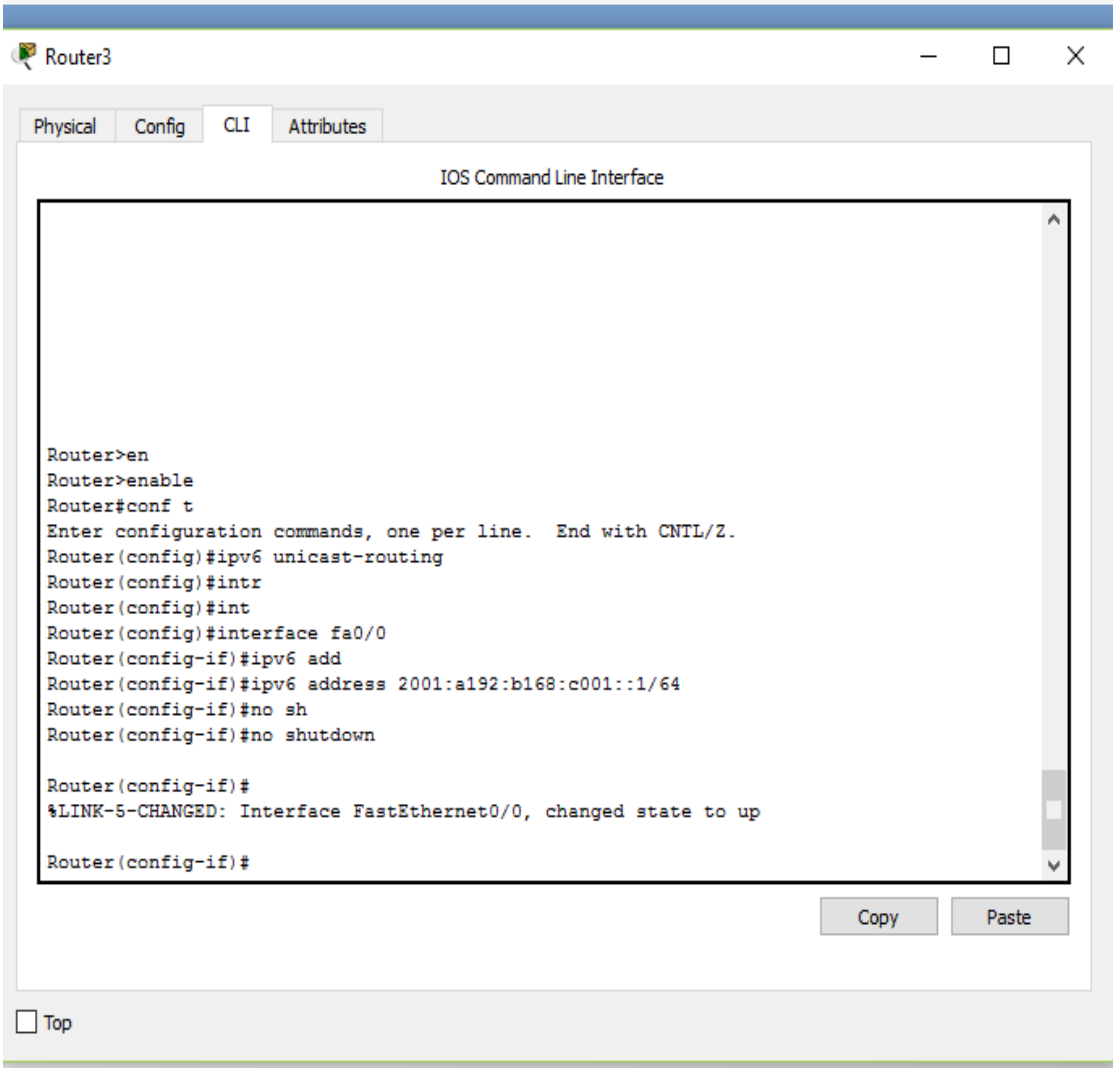


Figura 29: verificar las configuraciones

Fuente: el autor

La segunda opción que se plantea es tener Ipv6 para el exterior y configurar en la red local Ipv6.

Este ejemplo es similar al anterior, donde se activará la configuración Ipv6 por medio de DHCP en todos los equipos de red, pasando por el router hasta el firewall.

Se asume entonces que el mundo esté funcionando en Ipv6 completamente. Teniendo en cuenta esta suposición para acceder a internet solo sería necesario configurar el firewall haciendo uso del direccionamiento estático para Ipv6.

Seguidamente se muestra el diagrama diseñado para esta opción:

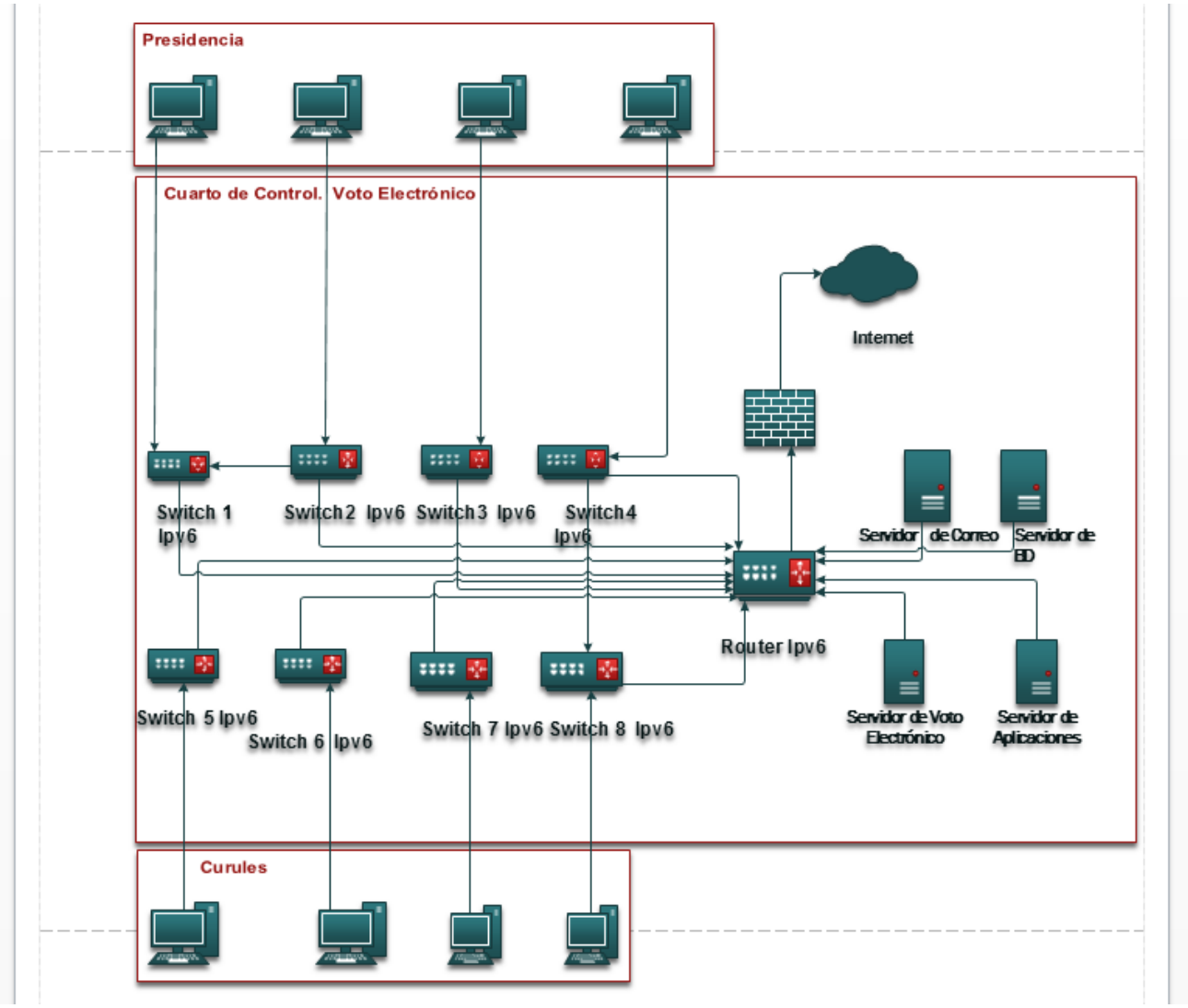


Figura 30: Segunda opción de migración

Fuente: el autor

4.3.2 Configuración de los dispositivos para la segunda opción

En esta ocasión se debe configurar una dirección Ipv6 para el router y el firewall.

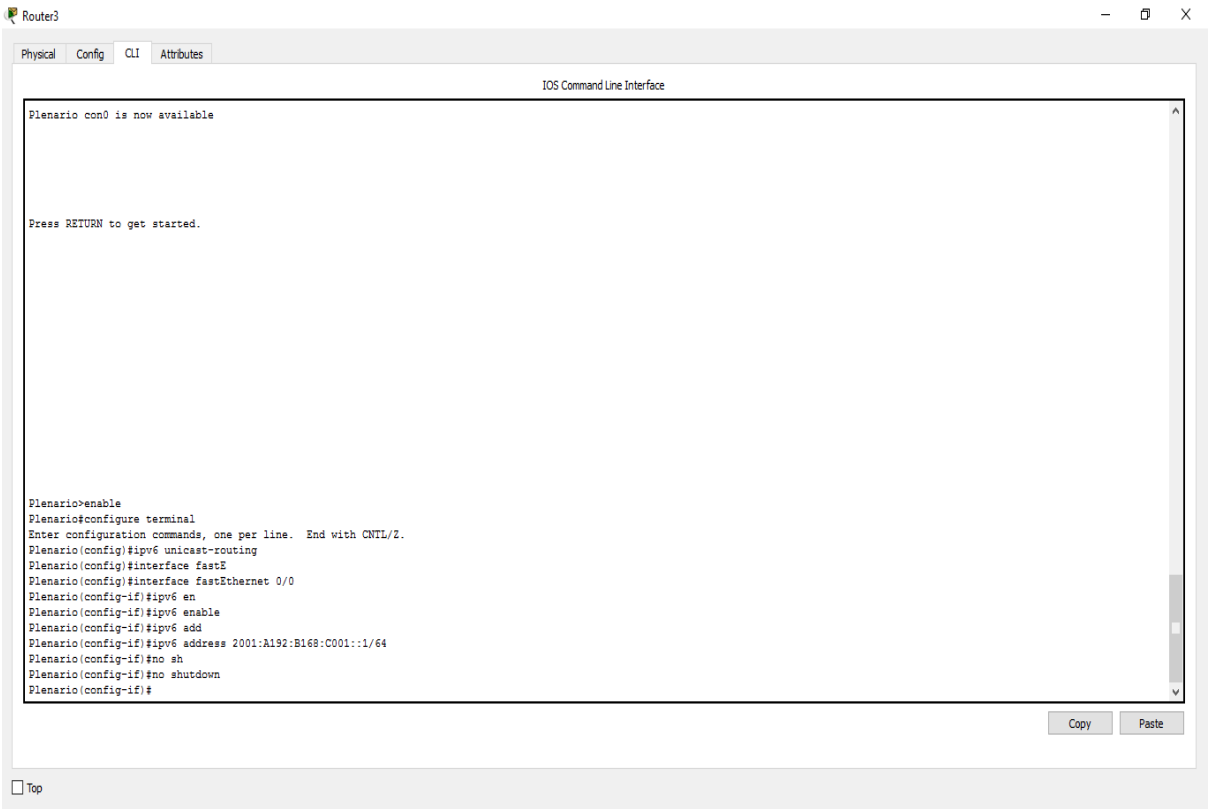


Figura 31: Configuración Ipv6 del router
Fuente: el autor

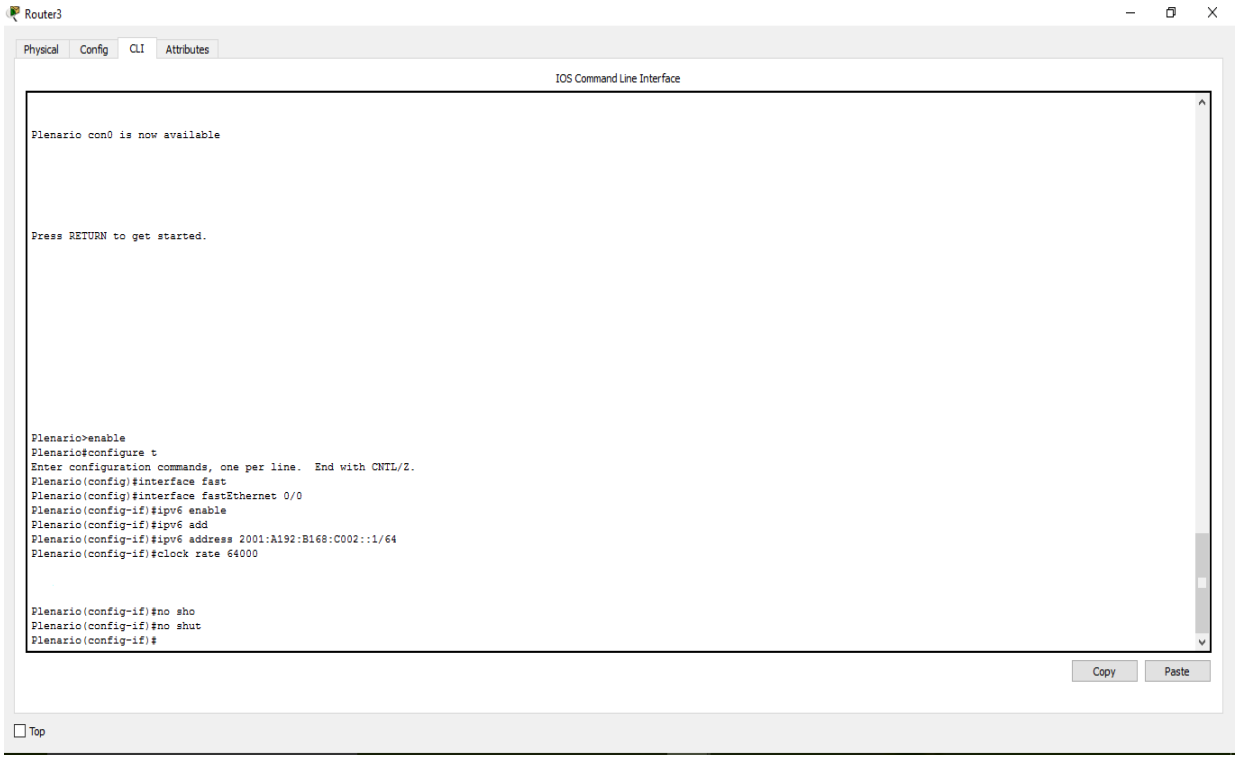


Figura 32: Configuración Ipv6 del router

Fuente: el autor

4.3.3 Configuración de ACLS en el firewall:

```
Router(config)#ipv6 access-list Administración
Router(config-ipv6-acl)# permit ipv6 any
2001:A192:B168:C001::/64 Router(config-ipv6-acl)# permit
ipv6 any 2001:A192:B168:C002::/64 Router(config-ipv6-acl)#
permit ipv6 any 2001:A192:B128:C003::/64 Router(config-ipv6-
acl)# permit ipv6 any 2001:A192:B198:C004::/64
Router(config-ipv6-acl)# permit ipv6 any 2001:A192:B198:C005::/64
Router(config-ipv6-acl)# permit ipv6 any 2001:A192:B198:C006::/64
Router(config-ipv6-acl)# permit ipv6 any 2001:A192:B198:C007::/64
Router(config-ipv6-acl)# permit ipv6 any 2001:A192:B198:C008::/64

Router(config-ipv6-acl)#exit
Router(config)#interface fastEthernet
1/0 Router(config-subif)#ipv6 traffic-filter
Administración in Router(config-
subif)#exit


Router(config)#ipv6 access-list Asambleistas
Router(config-ipv6-acl)# permit ipv6 any
2001:A192:B168:C004::/64 Router(config-ipv6-acl)# permit
ipv6 any 2001:A192:B168:C006::/64

Router(config-ipv6-acl)#exit
Router(config)#interface fastEthernet
2/0 Router(config-subif)#ipv6 traffic-filter
Asambleistas in Router(config-
subif)#exit


Router(config)#ipv6 access-list Comisión
Router(config-ipv6-acl)# permit ipv6 any
2001:A192:B168:C003::/64

Router(config-ipv6-acl)#exit
Router(config)#interface fastEthernet
3/0 Router(config-subif)#ipv6 traffic-filter
Comision in Router(config-subif)#exit


Router(config)#ipv6 access-list Presidencia
Router(config-ipv6-acl)# permit ipv6 any
2001:A192:B168:C003::/64 Router(config-ipv6-acl)# permit
ipv6 any 2001:A192:B168:C004::/64
Router(config-ipv6-acl)# permit ipv6 any 2001:A192:B168:C006::/64
```

Router(config-ipv6-acl)# permit ipv6 any 2001:A192:B168:C008::/64

Router(config-ipv6-acl)#exit
Router(config)#interface fastEthernet
6/0 Router(config-subif)#ipv6 traffic-filter
Presidencia in Router(config-subif)#exit

Seguidamente se muestra una tabla comparativa con los resultados de la conversión de IP.

Tabla 25: Configuración de las Vlans con los dos protocolos

Detalles de las Vlans con ambos protocolos			
Vlan	**Interfaz**	**Dirección de la sub_interfaz con Ipv4**	**Dirección de la sub_interfaz con Ipv6**
Administración	fa1/0	192.168.1.1/24	2001: A192:B168:C001::1/64
Asambleístas	fa2/0	192.168.2.1/24	2001: A192:B168:C002/64
Comisión	fa3/0	192.168.3.1/24	2001: A192:B168:C003::1/64
Móvil	fa4/0	192.168.4.1/24	2001: A192:B168:C004::1/64
Invitados	fa5/0	192.168.5.1/24	2001: A192:B168:C005::1/64
Presidencia	fa6/0	192.168.6.1/24	2001: A192:B168:C006::1/64
Funcionarios	fa7/0	192.168.7.1/24	2001: A192:B168:C007::1/64
Servidores	Fa8/0	192.168.8.1/24	2001: A192:B168:C008::1/64

Elaborado por: el autor

4.4 Diseño de la topología de red IPv6 revisa la sugerencia de la revisión anterior en este punto

La mayor parte de los equipos del Plenario son marca CISCO, y soportan Ipv6. El Plenario cuenta con un equipo de soporte que brindan adecuada atención a cada uno de los dispositivos.

Para la implementación del nuevo protocolo se ha mantenido la topología de la red.

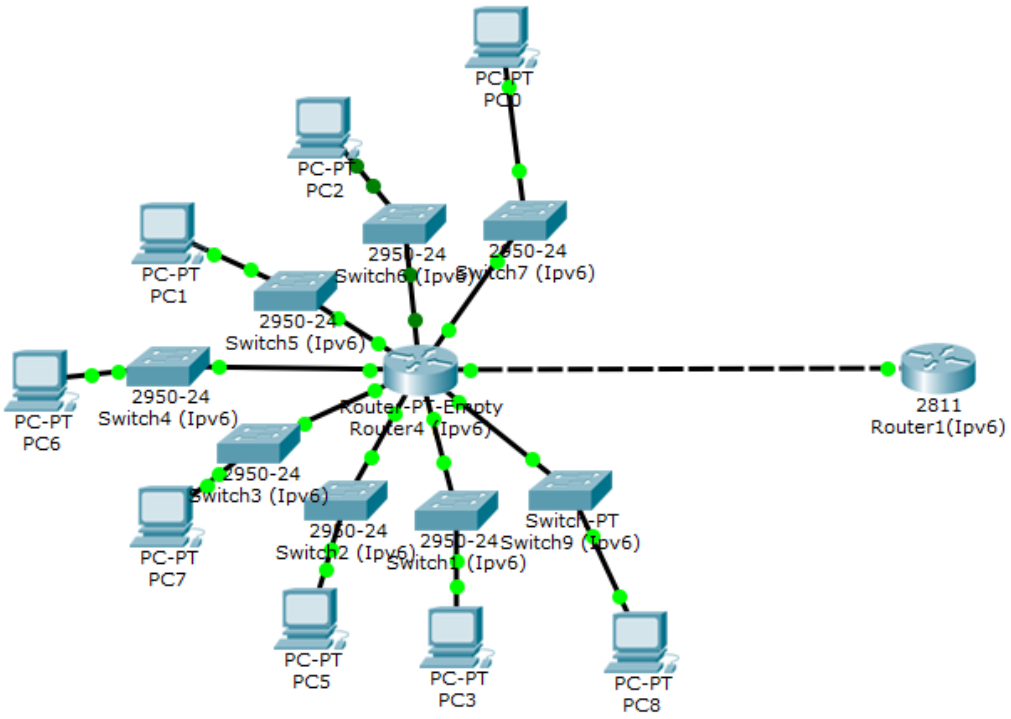


Figura 33: Topología de la red con Ipv6

Fuente: el autor

4.5 Configuración de las VLANS en IPv6

Para configurar una Vlan en Ipv6 se tienen las mismas consideraciones que en Ipv4.

A través del mecanismo de transición Dual Stack, las configuraciones en ambos protocolos pasan por la misma Vlan, con lo que el uso de Ipv6 en las Vlans de voz y datos son soportadas con facilidad.

4.5.1 Configuración de VLANS usando IPV6

Router# configure terminal

Router(config)# interface fastEthernet 1/0

Router(config-subif)# description VLAN Administracion

Router(config-subif)# encapsulation dot1Q 10 Router(config-subif)# ipv6 addess 2001:A192:B168:C001::1/64

4.5.2 Configurar ACLS en IPV6

Switch# configure terminal

Switch(config)# ipv6 **access-list** access-list-name Switch(config-ipv6-acl)# **deny | permit** protocol

{source-ipv6-prefix/prefix-length **| any | host** source-ipv6-address} [operator [port-number]]

{destination-ipv6-prefix/ prefix-length **| any | host** destination-ipv6-address} [operator [port-number]]

[dscp value] [fragments] [log] [log-input] [sequence value] [time-range name]

Para la configuración de las direcciones IPV6 de cada equipo se utilizó el mecanismo de autoconfiguración por DHCP existente en IPV6 a excepción de los equipos de red como switch, router, firewall en donde se realizó la asignación de direcciones IPV6 de forma manual para simplificar su configuración y administración.

4.6 Hardware

Para realizar la migración del Plenario se requiere que los equipos y dispositivos soporten Ipv6. En la tabla que se observa a continuación se pueden analizar los resultados del estudio realizado sobre cada uno de estos equipos.

Tabla 26: Hardware del Plenario

Hardware			
Equipos	**Marca/Modelo**	**Soporte Si/No**	**Actividad a realizar**
Firewall	Cisco ASA 5500	Si	Descartar las actualizaciones del SO.
Router	Cisco ASR 9922	Si	Descartar las actualizaciones del SO.
Switch	Cisco 3702	Si	Descartar las actualizaciones del SO.
Teléfonos		Si	Descartar las actualizaciones del SO.
Pc¨s	Pioneerpos Stealthtouch m5	Si	Instalar las actualizaciones últimas del SO para el soporte de Ipv6.
Servidores	IBM	Si	Instalar las actualizaciones últimas del SO para el soporte de Ipv6.

Elaborado por: el autor

4.7 Software

La mayoría de los Sistemas Operativos instalados soportan el protocolo Ipv6, ya que este está activado por defecto. E algunos dispositivos se necesita activar el soporte para Ipv6 por medio de comandos. Seguidamente se puede observar la lista de los Sistemas Operativos que han sido instalados en los equipos del Plenario.

Tabla 27: Software del Plenario

Software			
Servidor	**Sistema**	**Soporte**	**Acción**

Correo	Ubuntu 12.10	Si	En el caso de ser necesario, cargar el módulo IPv6 del sistema operativo.
Aplicaciones	Centos 5.0	Si	En el caso de ser necesario, cargar el módulo IPv6 del sistema operativo.
Base de Datos	Ubuntu 12.10	Si	En el caso de ser necesario, cargar el módulo IPv6 del sistema operativo.
Voto Electrónico (Jboss)	Ubuntu 12.10	Si	En el caso de ser necesario, cargar el módulo IPv6 del sistema operativo.

Elaborado por: el autor

Tabla 28: Software de las PC´s

SO de las PC del Plenario			
Usuarios	**Sistema**	**Soporte**	**Acción**
Administrativos	Ubuntu 12.4	Si	Activación del soporte Ipv6.
Comunes	Ubuntu 12.4	Si	Activación del soporte Ipv6.

Elaborado por: el autor

4.7.1 Costos de Software

Seguidamente se muestran los detalles de los costos estimados de los sistemas operativos instalados con los que cuentan los ordenadores y servidores.

Tabla 29: Costos de Software

Costos en software		
Software	**Costo**	**Detalles**
Ubuntu 12.4	$20	Este S.O de Software Libre soporta. Se debe realizar es descargar las actualizaciones buscando en Internet y almacenarlos en medios magnéticos como CD'S o DVD.
Ubuntu 12.10	$20	Este S.O de Software Libre soporta. Se debe realizar es descargar las actualizaciones buscando en Internet y almacenarlos en medios magnéticos como CD'S o DVD.
Centos 5.0	$20	Este S.O de Software Libre soporta IPV6 y se encuentra instalado en los servidores, solo debe realizar es descargar las actualizaciones buscando en Internet y almacenarlos en medios magnéticos como CD'S o DVD.
Total	$60	

Elaborado por: el autor

4.7.2 Costos en Hardware

Luego de realizar un previo análisis se ha determinado que los equipos del Plenario soportan Ipv6, por esta razón no es necesario que se realice la compra de nuevos equipos. Solo se realizará la configuración y actualización del SO para cada uno.

4.7.3 Costos en RRHH

Para poder establecer la migración para el nuevo protocolo Ipv6 debe prepararse al personal, de los cuales su mano de obra no se incluirá en la implementación lógica y física del protocolo. El Plenario cuenta con el grupo

de soporte, el cual está totalmente capacitado para llevar a cabo la migración guiados por el jefe de soporte, con lo cual se podrá obtener la calidad requerida en el proceso de migración.

4.7.4 Costos en Capacitación

La capacitación es otro aspecto importante para la implementación de la migración hacia ipv6 de la red del Plenario, para ello deben realizarse las pruebas de capacitación y funcionamiento del personal técnico.

Tabla 30: Costos en Capacitación

Capacitación		
Pruebas	**Tiempo**	**Costo**
Capacitación del personal técnico	100H	$3500
Pruebas de funcionamiento	50H	$1800
Total		$5300

Elaborado por: el autor

4.7.5 Inversión

Se debe tener en cuenta un porcentaje mayor del 30 % para los gastos que puedan presentarse de improviso, ya que puede ser necesario por ejemplo contratar personal externo que ayude en la configuración de procesos menos sencillos. Otros costos como inversiones de software y capacitación deben ser tomados en cuenta, ya que puede ser necesaria una modificación al instante de la migración.

Tabla 31: Costos del proyecto

Costo del proyecto	
Recurso	**Costo**
Capacitación	$ 5300
Software	$60

Extras	$40
Total	$ 5400

Elaborado por: el autor

Riesgos de la implementación del nuevo protocolo

Para implementar el protocolo Ipv6 en la red del Plenario, debe tenerse en cuenta que pueden existir factores que pongan en riesgo la migración. Seguidamente se listan algunos:

Tabla 32: Riesgos del proyecto

Riesgos	
No	**Detalles**
1	Perdida de la información.
2	Falta de disponibilidad de repuestos.
3	Daños en los equipos.
4	No compatibilidad del hardware.
5	Problemas funcionales del SO.
6	Fallas de corriente eléctrica.
7	Escasa o ninguna capacitación al personal técnico.

Elaborado por: el autor

Conclusiones

En la presente investigación se ha realizado un análisis el cual permitió diseñar un plan de implementación para migrar la red del Plenario de la Asamblea Nacional hacia el protocolo Ipv6. EL diseño se llevó a cabo mediante el software Pack Tracer, el cual permitió simular toda la red y la configuración que debe realizarse para lograr junto con el método Dual Stack conectar diversas subredes del Plenario.

Dado que el espacio de direccionamiento Ipv6 cuenta con una gran capacidad, se pueden lograr en el plenario identificar una gran cantidad de dispositivos de la red, también implementar los métodos de autoconfiguración y lograr niveles concretos de agregación de direcciones. El proceso de migración si se puede realizar dentro de la red del Plenario, ya que se analizaron las características de los dispositivos de la red y se determinó que todos cuentan con soporte para Ipv6, solo deben realizarse las configuraciones pertinentes.

Dado que la migración hacia Ipv6 se debe llevar a cabo paulatinamente se ha establecido un periodo de transición entre ambos protocolos con el objetivo de disminuir el impacto que esto tenga sobre el funcionamiento de la red.

Para implementar el protocolo Ipv6 se propusieron dos opciones, las cuales brindaban la posibilidad de manejar Ipv4/Ipv6 a través del método Dual Stack, y de esta forma se permite que los dos protocolos puedan coexistir. Con el diseño propuesto se ha tratado de mejorar la seguridad de las diferentes subredes estableciendo reglas de seguridad.

Los objetivos trazados para la investigación fueron cumplidos totalmente ya que la situación de la red de la asamblea fue analizada rigurosamente, así como sus elementos de hardware y software, lo que permitió definir en qué medida estos soportaban la migración. Algunas metodologías para la migración fueron analizadas dentro del marco teórico y se diseñó la solución para la migración a Ipv6 manteniendo en total funcionamiento los aplicativos utilizados en el Plenario como el E-Curul.

Recomendaciones

- Se recomienda no configurar inicialmente todos los nodos con soporte para Ipv6, ya que existen muchos dispositivos y servicios de red que continúan trabajando sobre Ipv4.
- Capacitar de forma inmediata al personal encargado para que estén en condiciones de implementar el nuevo protocolo, evitando percances.
- Es recomendable verificar el soporte Ipv6 en los dispositivos de red inalámbrica para evaluar las opciones que ayuden a otorgar direcciones Ipv6 junto a las direcciones Ipv4.

Bibliografía

6SoS. (2015). *El protocolo Ipv6.(Tesis de maestría).* Mexico.

Bartolo, M. (2013). *ANÁLISIS DE TRÁFICO PARA LA RED DE DATOS DE LAS INSTITUCIONES EDUCATIVAS DEL NÚCLEO 5 DE LA CIUDAD DE PEREIRA.* Colombia.

Camargo, A. E. (2006). *Plan de transicion del protocolo de red de ipv4 a ipvs en la Universidad Indutrial de Santander.* Santander.

Carabelli, M. (2011). *El protocolo IPv6. (Tesis de maestría). Universidad Nacional del Rosario.* Argentina.

Carballo, B. (04 de Marzo de 2013). *Pensamiento de Sistemas*. Obtenido de Pensamiento de Sistemas: http://pensamientodesistemasaplicado.blogspot.com/2013/03/definiendo-el-alcance-de-una.html

El Telégrafo. (2012). La migración a Ipv6. *El telégrafo*, 14.

Fernández, A. (2012). *Reporte del estado de Ipv6 en RedClara. (Tesis de pregrado). Universidad Nacional Autónoma de México.* . Mexico.

Fernández, F. (2013). *EVOLUCIÓN DE REDES FIJAS DEL PROTOCOLO IPv4 A IPv6 EN GUATEMALA. (Tesis de pregrado). UNIVERSIDAD DE SAN CARLOS DE GUATEMALA.* Guatemala.

Fuentes, R. (2012). *Análisis de tablas de ruteo en protocolos IPs. (Tesis de pregrado). INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY.* Mexico.

Gil, P. (2012). *Protocolo de mensajes de control de internet. (Tesis de pregrado). Universidad de Alicante.* España.

González, J. (2010). *Diseño de un proveedor de internet de servicios inalámbricos. (Tesis de pregrado). Universidad Técnica Particular de Loja.* . Quito.

Islas, O. (10 de Mayo de 2012). Los primeros años de internet en América Latina.Razonypalabra. Recuperado de http://www.razonypalabra.org.mx/N/N76/varia/5a%20entrega/47_Islas_V76.pdf . *razonypalabra*, pág. 8.

Landy, D. (2013). *Propuesta de un Plan de Implementacion para a migracion Ipv6 en la red de la Universidad Politecnica Salesiana sede Cuenca.(Tesis de pregrado) Universidad Politecnica Salesiana.* Cuenca.

Mansilla, C. (2013). *Redes de Computadoras. .* Argentina.

Martinez, C. (2014). *Direccionamiento Ipv6.(Tesis de maestría). Laonic.* Santiago de Chile.

MEGS. (2013, Octubre 20). *Multicast Listener Discovery (MLD o Descubrimiento de escucha de multidifusión)*. Retrieved from MEGS: http://dmrodriguez.50megs.com/IPV6/IPV6_9.html

Meisel, Y. (2016). *Comparación, ventajas, problemas y una metodología para la transicion de ipv4 a ipv6 en las redes de comunicaciones. (Tesis de pregrado). Universidad del Norte. .* Colombia.

Ministerio de Indutria, Enrgía y Turismo. (2015). *Ministerio de Indutria, Enrgía y Turismo*. Retrieved from Ministerio de Indutria, Enrgía y Turismo: http://www.ipv6.es/es-ES/transicion/quees/Paginas/10razones.aspx

Morató, D. (2013). *Direccionamiento IP. (Tesis de maestría). Universidad Pública de Navarra.* España.

Nic. (2012). *La nueva generacion del protocolo de internet.* Brasil.

Oicatá, D. (2014). *Protocolo de direccionamiento de redes Ipv4 e Ipv6.(Tesis de pregrado) Universidad de Boyacá. .* Boyacá.

ORACLE. (2013, Diciembre 10). *Guía de administración del sistema: servicios IP*. Retrieved from Guía de administración del sistema: servicios IP: https://docs.oracle.com/cd/E19957-01/820-2981/chapter1-40/index.html

Palet, J. (03 de Febrero de 2012). *'IPv6 es la única alternativa para seguir en Internet'*. Obtenido de ElMundo: http://www.elmundo.es/elmundo/2011/02/03/navegante/1296732593.html

Perez, J. (2013). *Tecnología y mecanismos de transicion de Ipv4 a Ipv6. (Tesis de maestría). Universidad Técnica del Norte.*

Pérez, N. J. (2014). *Tecnologías y mecanismos de transicion de Ipv4 a Ipv6.* Mexico.

Piquer, J. M. (2012). *Historia de Internet en America Latina y el Caribe.* Obtenido de https://interred.wordpress.com/1995/02/12/presencia-del-ecuador-en-el-internet/

Polak, B. (2014). *Introducción a la configuración de router Cisco. (Tesis de pregrado). Universidad ORT Uruguay. .* Uruguay.

Puerto, O. (2015). *Protoolo de direccionamiento de redes Ipv4 e Ipv6. (Tesis de pregrado). Universidad de Boyacá. .* Boyaca.

Redes Locales y Globales. (2 de Enero de 2012). *Formato de la Cabecera Ipv6*. Obtenido de Formato de la Cabecera Ipv6: https://sites.google.com/site/redeslocalesyglobales/6-arquitecturas-de-redes/6-arquitectura-tcp-ip/7-nivel-de-red/8-direccionamiento-ipv6/2-formato-de-la-cabecera-ipv6

Reina, T. F. (2004). *Redes de area local* .

Rivera, J. (2015). *MIGRACIÓN A IPV6 EN LA RED DE LA FACULTAD DE CIENCIAS ADMINISTRATIVAS DE LA UNIVERSIDAD DE GUAYAQUIL. (Tesis de maestría) Universidad de Guayaquil.* GUAYAQUIL.

Rivera, J. (2015). *Plan de implementacion para la migracion a Ipv6 de la red de la facultad de ciencias administrativas de guayaquil.(Tesis de maestría). Universidad de Guayaquil.* Guayaquil.

Rivera, J. (2015). *Plan de implementación para la migración a ipv6 en la red de la facultad de ciencias administrativas en la Universidad de Guayaquil. (Tesis de pregrado). Universidad de Guayaquil,.* Guayaquil.

Rivera, L. (2013). *Propuesta de un plan de implementación para la migración de ipv4 a ipv6(tesis de pregrado)Universidad Politécnica Salesiana.* Cuenca.

Salazar, W. (2013). *Propuesta de migración de IPv4 a IPvs de la red de la Universidad Simón Bolívar. (Tesis de maestría). Universidad Simón Bolívar.* Quito.

UAP(Universidad Alas Peruanas). (2015). Fundamentos de redes y conectividad. . Perú.

UNLAM. (2014). Redes y subredes.(Tesis de pregrado). Universidad Nacional de La Matanza. Argentina.

Zamora, L. (2014). Internet. (Tesis de maestría). Universidad Autónoma del Estado de Hidalgo. Mexico.

Anexo

De acuerdo al análisis realizado con la herramienta Wireshark a la red de comunicaciones de la Asamblea Nacional se determina las siguientes conclusiones.

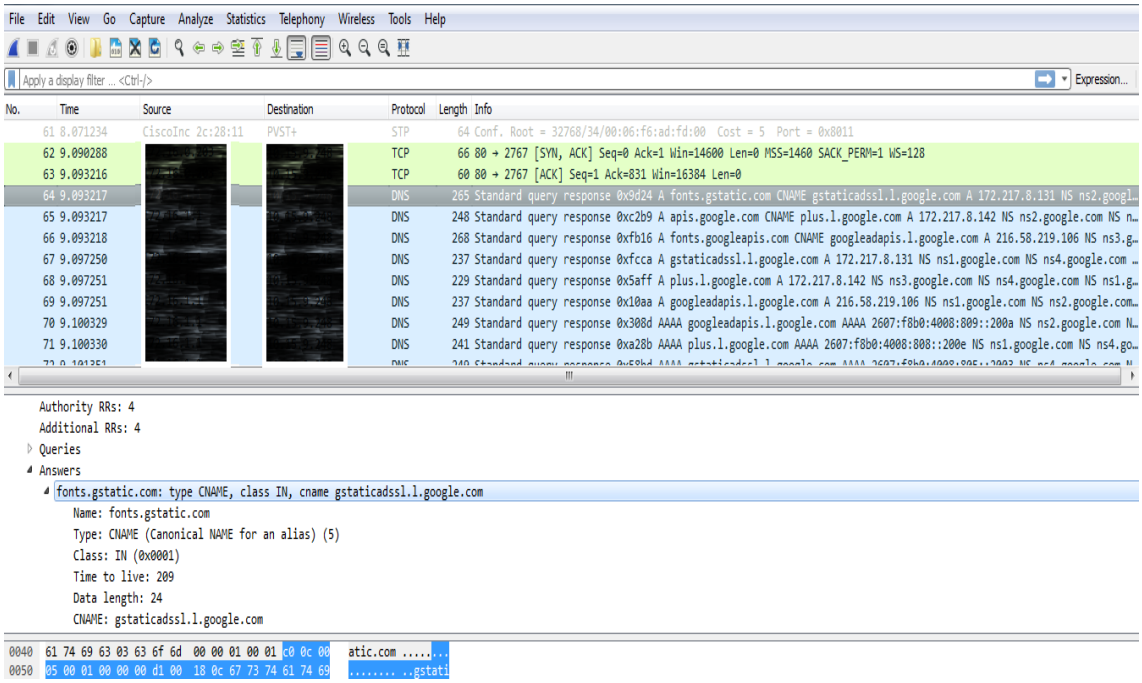


Figura 34: Anexo 1
Elaborado por: el autor

En este diagrama se evidencia las búsquedas que el cliente realiza al buscador google.

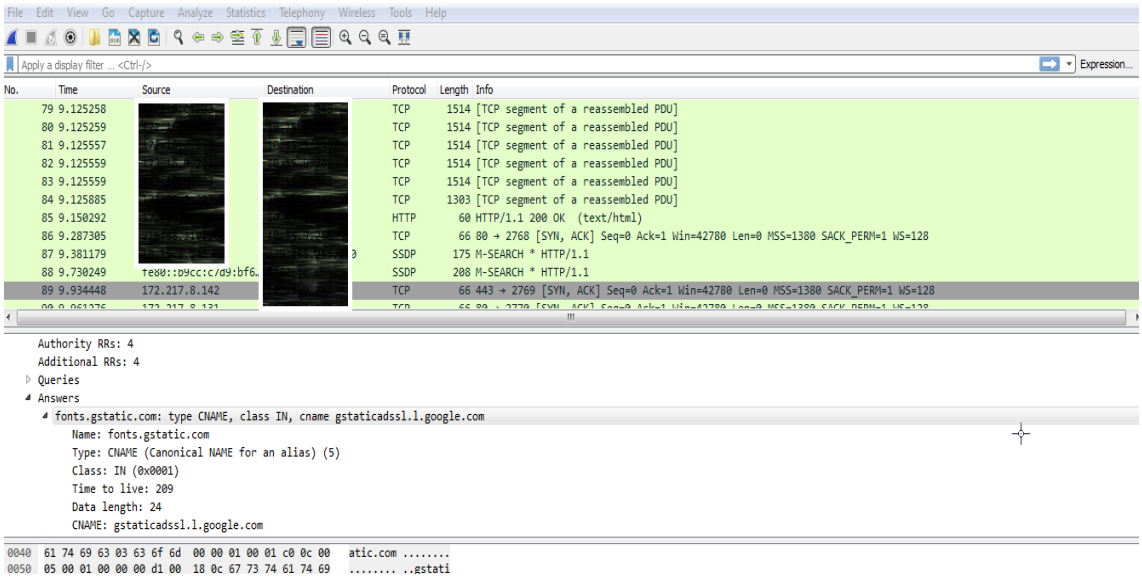


Figura 35: Anexo 2
Elaborado por: el autor

Los mensajes de “TCP segment of a reassembles PDU” permiten concluir que wireshark se encuentra uniendo segmentos ya que algunos paquetes se presentan fragmentados.

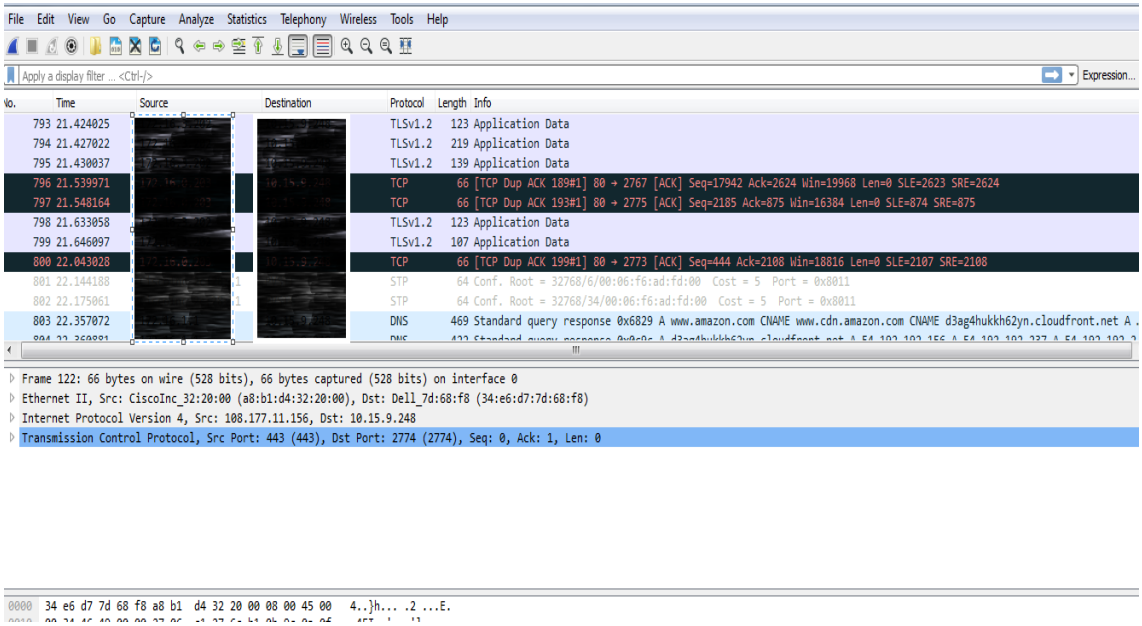


Figura 36: Anexo 3

Elaborado por: el autor

Se evidencia de ACK DUP hacia la página web de la Asamblea Nacional, determinando la pérdida de paquetes y existencia de alta latencia, por reordenamiento de segmentos.

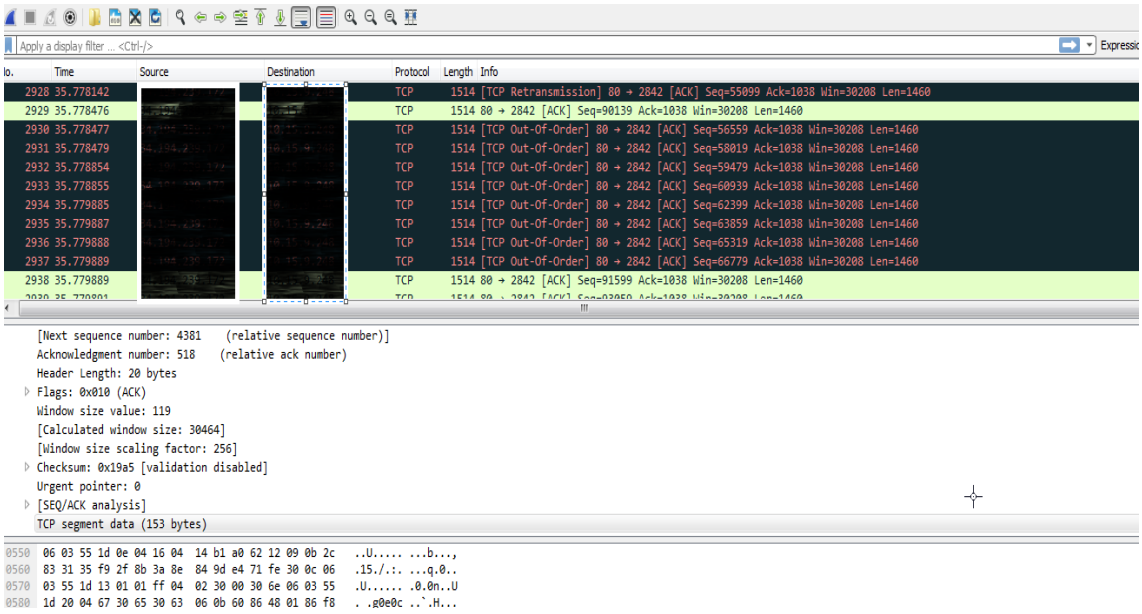


Figura 37: Anexo 4

Elaborado por: el autor

La información TCP Out-OF-Order muestra que el frame fue recibido con una orden diferente a la emitida. Al obtener esta información el protocolo TCP tarda un poco más (imperceptible) montar los segmentos en el orden emitidos.

La ventaja de la implementación del protocolo IPV4 en la Asamblea Nacional radica en la seguridad IPSEC que brinda en el cifrado de datos, lo cual es transparente para el usuario final.

Permite una mayor transmisión de información y optimización de velocidad al facilitar el envió de paquetes de tamaño más grande a los permitidos en IPV4.

Mediante la implementación de IPV6 se tiene una mejora en la calidad de servicio QoS.