UNIVERSIDAD NACIONAL DE LOJA

ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMAS

TÍTULO:

"INVESTIGACIÓN E IMPLEMENTACIÓN DEL PROTOCOLO IPV6 EN LA INFRAESTRUCTURA DE RED EXISTENTE DEL ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES COMO PROPUESTA HACIA LA MIGRACION A INTERNET 2".

Tesis de grado previa a la obtención del Título de Ingenieros en Sistemas.

AUTORES:

Gabriela Judith Burneo Nieto

Nixon Guillermo Delgado Jiménez.

DIRECTOR:

Ing. Hernán Leonardo Torres Carrión

Loja – Ecuador

2008

CERTIFICACIÓN

Ing. Hernán Leonardo Torres Carrión

DOCENTE DEL ÁREA DE LA ENERGÍA, LAS INDUSTRÍAS Y LOS RECURSOS NATURALES NO RENOVABLES

CERTIFICA:

Haber revisado durante el desarrollo, la tesis titulada: ***"INVESTIGACIÓN E IMPLEMENTACIÓN DEL PROTOCOLO IPV6 EN LA INFRAESTRUCTURA DE RED EXISTENTE DEL ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES COMO PROPUESTA HACIA LA MIGRACION A INTERNET 2"***, elaborada por los señores egresados Gabriela Judith Burneo Nieto y Nixon Guillermo Delgado Jiménez, previo a la obtención del grado de Ingenieros en Sistemas.

En tal virtud cumple los requisitos que exigen las normas de graduación de ésta institución, por lo expuesto autorizo su presentación y defensa.

Loja, Noviembre del 2008

Ing. Hernán Leonardo Torres Carrión

DIRECTOR DE TESIS

AUTORÍA

Las opiniones, ideas y generalizaciones expresadas en el presente trabajo de Tesis, son de absoluta responsabilidad de los autores.

Los Autores:

Gabriela Burneo Nieto

Nixon Delgado Jiménez

DECLARACIÓN DE AUTORÍA

Gabriela Judith Burneo Nieto y Nixon Guillermo Delgado Jiménez autores intelectuales del presente trabajo de investigación autorizamos a la Universidad Nacional de Loja, de hacer uso del mismo con la finalidad que estime conveniente.

Gabriela Judith Burneo Nieto

Nixon Guillermo Delgado Jiménez

AGRADECIMIENTO

Al concluir el presente trabajo de investigación, dejamos constancia de nuestra gratitud a la Universidad Nacional de Loja, y en especial a la Carrera de Ingeniería en Sistemas por constituir la principal fuente de enseñanza para la formación integral de los profesionales.

A todos nuestros maestros quienes con su sabiduría han forjado nuestro aprendizaje, a nuestros Padres y hermanos, quienes con su apoyo sincero y desinteresado nos han sabido apoyar en los momentos más difíciles de nuestras vidas.

Al Ing. Hernán Torres, quién dedicó sus conocimientos y tiempo en la dirección del presente trabajo de Tesis.

A nuestros compañeros y amigos, que siempre nos apoyaron y dieron su ayuda incondicional, y forman parte de este logro.

LOS AUTORES

DEDICATORIA

Gracias a ti se cumple una meta que añore hace seis años, gracias por darme las fuerzas y la perseverancia de seguir adelante, sin ti tu ayuda no hubiera alcanzado.

Gracias Jehová

Gracias a mi familia Vicente, Nelly, Jean Pierre, amigos y a todas las personas que nos han ayudado desinteresadamente a concluir esta meta.

Gaby

A Dios, por darme fuerza y fe para
Seguir adelante.

A mi madre y hermanos, por apoyarme
Y estar siempre conmigo.

Nixon

RESUMEN

El siguiente trabajo presenta una investigación del nuevo protocolo de Internet, conocido como IPv6 (Protocolo de Internet versión 6). Este protocolo supone mejor calidad, seguridad y facilidad de administración como características añadidas al mayor espacio de direccionamiento, el cual es catalogado como la idea base de la creación de esta nueva tecnología.

El objetivo que persiguen las redes avanzadas es otro punto que apoya la implantación de esta nueva tecnología, cuya idea es facilitar el avance de las tecnologías y nuevas aplicaciones de Internet. Este proyecto ha comenzado en EEUU como Internet2, y continuado en otros países con otros nombres, pero la esencia es la misma, dotar a las instituciones académicas nacionales, regionales e internacionales de los recursos necesarios para desarrollar nuevas herramientas de aprendizaje, que redundaran también en beneficio de la Internet de futuro.

En Latinoamérica la Organización encargada de las Redes Avanzadas es CLARA (Corporación Latinoamericana de Redes Avanzadas). Esta corporación incentiva a los centros de educación superior principalmente, a trabajar en la investigación y desarrollo de nuevas tecnologías informáticas y de telecomunicaciones.

En Ecuador, CEDIA (Consorcio Ecuatoriano de Desarrollo de Internet Avanzado) dirige y coordina proyectos de investigación que aprovechen la aplicación de tecnología avanzada enfocadas al desarrollo científico y educativo de la sociedad ecuatoriana. La Universidad Nacional de Loja pertenece a este Consorcio, por lo cual debe ocuparse de la exploración de conocimientos en conformidad con esta entidad.

La Universidad cuenta con una topología de red de datos en estrella extendida, diferenciando una zona pública (radio, modle cisco y estudios a distancia) y privada (proxys de áreas, sistemas internos). El backbone utiliza fibra óptica para conectarse a todas las áreas a excepción del A.E.I.R.N.N.R. (Área de la Energía, Industria y Recursos Naturales No Renovables) que se enlaza vía Dial-Up. Actualmente el backbone local del A.E.I.R.N.N.R. se ha migrado también a fibra óptica; al igual que el resto de la red de la Universidad, es una topología en estrella extendida sin enlaces redundantes.

Implementando el protocolo en una red de pruebas obtuvimos diferencias notables entre el protocolo actual IPv4 (Protocolo de Internet Versión 4) y el protocolo IPv6. Utilizando herramientas de generación y monitoreo de tráfico, constatamos que los protocolos mencionados responden de diferente forma ante situaciones de

congestionamiento (servidores DNS, FTP, HTTP, Mensajería y tráfico D-ITG), siendo IPv6 el que optimiza el flujo de tráfico en la red.

SUMMARY

The following work presents an investigation of the new protocol of Internet, well-known as IPv6 (Protocol of Internet version 6). This protocol supposes better quality,

security and administration easiness like characteristics added to the biggest direction space, which is classified as the idea bases of the creation of this new technology.

The objective that they pursue the advanced nets is another point that supports the installation of this new technology whose idea is to facilitate the advance of the technologies and new applications of Internet. This project has begun in USA like Internet2, and continued in other countries with other names, but the essence is the same one, to endow to the national, regional and international academic institutions of the necessary resources to develop new learning tools that also redounded in benefit of the future Internet.

ÍNDICE DE CONTENIDOS

Certificación…….. **I**
Autoría…… **II**

Declaración de Autoría…….. **III**
Agradecimiento……. **IV**
Dedicatoria…… **V**
2. Resumen…… **VII**
Summary …….. **VIII**
3. Índice.....…..…….. **XI**
3.1 Índice de Ilustraciones y Tablas..... **XII**
4. Introducción……...……... **XIV**
5. Metodología…..…… **XVI**
6. Marco Teórico……. **1**
6.1 Protocolo de Internet versión 6 (IPv6)……... **1**
6.1.1 Definiciones……... **2**
6.1.2 Características…… **3**
6.1.3 Arquitectura de direccionamiento…….. **5**
6.1.4 Técnicas de Transición…….. **15**
6.1.5 Comparaciones con el protocolo IPv4……... **18**
6.2 Internet Avanzado..... **20**
6.2.1 Definiciones……... **20**
6.2.2 Características de Redes Avanzadas……. **23**
6.2.3 Aplicaciones de Redes Avanzadas…… **24**
6.2.4 Estado actual de las Redes Avanzadas en el Ecuador……... **30**
7. Desarrollo de la Propuesta **33**
7.1 Análisis de la red de datos del Área de Energía, Industrias y Recursos Naturales no Renovables de la UNL…… **33**
7.1.1 Descripción de la topología física y lógica de comunicación…… **33**
7.1.2 Análisis de Tráfico y políticas de comunicación……... **37**
7.1.3 Especificaciones de los equipos de red……. **38**
7.1.4 Análisis de factibilidad para la implementación del protocolo…… **41**
7.2 Diseño de la solución para la migración de la red a IPv6…….. **42**
7.2.1 Análisis de la Técnica Dual Stack en la red del A.E.I.R.N.N.R…… **42**
7.2.2 Análisis de la Técnica de Tunneling en la red del A.E.I.R.N.N.R…… **44**
7.2.3 Análisis de la Técnica de Traducciones en la red del A.E.I.R.N.N.R….. **46**
7.2.4 Selección de la Solución Adecuada para la Migración de la **48**

Red del A.E.I.R.N.N.R……
7.2.5 Diseño de un Plan Piloto para la Implementación del Protocolo IPv6… **54**
7.2.5.1 Análisis de la Red y Selección de los Equipos de Comunicación…… **54**
7.2.5.2 Definición de los Recursos Necesarios para la Migración de la Red del A.E.I.R.N.N.R……... **55**
7.2.5.3 Diseño de un esquema de direccionamiento y Configuración de servicios IPv6……..…….. **55**
7.2.5.4 Pruebas de rendimiento y evaluación de resultados……... **56**
8. Evaluación del Objeto de Investigación **57**
8.1 Implementación de IPv6…… **57**
8.1.1 Definición de un escenario para pruebas y evaluación del protocolo…… **57**
8.1.2 Análisis de rendimiento y evaluación de resultados…….. **60**
9. Valoración Técnico-Económico-Impacto Ambiental……. **66**
9.1 Técnico-Económico……... **66**
9.2 Impacto Ambiental…… **70**
10. Conclusiones…… **71**
11. Recomendaciones..... **73**
12. Bibliografía..... **75**
13. Anexos……... **77**
Anexo 1 Configuraciones de los Equipos Encaminadores…….. **77**
Anexo 2 Configuraciones de IPv6 en las Plataformas Linux y Windows…….. **80**
Anexo 3 Configuraciones de los Servidores DNS y DHCP…… **89**
Anexo 4 Configuración de los Servidores HTTP, FTP Mensajería…… **97**
Anexo 5 Análisis Packet Analizer……. **103**
Anexo 6 Análisis con DITG…… **106**
Anexo 7 Monitoreo Wireshark…… **111**
Anexo 8 Cableado Estructurado del A.E.I.R.N.N.R…….. **113**
Anexo 9 Fotografías de la Red del A.E.I.R.N.N.R…… **116**
Anexo 10 Distribución de los Equipos Actuales en la Red del A.E.I.R.N.N.R **122**
Anexo 11 Topología Actual del A.E.I.R.N.N.R…… **125**
Anexo 12 Simbología de Esquemas…….. **127**

Anexo 13 Glosario……..…….. **129**

Anexo 14 Anteproyecto….……..…….. **135**

ÍNDICE DE ILUSTRACIONES Y TABLAS

Figuras:

Figura 1.3.1 Formato de Datagrama IPv6…… **6**

Figura 1.3.2 Siguiente Cabecera IPv6……. **7**

Figura 1.3.3 Cabecera IPv6 Básica y Datos……... **8**

Figura 1.3.4 Cabecera IPv6 Básica, Fragmentos y Datos…… **8**

Figura 2.3.1 Ejemplo de Mallas…….…….. **25**

Figura 2.3.2 Ejemplo de Instrumentación Remota (Medicina)…… **26**

Figura 2.3.3 Ejemplo de Instrumentación Remota (Musical)…….. **27**

Figura 2.3.4 Ejemplo de Ambientes Virtuales……. **29**
Figura 2.4.1 Red CEDIA……. **31**
Figura 3.1.1 Topología de la UNL…….. **34**
Figura 3.1.2 Topología del A.E.I.R.N.N.R..…….. **36**
Figura 3.2.1 Representación del Tráfico en la Red UNL…… **37**
Figura 3.2.2 Representación del Tráfico en la Red A.E.I.R.N.N.R…… **38**
Figura 4.1.1 Topología Técnica Dual……. **43**
Figura 4.2.1 Topología Técnica Túneles…… **45**
Figura 4.3.1 Topología Técnica Traducción NAT-PT…… **47**
Figura 4.4.1 Opción 1 para la Implementación de IPv6 en el A.E.I.R.N.N.R. **49**
Figura 4.4.2 Opción 2 para la Implementación de IPv6 del **51**

A.E.I.R.N.N.R...

Figura 5.1.1 Escenario de Laboratorio……. **58**
Figura 5.2.1 Resultados IPv4 con ICMP sin Servicios…… **61**
Figura 5.2.2 Resultados IPv6 con ICMP sin Servicios…… **61**
Figura 5.2.3 Gráficas de Comparación de IPv4 e IPv6…… **62**
Figura 5.2.4 Resultados IPv4 con D-ITG…… **63**
Figura 5.2.5 Resultados IPv6 con D-ITG…… **64**
Figura 5.2.6 Resultados IPv4 con ICMP con servicios…… **65**
Figura 5.2.7 Resultados IPv6 con ICMP con servicios…… **65**

Tablas:

Tablas 1.1 Posibles Valores de Opciones de Campo Siguiente Cabecera…... **7**
Tablas 1.2 Nomenclatura de Direcciones IPv6…..……. **12**
Tablas 1.3 Asignación de Prefijos……... **13**
Tablas 1.4 Túneles Dinámicos de IPv6 sobre IPv4……. **14**
Tablas 1.5 Representación Automáticas de Direcciones IPv4 sobre IPv6…. **15**
Tablas 1.6 Comparación IPv4/IPv6……. **18**
Tablas 3.1 Equipos Principales de la Red U.N.L…..…… **39**
Tablas 3.2 Equipos de la Red A.E.I.R.N.N.R……..…….. **40**

Tablas 4.1 Equipos de Comunicación…….. **52**
Tablas 4.2 Sistemas Operativos que soportan IPv6…..……. **53**
Tablas 4.3 Aplicaciones y Servicios que soportan IPv6…….. **53**

INTRODUCCIÓN

IPv6 es la solución ideal para la implementación de redes de alta velocidad, las cuales fueron creadas para aumentar la productividad, mejorar la comunicación, y estar al margen de la disponibilidad de nuevas aplicaciones que generan cada vez más tráfico en la red.

Esta solución realiza modificaciones al protocolo de Internet actual (IPv4). La cabecera de un paquete IPv4 es variable, por lo que necesita un campo de tamaño o LENGHT. Sin embargo, para simplificar la vida de los encaminadores, IPv6 utiliza un tamaño de cabecera fija de 40 bytes, que componen un total de 8 campos entre ellos tenemos: Versión, Dirección, Origen y Destino, Clase de Tráfico, Etiqueta de Flujo, Siguiente Cabecera, Tamaño De Payload, Limite De Saltos.

IPv6 no solo multiplica el número de posibles direcciones IP, sino que añade una serie de características al protocolo que mejoran enormemente la capacidad de enrutamiento y la autoconfiguración de redes. Esto redundará en sistemas de comunicación fiables, sencillos y, sobre todo más rápidos.

La implementación de este protocolo reduce en gran medida costos operativos de comunicación; como por ejemplo los gastos adicionales que proporcionan procedimientos como el uso de NAT en una red, las seguridades que son deficientes, los juegos en línea, transacciones comerciales, etc. son algunas actividades que al salir al Internet implican costos extras.

Actualmente IPv6 es una realidad, todas las redes de Investigación y Educación del mundo soportan IPv6. Los ISP (proveedores de Servicio de Internet) están trabajando en ello, y sólo unos pocos ofrecen esta tecnología.

La Universidad Nacional de Loja tiene un fuerte compromiso en marcar la pauta en los avances tecnológicos, adoptando nuevas ideas a fin de mantener un entorno actualizado, eficaz y apto para el desarrollo integral de la sociedad universitaria. Por esto, se expone la posibilidad de adoptar esta nueva tecnología como proyecto de

implementación para la red académica del Área de la Energía, Industrias y Recursos Naturales No Renovables de la Universidad.

La topología de comunicación utilizada en la red del campus de la Universidad presenta ciertas limitantes para la implementación de nuevas tecnologías. La falta de aplicación de estándares de diseño convierte a esta estructura en una plataforma inestable pero con los requerimientos mínimos. El medio de transmisión utilizado es uno de los más adecuado para los servicios de comunicación (fibra óptica).

En cuanto a la red del Área, está diseñada en base a una topología en estrella jerárquica sin niveles de comunicación. Esto origina que existan demasiados puntos de fallo que corten la comunicación en toda la red. El servicio principal que circula en esta red es HTTP (55%), existiendo un déficit de aplicaciones de tiempo real (Voz, Multimedia), por lo que no cuenta con políticas de tráfico que den prioridad a aplicaciones más sofisticadas.

Para el análisis de rendimiento y evaluación de resultados del laboratorio de pruebas se han seleccionado herramientas que permiten observar el tráfico en tiempo real con el objetivo de obtener datos para el correspondiente análisis comparativo, levantada la topología DUAL se procede a realizar una evaluación detallada con las herramientas de generación de tráfico como ICMP (Protocolo de Mensajes de Control de Internet) y D-ITG. Dentro de la evaluación distinguimos que las comunicaciones con IPv6 son mucho más rápidas que con IPv4, con una disminución de retardo de hasta un 50%.

METODOLOGÍA

La metodología de este proyecto se basa en las adaptaciones de estándares ITU-T[1](Unión Internacional de Telecomunicaciones), el modelo TMN (Telecommunications Management Network), los modelos OSI-NM (Modelo de Referencia de Interconexión de Sistemas Abiertos) de ISO(Organización Internacional para la Estandarización) y en la infraestructura CODAREC6 Test Bed[2] (Red Informática Autónoma de Pruebas) que enfatizan en todos los aspectos relacionados a la buena operación de una red, como lo son el control sobre los sucesos en la red, la visualización de los tipos de tráfico, la detección y atención oportuna de problemas, aspectos de seguridad, etc. Además de ensayar y verificar las distintas funcionalidades IPV6 y el cumplimiento de las normativas del IETF (Grupo de Trabajo en Ingeniería de Internet) a través de sus RFCs (Request For Comments).

Con la aplicación de cada una de las metodologías indicadas se ha resumido el proyecto en cuatro fases. Cada una de ellas tiene objetivos específicos y ordenados, lo que permite obtener resultados exitosos en el desarrollo de la investigación. Las fases que a continuación se presentan definen el problema planteado a resolver.

En la *Fase1: Investigación del Protocolo IPV6 y el Internet Avanzado;* se explora profundamente el protocolo IPV6. Se realiza un estudio y análisis detallado de sus principales características y ventajas. Como métodos y técnicas utilizadas para esta fase se recurre a libros, recortes, revistas científicas e Internet. Entre la información obtenida se destaca estudios previos de este protocolo en diferentes universidades y empresas del mundo con el fin de contar con resultados aproximados a los ideales de acuerdo a los requerimientos de esta investigación, así como también la mejor solución de migración a implementarse.

En la *Fase2: Reconocimiento del Escenario;* comprende la evaluación de la red para determinar las deficiencias y problemas que en ella se presentan, para luego proceder a plantear un rediseño de la topología implementando modelos jerárquicos de diseño, para ello se recurre a métodos y técnicas tradicionales de recolección de

[1] www.aprendaredes.com/downloads/Como_Administrar_Redes.pdf
[2] codarec6.frm.utn.edu.ar/publicaciones//papers//CACIC-2006.pdf

información como entrevistas, encuestas, cuestionarios junto con la observación directa del medio. Dentro de las entrevistas realizadas se clasifica a los usuarios en dos grupos, usuarios finales y administradores de red. Con la información recolectada se definen recursos disponibles, políticas de comunicación y deficiencias en la red del Área lo cual permite plantear una solución eficaz de comunicación.

En la *Fase3*: *Análisis de Alternativas para la migración a IPv6*; se estudian todas las técnicas posibles para la transición de IPv4 a IPv6 analizando las ventajas y desventajas de su implementación en la red del Área. Además se detalla cada uno de los pasos a seguir para la migración al nuevo protocolo (IPv6), configuraciones de servicios como DNS (Servidor de Nombres de Dominio), FTP (Protocolo de Transferencia de Archivos), HTTP (Protocolo de Transferencia de Hiper Texto), etc. Básicamente esta fase se enfoca en la aplicación de la mejor solución de migración y se realizan pruebas elementales que ayudarán a demostrar las características que hacen de este un protocolo de comunicación superior al actual.

La *Fase4: Implementación de la solución y análisis de Resultados;* presenta un escenario de laboratorio para pruebas de comunicación y evaluación de los resultados obtenidos de la implementación del proyecto. Se realiza comparaciones de datos con similares aplicaciones en ambos protocolos, para demostrar las mejoras realizadas a la nueva versión. Los métodos de pruebas de validación se aplican conjuntamente con los administradores encargados de la red del Área de Energía.

6. MARCO TEÓRICO

6.1 Protocolo de Internet Versión 6 (IPv6)

Los protocolos TCP/IP (Protocolo de Control de Transmisión /Protocolo de Internet) han gobernado el funcionamiento de la red de redes INTERNET. No obstante, estos han ido sufriendo algunos cambios en sus definiciones originales para corregir imperfecciones o ajustarse a las necesidades actuales. Estos cambios han creado nuevas versiones de los protocolos, de esta forma, la Internet en el año 2000 viene gobernada por la versión 4 del protocolo IP (también denominado IPv4).

Desde hace unos años Instituciones, Universidades y Empresas trabajan en la actualización del protocolo IP. Esta versión del protocolo IP es la número 6, denominada IPv6 (IP versión 6) o IPng (IP next generation). Esta actualización de las especificaciones del protocolo IP ha sido motivada principalmente por el hecho de que el sistema de direccionamiento (actualmente de 32 bits), se ha quedado pequeño debido al gran auge de la Internet, y no se puede absorber la demanda de nuevas direcciones. Este aumento ha llevado al límite las posibilidades de los diferentes protocolos de *encaminamiento,* haciendo excesivamente lento el movimiento de los datagramas que circulan por la Internet.

Además, los últimos servicios que se ofrecen sobre esta red (comercio electrónico, redes corporativas o Virtual Private Networks, video-conferencia) requieren de componentes tanto de velocidad como de seguridad y autenticidad que la versión 4 del protocolo IP no contempla. Todo esto ha provocado la creación de algunas extensiones de seguridad, que no forman parte de la definición del protocolo IP inicial.

Debido a las carencias anteriormente citadas, se ha motivado esta nueva revisión del protocolo IP. Esta debe realizarse de una forma transparente al usuario y rápidamente, puesto que si se mantiene el ritmo de crecimiento actual de la Internet, en los años se habrán agotado todas las direcciones.

6.1.1 Definiciones

IPv6 es la evolución del protocolo IP (actualmente en su versión 4) que aporta mejoras significativas, tales en enrutamiento, mayor rango de direcciones IP, en autoconfiguración, etc.[3] Es una solución que reemplazará al TCP/IP actual (IPv4) para las comunicaciones de Internet en el futuro. Es la nueva tecnología de comunicaciones que tiene como objetivo convertirse en la plataforma base de las aplicaciones y servicios revolucionarios de desarrollo. Para ello es importante estar preparados para este cambio desde ahora mismo.

IPv4, es el protocolo de Internet actualmente utilizado, que está plagado de numerosos parches y limitaciones que en ocasiones incómoda la estancia en la Internet. IPv6 es el protocolo encargado de acabar con esas carencias y fallos, y actualmente se encuentra en fase de implementación a gran escala.

Cabe recalcar que el número de direcciones IP asignables vía IPv4 es de 4294967296, mientras que el de IPv6 es de 340282366920938463463374607431768211456 es casi infinita. Esto derivará en un descenso en el precio de la dirección, y en que se podrá disponer de más direcciones IP simultáneamente de las que podamos imaginar (se habla de 65535 direcciones IP por cliente), para poder así otorgar a cada ordenador de nuestra red local una IP pública.

Para representar una dirección IPv6 ya no se utiliza el tradicional formato "255.255.255.255", sino que se utiliza el sistema hexadecimal para representar los 128 bits de la dirección, (16 bits por sección) que pasa a tener este formato: “FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF”. Este formato es comprimible, de modo que los espacios de 16 bits de ceros quedan eliminados, como máximo una vez. Por ejemplo, la dirección 3ffe:b80:1b64:1:0:0:0:2 puede comprimirse como 3ffe:b80:1b64:1::2, que es bastante más corto. El tradicional "127.0.0.1" pasa a ser ::1 (0:0:0:0:0:0:0:1). [4]

6.1.2 Características

El nuevo protocolo de comunicación resalta las siguientes características

- *Aumento del Espacio de Direcciones*

[3] http://bulma.net/body.phtml?nIdNoticia=1840
[4] Asociación de Usuarios LINUCA, IPV6 en 5 minutos [http://www.tasio.net/], [Consulta 15 Abril 2003]

El protocolo IPV4 que forma la Internet de hoy en día está basado en una arquitectura que utiliza direcciones de 32 bits. Con la nueva versión del protocolo, las direcciones constan de 128 bits. Esto significa, entre otras cosas, que soluciones al agotamiento de direcciones IPv4, como el NAT-PT (Network Address Translation and Protocol Translation), no serán necesarias. Podemos decir que una desventaja de estas nuevas direcciones es su dificultad para recordarlas dado su tamaño: 3FFE:3330:2:0:2E0:C9FF:FE10:CB02 podría ser tranquilamente nuestra dirección IPv6. Es de suponer que el servicio DNS tendrá más importancia aún.

- *Autoconfiguración*

Plug & Play, cuando un nodo se conecta a la red, este recibe los datos necesarios para empezar a comunicarse por parte del router: dirección IPv6, máscara de red y rutas. Hay que recordar que este nuevo protocolo trata de simplificar el concepto de conexión. Con IPv4 tenemos el DHCP (Dinamic Host Configuration Protocol) para conseguir algo equivalente.

Existen dos tipos de autoconfiguración:

- Stateless: un ruteador que participa en la configuración de la dirección IPv6 del host.
- Stateful: (DHCP para IPv6) Un servicio DHCP IPv6 configura a los host con una dirección y otros parámetros de IPv6.

- *Movilidad*

El término movilidad de IP describe la habilidad de una máquina que es capaz de mover su conexión de red de un punto de Internet a otro sin cambiar su dirección IP o perder conectividad. Normalmente cuando una máquina con IP cambia su punto de conexión también debe cambiar su dirección IP. La Movilidad de IP soluciona este problema asignando una IP fija a la máquina móvil y usando encapsulación IP (Tunneling) con encaminado automático para asegurar que los datagramas destinados a ella se encaminan a la verdadera dirección IP que esté usando en ese momento.

Movilidad es la facilidad para cambiar de red, tanto a nivel físico como a nivel lógico, sin perder el transporte ni las conexiones establecidas por capas de nivel superior al IP. Para que esto sea posible, se debe mantener una misma dirección IPv6 en cualquier lugar donde se encuentre y los paquetes enviados deberán que ser encaminados hacia un destino.

- *Seguridad*

Este fue otro de los requerimientos de diseño del nuevo protocolo: todas las aplicaciones se deben beneficiar de las facilidades de autenticación y encriptación de forma transparente. El estándar escogido para eso fue el IPSec (Internet Protocol Security). Algunos de los tipos de mecanismos de seguridad:

- Autenticación: Autenticación de los paquetes, realizada con el Autenticación Header (RFC 2402).
- Payload Security: Encriptación "End to End" del paquete, realizada con el Encapsulating Security Payload Header (RFC 2406)[5].

- *Encaminamiento Jerárquico*

El encaminamiento bajo IPv6 es bastante similar al IPv4 con CIDR (Classless Inter-Domain Routing), es decir, jerárquico y sin clases. Con esto se pretende conseguir que las entradas en las tablas de rutas en los backbones no abunden más de lo necesario. Al mismo tiempo, se consigue simplificar el enrutamiento y se espera que los routers sean muy rápidos. Por ejemplo tenemos algunos protocolos de ruteo IPv6[5]:

- RIng o RIPv6 (RFC 2080, Routing Information Protocol)
- BGP4+ (RFC 2283, Border Gateway Protocol)
- OSPFv6 (Open Shorest Path First)
- EIGRPv6 (Adaptation IGRP, Interior Gateway Routing Protocol)

- *Multi-Homing*

Esta funcionalidad se consigue con direcciones anycast. Una dirección anycast identifica a un conjunto de distintas interfaces, encontrándose esos, por norma general, en distintos lados. Un paquete a una dirección Anycast será entregado a un solo miembro del conjunto. En principio, el paquete será entregado al miembro más cercano según el concepto de cercano de los protocolos de encaminamiento.

- *Calidad de Servicio*

[5] Universidad Nacional Autónoma de México, 2000 "Tutorial de IPV6"

Si bien con IPV4 tenemos unos pocos bits para el control del tipo de servicio, ToS, con IPV6 disponemos de campos más amplios para definir la prioridad del flujo de cada paquete. Según el contenido de este campo, el router deberá darle un trato más o menos especial.

El formato del paquete IPv6 fue especialmente diseñado para que pudiese ser tratado de manera eficiente por los routers, éste tiene menos campos.

Las etiquetas de flujos tienen un campo de 20 bits en la cabecera IPv6, también estos identifican el mismo origen y destino con el objetivo de tratarlos de manera especial.

6.1.3 Arquitectura de Direccionamiento

El Formato de datagrama IPv6 es**:**

<table>
<tr><td>VERSION</td><td colspan="2">CLASE DE TRÁFICO</td><td>ETIQUETA DE FLUJO</td></tr>
<tr><td colspan="2">TAMAÑO DE PAYLOAD</td><td>SIGUIENTE CABECERA</td><td>LIMITE SALTO</td></tr>
<tr><td colspan="4">DIRECCIÓN ORIGEN</td></tr>
<tr><td colspan="4">DIRECCIÓN DESTINO</td></tr>
</table>

Figura 1.3.1: *Formato de datagrama IPv6.*

La cabecera de un paquete IPv6, es sorprendente, más sencilla que la del paquete IPV4. Y recordemos que además la funcionalidad del protocolo IPv6 es mucho mayor. [6]

La cabecera de un paquete IPv4 es variable, por lo que necesita un campo de tamaño o LENGHT. Sin embargo, para simplificar la vida de los encaminadores, IPv6 utiliza un tamaño de cabecera fija de 40 bytes, que componen un total de 8 campos:

- VERSION (4 bits), sirve para que el router se entere que es un paquete IPv6.
- DIRECCION, ORIGEN Y DESTINO (128 bits c/u), son las direcciones de los nodos IPV6 que realicen la comunicación.

[6] PALET M., Jordi; 2005, "Todo sobre protocolo IPv6".

- CLASE DE TRÁFICO (8 bits), para poder diferenciar entre servicios sensibles a la latencia como VoIP, de otros que no necesitan prioridad, como tráfico HTTP.
- ETIQUETA DE FLUJO (20 bits), permite la diferenciación de flujos de tráficos. Esto tiene importancia a la hora de manejar la Calidad de Servicio (QoS).
- SIGUIENTE CABECERA (8 bits), este campo permite a routers y host examinar con más detalle el paquete. A pesar de que el paquete básico IPv6 tiene cabecera de tamaño fijo, el protocolo puede añadir más para utilizar otras características como encriptación y autentificación.
- TAMAÑO DE PAYLOAD (16 bits), describe el tamaño en octetos de la sección de datos del paquete. Al ser este campo de 16 bits, podremos usar paquetes de hasta más 64.000 bytes.
- LIMITE DE SALTOS (8 bits), específica el número de saltos de router que puede hacer el paquete antes de ser desechado. Con 8 bits podremos tener un máximo de 255 saltos.

Las Cabeceras de un paquete IPv6 se describen a continuación:

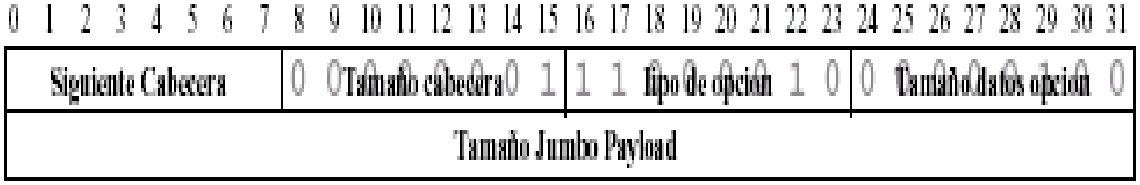


Figura 1.3.2: *Siguiente Cabecera IPV6*

Como hemos dicho antes, el tamaño de la cabecera IPv6 básica es fijo. Dentro de esta cabecera existe un campo llamado de siguiente cabecera que permite describir con más detalle las opciones del paquete. Esto quiere decir que en realidad tendremos una cabecera de tamaño fijo por norma general (64k, o mas con la opción[7]) y otra cabecera de tamaño variable en caso de que utilicemos alguna de las características avanzadas.

En el campo de siguiente cabecera se codificaran las opciones presentes en la siguiente tabla:

Siguiente Cabecera	Valor de Campo
Opciones del Hop-by- Hop	0
Opciones de destino	60

[7] http://es.wikipedia.org/wiki/IPv6

Encaminamiento	43
Fragmento	44
Autentificación	51
Encapsulación	50
Ninguna	59

Tabla 1.1: *Posibles Valores de Opciones campo siguiente cabecera*

Esta arquitectura es muy flexible, ya que cada cabecera tiene un campo de siguiente cabecera, con lo que podemos tener varias opciones agregadas. Un ejemplo ilustrativo lo podemos ver en las figuras 1.3.3 y 1.3.4

Con la cabecera de encaminamiento conseguimos la funcionalidad equivalente de IPv4 de Source-Routing, es decir, especificar los nodos intermedios por los que ha de pasar el paquete.

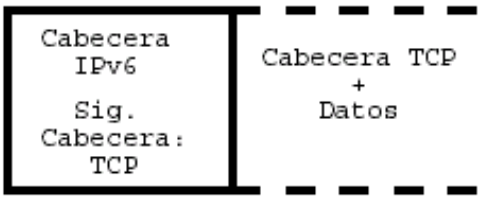


Figura 1.3.3: *Cabecera IPV6 básica y datos.*

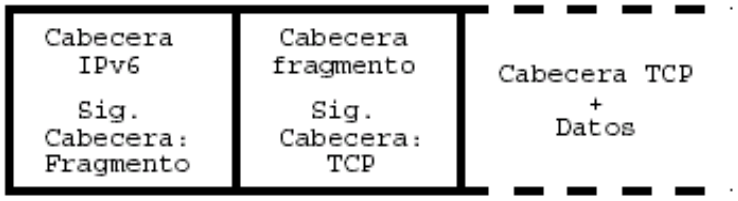


Figura 1.3.4: *Cabecera IPv6 básica, fragmentos y datos.*

Una cosa que ha de quedar bien clara es que los nodos intermedios o encaminadores NO deben examinar más que la cabecera IPv6 básica. Existen excepciones como en el caso de que existan cabeceras de opciones Hop-by-Hop o, como en el caso anterior, que exista una cabecera de encaminamiento en el que solo los nodos en ella definidos deberán alterar el paquete.

Las especificaciones recomiendan además el siguiente orden para las cabeceras adicionales:

- Cabecera IPv6 básica.
- Opciones Hop-by-Hop.

- Opciones de destino.
- Encaminamiento.
- Fragmento.
- Autenticación.
- Encapsulación.
- Opciones de destino.
- Cabecera nivel superior.

Las opciones de destino pueden ser procesadas en momentos distintos dependiendo de si el paquete atraviesa un nodo intermedio o llega al nodo destino. La única restricción de la especificación es que las opciones de Hop-by-Hop han de ir siempre de la cabecera básica.
El protocolo de internet versión 6 reconoce los siguientes tipos de direcciones:

UNICAST[8]: Identificador para una única interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz con dicha dirección. Es el equivalente a las direcciones IPv4 actuales.

ANYCAST[7]: Identificador para un conjunto de interfaces (típicamente pertenecen a diferentes nodos). Un paquete enviado a una dirección anycast es entregado en una de las interfaces identificadas con dicha dirección (la más próxima, de acuerdo a las medidas de distancia del protocolo de encaminado). Nos permite crear, por ejemplo, ámbitos de redundancia, de forma que varias máquinas puedan ocuparse del mismo tráfico según una secuencia determinada (por el routing).

MULTICAST[7]: Identificador para un conjunto de interfaces (por lo general a diferentes nodos). Un paquete enviado a una dirección multicast es entregado a todas las interfaces identificadas por dicha dirección. La misión de este tipo de paquete es evidente: aplicaciones de retransmisión múltiple (broadcast).

[8] COMER, Douglas, 1996, Redes Globales de Información con Internet y TCP/IP, México, Prentice-Hall Hispanoamericana S.A.

Cualquier tipo de dirección se asigna a interfaces, no nodos. Todas las interfaces han de tener, por los menos, una dirección de enlace local (Link-Local) de tipo unicast. Una mismo interfaz puede tener asignadas múltiples direcciones de cualquier tipo (unicast; anycast, multicast) o ámbito (scope). Direcciones unicast con ámbito mayor que el de enlace no son necesarias para interfaces que no son usados como origen y destino de paquetes IPv6 hacia o desde no vecinos. Esto significa que para la comunicación dentro de una LAN no nos hacen falta direcciones lPV6 globales, sino que tenemos más que suficiente con direcciones de ámbito local. De hecho, es lo aconsejable para enlaces punto a punto.

Respecto a los prefijos de subred, IPv6 sigue el mismo modelo que IPv4, es decir, un prefijo se asocia a un enlace, pudiendo haber varios prefijos en un mismo enlace.

A continuación se explica la nomenclatura de las direcciones IPv6:

1) x:x:x:x:x:x:x:x, donde “x” es un valor hexadecimal de 16 bits, de la porción correspondiente a la dirección IPv6. No es preciso escribir los ceros a la izquierda de cada campo. Ejemplos:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

1080:0:0:0:8:800:200C:417A

2) Dado que, por el direccionamiento que se ha definido, podrán existir largas cadenas de bits “cero”, se permite la escritura de su abreviación, mediante el uso de “::”; que representa múltiples grupos consecutivos de 16 bits “cero”. Este símbolo sólo puede aparecer una vez en la dirección IPv6. Ejemplos: Las direcciones:

1080:0:0:0:8:800:200C:417A (una dirección unicast)

FF01:0:0:0:0:0:0:101 (una dirección multicast)

0:0:0:0:0:0:0:1 (la dirección loopback)

0:0:0:0:0:0:0:0 (una dirección no especificada)

3) Una forma alternativa y muy conveniente, cuando nos hallemos en un entorno mixto IPv4 e IPv6, es x:x:x:x:x:x:d:d:d:d, donde "x" representa valores hexadecimales de 16 bits (6 porciones de mayor peso), y "d" representa valores

decimales de las 4 porciones de 8 bits de menor peso(representación estándar IPv4). Ejemplos:

0:0:0:0:0:0:13.1.68.3

0:0:0:0:0:FFFF:129.144.52.38

Pueden representarse como:

::13.1.68.3

::FFFF:129.144.52.38

La representación de los prefijos IPv6 se realiza del siguiente modo:

dirección-IPv6/longitud-del-prefijo

donde:

- Dirección-IPv6 = una dirección IPv6 en cualquiera de las notaciones válidas.
- Longitud del Prefijo = valor decimal indicando cuantos bits contiguos de la parte izquierda de la dirección componen el prefijo.

Por ejemplo, las representaciones válidas del prefijo de 60 bits12AB00000000CD3, son:

12AB:0000:0000:CD30:0000:0000:0000:0000/60

12AB::CD30:0:0:0:0/60

12AB:0:0:CD30::/60

Por tanto, para escribir una dirección completa, indicando la subred podríamos hacerlo como:

12AB:0:0:CD30:123:4567:89AB:CDEF/60

REPRESENTACIÓN NORMAL	***REPRESENTACIÓN ABREVIADA***	***TIPO***
1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A	Unicast
FF01:0:0:0:0:0:0:101	FF01::101	Multicast
0:0:0:0:0:0:0:1	::1	Loopback
0:0:0:0:0:0:0:0	::	Dirección no especificada

Tabla 1.2: *Nomenclatura de Direcciones IPv6* [9]

La representación de los prefijos[10] de direcciones con IPv6 es similar a la que tenemos con CIDR con IPv4 (dirección-IPv6/tamaño-prefijo), donde dirección IPv6 es alguna de las notaciones vistas anteriormente y tamaño-prefijo es un valor decimal que especifica cuantos bits de la dirección corresponden al prefijo.

Por ejemplo; el prefijo de una dirección cualquiera en hexadecimal es 3FFE33300002, que son 48 bits, lo podemos escribir como:

3FFE:3330:0002:0000:0000:0000:0000:0000/48

3FFE:3330:2:0:0:0:0:0/48

3FFE:3330:2::/48

El tipo específico de cada dirección IPv6 viene dado por los primeros bits de ésta, dentro de lo que se llama el campo de formato de prefijo. El tamaño de este campo es variable. La asignación de estos prefijos[11] la podemos ver en la siguiente tabla:

Asignación	***Prefijo***
Reservado	0000 0000
No Asignado	0000 0001
Reservado para asignación NSAP	0000 001
Reservado para asignación IPX	0000 010
No Asignado	0000 011
No Asignado	0000 1
No Asignado	0001
Direcciones Unicast Globales	001

[9] PERALTA, Luis; "IPV6", Febrero 2002
[10] ROCHA, M.; "*Interconectandonos con IPV6*", Fundación RETINA NAP CASE, 2006
[11] PALET M., Jordi; 2005, "Todo sobre protocolo IPv6".

Agregables	
No Asignado	001
No Asignado	010
No Asignado	011
No Asignado	100
No Asignado	101
No Asignado	110
No Asignado	1110
No Asignado	1111 0
No Asignado	1111 10
No Asignado	1111 110
No Asignado	1111 1110 0
Direcciones Unicast Link-Local	1111 1110 10
Direcciones Unicast Site-Local	1111 1111 11
Direcciones Multicast	1111 1111

Tabla 1.3: *Asignación de Prefijos*

Los prefijos desde 001 a 111 tienen la obligación de tener los identificadores de interfaz de 64 bits, excepto para las direcciones Multicast (1111 1111). Las direcciones unicast se distinguen por el valor del octeto de mayor peso; que tiene algún valor distinto de '1'.

Las direcciones Anycast se asignan dentro del espacio de las Anycast y no son distinguibles entre sí observando sus bits.

Como podemos ver, hay mucho espacio no asignado (el 85%), lo que en un futuro permitirá expandir el espacio posible o incluso dar nuevos usos.

Se han definido también las direcciones para usos especiales[12] como:

- *Dirección de Auto-remoto o Loopback (::1).-* No ha de ser asignada a una interfaz física; se trata de una interfaz "virtual ", pues se trata de paquetes que no salen de la máquina que los emite; nos permite hacer un bucle para verificar la correcta inicialización del protocolo (dentro de una determinada máquina).

- *Dirección No Especificada(::).-* Nunca debe ser asignada a ningún nodo, ya que se emplea para indicar la ausencia de dirección; por ejemplo, cuando se halla en

[12] Consultores Informáticos de Telecomunicaciones, IPv6FORUM; *"Tutorial IPV6"*

el campo de dirección fuente, indica que se trata de un host que está iniciándose, antes de que haya aprendido su propia dirección.

- *Túneles dinámicos/automáticos de IPv6 sobre IP4(::<direcciónIPv4>).-* Se denominan direcciones IPv6 compatibles con IPv4, y permiten la retransmisión de tráfico IPv6 sobre infraestructuras IPv4, de forma transparente.

80 bits	16 bits	32 bits
0000…0000	0000	Dirección IPv4

Tabla 1.4: *Túneles Dinámicos de IPv6 sobre IPv4*

- *Representación Automática de Direcciones IPv4 sobre IPv6.-* Permite que los nodos que sólo soportan IPv4, puedan seguir trabajando en redes IPv6. Se denominan "direcciones IPv6 mapeadas desde IPv4".

80 bits	16 bits	32 bits
0000…0000	FFFF	Dirección IPV4

Tabla 1.5: *Representación Direcciones IPv4 sobre IPv6*

Todos los nodos, en el proceso de identificación, al unirse a la red, deben reconocer como mínimo las siguientes especificaciones:

- Su dirección de enlace local (link-local) para cada interfaz.
- Su dirección anycast asignada.
- Su dirección loopback
- La dirección multicast de "Todos los nodos".
- Las direcciones multicast de todos los grupos a los que pertenezca.

Además, si el nodo es un router, se requiere que reconozca también:

- La direcciones anycast de cada subred para las que es router.
- Las direcciones anycast que se le han asignado.
- La dirección multicast de "Todos los routers".

En cuanto a prefijos, los únicos predefinidos en una implementación son:

- La dirección especifica.
- La dirección de loopback.

- El prefijo multicast.
- Los prefijos locales de enlace y de sitio.
- Las direcciones multicast predefinidas.
- Los prefijos compatibles IPv4.

6.1.4 Técnicas de Transición

El cambio de IPv4 a IPv6 ya ha comenzado. Durante 20 años se espera que convivan ambos protocolos, y que la implantación de IPv6 sea paulatina.

Existe una serie de mecanismos que permiten la convivencia y la migración progresiva tanto de las redes cómo de los equipos de usuarios.

Puesto que Internet no va a amanecer un día utilizando de repente IPv6 en lugar de IPv4, se han debido desarrollar una serie de métodos que permiten la convivencia y comunicación entre nodos, sea cual sea su versión de protocolos IP. Como pronto veremos, se han desarrollado unos cuantos, cada uno de ellos con sus ventajas e inconvenientes, pero sobre todo pensados en un principio para casos de migración distintos.

Durante el periodo de transición, los datagramas enfrentarán casos como el tener que atravesar caminos con proveedores mezclados, es decir, proveedores de versión 4 con proveedores de versión 6.

No utilizar un mecanismo de los aquí descritos u otro no tiene mucho sentido dada la pequeña cantidad de servicios que se están ofreciendo bajo la Internet IPv6 actual. Mas el objetivo principal de estos métodos de transición[13] es adentrar a los usuarios y administradores de red a lo que en un futuro cercano será la tecnología predominante de las comunicaciones e Internet. Estos mecanismos son un conjunto de técnicas y de protocolos implementados en host y routers, junto con algunas guías operativas de direccionamiento designadas para hacer la transición de IPv4 al IPv6 con la menor interrupción posible.

A continuación detallaremos tres mecanismos básicos de transición:

- ***Dual Stack.-*** (Doble Pila), el más lógico y evidente de transición es el uso simultáneo de ambos protocolos, en pilas separadas. Los dispositivos con ambos protocolos también se denominan "nodos IPv6/ IPv4". Aunque parezca la técnica de coexistencia más costosa debido a que es necesario

[13] RALLI, Carlos: *"Introducción de Mecanismos de Transición IPV4-IPV6"*

actualizar cada dispositivo en el camino de comunicación, ésta es la recomendada ya que no se rompe la armonía de la tecnología, manteniendo soporte nativo tanto para IPv4 como para IPv6, mientras se preserva vigente el concepto extremo a extremo de la Internet.

De esta forma, un dispositivo con ambas pilas pueden recibir y enviar tráfico a nodos que sólo soportan uno de los dos protocolos (nodos sólo IPv4 o sólo IPv6). Entre las ventajas encontramos facilidad en su despliegue y es extensamente soportando por el hardware actual, y como desventajas podemos mencionar el manejo de tablas de encaminamiento y dos procesos de encaminamiento (gestión de dos redes paralelas). Cada nodo en la red necesita tener actualizado las dos pilas, además incrementa la complejidad en el desarrollo de nuevas aplicaciones

- ***Tunneling.-*** El principio detrás de la *"tunelación"* es el encapsular paquetes IPv6 en paquetes IPv4; empaquetar paquetes dentro de otros paquetes en realidad es una técnica muy poderosa. Este mecanismo es muy útil para conectar dos islas informáticas bien conocidas y muy poco probable que cambien, como pueden ser una sucursal y la oficina principal.

  La idea central es entender que al igual que los encabezados Ethernet rodean los paquetes IP, los que rodean encabezados TCP y UDP (User Datagram Protocol), los que rodean protocolos como SMTP (Simple Mail Transfer Protocol), podemos fácilmente insertar otro paquete donde iría un paquete TCP y confiar en el sistema de enrutamiento para que lleve el paquete al lugar ideal, siempre y cuando tanto el origen como el destino sepan cómo tratar estos paquetes. Ejemplo:

  6over4

  Es un mecanismo para correr una red IPv6 usando IPv4 como la capa 2 de transporte. Permite ND (Neighbor Discovery) con la red IPv4 actuando como la LAN (Red de Área Local).

Hay que recordar que IPv6 usa la capa 2 para hacer multicast, así que 6over4 logra todo esto usando multicast en IPv4.[14]

- ***Traslación o Traducción.-*** es necesaria cuando un nodo solo IPv4 intenta comunicar a otro nodo solo IPv6. Los mecanismos de traducción pueden ser divididos en dos grupos basándose en si la información de estado está guardada:
    1) Con Estado.- NAT-PT, TCP-UDP relay, SOCKS-BASED GATEWAY
    2) Sin Estado.- BUMP-IN-THE-STACK, BUMP-IN-THE-API

La aplicación de la traducción puede hacer necesario incrementar módulos a las aplicaciones y también presenta obstáculos a la escalabilidad.

6.1.5 Comparaciones con el protocolo IPv4

Para tener una idea más clara de las diferencias entre ambos protocolos, en el siguiente cuadro se realiza una comparación más precisa entre IPv4 e IPv6.

	IPv4	IPv6
Direcciones	Las direcciones de origen y destino tienen una longitud de 32 bits (4 bytes).	Las direcciones de origen y destino tienen una longitud de 128 bits (16 bytes).
Seguridad (IPSec)	La compatibilidad es opcional.	La compatibilidad es obligatoria.
Identificación del número de paquetes	No existe ninguna identificación de flujo de paquetes para que los enrutadores controlen la QoS en el encabezado IPv4.	Se incluye la identificación del flujo de paquetes para que los enrutadores controlen la QoS en el encabezado IPv6, utilizando el campo Flow Label (etiqueta de flujo).
Fragmentación	La llevan a cabo los enrutadores y el host que realiza el envío.	No la llevan a cabo los enrutadores, sino únicamente el host que realiza el envío.

[14] http://www.geeks.ms/blogs/eliasmereb/archive/2007/08/19/IPv6-mecanismos-de-transici-243-n.aspx

Encabezado	Incluye una suma de comprobación.	No incluye una suma de comprobación.
Opciones	El encabezado lo incluye.	Todos se trasladan a los encabezados de extensión IPv6.
Marcos de solicitud ARP	El Protocolo de resolución de direcciones (ARP) utiliza los marcos de solicitud ARP de difusión para resolver una dirección IPv4 como una dirección de capa de vínculo.	Los marcos de solicitud ARP se sustituyen por mensajes de solicitud de vecinos de multidifusión.
Administrar la pertenencia a grupos locales de subred	Se utiliza el Protocolo de administración de grupos de Internet (IGMP).	IGMP se sustituye con los mensajes de Descubrimiento de escucha de multidifusión (MLD).
Determinar la dirección IPv4 de la mejor puerta de enlace predeterminada	Se utiliza el Descubrimiento de enrutadores ICMP, y es opcional.	ICMP queda sustituido por la Solicitud de enrutadores ICMPv6 y los mensajes de anuncio de enrutador, y es obligatorio.
Direcciones de multidifusión	Se utilizan para enviar tráfico a todos los nodos de una subred.	No hay direcciones de multidifusión IPv6. De forma alternativa, se utiliza una dirección de multidifusión para todos los nodos.
Configuración manual	Debe configurarse manualmente o a través de DHCP.	No requiere configuración manual o a través de DHCP.
DNS	Utiliza registros de recurso (A) de dirección de host en el Sistema de nombres de dominio (DNS) para correlacionar nombres de host con direcciones IPv4.	Utiliza registros de recurso (AAA) de dirección de host en el Sistema de nombres de dominio (DNS) para correlacionar nombres de host con direcciones IPv6.
Direcciones IP relacionados con host	Utiliza registros de recurso (A) de puntero en el dominio DNS IN-ADDR.ARPA para correlacionar direcciones IPv4 con nombres de host.	Utiliza registros de recurso (PTR) de puntero en el dominio DNS IP6.INT para correlacionar direcciones IPv6 con nombres de host.
Tamaño de paquete	Debe admitir un tamaño	Debe admitir un tamaño

	de 576 bytes (posiblemente fragmentado).	de 1280 bytes (sin fragmentación).

Tabla 1.6: *Comparación entre IPv6 / IPv4*

6.2 Internet Avanzado

La Internet de hoy en día ya no es una red académica, como en sus comienzos, sino que se ha convertido en una red que involucra, en gran parte, intereses comerciales y particulares. Esto la hace inapropiada para la experimentación y el estudio de nuevas herramientas en gran escala.

Adicionalmente, los proveedores de servicios sobre Internet "sobrevenden" el ancho de banda que disponen, haciendo imposible garantizar un servicio mínimo en horas pico de uso de la red. Esto es crítico cuando se piensa en aplicaciones que necesiten calidad de servicio garantizada, ya que los protocolos utilizados en la Internet actual no permiten esta funcionalidad.

Por otro lado, los enlaces de alta velocidad son aún demasiado costosos para poder realizar su comercialización masiva. Todo esto, entonces, nos lleva a la conclusión que Internet no es un medio apto para dar el salto tecnológico que se necesita para lograr un desarrollo más competitivo.

6.2.1 Definiciones

Internet Avanzado es una red de cómputo con capacidades avanzadas separada de la Internet comercial actual. Su origen se basa en el espíritu de colaboración entre las universidades del país y su objetivo principal es desarrollar la próxima generación de aplicaciones telemáticas para facilitar las misiones de investigación y educación de las universidades, además de ayudar en la formación de personal capacitado en el uso y manejo de redes avanzadas de cómputo.

Internet Avanzado es una red con canales de salida exclusivos que permiten trabajar en proyectos de manipulación de información con fines investigativos-académicos, para lograr esto, la plataforma brinda características como:

- Gran ancho de banda
- Retardos muy bajos

- Multidifusión (Multicast)
- IPv4/IPv6
- Calidad de Servicio (Qos)
- Menos saltos y congestionamiento[15]

Las Universidades son las principales impulsoras de esta nueva tecnología de comunicación. Por cuanto la Internet actual no satisface ciertas necesidades como mayores anchos de banda, conexiones dedicadas. etc. Geánt (Red Informática Europea) fue la primera red avanzada que funcionó por primera vez en el año 2001, interconectando 28 redes nacionales y regionales en Europa. En el 2005 esta misma red se moderniza y evoluciona a GEANT2 utilizando cables de fibra óptica negra alcanzando velocidades de 320Gb/s.

Hoy Internet 2, es la red de mayor prestación en cuanto a redes avanzadas se refiere. Está formado por Universidades de EEUU principalmente, pero también se enlaza a GEANT2 de EUROPA y a CLARA (Corporación Latinoamericana de Redes Avanzadas) en América Latina.

Las instituciones conectadas a Internet2 se comunican entre ellas a través de redes de alto rendimiento por la misma conexión usada a Internet actual, es decir, es el ISP (Internet Service Provider) conectado a Internet2 el que se encarga de dirigir el tráfico a través de Internet2 o Internet comercial según corresponda.

No es necesario equipamiento especializado para conectarse a Internet2, basta con que el enlace de la Universidad esté conectado a Internet2 para que cualquier computador dentro de la Universidad haga uso de esta red.

El uso de Internet como herramienta educativa y de investigación científica ha crecido aceleradamente debido a la ventaja que representa el poder acceder a grandes bases de datos, la capacidad de compartir información entre colegas y facilitar la coordinación de grupos de trabajo.

Internet2 no es una red que reemplazará a la Internet actual. La meta de Internet2 es el unir a las instituciones académicas nacionales y regionales con los recursos

[15]http://ocw.mit.edu/RAAP2_RAGIE.pdf

necesarios para desarrollar nuevas tecnologías y aplicaciones, que serán las utilizadas en la futura Internet.

Las Universidades tienen una larga historia de desarrollo de redes avanzadas de investigación y de ponerlas en funcionamiento. Esta combinación de necesidades y recursos proporciona el marco perfecto para desarrollar la próxima generación de posibilidades de Internet.

Las universidades son la fuente principal de demanda tanto por las tecnologías de intercomunicación como por el talento necesario para ponerlas en práctica. Las investigaciones en las diversas áreas del conocimiento se llevan a cabo principalmente en las universidades. Las aplicaciones que actualmente se están desarrollando en Internet2 abarcan diversas disciplinas como astronomía, medicina, educación a distancia, arquitectura, física, ciencias sociales, etc. Los educadores e investigadores requieren cada vez más de tareas de colaboración y de infraestructura de comunicaciones. Estos son exactamente los elementos para los cuales la Internet de hoy brinda herramientas insuficientes, y que necesitan las tecnologías que Internet2 se propone crear.

Al mismo tiempo, es en las universidades donde reside el mayor nivel de pericia en redes de computadoras y donde se encuentran usuarios especializados en las diversas disciplinas. Por último, el académico es, de los sectores con capacidad para llevar adelante este tipo de investigaciones y es el menos permeable a las presiones comerciales.

Lo anterior no excluye al sector privado, ya que el mismo es un socio importante en este proyecto, y se beneficiará con las nuevas aplicaciones y tecnologías desarrolladas al integrarse como socios en este esfuerzo.

6.2.2 Características de Redes Avanzadas

En el mundo de las Redes Avanzadas se define como aplicación a toda aquella herramienta que se construye y utiliza sobre la red para el desarrollo de la ciencia, la educación y la investigación. En estricto rigor, en las Redes Avanzadas todas las herramientas y servicios son productos de aplicaciones que han sido desarrolladas por expertos.

Estas aplicaciones marcan una gran diferencia en el cómo se llevan a cabo los procesos de enseñanza y aprendizaje e investigación. Las aplicaciones desarrolladas en este ámbito requieren para su funcionamiento de las Redes Avanzadas, lo que implica que ellas no correrán ni funcionarán sobre la Internet comercial. Éstas requieren de funcionalidades de red avanzadas, tal como amplio ancho de banda, baja latencia (retraso) o multidifusión; ninguna de estas funcionalidades está disponible en las conexiones de la Internet comercial.

Desde los inicios de las Redes Avanzadas se han desarrollado muchas aplicaciones, varias de ellas ya han sido traspasadas a la Internet comercial para su uso expandido, eso sí, con calidades inferiores a las que se pueden alcanzar en las Redes Avanzadas. El correo electrónico, las videoconferencias, la telefonía IP, son sólo algunos de los ejemplos de aplicaciones que ya son masivas en el escenario comercial de Internet.

En las Redes Avanzadas, si bien es cierto existen y se están desarrollando una enorme cantidad de aplicaciones para las distintas áreas de la ciencia y del conocimiento, hoy existen aplicaciones consideradas de punta o de "próxima generación". Cuatro son los atributos principales de estas aplicaciones:

- Ambientes de colaboración interactivos, en los que realmente se pude interactuar con otros sin importar las distancias y las barreras geográficas.
- Provisión de acceso común a recursos remotos y distribuidos, tales como telescopios, microscopios, entre otros instrumentales científicos de alto valor.

- Utilización de la red como base para construir redes globales de servicios conexiones computacionales y de procesamiento de datos; esto posibilita la existencia de las Grid o Mallas.

- Despliegue de información en ambientes de realidad virtual, lo que supone pasar de gráficos estáticos a flujo de imágenes en tiempo real y a animaciones tridimensionales. Esto permite el desarrollo de aquellas aplicaciones basadas en el uso del video, lo que cubre un amplísimo espectro que va desde la videoconferencia pasando por el video en demanda hasta llegar al control en forma remota de instrumental científico.

6.2.3 Aplicaciones de Redes Avanzadas:

- **Mallas (Grids):**

  "Los proyectos científicos de comienzos de este siglo abordan objetivos cada vez más ambiciosos que requieren la resolución de problemas computacionales complejos, tanto por el volumen de los cálculos a realizar como por el tamaño y complejidad de las bases de datos utilizadas. Del mismo modo, los equipos científicos son en muchos casos colaboraciones internacionales, con miembros distribuidos por todo el planeta. Áreas científicas como la Física de Altas Energías, Ciencias del Espacio, Medicina, Genómica y Proteómica, o Meteorología, basan su desarrollo en estos proyectos. El término e-Ciencia se utiliza para denominar la vertiente computacional de estos proyectos. La organización de los correspondientes recursos de computación, es un desafío" ("GRID y E-Ciencia", Jesús Marco Boletín de RED IRIS N°61). Para enfrentar este desafío existen varias soluciones, entre ellas las que se basan en tecnologías de Mallas (Grid). Éstas proponen, mediante redes de alta velocidad, agregar y compartir recursos de computación distribuidos entre diferentes organizaciones e institutos, así el acceso de los científicos a ellos –por ejemplo, para sus necesidades de cálculo- resulta tan sencillo, flexible y fiable como el uso de la corriente eléctrica que satisface sus necesidades de energía.

  Actualmente REUNA (Red Universitaria Nacional) participa en forma activa en dos proyectos internacionales de Mallas, financiados por la Comisión Europea, éstos son: EELA (E-Infrastructure shared between Europe and Latin America), y RINGrid (Remote Instrumentation in Next-Generation Grids).

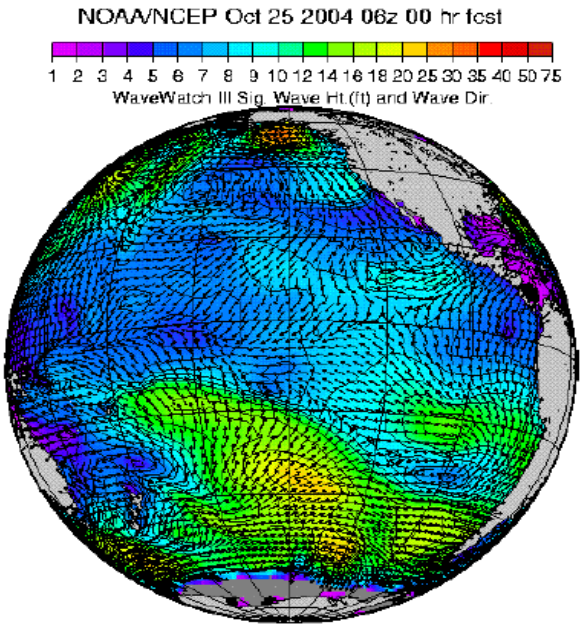


Figura 2.3.1 Ejemplo de Mallas

- **Instrumentación Remota:**

  Su principal objetivo es utilizar a distancia, mediante las Redes Avanzadas, el instrumental científico (generalmente de muy alto valor y por lo tanto de difícil acceso) en un ambiente de colaboración entre investigadores y usuarios. Esta tendencia se ha reforzado por la aparición de productos computacionales complementarios y que permiten acceder en red a la operación parcial y a la visualización de resultados en algunos equipos muy sofisticados.

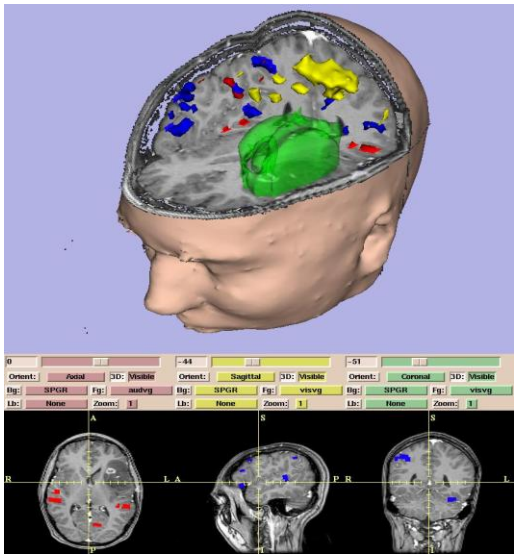


Figura 2.3.2 Ejemplo de Instrumentación Remota (Medicina)

REUNA ejecutó el proyecto UCRAV (Uso Compartido e Recursos de Alto Valor), mediante el cual se desarrolló, por primera vez en Chile, el servicio (fruto de la aplicación construida) de instrumentación remota; utilizando recursos disponibles en las universidades participantes del proyecto, sus principales beneficiarios se identificaron en el ámbito de la investigación y la docencia de universidades, centros de investigación y empresas públicas y privadas.

Siempre en la misma línea de instrumentación remota, REUNA participa hoy el proyecto internacional, financiado por la Comisión Europea, RINGrid (Remote Instrumentation in Next-Generation Grids).

Figura 2.3.3 Ejemplos de Instrumentación Remota (Musical)

- **Multicast:**

  Esta aplicación también llamada Multidifusión sirve principalmente para poner "contenido" en las redes optimizando el uso de ancho de banda. Ahora bien, por contenido entendamos todo: datos, video, audio; así de plural. La gran ventaja del Multicast sobre el streaming corriente (conocido como Unicast), es que en vez de derrochar ancho de banda por cada usuario que se conecta a una transmisión (difusión), solo se gasta el ancho de banda correspondiente única y exclusivamente a la emisión; Así, si por ejemplo usted tiene un streaming

normal de video, que consume digamos 100 Kbps, al haber un único usuario viéndolo, en la red del servidor que alberga el video se usarán 100 Kbps; pero si se conectan más personas a dicha transmisión, ese ancho de banda será multiplicado, de modo tal que si hay 10 personas queriendo ver el video, quien maneja el servidor debe disponer de 1000 Kbps (1 Mbps) de ancho de banda. Y así suma y sigue; finalmente, para el encargado del servidor, la tarea puede ser titánica.

Ahora, mediante Multicast, tomando el mismo ejemplo anterior, las cosas funcionan de plano distinto: ya sea que se conecten una o 10.000 personas, el ancho de banda que se necesita es y será siempre el mismo; volviendo a nuestro ejemplo, sólo 100 Kbps. Esto brinda no sólo una solución en términos de transferencia masiva de datos, sino que la posibilidad de llevar a cabo emisiones de mayor calidad puesto que no se saturan las redes ni los servidores. Entonces, en vez de usar 100 Kbps, se pueden utilizar 500 Kbps o 1 Mpbs y tener algo de muy buena definición audio/video, a muchos años luz de las emisiones que no emplean esta tecnología. Además, usted puede dejar un video en permanente emisión –estilo parrilla programática de TV- y si nadie se conecta a él, pues no se utiliza ancho de banda.

Multicast también puede emplearse para distribuir software o archivos, en determinados horarios. Finalmente, considere que algunas de las aplicaciones nuevas de videoconferencia (como AccessGrid) requieren necesariamente de redes con Multicast habilitado.

- **Ambientes Virtuales de Colaboración:**

  Las colaboraciones en gran escala, ya sean científicas, técnicas o académicas, usualmente involucran las participación de muchos actores geográficamente dispersos. Ahí es donde entran a jugar un rol preponderante los ambientes virtuales de colaboración, posibilitando, a través del uso de las tecnologías de video y videoconferencia (como base), la interacción cara a cara en tiempo real, lo que mejora la comunicación y, por lo tanto, las condiciones para la colaboración en un ambiente común.

Access Grid es una aplicación que explora y soporta los requerimientos de interacciones grupo a grupo a través de mallas computacionales. Conformado por un conjunto de elementos multimedia (audio, video, soporte para presentaciones) y software de interacción de ambientes, interfaces de middleware de Malla e interfaces de visualización remota de ambientes, los nodos Access Grid son "espacios diseñados" que soportan tecnología de audio/video de alta calidad, requerido para proveer una experiencia colaborativa estimulante y productiva. Al proveer acceso a estos recursos, Access Grid apoya el desarrollo a gran escala de reuniones distribuidas, seminarios, presentaciones, tutoriales y capacitaciones, entre otras. Otra aplicación en esta área es VRVS (Virtual Room Videoconferencing System), plataforma de colaboración basada en salas virtuales, donde los participantes interactúan mediante tres elementos: videoconferencia entre todos los usuarios que "ingresan" a una Sala Virtual, pantalla de conversación escrita (chat) entre los participantes, y un mecanismo para compartir documentos y aplicaciones.

Los participantes –conectados a la Red Mundial de Investigación y Desarrollo (ReD+I), las Redes Académicas Avanzadas– ingresan a una reunión "virtual" nacional o internacional donde interactúan en forma simultánea y en tiempo real, mediante conversación verbal y escrita y transmisión de imagen en movimiento. Las reuniones se pueden programar en "salas virtuales" previamente reservadas (se ingresa con clave de acceso) o en "salas de prueba" públicas (acceso liberado).

REUNA es parte de la red mundial de reflectores VRVS, lo que asegura un servicio de calidad a los miembros de la Corporación. Los 62 reflectores se localizan en universidades de Estados Unidos, Europa, Asia y América del Sur.[16]

[16] http://www.reuna.cl/joomla/index.php?option=com_content&task=view&id=118&Itemid=143

Figura 2.3.4 Ejemplo de Ambientes Virtuales

6.2.4 Estado actual de las Redes Avanzadas en Ecuador

En América Latina: el futuro de las redes avanzadas a fomentado un proyecto denominado CLARA (Cooperación Latinoamericana de Redes Avanzadas) y consiste en una alianza que han formado las redes académicas de Panamá, México, Argentina, Ecuador, Perú, Cuba, Costa Rica, Uruguay, Bolivia, Colombia, Guatemala, Brasil, Venezuela, Paraguay, El Salvador, República Dominicana y Chile, para materializar la interconexión de América Centro y Sur con las redes avanzadas del mundo.

En Ecuador el Internet Avanzado lo dirige CEDIA (Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado), el cual reúne a diferentes Universidades a nivel Nacional como grupo de apoyo para desarrollar este proyecto.

La misión de CEDIA es:

"Promover y coordinar el desarrollo de redes avanzadas de informática y telecomunicaciones, enfocadas al desarrollo científico, tecnológico, innovador y educativo en el Ecuador"[17].

Sus objetivos son:

- Fomentar y Coordinar proyectos de investigación que aprovechen aplicaciones de tecnología avanzada enfocadas al desarrollo científico y educativo de la sociedad ecuatoriana.

[17] JARAMILLO, Marcelo; Presentación de CEDIA. 2004 [diapositiva] Quito, Ecuador.

- Promover el desarrollo y formación de recursos humanos para la innovación y desarrollo de aplicaciones educativas y de tecnología avanzada.
- Promover la interconexión e interoperabilidad de la redes de las Instituciones Asociadas y de los Afiliados al CEDIA
- Promover el desarrollo de nuevas aplicaciones entre sus miembros.
- Difundir entre sus miembros todos los desarrollos que se realicen.
- Relevar y determinar las necesidades de desarrollo de Tecnología de Información, Telecomunicaciones e Informática de la red avanzada.
- Responsable de la administración, control y gestión del punto de conexión en el Ecuador.

La estructura de la Red CEDIA (figura 2.4.1) abarca en todo el país uniendo en cada provincia a las instituciones académicas participantes. Esta topología inicial tiene como objetivo comunicar a todos los entes involucrados para posteriormente conectarse con el proyecto CLARA en el resto de Latinoamérica.

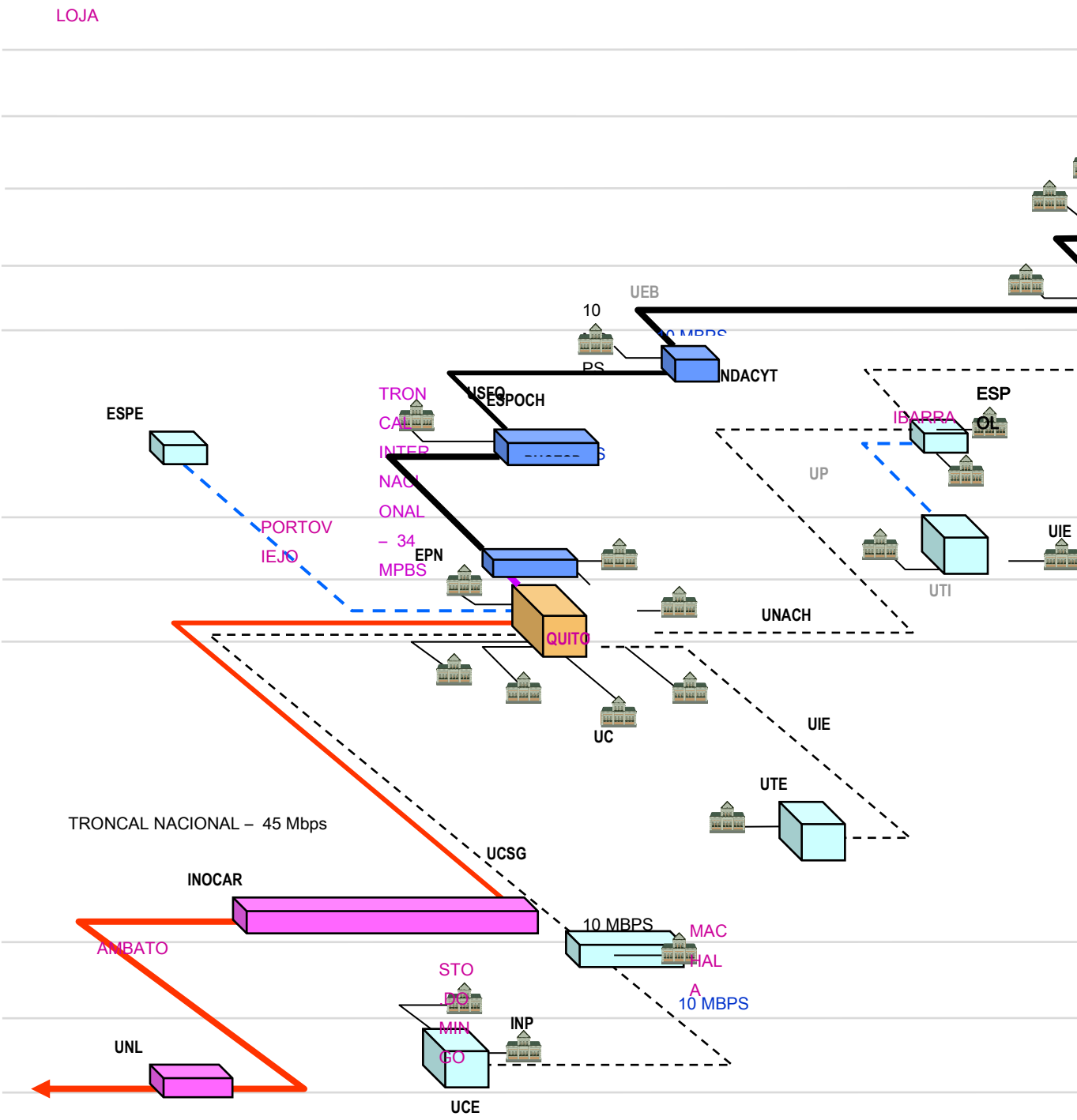


Figura 2.4.1: *Red CEDIA*[18]

Desde algunos años la Universidad Nacional de Loja pertenece a CEDIA. La idea principal de CEDIA es integrar a todas las universidades y centros de investigación y desarrollo del país, a través de una red académica de alta velocidad, permitiendo el acceso a las redes avanzadas, al desarrollo de nuevas aplicaciones con alta tecnología y

[18] www.cedia.org.ec/educacion_investigacion.ppt

cooperación entre científicos del mundo. Para lograr esto, las entidades que lo conforman deben contar con tecnologías como el protocolo de nueva generación (IPv6), por esta razón la Universidad está en la obligación de contar con esta tecnología.

7. DESARROLLO DE LA PROPUESTA

7.1 Análisis de la Red de Datos del Área de Energía, Industrias y Recursos Naturales no Renovables de la UNL.

La Universidad Nacional de Loja (UNL) es una institución de educación superior que abarca varias Áreas. Para lograr una adecuada comunicación, se ha diseñado una red de datos WAN (Red de Área Amplia), LAN (Red de Área Local) y WLAN (Red de Área Local/Amplia) que permita servir a todas las Áreas con alto rendimiento. La información se encuentra centralizada y la asignación de los recursos de comunicación es controlada por una sola entidad.

7.1.1 Descripción de la Topología Física y Lógica de Comunicación

La topología física de comunicación para la red LAN se presenta a continuación:

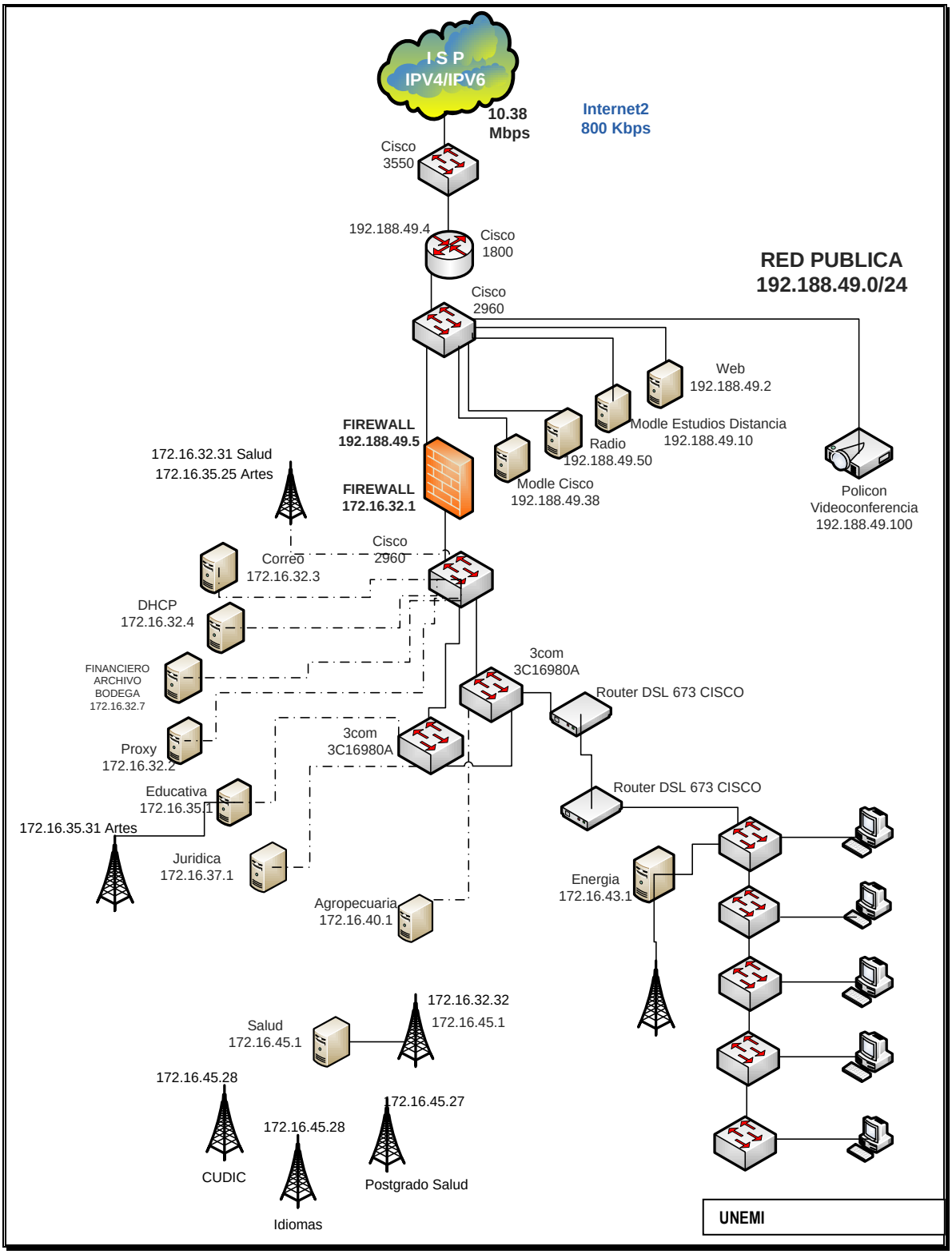


Figura 3.1.1: *Topología UNL 1*
Fuente: Administradores Red UNL

En la figura 3.1.1 de la topología se muestran las opciones que tiene la red para salir al internet a través del proveedor TELCONET. En la DMZ (Zona Desmilitarizada) se ha ubicado los servicios principales a los que pueden acceder los usuarios a través del

internet. La red local del Área se encuentra separada por medio de un firewall lógico que permite controlar seguridades locales. A partir de este nivel, la UNL presenta una topología física con el diseño de una estrella extendida Giga bit Ethernet (1000Mbps) en el backbone de la comunicación. Se ha seleccionado como medio de comunicación para todo el campus de la universidad a la fibra óptica multimodo con excepción de 2 Áreas. Una de ellas (Área de Salud) se comunica a través de enlaces radiales inalámbricos WiFi(Wireless Ethernet Compatibility Alliance) y la otra (Área de Energía) a través de un enlace DSL(Digital Subscriber Line) por líneas telefónicas.

Para la red del Área de Energía (Figura 3.1.2) se ha asignado un ancho de banda de 10Mbps para la comunicación a través de un enlace DSL. Los servicios que presta esta red son bastante limitados, enfocándose principalmente al servicio de internet a todos los usuarios (95 usuarios). El cableado estructurado se ha diseñado para una red FastEthternet (100Mbps) con el medio UTP-cat5e para las comunicaciones horizontales y verticales. Para la comunicación entre edificios de la red del Área se utiliza una topología en estrella extendida con niveles jerárquicos de acceso a través de dispositivos de capa 2 (switchs).En el Anexo 8 se muestra el cableado estructurado para la comunicación de datos existente en la red del área.

El esquema lógico de comunicación está planteado específicamente para el protocolo IPv4 por lo que se ha seleccionado una dirección de red privada clase B 172.16.0.0/16 con división en 16 subredes para la asignación de las Áreas. El Área de Energía utiliza la dirección de subred ***172.16.43.0/20*** para la comunicación local.

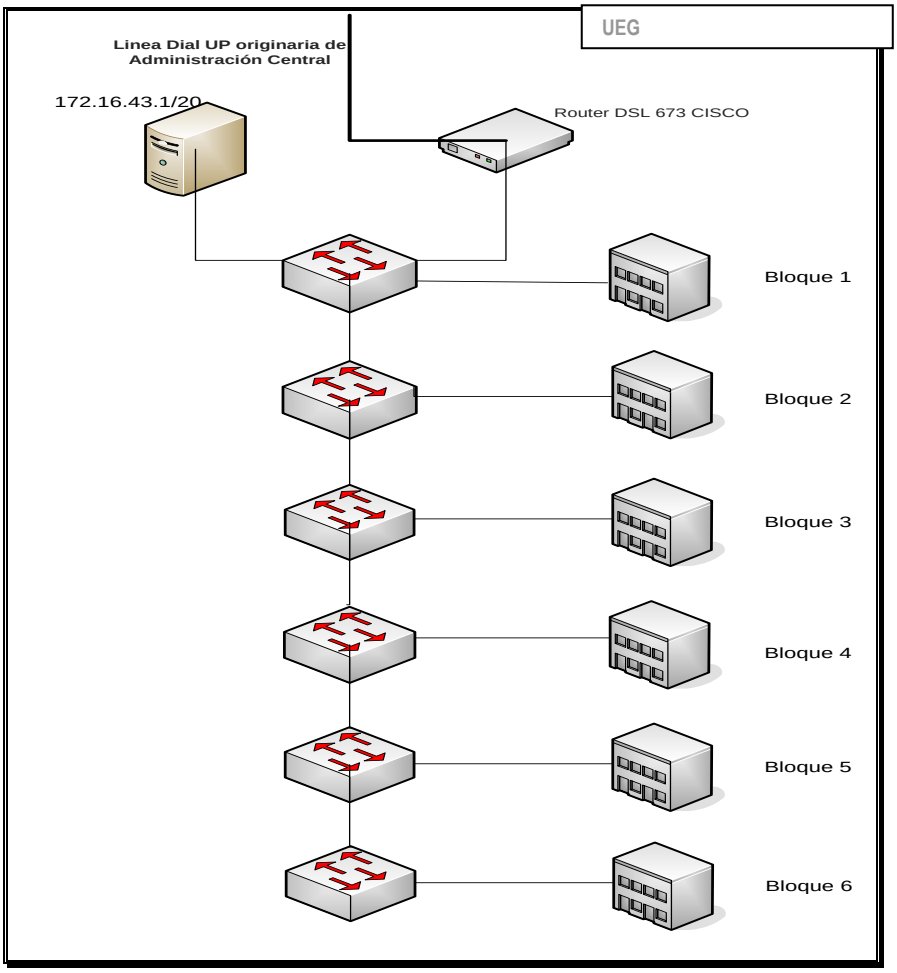


Figura 3.1.2: *Topología AEIRNNR*

Actualmente la red de datos del A.E.I.R.N.N.R. ha experimentado una serie de cambios en su diseño físico y lógico de comunicación con el objetivo de mejorar el servicio a los usuarios. Para esto, los administradores de la red han cambiado principalmente el medio de comunicación del backbone, reemplazando el medio UTP por Fibra óptica multimodo; además se han instalado nuevos equipos activos de comunicación (switchs) con capacidades acorde a la tecnología y se ha estructurado un diseño de 3 niveles de conmutación. En el anexo 11 se presenta la nueva topología de comunicación instalada así como el inventario de los equipos activos utilizados.

7.1.2 Análisis Tráfico y Políticas de Comunicación

La red de datos del campus de la U.N.L. maneja tráfico de todos los servicios que se encuentran instalados entre los que se mencionan:

- DHCP (Protocolo para la asignación dinámica de direcciones)
- SMTP (Correo Electrónico)
- PROXY (Autentificación de usuarios)
- Sistemas Financiero, de Bodega y Archivo
- HTTP (web), entre otros.

Cabe indicar que todos estos servicios se encuentran instalados para IPv4 y la utilización de los recursos de red en horas pico de trabajo se muestra en la figura:

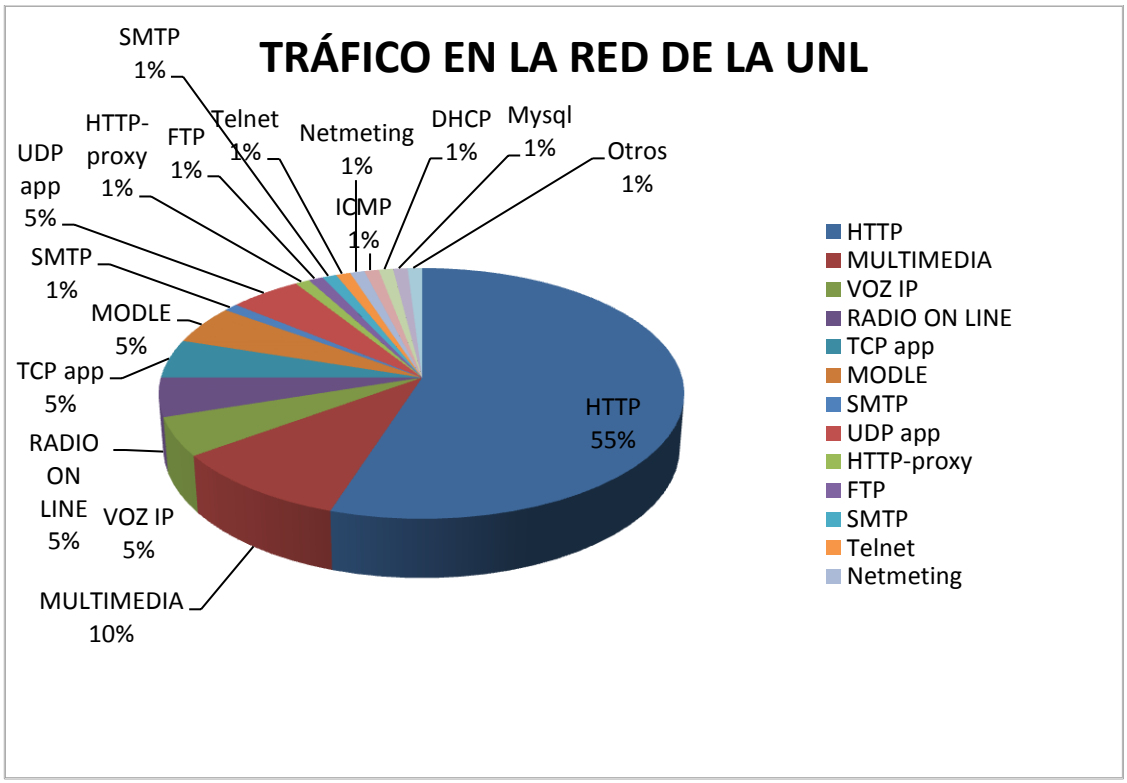


Figura 3.2.1: *Representación de Tráfico Red UNL*

Existen servicios adicionales que se utilizan ocasionalmente y que saturan por completo el ancho de banda de la red como son: videoconferencia y VoIP(Voz sobre IP).

Las políticas implementadas en la red están diseñadas con el principal objetivo de no permitir que intrusos accedan a la red interna del campus. El firewall lógico que se encuentra separando la DMZ niega cualquier intento de acceso de un usuario no identificado. Las principales políticas aplicadas a este firewall son:

- Bloqueo de intrusos
- Control de contenidos

- Bloqueo de puertos
- Asignación de ancho de banda por IP
- Control de spam y virus

Existe también un servidor de autentificación (proxy) que es utilizado para identificar a los usuarios internos de la red y permitirles o no el acceso a internet. Esta autentificación es manejada por la dirección de red de cada máquina y no por usuario.

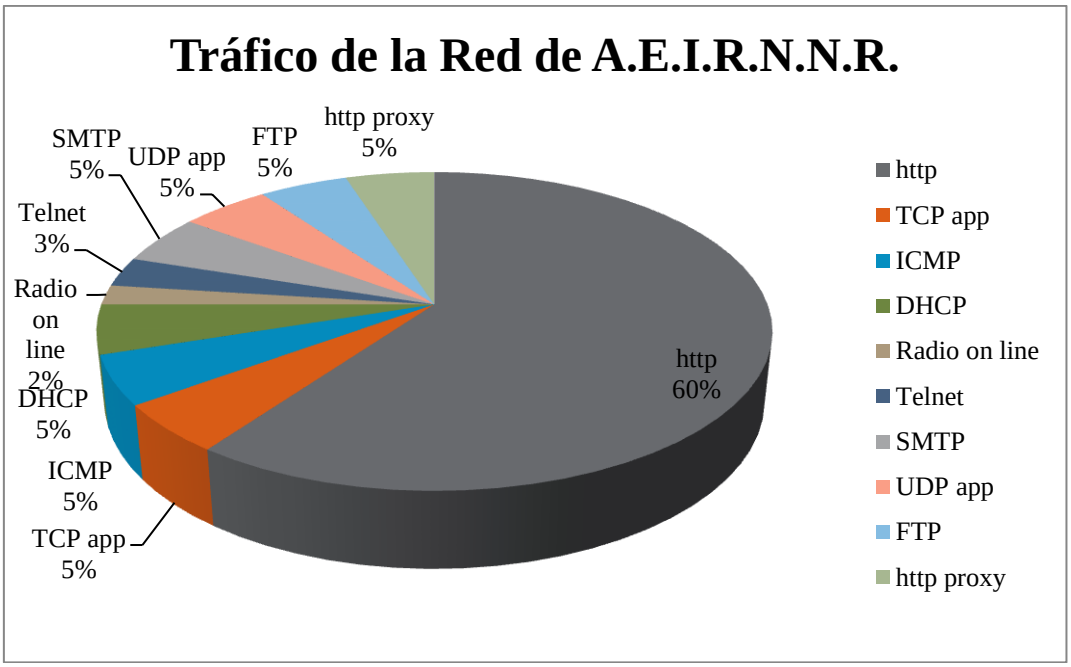


Figura 3.2.2: *Representación de Tráfico Red A.E.I.R.N.N.R*

7.1.3 Especificaciones de los Equipos de Red

La mayor parte de los equipos activos que conforman la red del campus operan con el estándar Fast Ethernet a excepción de algunos que manejan puertos Giga bit para fibra óptica. En el siguiente cuadro se presentan las descripciones de los equipos activos de comunicación de la red la Universidad:

CANT.	DESCRIPCIÓN	FABRICANTE	MODELO	# PUERTOS
1	Router border	Cisco	1800	2/fast 2/serial 2/giga
1	Switch capa 2	Cisco	3550	16/fast
2	Switch capa 2	Cisco	2960	24/fast
1	Firewall lógico	HP	HP Proliant Ml150 G5	2/fast

2	Router DSL	Cisco	673	Trans DSL

Tabla 3.1: *Equipos Principales de la Red UNL.*

Fuente: Administradores Red UNL

Como se puede observar en el cuadro descrito no existe una tendencia para seleccionar un solo tipo de fabricante de equipos, por lo que presenta una incompatibilidad en los estándares de comunicación. Estos equipos han sido seleccionados en base a requerimientos de comunicación no planificados inicialmente y a bajos costos de adquisición.

Todos los equipos de red trabajan con el protocolo IPv4 a excepción del router de borde que es gestionado por el ISP y es capaz de enrutar cierto rango de direcciones IPv6.

En la siguiente tabla se indican los equipos de comunicación que se encuentran en el A.E.I.R.N.N.R.

CANT.	DESCRIPCIÓN	FABRICANTE	MODELO	# PUERTOS
1	Switch capa 2	Cnet	CNSH-1600	16/fast
3	Switch capa 2	DLink	DES-1016D	16/fast
4	Switch capa 2	3com	4500 3CR17561-91	26/fast
1	Switch capa 2	3com	3C16476	48/fast
1	Switch capa 2	3com	3C167994	8/fast
1	Switch capa 2	3com	2024-3C16471	24/fast
4	Switch capa 2	Dlink	DES-1008D	8/fast
2	Acces point	Airplus Xtreme	DWL-2100AP	1/fast
3	Switch capa 2	DLink	DES-1024D	24/fast
1	Switch capa 2	3com	3C16476	48/fast

2	Switch capa 2	3com	2024-3C16471B	16/fast

Tabla 3.2: *Equipos de la Red del A.E.I.R.N.N.R*

Todos los switchs son utilizados para conmutación (nivel de capa 2). Los Dlink (switchs) en cuanto a rendimiento se encuentran diseñados principalmente para ser utilizados en grupos de trabajo que requieran conexiones de 10/100Mbps seguras, fiables y disponibles en todo momento, sin bloqueos del dispositivo, ni saturaciones en los momentos de máxima demanda de red y con las características básicas de todo dispositivo de conmutación (autonegociación, Estándares IEEE 802.3, 802.3u, full-dúplex y half-dúplex, etc.). El switch CNet soporta la función QoS en cada puerto, basado en 802.1p/802.1q VLAN Tag priority y cabeceras TCP/IP TOS/D, además soporte para trunk de 4 grupos, auto MDI/MDIX, ancho de banda independiente para cada puerto, puertos TP de 10/100Mbps con auto-negociación, capacidad de unión de segmentos de 100Mbps y 10Mbps (4MB de RAM no expandible.). El 3COM 3CR17561-91 10/100 Ethernet 26-Port (24 puertos 10/100 y dos puertos Gigabit de uso dual) ofrece switching de Capa 2 y routing dinámico de Capa 3 con amplia variedad de características, en una plataforma competitiva de alto rendimiento. Los demás 3COM solo brindan las características básicas de conmutación similares a los DLink.

7.1.4 Análisis de Factibilidad.

Después de haber realizado el análisis de la red de datos del campus actual se considera que la implementación del nuevo protocolo mejorara notablemente las comunicaciones sin necesidad de invertir en mejoras de los medios de transmisión, así como de los equipos de comunicación. La infraestructura tecnológica de comunicación con la que dispone la Universidad es capaz de soportar a IPv6 como el protocolo de comunicación. Por otro lado la Universidad Nacional de Loja dispone de administradores de red capacitados para operar esta nueva tecnología.

Hablando específicamente de la red del A.E.I.R.N.N.R los equipos con los que cuenta (equipos para tráfico a nivel de capa 2) permiten una implementación sin inconvenientes técnicos, ni físicos, por cuanto el nuevo protocolo trabaja a nivel de capa 3 y esto lo hace transparente a equipos de capa 2.

Los beneficios que ofrecerá la implementación de esta nueva tecnología son directamente heredados de las características positivas de IPv6. Entre estas podemos citar:

- Dotación de una tecnología de punta a la red académica de la Universidad y por ende del Área.
- Estimulación de proyectos de investigación e implantación de nuevas herramientas.
- Provisión de plataformas estables que logren desempeños óptimos para aplicaciones en tiempo real.
- Sencillez y eficacia en el manejo y administración de red.
- Cumplir con las exigencias establecidas por CEDIA para interconexión a redes avanzadas.

7.2 Diseño de la Solución para la Migración de la Red del Á.E.I.R.N.N.R a IPv6

La transición al nuevo protocolo IPv6 supone una serie de cambios a nivel lógico y físico de la red. Inicialmente, se debe buscar la coexistencia de los dos protocolos al mismo tiempo con el objetivo de no perder la comunicación. Para buscar la mejor alternativa hacia esta migración se analizan las técnicas más recomendadas.

7.2.1 Análisis de la Técnica Dual Stack en la Red del Á.E.I.R.N.N.R

Esta técnica es la más optima y adaptable para todas la redes que cuenten con los recursos suficientes, pero no es aconsejable debido a los costos de implementación. Es la opción más recomendada porque permite la comunicación directa de los dos tipos de redes pero involucra una selección de cada dispositivo de comunicación (routers, switchs y servidores principalmente). La topología dual de comunicación para el campus se presenta a continuación:

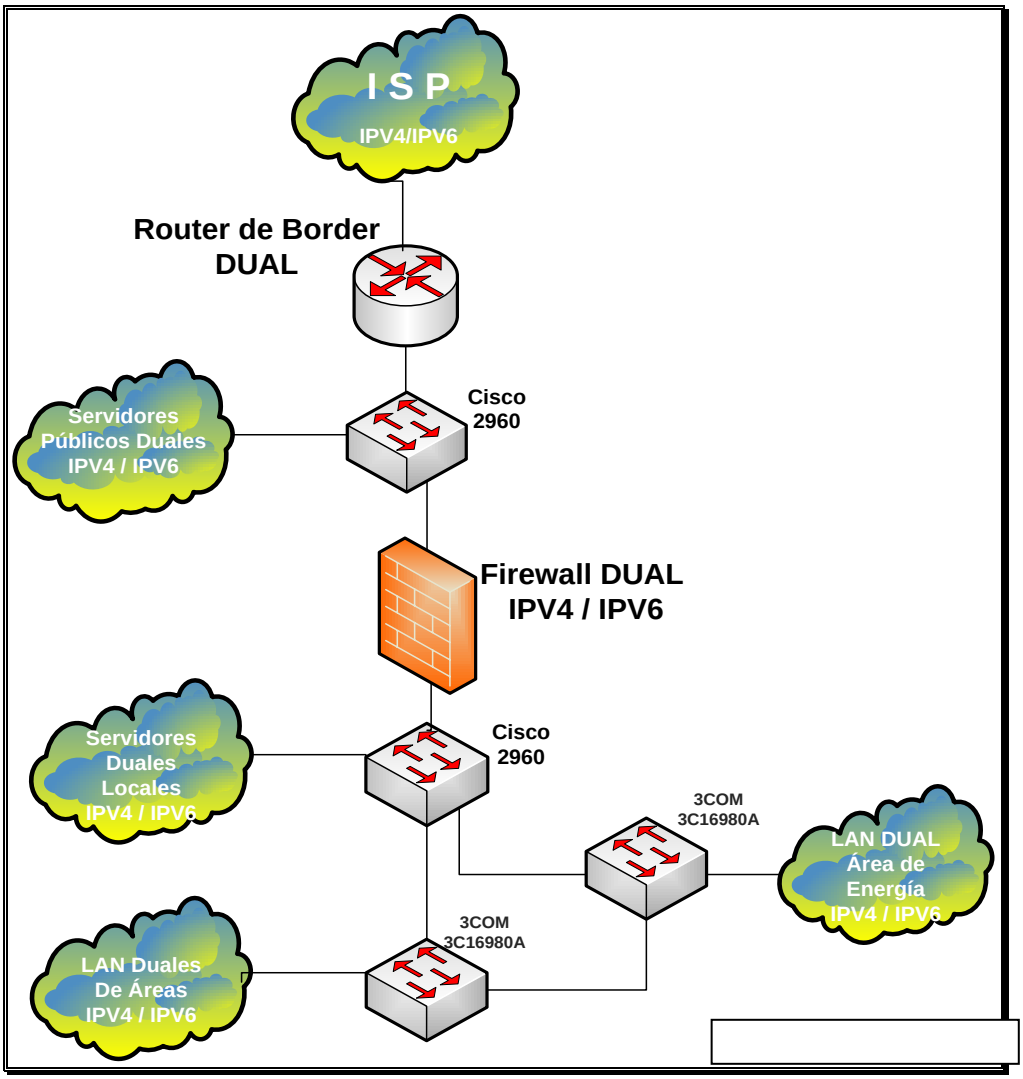


Figura 4.1.1. *Topología Técnica Dual*

Aparentemente esta topología representa la solución más conveniente, pero se debe analizar:

1. En la actualidad, ningún dispositivo de red del campus soporta configuraciones IPv6 en sus sistemas. La aplicación de estas configuraciones resulta complicada y en algunos de los casos no es aceptada en el hardware de los dispositivos por lo que conviene mejorar sus recursos o reemplazarlos.
2. El Router de Border no es gestionado por los administradores de la red del campus por lo que no se conoce las técnicas de enrutamiento IPv6 a nivel superior. El firewall lógico enruta únicamente direcciones IPv4 en su sistema por lo que se lo debe actualizar para que reconozca al nuevo protocolo.

3. Los dispositivos de capa 2 como son los switchs no presentan inconvenientes para enrutar tráfico IPv6 puesto que es un protocolo de capa superior.
4. Los dispositivos de usuario final (PC) soportan configuraciones IPv6 en sus sistemas operativos y aplicaciones sin ningún tipo de inconvenientes.
5. Los administradores de red deberán manejar servicios para los dos protocolos simultáneamente lo que implica un desperdicio de recursos.

7.2.2 Análisis de Túneles en la Red del Á.E.I.R.N.N.R

La implementación de este método es adaptable a la red del campus y además minimiza los costos de instalación y administración. Con esta técnica se soluciona el problema de conectividad entre dispositivos IPv6 en redes IPv4 y viceversa pero se pierden ciertas virtudes del nuevo protocolo (seguridad). Además, la aplicación de este método no permite la comunicación de dispositivos IPv6 con dispositivos IPv4. La topología empleando túneles lógicos se presenta a continuación:

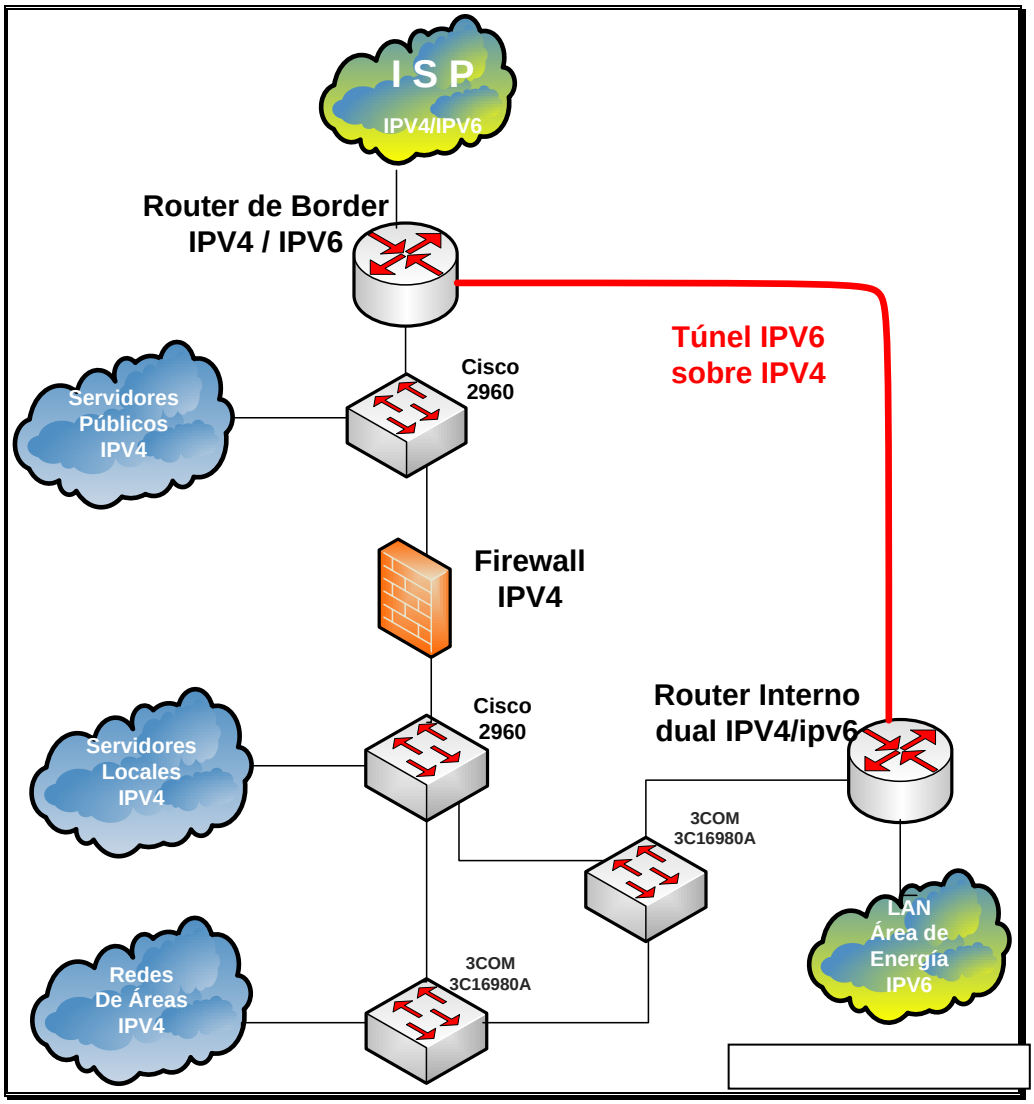


Figura 4.2.1. *Topología Técnica de Túneles*

En la implementación de este método se observa:

1. Es un método económico para la implementación puesto que únicamente se debería trabajar en dos ruteadores duales. Uno en el origen del túnel y el segundo al final de la comunicación IPv4.
2. La implementación de esta solución presenta un solo punto de fallo para la comunicación IPv6.
3. Aumentan los retardos en la comunicación debido a que se empaquetan los paquetes IPv6 sobre los paquetes IPv4. Además se pierden características importantes como lo es la seguridad (IPSec).

4. Los administradores de la red y específicamente del túnel deberán conocer con exactitud las rutas de los paquetes IPv6 procedentes desde el exterior para que sean admitidas a través del túnel, lo que se vuelve un proceso complicado y tedioso.
5. Esta técnica de migración sobrecarga los recursos de memoria y procesamiento de los enrutadores encargados de procesar el tráfico del túnel.

7.2.3 Análisis de la Técnica de Traducciones en la Red del Á.E.I.R.N.N.R

Esta técnica es la menos recomendada pero si se combina con otras es capaz de resolver el problema de la comunicación entre dispositivos que solo soportan IPv4 con los que soportan IPv6. No es recomendada puesto que disminuye el desempeño y agrega problemas de seguridad. Se lo puede implementar para resolver el problema de comunicación interna pero solo dentro de la institución. Actualmente se usa el NAT-PT (Traslación de direcciones de red-Traslación protocolo) como una buena solución.

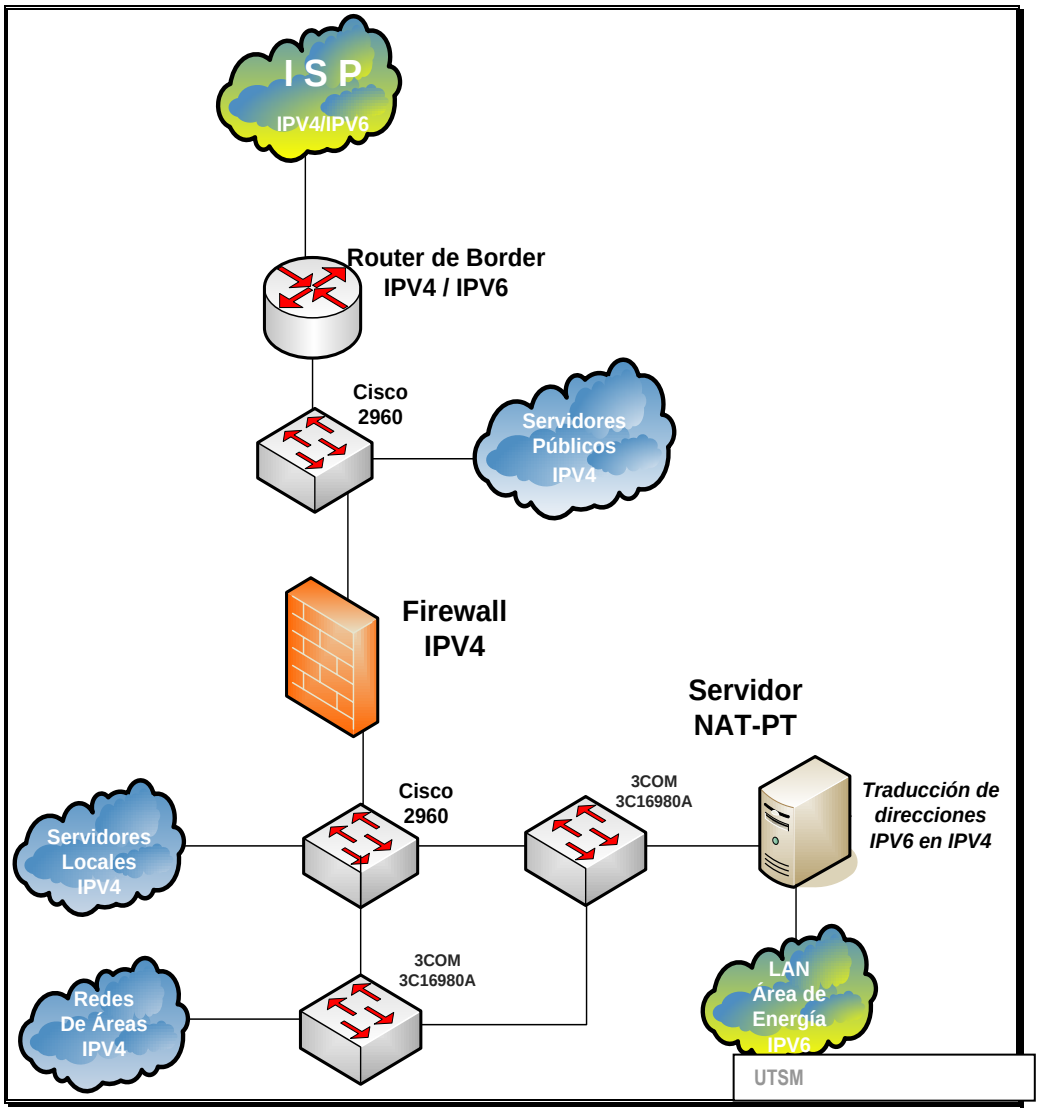


Figura 4.3.1: *Topología de Técnica Traducción NAT-PT*

Con esta técnica se obtiene:

1. Es un método con costos elevados de implementación y administración debido a que un solo servidor gestiona todas las direcciones para la comunicación IPv6.
2. Se pierden las principales características del nuevo protocolo. Se agregan retardos considerables en las transmisiones de datos.
3. Los equipos que soportan el servicio de traducción de direcciones (NAT) deben ser manejados con mucho cuidado con el objetivo de no saturar sus recursos de procesamiento.
4. Si bien la técnica permite la comunicación entre ambos protocolos, su implementación solo debe realizarse dentro de una red LAN aplicando normas de ingeniería de tráfico.

7.2.4 Selección de las Opciones Adecuadas para la Migración de la Red del Á.E.I.R.N.N.R

Una vez analizadas todas las técnicas de migración existentes se plantean dos soluciones para la red del A.E.I.R.N.N.R. en base a los requerimientos de comunicación y de fácil administración del nuevo protocolo.

- ***Primera Opción***

La primera opción consiste en implementar una topología de comunicación con un segmento aislado que soporte el protocolo IPv6 como se presenta en el siguiente gráfico:

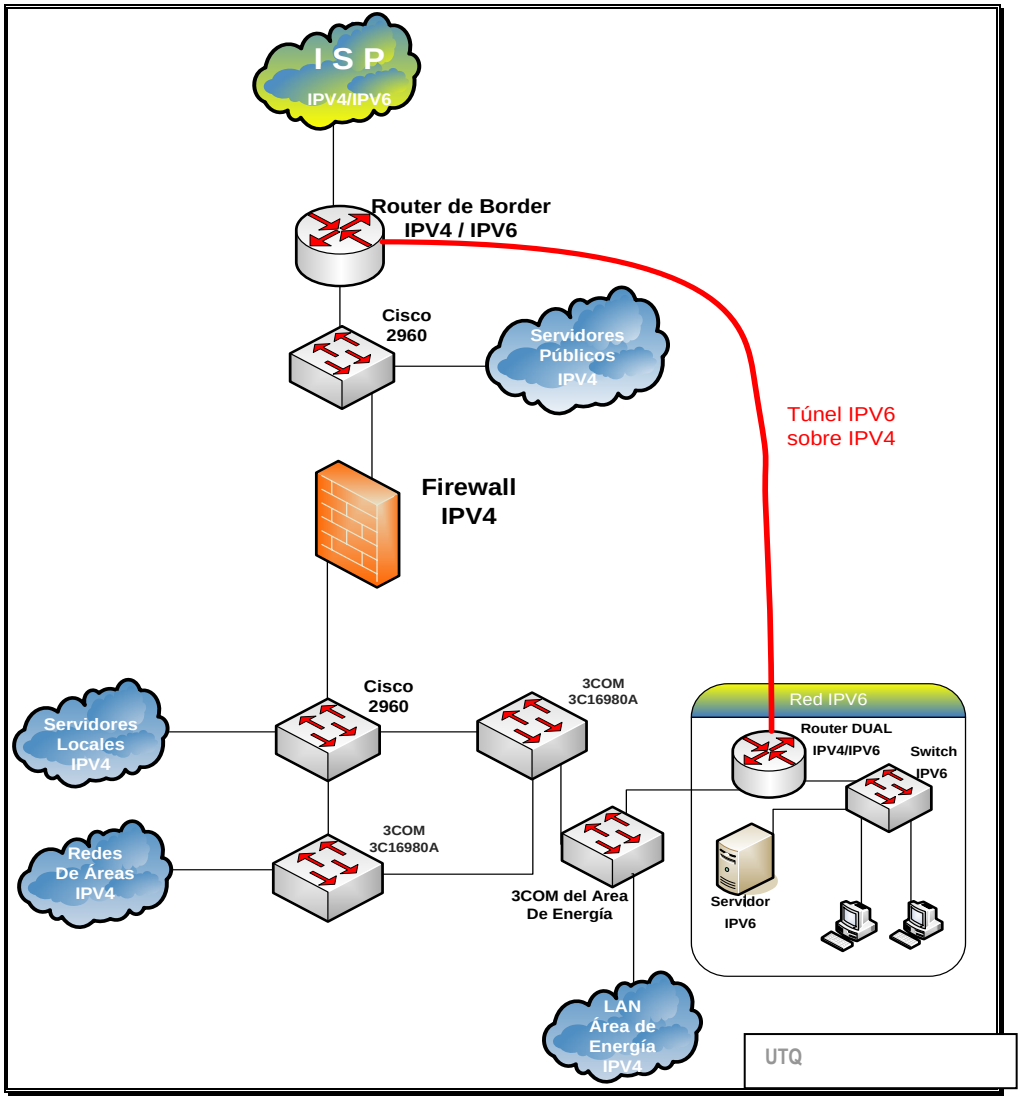


Figura 4.4.1. *Opción 1 para la implementación de IPv6 del AEIRNNR*

En el diseño planteado se puede observar la creación de un segmento independiente que soporta IPv6 y que se comunica a través de un router conectado a la red IPv4. El objetivo de este diseño consiste en aislar el tráfico IPv6 por motivos de evaluación hasta luego concluir en qué áreas se implementará el nuevo protocolo de comunicación. Para enrutar el tráfico IPv6 desde el segmento hacia el enlace de internet del proveedor se ha creado un túnel IPv6 sobre IPv4 con el objetivo de no solicitar nuevos enlaces al proveedor para llevar este tráfico y utilizar los medios de transmisión existentes. La red IPv6 también soporta el protocolo IPv4 (red dual) por lo que la comunicación entre las dos redes inicialmente será a en de IPv4 de ser necesario.

- ***Segunda Opción***

La segunda opción para la migración implica la implementación del nuevo protocolo de comunicación en toda la red del Área para el uso general y la conexión a internet avanzado. Esta opción se presenta en el siguiente gráfico.

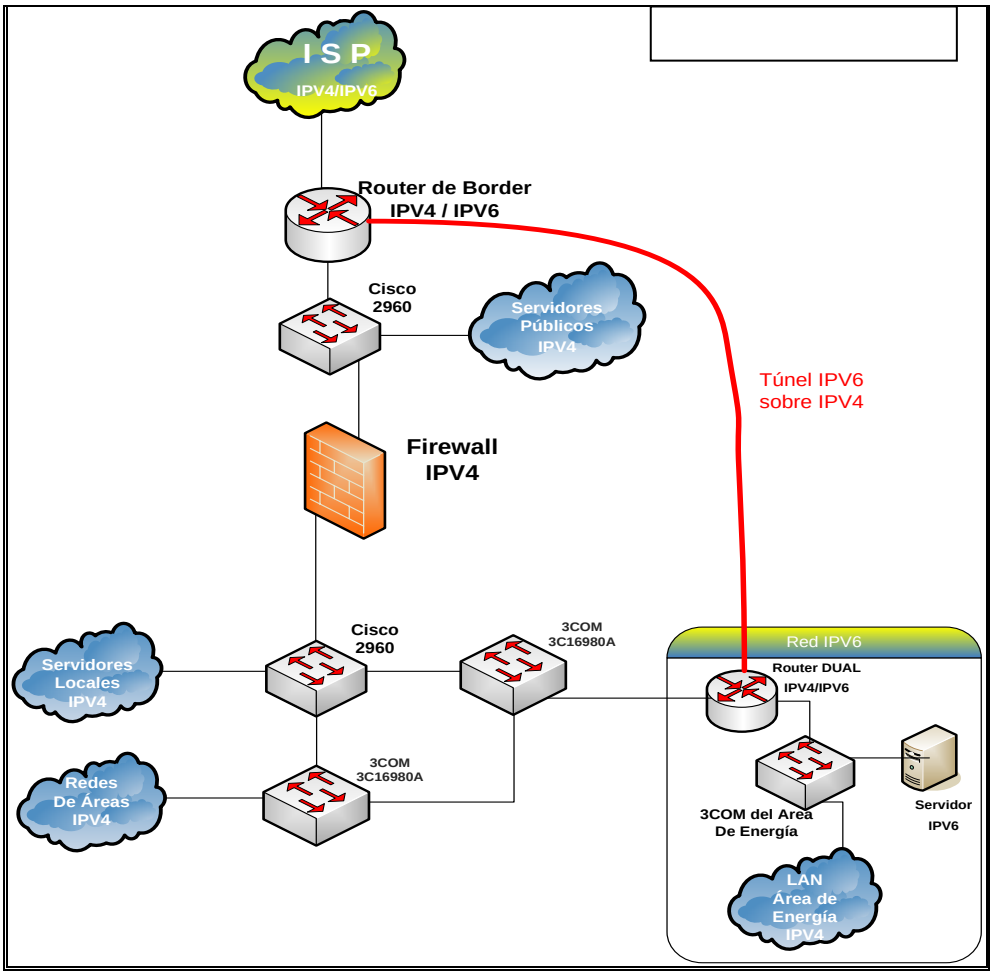


Figura 4.4.2. *Opción 2 para la implementación de IPv6 del AEIRNNR*

Esta topología planteada es el resultado de la implementación de una red dual con servicios independientes para los dos protocolos. Si bien los costos de implementación son elevados el resultado final de la coexistencia de los dos protocolos no afectara el rendimiento de la red. Es necesario implementar un equipo enrutador de tráfico en el inicio del segmento de la red, con el principal objetivo de no inundar el resto de la red del campus de la UNL con peticiones IPv6 que no serán resueltas por otros dispositivos. Además este equipo soluciona el problema en la implementación de la pasarela de comunicación con el enrutador de borde IPv6 del proveedor.

La universidad, al formar parte de CEDIA ya tiene asignado un bloque de direcciones IPv6 para la comunicación en internet avanzado. La dirección asignada es: ***2800:68:7::*** con un prefijo ***/48***, para uso interno de la institución.

En la actualidad, existen equipos y aplicaciones que permiten comunicaciones y servicios para el protocolo IPv6 entre las que se presentan las siguientes:

- Equipos de comunicación de capa 3 (routers):

ROUTER	IOS
Cisco	12.2T o mayores
Juniper	todas las versiones JunOS
Huawei	NE Series

Tabla 4.1: *Equipos de Comunicación*

- Sistemas operativos para dispositivos de usuario final

PLATAFORMA	SISTEMA OPERATIVO
Microsoft	Windows 2000 profesional en adelante
Macintosh	Mac OS 10.0 Jaguar o superior
Linux	Kernel 2.0 o superiores
SUN	Solaris 8.0 en adelante
Unix	FreeBSD 4.0 o superiores.
IPV6 Forum	IPV6Ready
PDA	Symbian OS
Compaq	Tru64, OpenVMS
HP	HP/UX 11.0+
Ericsson Telebit	Router RXI 820
IBM	AIS 4.3, OS/390
Hitachi	Toolnet6
Trumpet	Winsock 5.0
3com	NetBuilder, PathBuilder
GateD	GateD 1.0

Tabla 4.2: *Sistemas Operativos que soportan IPv6*

- Aplicaciones y servicios:

SERVICIOS	VERSIONES
DNS	Bind 9.0, Totd
Mail	Postfix, Sendmail 8.10.0,Exim, Qmail
HTTP	Apache 2.0, IIS 6.0, Mozilla 5.0, Explorer 4
FTP	Libra FTP server, NcFTP (Windows, BSD), LFTP-2.0
RUTEO	BGP, ISIS, OSPFv3
Monitoreo	NTOP, MRTG, ASPath-tree, Link View
Chat	RAT y SDR
Firewalls	ipfilter, IPFW
Java	IPv6 java (Windows)
Noticias	INN v2.2.2, Mnews
Juegos	Quakeforge

Tabla 4.3: *Aplicaciones y Servicios que soportan IPv6*

7.2.5 Diseño de un Plan piloto para la Implementación del Protocolo IPv6 (Segunda Opción)

Para realizar la implementación de IPv6 en toda la red del A.E.I.R.N.N.R se han definido lineamientos agrupados en:

1.- Análisis de la red y selección de los equipos de comunicación.
2.- Definición de los recursos necesarios para la migración de la red del Área
3.- Diseño de un esquema de direccionamiento y Configuración de servicios de red IPv6.
4.- Pruebas de rendimiento y evaluación de resultados.

Las tareas definidas para cada área han sido seleccionadas de acuerdo a criterios y recomendaciones de implementación en otras redes con características similares a las que presenta el campus.

7.2.5.1 Análisis de la Red y Selección de los Equipos de Comunicación.

1. El A.E.I.R.N.N.R. debe contar con administradores de red que conozcan al nuevo protocolo y con enlaces eficientes para su comunicación.
2. Seleccionar e implementar un enrutador local en el área que permita configuraciones avanzadas (CIDR) de IPv6 e IPv4.
3. Buscar los equipos activos que se adapten a las necesidades de la red del área pero que soporten configuraciones para el funcionamiento de los dos protocolos.
4. Verificar que los dispositivos de usuario final (PC) cuenten con sistemas operativos que soporten aplicaciones IPv6.
5. Seleccionar los equipos adecuados para instalar servicios especiales como servidores locales. No es recomendable el uso de un mismo equipo como servidor para ambos protocolos.

7.2.5.2 Definición de los Recursos Necesarios para la Migración de la Red del Área.

1. Se debe establecer un cronograma de trabajo para la implementación de IPv6 de acuerdo al número de personas que conformen el equipo de trabajo. Si el equipo de trabajo está capacitado en el nuevo protocolo, en un periodo de 42 días laborables con 4 integrantes se puede implementar la red dual.
2. El costo de la implementación varía dependiendo de los equipos seleccionados (enrutador y servidores). En el presupuesto asignado para la implementación del proyecto se debe hacer constar todos los rubros que impliquen gastos imprevistos.
3. Se pueden realizar tareas paralelas no dependientes en la implementación con el objetivo de acelerar la migración.

7.2.5.3 Diseño de un Esquema de Direccionamiento y Configuración de Servicios IPv6.

1. Definir el rango de direcciones para ser asignadas en los dispositivos que intervienen en la red de evaluación. Se recomienda utilizar el rango IPv6 definido para la UNL
2. Seleccionar las técnicas de enrutamiento (Protocolos) que serán configuradas en los enrutadores.
3. Se debe implementar un servidor DNS que resuelva direcciones con registros AAAA y enrutables a un nivel superior (SLA).
4. Configurar servicios adicionales como: DHCP, HTTP, FTP para IPv6 (ver anexos).

5. Verificar que las aplicaciones clientes accedan a los servicios IPv6.

7.2.5.4 Pruebas de Rendimiento y Evaluación de Resultados.

1. Evaluar la funcionalidad y adaptabilidad del nuevo protocolo mediante la verificación de los servicios.
2. Comparar los resultados obtenidos para solucionar posibles errores.
3. Concluir el rendimiento del nuevo protocolo.

8. EVALUACIÓN DEL OBJETO DE INVESTIGACIÓN

8.1 Implementación del Protocolo (IPv6)

Después de haber recolectado y analizado toda la información necesaria de la red del campus se plantea el diseño de un escenario de pruebas que funcione en las mismas condiciones de tráfico y comunicación de la red actual.

8.1.1 Definición de un Escenario para Pruebas y Evaluación del Protocolo

El escenario descrito a continuación representa la topología ideal para motivos de evaluación y pruebas del protocolo en cualquier segmento de la red del área.

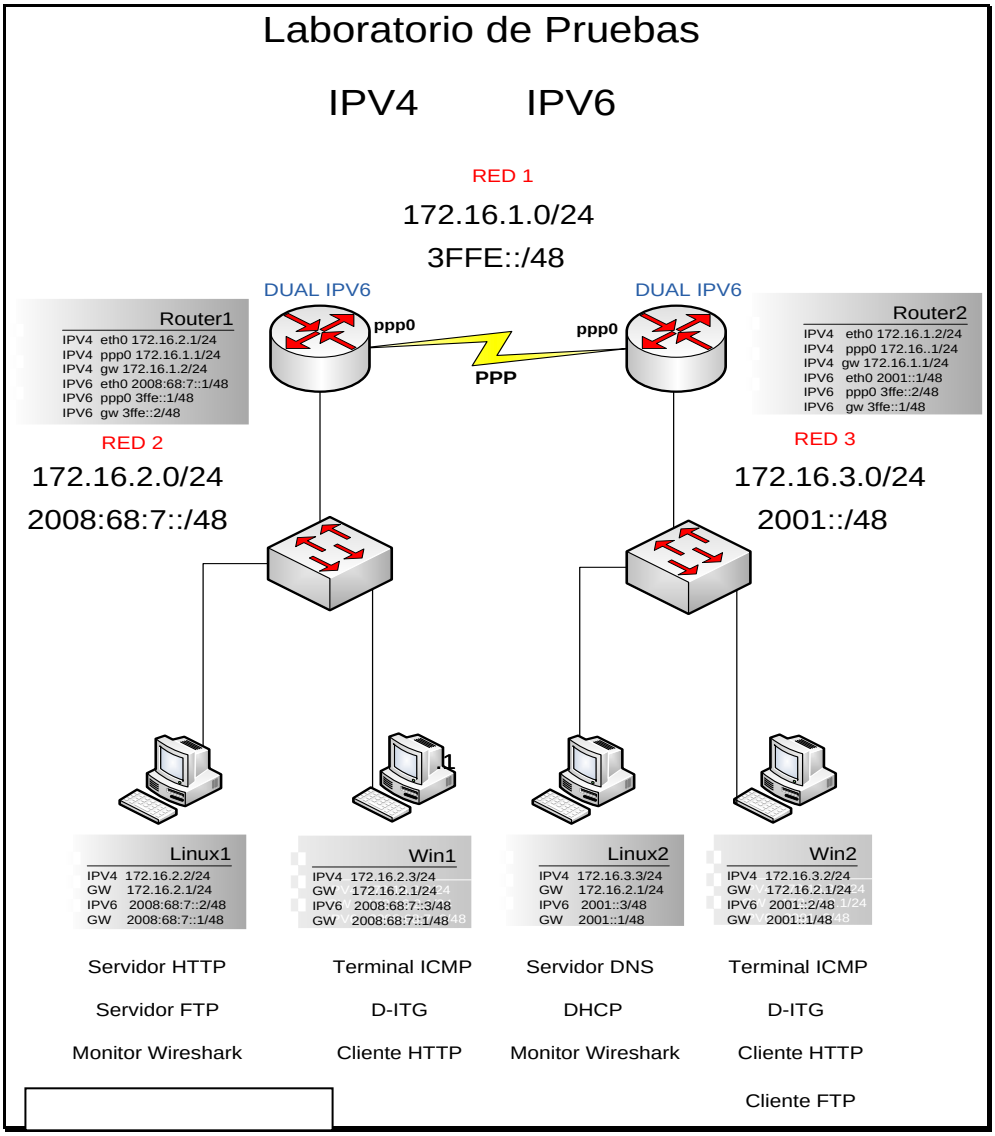


Figura 5.1.1: *Escenario de Laboratorio*

La red diseñada utiliza ambos protocolos de comunicación (red dual) con el objetivo de demostrar:

- Funcionalidad del nuevo protocolo
- Rendimiento de las comunicaciones

El diseño presenta 3 redes diferentes descritas a continuación:

La red 1 consiste en un enlace serial con el protocolo PPP (Protocolo Punto a Punto) configurado a una velocidad promedio de una comunicación dial up (32000kbps). Para la red IPv4 se trabaja con la dirección de red ***172.16.1.0/24*** y para IPv6 ***3ffe::/48***. Este enlace conecta las dos estaciones que cumplen las funciones de encaminadores (router1 y router2) con técnicas de enrutamiento estáticas. No se aplica ninguna configuración de políticas de seguridad. En el Anexo 1 se presenta las configuraciones de los equipos encaminadores.

La red 2 de la topología es un segmento de red FastEthernet (100Mbps) que interconecta equipos a través de un dispositivo de capa 2 (switch). En este segmento se ha instalado un servidor HTTP y FTP para servir a todos los clientes que puedan acceder a esta red. Estos servicios se encuentran instalados en una estación con el sistema operativo Fedora Core 7 y sus configuraciones se presentan en el Anexo 2. Para configurar el servicio HTTP se utiliza un solo archivo de configuración y puede escuchar peticiones IPv4 e IPv6 al mismo tiempo. En el servicio FTP se debe seleccionar que protocolo se decide escuchar. No se puede atender a los dos protocolos al mismo tiempo en el mismo servidor. También se realiza monitoreo a través de la Herramienta Wireshark para analizar el tráfico que fluye por el servidor. En esta red también se encuentra una estación cliente con el sistema operativo Windows XP que realiza peticiones constantes al servidor y utiliza aplicaciones especializadas para el análisis del rendimiento de la comunicación (aplicación ICMP y D-ITG). Para esta red se trabaja con las direcciones: ***172.16.2.0/24*** para IPv4 y ***2008:68:7::/48*** para IPv6.

En la red 3 de la topología se han instalado servidores DNS y DHCP para los dos protocolos con el objetivo de inundar la red con este tipo de tráfico. Se utiliza también un switch de capa 2 (fastethernet) para interconectar los equipos y también existe un equipo cliente para monitoreo de tráfico. Las direcciones de red son: para IPv4 ***172.16.3.0/24*** y para IPv6 ***2001::/48***. En el Anexo 3 se presentan las configuraciones de los servidores DNS y DHCP.

Para evaluar la funcionalidad del protocolo se ha utilizado dos plataformas (Linux y Windows) con las respectivas aplicaciones que soportan IPv6. En el Anexo 2 se muestran las técnicas de configuración de IPv6 en las dos plataformas para estaciones clientes.

Además en las estaciones clientes se han instalado aplicaciones dependiendo de la plataforma. Los clientes HTTP en Windows han sido evaluados con el Internet Explorer 6 y en Linux con el Mozilla Firefox 2.0.0.14. Como clientes FTP se tiene a las aplicaciones ncftp para Windows y para Linux. En el anexo 4 se presentan ejemplos de estas aplicaciones.

En el anexo 7 se adjunta una demostración de la funcionalidad del protocolo IPv6 con la herramienta de monitoreo

8.1.2 Análisis de Rendimiento y Evaluación de Resultados

Para realizar el respectivo análisis de funcionalidad y rendimiento del nuevo protocolo en la topología descrita anteriormente se han seleccionado herramientas que permiten observar el tráfico en tiempo real con el objetivo de obtener datos para el correspondiente análisis comparativo.

Una vez demostrada y evaluada la funcionalidad de la topología dual se procede a realizar una evaluación detallada con herramientas de monitoreo como son: ICMP echo- request echo-replay (PING) y D-ITG.

El análisis de rendimiento se realiza con los siguientes procesos:

1.- Con el objetivo de lograr inundar la red con tráfico de diferente tipo, se levantan los servicios en todas las estaciones y se realizan solicitudes permanentes desde los clientes hasta lograr saturar la red con los dos protocolos.

2.- Con la herramienta PING (ICMP) se realiza peticiones con paquetes de diferentes tamaños en los dos protocolos obteniendo los siguientes resultados:

- Al realizar una petición desde la estación linux1 hacia win2 de 10 paquetes con un tamaño de 1000 bytes se obtiene:

Con IPv4

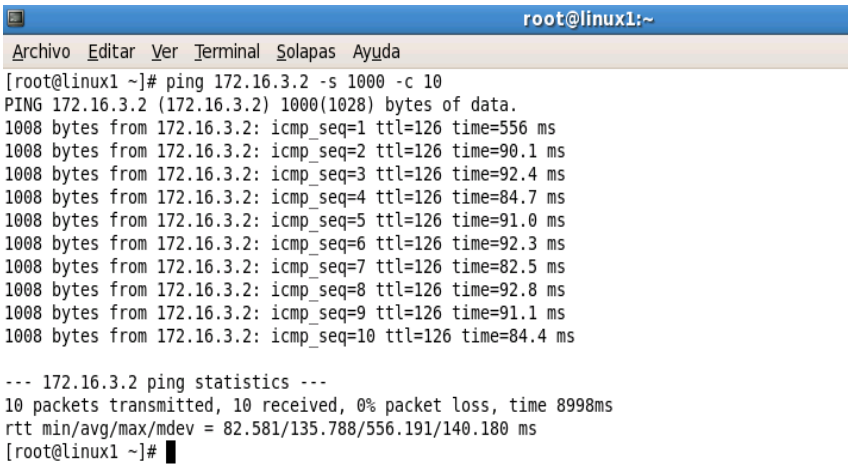


Figura 5.2.1: *Resultados IPv4 con ICMP sin servicios*

Con IPv6

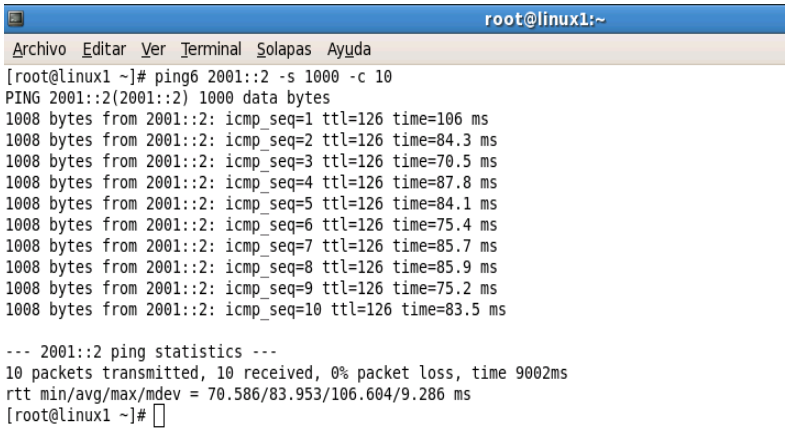
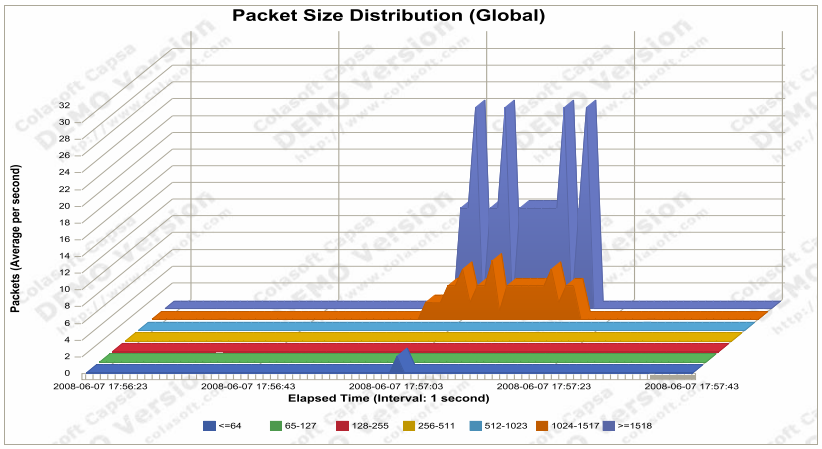


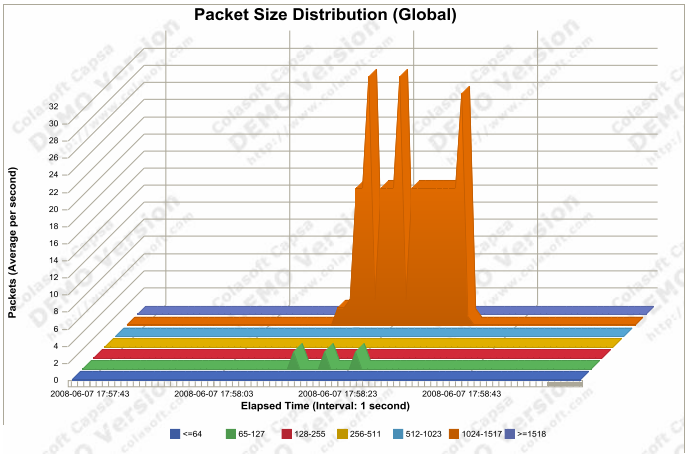
Figura 5.2.2: *Resultados IPv6 con ICMP sin servicios*

ANÁLISIS: En estos datos se puede observar los tiempos de respuesta de cada paquete en ambos protocolos en una red con carga de tráfico. Mientras que con el protocolo IPv6 se tiene un promedio de 83ms, en IPv4 se tiene 135ms. Es decir que IPv4 necesita más tiempo para responder cada petición. Además en IPv6 se reciben mayor cantidad de paquetes en un menor periodo de tiempo. En

la siguiente gráfica se muestra una representación del consumo de ancho de banda de la red con los dos protocolos.



IPV4 ---- 1000/10000K



IPV6 ---- 1000/10000K

Figura 5.2.3: *Gráficas de Comparación de IPv4 e IPv6*

FUENTE: Software Packet Analyzer

Estas gráficas representan las estadísticas de los tiempos de los paquetes transmitidos durante una petición ICMP. En IPv4 se puede observar que la cantidad de paquetes transmitidos por segundo es dividido, dependiendo de su tamaño (MTU Unidad Máxima de Transferencia) razón por la cual se identifican dos tipos de tráfico. En IPv6 el tráfico es manejado con un tamaño fijo establecido por los enlaces WAN (Red de Área Amplia) (seriales) por lo que en la gráfica de puede observar un solo flujo de tráfico en un periodo de tiempo al requerido por IPv4. En el anexo 5 se presenta un análisis del rendimiento de los dos protocolos con paquetes de diferente tamaño.

3.- Para evaluar de manera más exacta parámetros adicionales del protocolo IPv6 se utiliza la herramienta D-ITG que permite medir: Consumo de Ancho de banda, confiabilidad, retardos y jitter. Con estos datos se procede a realizar un análisis comparativo en los dos protocolos.

- Los resultados obtenidos al enviar tráfico en tiempo real como la voz sobre IP son:

Para IPv4

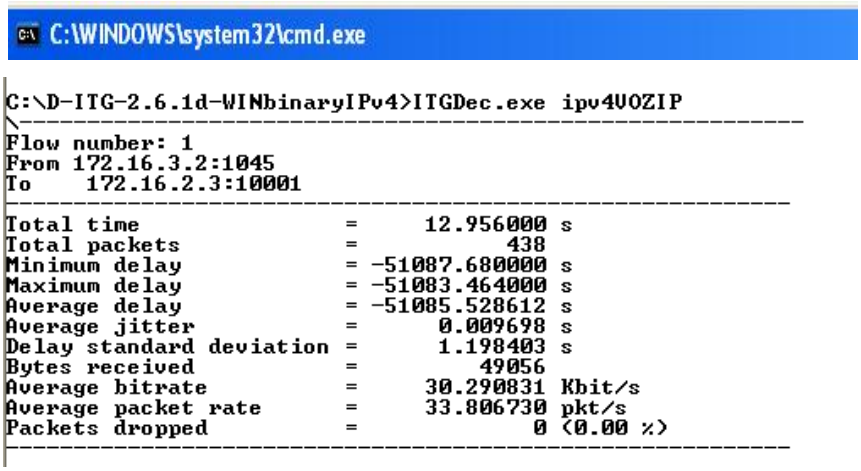


Figura 5.2.4: *Resultado de IPv4 con D-ITG*

Para IPv6

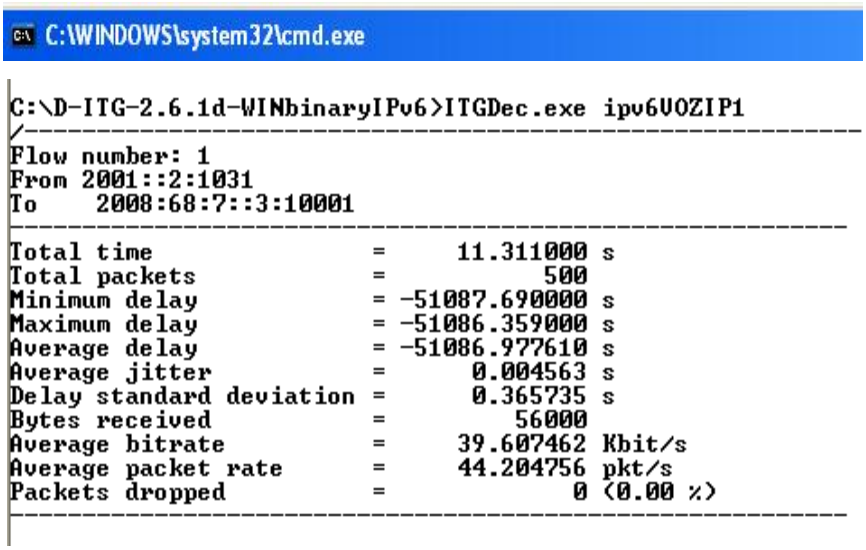


Figura 5.2.5: *Resultado de IPv6 con D-ITG*

ANÁLISIS: En estos datos se puede observar el comportamiento de ambos protocolos frente al tráfico de voz. En condiciones normales de funcionamiento de una red se puede observar que con IPv6 se obtiene una tasa de transferencia de 44 Paquetes por segundo en contraste con 33 que se presentan con IPv4. El consumo de ancho banda con IPv6 es de 39Kbps más que en IPv4. Por otro lado en estos datos no se observa ninguna pérdida de paquetes con ningún protocolo debido que la voz trabaja con UDP. Además, otros datos mejores que se observan en IPv6 son el retardo y la varianza (jitter) de tiempos entre llegadas que son menores que en el protocolo IPv4 lo que permite una mayor entrega de paquetes en el mismo periodo de tiempo (62 paquetes más, en un tiempo de 12 segundos).

- Al enviar tráfico TCP con paquetes de tamaño 3000 bytes en los dos protocolos se obtiene:

En IPv4

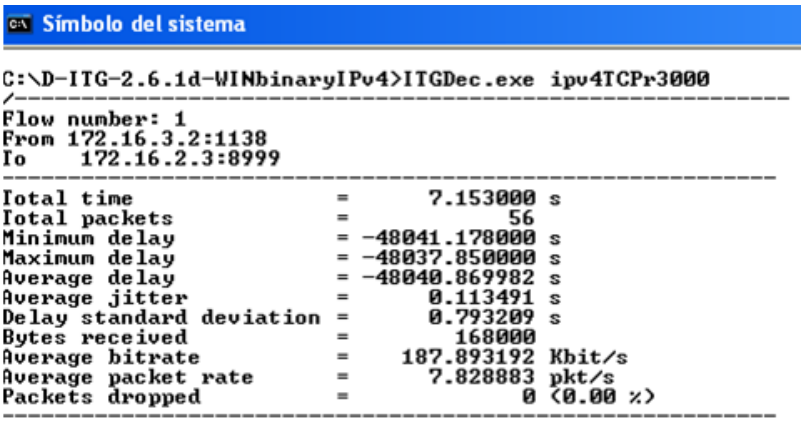


Figura 5.2.6: *Resultado de IPv4 con D-ITG*

En IPv6

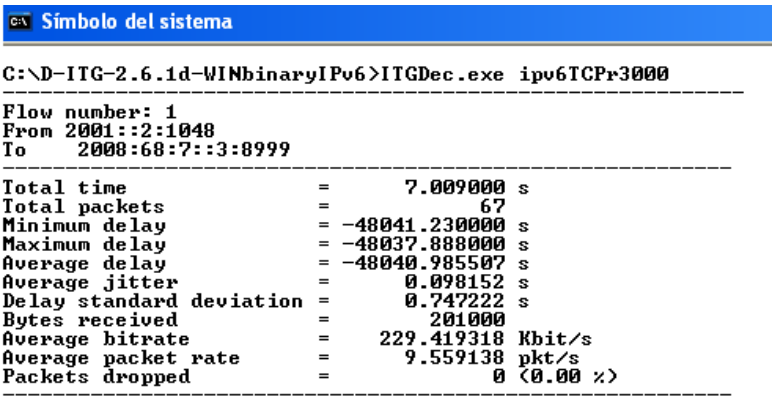


Figura 5.2.7: *Resultado de IPv6 con D-ITG*

ANÁLISIS: En estos resultados se puede diferenciar que la cantidad de paquetes recibidos con IPv6 es mayor que con IPv4 y en un menor intervalo de tiempo. Además otros valores como el jitter promedio en IPv6 se encuentra por debajo de 0.1s lo que mejora notablemente las comunicaciones para aplicaciones que trabajan con el protocolo TCP (HTTP, FTP, TELNET, etc.). En el anexo 6 se adjuntan análisis de los dos protocolos con diferentes tipos de tráfico.

9. VALORACIÓN TÉCNICO - ECONÓMICA – AMBIENTAL

9.1 Valoración Técnico – Económica

A continuación se indica los costos de las dos propuestas planteadas en la investigación:

La opción 1 planteada en la figura 4.4.1 (Laboratorio de Pruebas) representa la alternativa más adecuada para implementar la nueva tecnología de comunicaciones en la red del campus del A.E.I.R.N.N.R.; para lo cual es conveniente presentar los costos que implica esta implementación. En la siguiente tabla se detallan los principales ítems con sus costos a considerar:

OPCIÓN 1: Construir un Laboratorio de Pruebas

E Q U I P O S

Descripción	Fabricante o Modelo	Valor
1 Router IPv6	Cisco 1800 o superior	$1500,00
1 Switch capa 2	Cisco Catalyst 2700 o superior	$1000,00
1 Servidor de red	Servidor HP ProLiant ML370 G5	$2000,00
2 PCs	clones	$2000,00

M I S C E L A N E O S

Descripción	Valor
Diseño de Cableado estructurado para Laboratorio.	$ 400,00
Puesta en marcha de la Red Dual.	$400,00
Configuración del Túnel para IPv6.	$200,00
Subtotal	$7500,00
Imprevistos (2%)	$150,00
TOTAL	**$ 7650,00**

El costo total de la implementación de un Laboratorio de Pruebas IPv6 en la red del A.E.I.R.N.N.R es de $ 7650,00. Esta inversión se recuperara a corto plazo con el auge de nuevos proyectos que se basan en esta tecnología. Sin esta infraestructura de comunicación no se puede realizar ningún tipo de investigación para las redes avanzadas.

La opción dos implica implementar el protocolo en la red actual del A.E.I.R.N.N.R. Esta solución es práctica y permitirá trabajar con IPv6 en todas sus formas.

OPCIÓN 2: Implementar el Protocolo IPv6 en la Red Actual

A D Q U I S I C I Ó N D E E Q U I P O S

Cant.	Descripción	V. Uni	V. Total
1	Router Cisco 1800 o superior	$1500,00	$1500,00
1	Servidor HP ProLiant ML370 G5	$2000,00	$2000,00

C A P I T A L H U M A N O

Cant.	Descripción	V. Uni	V. Total

2	Especialistas en Redes Avanzadas por 2 meses	$500,00	$1000,00
2	Ayudantes de Redes	$200.00	$ 400.00

MATERIAL Y HERRAMIENTAS

Cant.	Descripción	V. Uni	V. Total
1	Kit de Herramientas de Red	$30,00	$30,00
1	Materiales de Red (cable Cat6, conectores, canaletas, etc)	$80,00	$80,00

SOFTWARE

Cant.	Descripción	V. Uni	V. Total
1	Paquetes de Actualización (Clientes)	$50,00	$50,00
1	Paquetes de Actualización (Servidores)	$100,00	$100,00

Subtotal	$5160,00
Imprevistos (2%)	$103,20
TOTAL	**$5263,20**

El gasto que con lleva la implantación de IPv6 en la red actual del Área es de $5263,20; donde se toma en cuenta la incorporación de dos equipos de última generación(router, servidor) y de recursos humanos profesionales en redes avanzadas que lograrán concebir que este proyecto sea todo un éxito.

Contando con la infraestructura básica se procede a realizar un cronograma de actividades, basados en un tiempo de 42 días laborables (2 meses) para la implementación del protocolo:

Cronograma de Actividades

#	ACTIVIDAD	DESCRIPCIÓN	TIEMPO (DÍAS)
1	Revisión de Software en la red	Comprobar que todos los sistemas soporten el Protocolo IPv6, en caso de no soportar dicho protocolo proceder a instalar los módulos correspondientes.	10
2	Realizar un esquema de direccionamiento	Seleccionar el prefijo de red.	5

3	Configurar el servidor DNS	Asignar nombres a los equipos	10
4	Configurar el servidor DHCP	Configuración automática de usuarios	3
5	Configuración de servidores HTTP, FTP.	Servicios para pruebas	3
6	Pruebas de Rendimiento	Comprobar que la red funcione en óptimas condiciones.	11
		TOTAL	42

Para demostrar la solución seleccionada se construyo un escenario para pruebas de evaluación y rendimiento de IPv6 el cual es el objetivo principal de investigación. Ésta inversión es realizada por los investigadores de forma particular para demostrar lo planteado. Los costos del proyecto de tesis se resumen a continuación:

ADQUISICIÓN DE EQUIPOS

Cant.	Descripción	V. Uni	V. Total
6	Renta de PCs durante 6 meses (diario $6 p/c pc)	$220,00	$1320,00
2	Adquisición de Switch DLINK	$20,00	$40,00
10	Adquisición de Patchcort	$6,00	$60,00

CAPACITACIÓN

Cant.	Descripción	V. Uni	V. Total
200	Horas de Capacitación del S.O. Linux Fedora Core 7	$5,00	$1000,00
50	Horas de Capacitación de Herramientas de Monitoreo	$3,00	$150,00

CAPITAL HUMANO

Cant.	Descripción	V. Uni	V. Total
200	Horas de Investigación teórica-practica por dos personas (horas de internet, bibliografía, encuestas, entrevistas)	$6,00	$1200,00

MATERIAL DE OFICINA

Cant.	Descripción	V. Uni	V. Total
1	Materiales de necesarios para presentación del proyecto (Impresiones, papel, copias, anillados, etc.)	$300,00	$300,00

ASESORIA TÉCNICA

Cant.	Descripción	V. Uni	V. Total
100	Horas de Asesoría técnica para el desarrollo del proyecto	$5,00	$500,00
		Subtotal	$4570,00
		Imprevistos (2%)	$91.40
		TOTAL	**$4661.40**

El presupuesto total para el desarrollo de este proyecto es de $4661,40; valor el cual se asume por los desarrolladores.

9.2 Impacto Ambiental

El presente proyecto investigativo no genera daños al medio ambiente, ya que la puesta en marcha de la nuevas herramientas, no requiere del uso de tecnologías contaminantes ni tampoco constituye peligro alguno para el medio ambiente y la sociedad por las razones que se destacan a continuación:

- Se utiliza equipos electrónicos que no provocan ruido, vibraciones, luces o calor en el medio ambiente.
- El proyecto no contempla cambios físicos en el medio ambiente por lo tanto no afectará las micro condiciones climáticas.
- Se realizará en un área donde no podrá ser observado por un gran número de personas.

10. CONCLUSIONES

1) Es factible implementar el Protocolo de Internet Versión 6 en la topología actual de la red del Área de Energía Industrias y Recursos Naturales No Renovables de la UNL incorporando a dicha infraestructura dos equipos especializados: un encaminador y un servidor.

2) La topología de comunicación utilizada en la red del A.E.I.R.N.N.R. presenta ciertas limitantes en cuanto a algunos medios de transmisión (cableado estructurado UTP-Cat5 implementado sin la utilización de estándares de comunicación), pero cuenta con los requerimientos mínimos en cuanto a la aplicación de nuevas tecnologías. El medio físico de transmisión utilizado en el backbone es el más adecuado para los servicios de comunicación actuales (fibra óptica).

3) La red del área, se ha diseñado una topología en estrella jerárquica basada en switch (Ver Anexo 11). Los niveles empleados: núcleo, distribución y acceso logran una comunicación aceptable y suficiente para la investigación y desarrollo de esta tecnología.

4) Las políticas de comunicación empleadas en la red de la Universidad Nacional de Loja han sido aplicadas en un bajo nivel dejando huecos de seguridad. El firewall lógico identifica únicamente la dirección del dispositivo y no a los usuarios ni sus aplicaciones. Por otro lado, toda la red pertenece a un solo dominio de comunicación debido a la inexistencia de políticas para la agrupación lógica de usuarios (VLANs Red de Área Local Virtual).

5) Los equipos de comunicación presentan una incompatibilidad entre marcas lo que origina retardos en las transmisiones (Ver Tabla 3.2).

6) Para implementar IPv6 en la red del Área se deberá seleccionar los equipos que soporten enrutamiento de este tipo de tráfico y de no ser así actualizarlos. IPv6 es un protocolo de capa 3 por lo que en el mismo medio de transmisión y los dispositivos de capa 2 implementados no presentan obstáculos para su ejecución.

7) IPv6 representa la mejor solución para las aplicaciones que requieren mayor consumo de ancho de banda y que trabajan en tiempo real (VoIP, videoconferencia).

8) Las comunicaciones con IPv6 son mucho más rápidas que con IPv4. La tasa de transferencia en una red saturada aumenta de 30 kbps a 40 kbps y con una disminución de retardo de hasta un 50% (Ver Anexo 5).

9) Con el protocolo IPv6 se logra una alta confiabilidad en las transmisiones que involucran paquetes con tamaños mayores a 20 kbytes. Mientras que con IPv4 se pierden todos los paquetes, con IPv6 recibe hasta un 80% los paquetes transmitidos (ver Anexo 5).

10) IPv6 garantiza las comunicaciones utilizando la fragmentación, estos valores dependerán de las velocidades de los enlaces así como de la MTU (unidad máxima de transferencia) de la comunicación.

11. RECOMENDACIONES

1) Realizar una planificación detallada de la estructura de datos, así como también, aplicar técnicas de ingeniería de tráfico y políticas adecuadas de comunicación, con el fin de obtener una mejor calidad de transmisión en la red.

2) Planear y evaluar un plan piloto para la implementación de nuevas tecnologías como IPv6, en una red prototipo independiente, con el objetivo de no intervenir en el normal funcionamiento de las comunicaciones, para luego migrar definitivamente y sin problemas a la red del Área.

3) Seleccionar una sola plataforma de equipos activos, con el objetivo de lograr un mejor estándar de comunicación.

4) La UNL debe implementar nuevas tecnologías como IPv6 para cumplir con los requerimientos impuestos por CEDIA (Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado).

5) Impulsar el desarrollo de nuevos proyectos adjuntos con esta tecnología, como: Multicast, VoIP para IPv6 y calidad de servicio con la finalidad de explotar al máximo esta nueva versión del Protocolo de Internet y sobre todo, familiarizar a los usuarios en el uso de este estándar de comunicaciones.

6) Mejorar el rendimiento de IPv6, utilizando equipos encaminadores especializados, por cuanto estos destinan sus recursos lógicos y físicos únicamente al encaminamiento de paquetes.

7) A los directivos del A.E.I.R.N.N.R. y en especial de la Carrera de Ingeniería en Sistema a adoptar esta nueva tecnología lo antes posible, ya que el nivel

investigativo y tecnológico cree aceleradamente y debemos estar a la par con el resto de Universidades del país y del mundo

8) Utilizar UTP-Cat 6 para la comunicación horizontal (entre departamentos de cada bloque) ya que el uso de nuevos medios de transmisión ayuda a la eficiencia de toda la red.

12. BIBLIOGRAFÍA

Referencias Primarias

- COMER, Douglas, 1996, Redes Globales de Información con Internet y TCP/IP, México, Prentice-Hall Hispanoamericana S.A.

Referencias Secundarias

- www.aprendaredes.com/downloads/Como_Administrar_Redes.pdf
- Codarec6.frm.utn.edu.ar/publicaciones//papers//CACIC-2006.pdf
- http://bulma.net/body.phtml?nIdNoticia=1840
- Asociación de Usuarios LINUCA, IPV6 en 5 minutos [http://www.tasio.net/], [Consulta 15 Abril 2003]
- Universidad Nacional Autónoma de México, 2000 "Tutorial de IPV6"
- PALET M., Jordi; 2005, "Todo sobre protocolo IPv6".
- PERALTA, Luis; "IPV6", Febrero 2002
- ROCHA, M.; "*Interconectándonos con IPV6*", Fundación RETINA NAP CASE, 2006
- Consultores Informáticos de Telecomunicaciones, IPv6FORUM; *"Tutorial IPV6"*
- RALLI, Carlos: *"Introducción de Mecanismos de Transición IPV4-IPV6"*
- http://www.geeks.ms/blogs/eliasmereb/archive/2007/08/19/IPv6-mecanismos-de-transici-243-n.aspx
- http://ocw.mit.edu/RAAP2_RAGIE.pdf
- http://www.reuna.cl/joomla/index.php?option=com_content&tasew&id=118&Itemid=14
- JARAMILLO, Marcelo; Presentación de CEDIA. 2004 [diapositiva] Quito, Ecuador.

- www.cedia.org.ec/educacion_investigacion.ppt
- http://ocw.mit.edu/RAAP2_RAGIE.pdf
- www.IPv6.org/specs.html
- www.consulintel.es/Html/ForoIPv6/RFCs.htm
- www.es.wikipedia.org/wiki/IPv6.

ANEXO 1

Configuración de Equipos Encaminadores

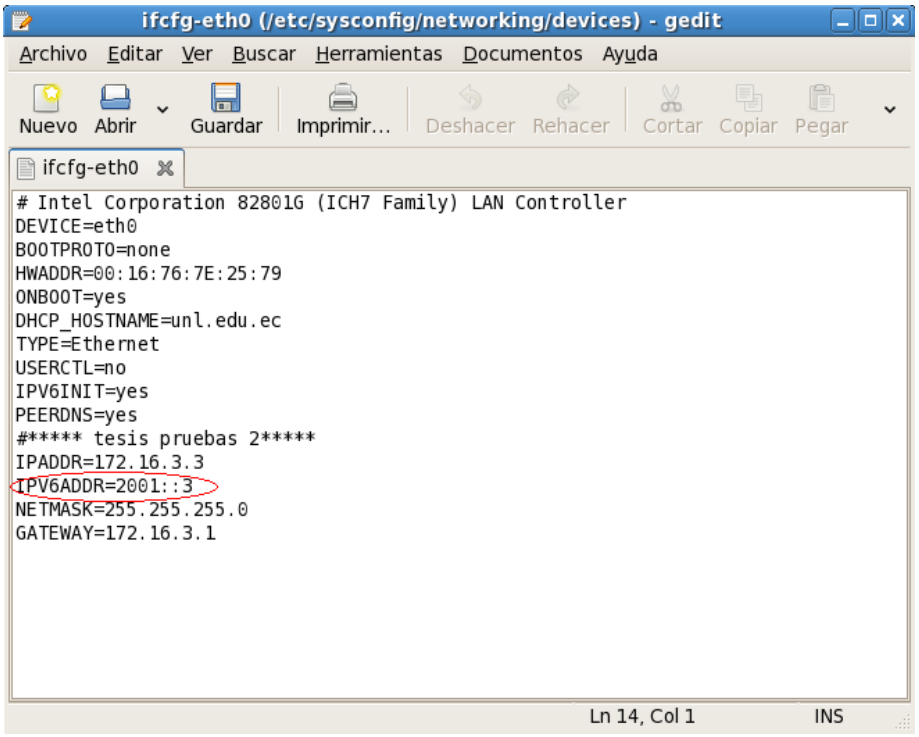
Los equipos encaminadores están levantados de forma lógica en sistemas LINUX Fedora Core 7.0, los cuales disponen de una interfaz FastEthernet (eth0) y un puerto COM (COM2 para enlace serial)

1. Activar el soporte para IPV6 en el kernel y agregar la variable *NETWORKING_IPV6=yes.*

```
NETWORKING=yes
HOSTNAME=router1.unl.edu.ec
NETWRKING_IPV6=yes
```

/etc/sysconfig/network

2. Configuración de la interfaz FastEthernet:



/etc/sysconfig/networking/devices/ifcfg-eth0

3. Para realizar el enlace serial, lo levantamos de manera temporal, ingresando los siguientes comandos:

```
[root@router2 ~]# pppd -detach crtscts  172.16.1.2:172.16.1.1 /dev/ttyS0 32000 &
//enlace serial temporal

[root@router2 ~]# route add default gw 172.16.1.1
//ruta por defecto ipv4

[root@router2 ~]# ip -6 addr add 3ffe::2/48 dev ppp0
//asignamos dirección ipv6 enlace serial

[root@router2 ~]# ip -6 route add ::/0 via 3ffe::1
//ruta por defecto ipv6
```

4. Para permitir flujo de tráfico ipv6 ingresamos en una consola el comando:

```
[root@router2 ~]#echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
```

ANEXO 2

Configuraciones de IPv6 en las Plataformas LINUX y WINDOWS

LINUX FEDORA 7.0

Las configuraciones para este tipo de estaciones se detallan a continuación:

1. Activar el soporte para IPV6 en el kernel en el archivo /etc/sysconfig/network y agregar la variable *NETWORKING_IPV6=yes.*

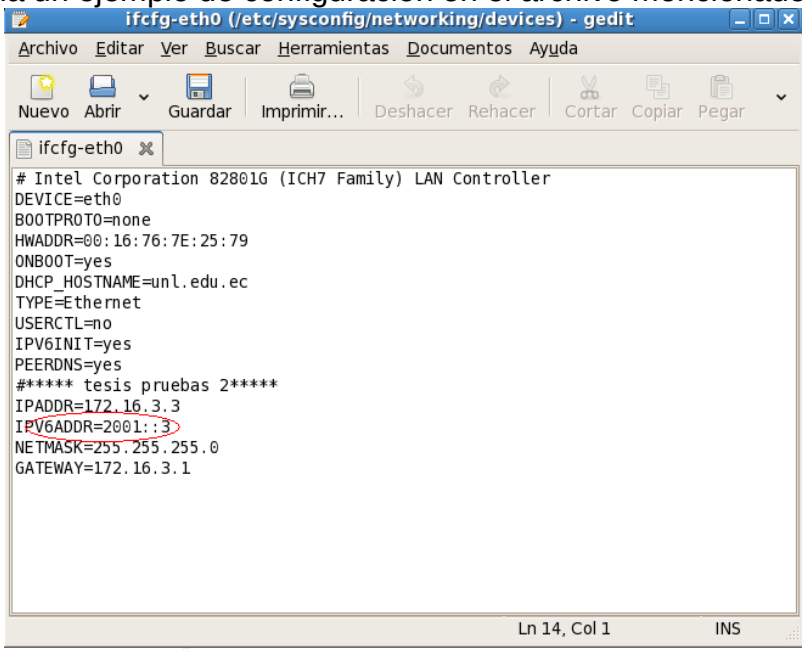
```
NETWORKING=yes
HOSTNAME=router1.unl.edu.ec
NETWRKING_IPV6=yes
```

2. Especificar las configuraciones requeridas para ipv6 en el archivo *IFCFG-ETH0* (/etc/sysconfig/network-sripts/). *eth0* es el identificador del dispositivo conectado a la red IPV6 y se debe activar las variables de acuerdo a lo requerido.

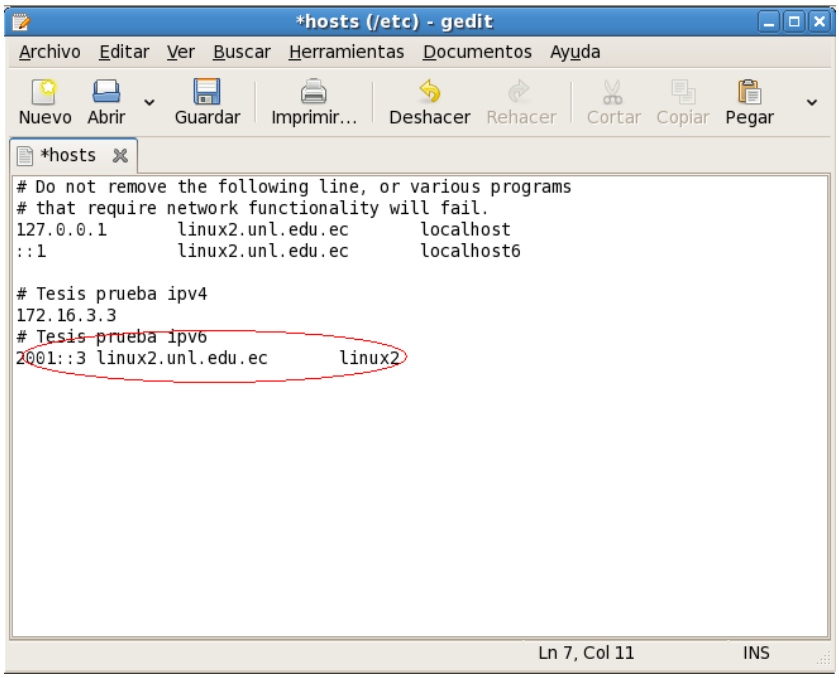
IPV6INIT=yes	Se encarga de inicializar el soporte de IPV6 en la interfaz. Es necesaria para todos los casos de configuración.
IPV6_AUTOCONF=yes	Habilita la técnica de auto configuración en la interfaz. Si se desea realizarlo estáticamente o con un servidor DHCPv6 tiene que estar configurada

	en *“no”*.
IPV6ADDR=”dirección ipv6”	Debe ser activada si se decide por la configuración estática. Se debe especificar la dirección IPV6 con la que se va a comunicar en la red seguida del prefijo. Por ejemplo IPV6ADDR=2008:68:7::1/48.

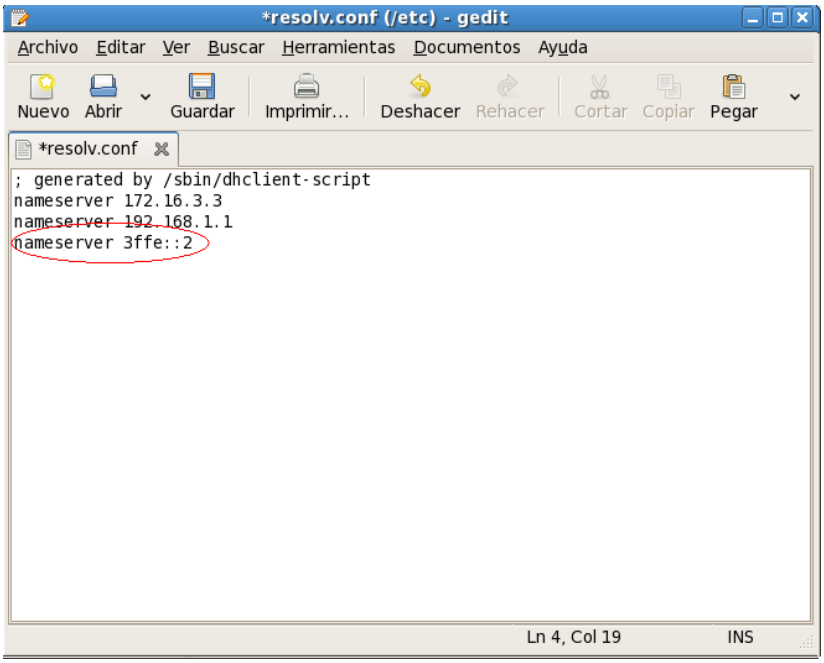
Se detalla un ejemplo de configuración en el archivo mencionado:



3. Se debe hacer un cambio adicional en el archivo *HOST* (/etc/) en el que se incluye la dirección IPV6 de loopback (::1), seguida del nombre la estación.

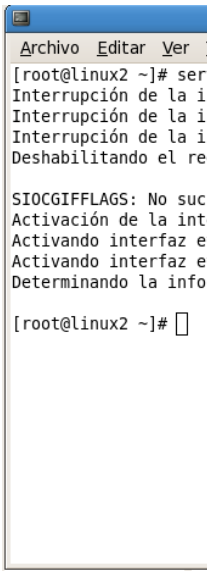


4. Para que las solicitudes de resolución de nombres se dirijan a un DNSv6, el archivo /etc/resolv.conf debe incluir el nombre del servidor.



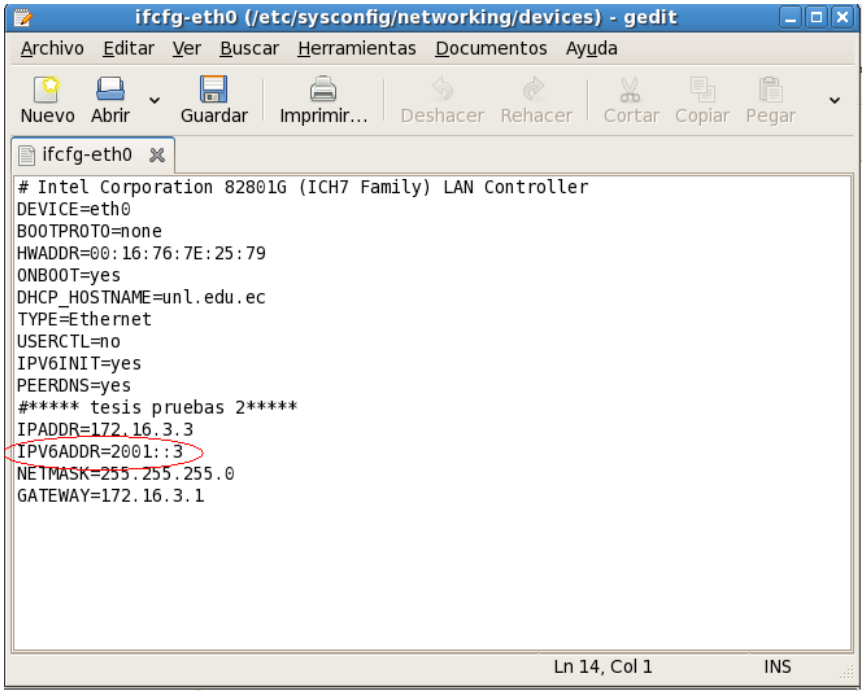
5. Para finalizar es necesario reiniciar los servicios de red y realizar las pruebas convenientes. El comando para reiniciar los servicios desde consola es la siguiente:

```
root@----root#service network restart
```



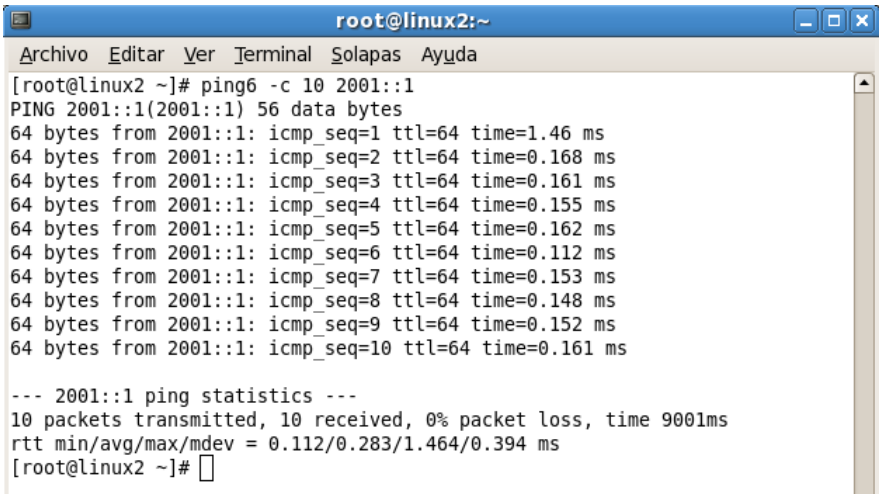
Verificar las configuraciones con es el siguiente comando:

```
root@----root#ifconfig
```



Ahora se utiliza la herramienta PING6 para comprobar la dirección presentada.

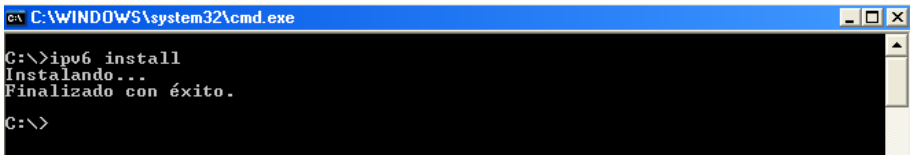
```
root@----root#ping6 –c 10 2008:68:7::1
```



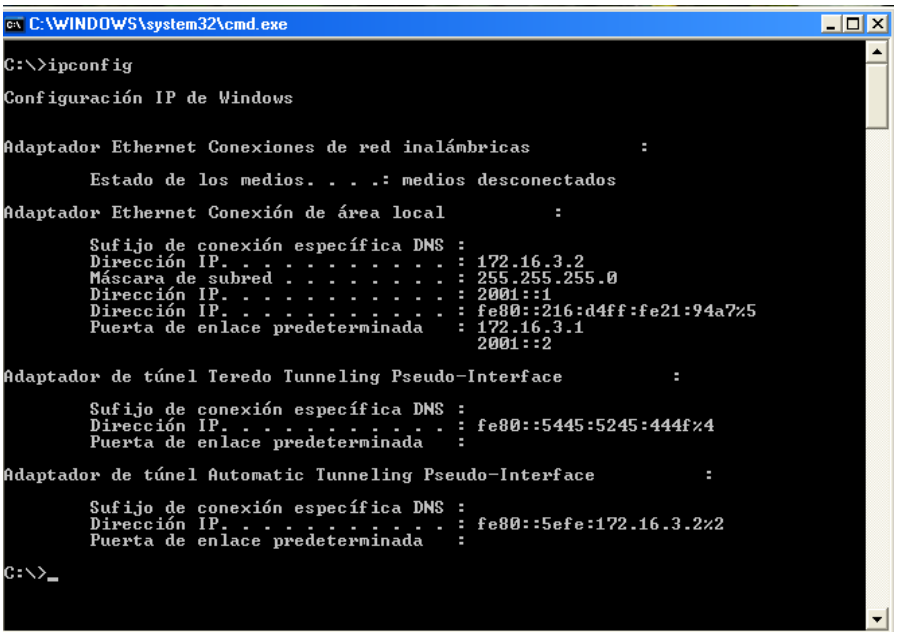
MICROSOFT WINDOWS XP

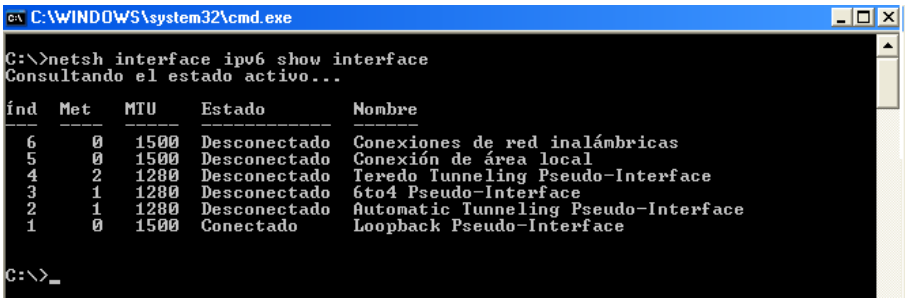
Las configuraciones para este tipo de estaciones se detallan a continuación:

1. Se debe instalar el componente IPV6 para el sistema operativo (excepto Windows Vista, donde viene habilitado por defecto). Para ello se ejecuta en una ventana DOS el comando "`ipv6 install`"



2. Una vez finalizada la instalación se verifica la configuración IPV6 cargada por defecto. Para ello se ejecuta el comando "`ipconfig`" y "`netsh interface ipv6 show interface`"



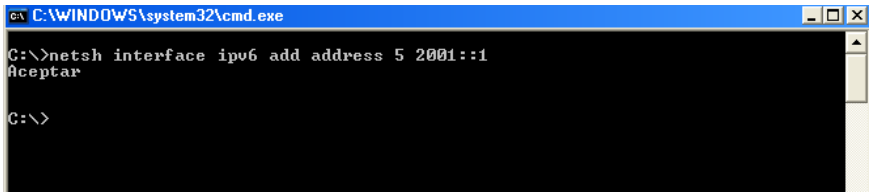


Como vemos, Windows se encarga de levantar las configuraciones del modo automático hasta que se especifiquen otras.

3. Para asignar una dirección IPV6 a la interfaz se utiliza el comando "`netsh interface ipv6 add address <nombre de la conexión> <dirección ipv6>`". Por Ejemplo:

```
C:\netsh interface ipv6 add address "Conexión de área local" 2001::2
```

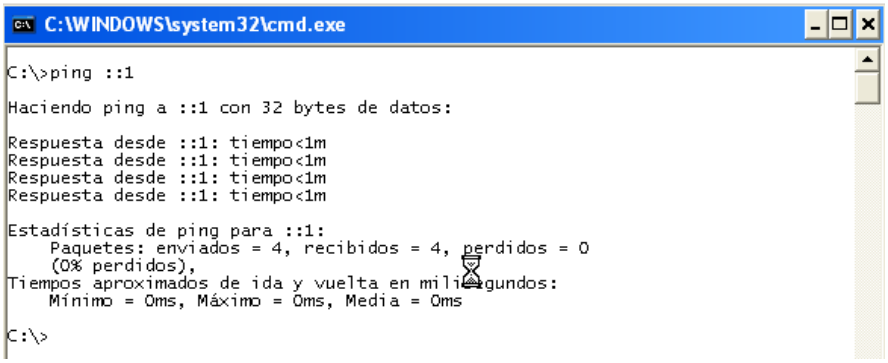
Es importante recalcar que se debe ingresar el nombre de la conexión tal como nos muestra el comando "`ipconfig`" puesto que hay distinción entre mayúsculas, minúsculas y tildes.

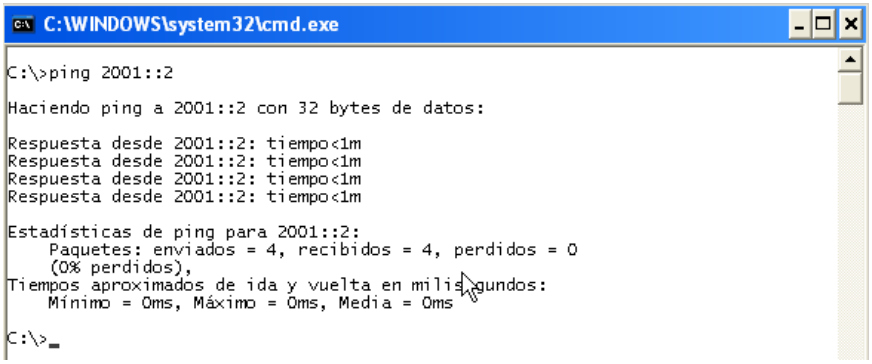


Si se desea trabajar con DHCPv6 no es necesario especificar la dirección estática. Windows detecta la configuración del servidor en caso de existir en la red. Si no existe un DHCPv6 ni una dirección estática ingresada, se procede a la autoconfiguración.

4. Se puede probar la configuración realizada con la herramienta PING.

```
C:\ping 2001::2
C:\ping ::1
```





ANEXO 3

Configuraciones de los Servidores DNS y DCHP

DNS (Servidor Nombres de Dominio)

El servidor DNS es una de las claves fundamentales al momento de diseñar una técnica de migración. Este debe ser capaz de resolver cualquier nombre de una estación en la red. A diferencia de la configuración normal de un DNS para IPV4, este servidor trabaja con otro tipo de registros para direcciones IPV6. Estos son los registros “AAAA” que no son entendidos por un DNS versión 4 puesto que trabaja con registros ”A”.

Para instalar este servicio se requiere una aplicación para soporte IPV6. En la actualidad Linux trabaja con la versión 9.0 BIND para resolver este tipo de nombres.

A continuación se detalla los pasos a seguir para la configuración del servidor DNS para IPV6.

1. Las configuraciones generales del servidor se presentan a continuación:

En los archivos

```
NETWORKING=yes
HOSTNAME=linux2.unl.edu.ec
NETWORKING_IPV6=yes
```

/etc/sysconfig/network

```
DEVICES=eth1
ONBOOT=yes
TYPE=Ethernet
USERCTL=no
PEERDNS=no
IPV6INIT=yes
IPV6_AUTOCONFIG=no
IPV6ADDR=2001::3
```

/etc/sysconfig/network-scripts/devices/ifcfg-eth1

```
127.0.0.1       localhost.localdomain   localhost
::1             linux2.unl.edu.ec         linux2
2001::3         linux2.unl.edu.ec         linux2
```

/etc/hosts

```
domain          unl.edu.ec
nameserver      172.16.3.3        #direccionIPV4
nameserver      2001::3           #direccionIPV6
```

/etc/resolv.conf

2. Para instalar la resolución de nombres se editan los siguientes archivos que se encuentran en el paquete BIND:

- Crear el archivo "**/var/named/chroot/etc/named.conf**" con:

```
options {
   listen-on port 53 { 127.0.0.1;any; };
   listen-on-v6 port 53 { ::1; any;};
   directory    "/var/named";
   dump-file    "/var/named/data/cache_dump.db";
   statistics-file "/var/named/data/named_stats.txt";
   memstatistics-file "/var/named/data/named_mem_stats.txt";
};
logging {
   channel default_debug {
   file "data/named.run";
   severity dynamic;
  };
};
view localhost_resolver {
        include "/etc/named.rfc1912.zones";
};
```

- Editar el archivo "**/var/named/chroot/etc/named.rfc1912.zones**" con:

```
zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};
zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};
zone "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa"
IN {
        type master;
        file "named.ip6.local";
        allow-update { none; };
};
zone "255.in-addr.arpa" IN {
        type master;
        file "named.broadcast";
        allow-update { none; };
};
zone "0.in-addr.arpa" IN {
        type master;
        file "named.zero";
        allow-update { none; };
};
zone "unl.edu.ec" IN {
        type master;
        file "unl.edu.ec";
        allow-update { none; };
};
zone "2.16.172.in-addr.arpa" IN {
        type master;
        file "172.16.2.zone";
        allow-update { none; };
};

zone "3.16.172.in-addr.arpa" IN {
        type master;
        file "172.16.3.zone";
        allow-update { none; };
};

zone "1.16.172.in-addr.arpa" IN {
        type master;
        file "172.16.1.zone";
        allow-update { none; };
};
zone "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.f.f.3.ip6.arpa"
IN {
        type master;
        file "named.3ffe";
        allow-update { none; };
};
zone "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.2.ip6.arpa"
IN {
        type master;
        file "named.2001";
        allow-update { none; };
};
zone
"0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.0.0.8.6.8.0.0.2.ip6.arpa" IN
{
        type master;
        file "named.2008:68:7";
        allow-update { none; };
};
```

- Crear el archivo “/var/named/chroot/var/named/unl.edu.ec” con

```
$TTL    86400
@       IN      SOA     linux2.unl.edu.ec. root.unl.edu.ec.  (
                                              1997022700 ;
Serial
28800      ; Refresh
14400      ; Retry
3600000    ; Expire
86400 )    ; Minimum

           IN      NS      linux2.unl.edu.ec.

router1 IN      A       172.16.1.1
router11IN      A       172.16.2.1
router2 IN      A       172.16.1.2
router21IN      A       172.16.3.1

linux1  IN      A       172.16.2.2
linux2  IN      A       172.16.3.3

win1            IN      A       172.16.2.3
win2            IN      A       172.16.3.2

;PARA DIRECCIONES IPV&

router1IP6      IN      AAAA    3ffe::1
router2IP6      IN      AAAA    3ffe::2
linux1IP6       IN      AAAA    2008:68:7::1
linux2IP6       IN      AAAA    2001::3
win1IPV6IN      AAAA    2008:68:7::1
win2IP6         IN      AAAA    2001::1
```

- Crear el archivo "/var/named/chroot/var/named/named.2008:68:7" con

```
$TTL    86400
@       IN      SOA     linux2.unl.edu.ec. root.unl.edu.ec.  (
1997022700 ; Serial
28800      ; Refresh
14400      ; Retry
3600000    ; Expire
86400 )    ; Minimum

        IN      NS      linux2.unl.edu.ec.
3       IN      PTR     win1IP6.unl.edu.ec.
2       IN      PTR     linux1IP6.unl.edu.ec.
```

- Crear el archivo "/var/named/chroot/var/named/named.2001" con

```
$TTL    86400
@       IN      SOA     linux2.unl.edu.ec. root.unl.edu.ec.  (
1997022700 ; Serial
28800      ; Refresh
14400      ; Retry
3600000    ; Expire
86400 )    ; Minimum

        IN      NS      linux2.unl.edu.ec.

2       IN      PTR     win2IP6.unl.edu.ec.
3       IN      PTR     linux2IP6.unl.edu.ec.
```

- Crear el archivo "/var/named/chroot/var/named/named.3ffe" con

```
$TTL    86400
@       IN      SOA     linux2.unl.edu.ec. root.unl.edu.ec.  (
1997022700 ; Serial
28800      ; Refresh
```

```
14400      ; Retry
3600000    ; Expire
86400 )    ; Minimum

        IN      NS      linux2.unl.edu.ec.

1       IN      PTR     router1IP6.unl.edu.ec.
2       IN      PTR     router2IP6.unl.edu.ec.
```

3. Reiniciamos el servicio:

```
root@linux2 ~#service named start
```

DHCP(Protocolo de Control de Host Dinámico)

En los siguientes puntos se va a describir los pasos a seguir para la configuración del servidor DHCP. Se procede a descargarlo con el siguiente comando:

```
root@linux2 ~#yump install dhcpv6
```

1. Para configurar el servidor DHCPv6 se realiza:

- Editar el archivo “dhcpv6.conf” que se encuentra en el directorio “/etc/” e incluir las configuraciones generales del servidor.

```
interface eth0 {
          server-preference 255;
          renew-time 60;
          rebind-time 90;
          prefer-life-time 130;
          valid-life-time 200;
          allow rapid-conmit;
          option linux2 2001::3 unl.edu.ec;
          link AAA {
               pool {
               range 2001::4 to 2001::10/48;
               prefix 2001::/48;
               };
          #rango 2001::4 to 2001::10/48;
          };
};
```

En este archivo se especifican parámetros de tiempo

generales para el servicio, y además incluye información del cliente DNSv6 y el nombre de dominio.

- Se configura el archivo “server_addr.conf” que se encuentra en el directorio “/etc/” en donde se especifica el rango de direcciones IPV6 que el servidor pueda rentar.

```
interface eth0 {
                    link AAA {
               pool {
               range 2001::4 to 2001::10/48;
               prefix 2001::/48;
               };
          #rango 2001::4 to 2001::10/48;
          };
};
```

- Ahora se edita el archivo “dhcv6” que se encuentra en el directorio “/etc/sysconfig/” para especificar la interfaz donde va atrabajar el servidor DHCPv6:

```
#se especifica la interfaz para dhcpv6
DHCP6SIF=eth0
```

- Para iniciar el servicio dhcp6s se coloca en la línea de comandos la siguiente instrucción:

```
root@linux2 ~#service dhcp6s start
```

- Para finalizar el dhcp6s se coloca en la línea de comandos la siguiente instrucción:

```
root@linux2 ~#service dhcp6s stop
```

2.Para configurar los clientes DHCPv6 se realiza:

- Editar el archivo “dhcpc.conf” que se encuentra en el directorio “/etc/” para que contenga el identificador de la interfaz que va a realizar la petición al servidor.

```
interface eth0 {
#         solo información;
          send rapid-commit;
          request prefix-delegation;
           request temp-address;
#
 };
```

- Editar el archivo “dhcp6c” que se encuentra en el directorio “/etc/sysconfig/” y activar la interfaz para que soporte peticiones DHCPv6.

```
#Especifica la interfaz para dhcp6c
DHCP6CIF=eth0
#Linea de comando opcional
DHCP6CARGS=
```

- Para iniciar la petición al servidor DHCPv6 se coloca en la línea de comandos la siguiente instrucción:

```
root@linux2 ~#service dhcp6s start
```

- Para finalizar el cliente se coloca en la línea de comandos la siguiente instrucción:

```
root@linux2 ~#service dhcp6s stop
```

ANEXO 4

Configuración del Servidor HTTP y FTP

HTTP

El servidor HTTP es un sistema DUAL que se encuentra instalado con el sistema operativo Linux Fedora 7.0 que ejecuta el servicio HTTPD-Apache Web Server para atender peticiones a clientes web (Mozila e Internet Explorer). Detallamos los archivos modificados:

```
HOSTNAME=linux1.unl.edu.ec
NETWORKING=yes
NETWORKING_IPV6=yes
```

/etc/sysconfig/network

```
DEVICES=eth0
ONBOOT=yes
TYPE=Ethernet
USERCTL=no
PEERDNS=no
```

```
IPADDR=172.16.2.2/24
NETMASK=255.255.255.0
IPV6INIT=yes
IPV6_AUTOCONFIG=no
IPV6ADDR=2008:68:7::2/48
BOOTPROTO=none
```

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

```
127.0.0.1        localhost.localdomain   localhost
::1              linux1.unl.edu.ec         linux1
2008:68:7::2     linux1.unl.edu.ec         linux1
```

/etc/hosts

Reiniciar el servicio de red y probar la configuración con los comandos:

```
root@linux1 # service network restart
root@linux1 # ping6 2008:68:7::2
root@linux1 # ping 172.16.2.2
```

El servicio HTTP se lo instaló previamente en la instalación del sistema, por lo que se procede a configurarlo, dicha configuración se la realiza en el archivo **/etc/httpd/httpd.conf** para que escuche peticiones con direcciones IPV6.

En este archivo se debe agregar la directiva LISTEN y direccionar la página de inicio.

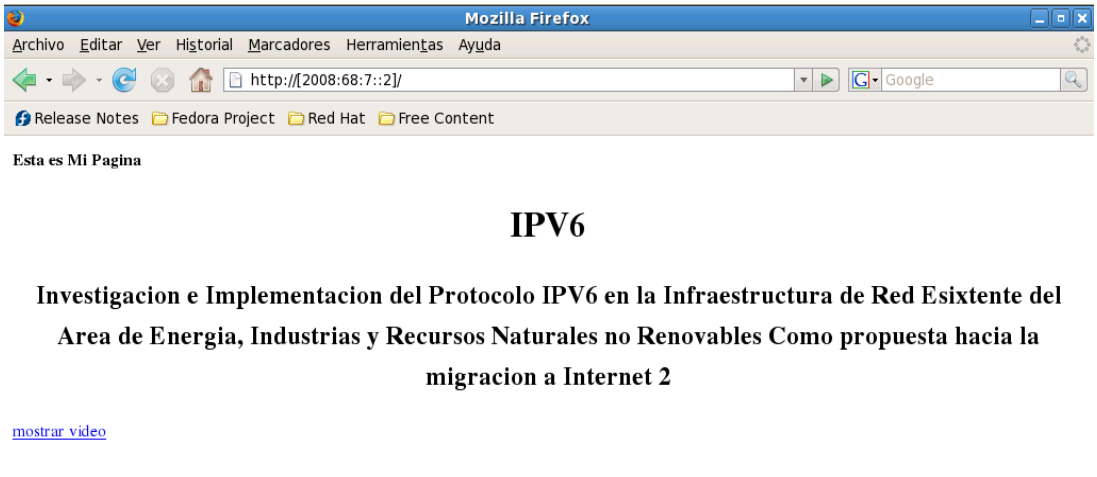
```
#.....................................
#.....................................
#.....................................
Listen [::1]:80
Listen 127.0.0.1:80
Listen [2008:68:7::2]:80
Listen 172.16.2.2:80
#.............................................
#.........................................
DirectoryIndex index.html index.html.var
#.............................................
# ...........................................
```

Para finalizar ubicamos la página web llamada index.html en el siguiente directorio **/var/www/html/index.html.** Luego inicializamos en servicio de la siguiente manera:

```
root@linux1 # service httpd start
```

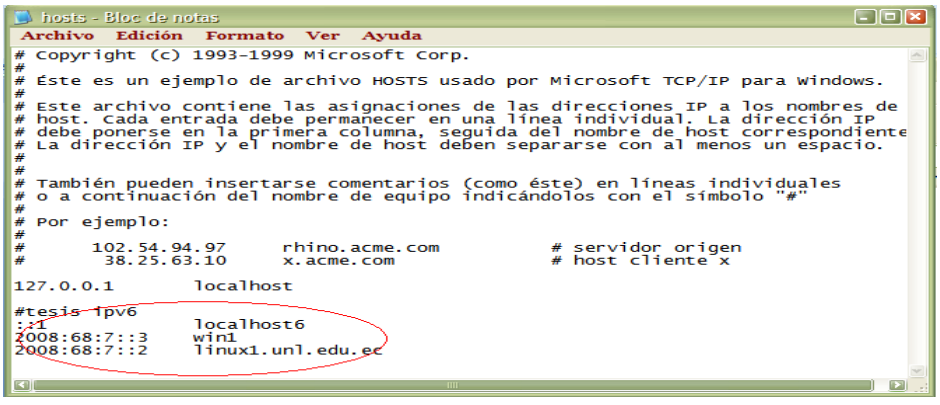
Se realizan pruebas con cualquier cliente web de la red. Por ejemplo Mozila o Internet Explorer.

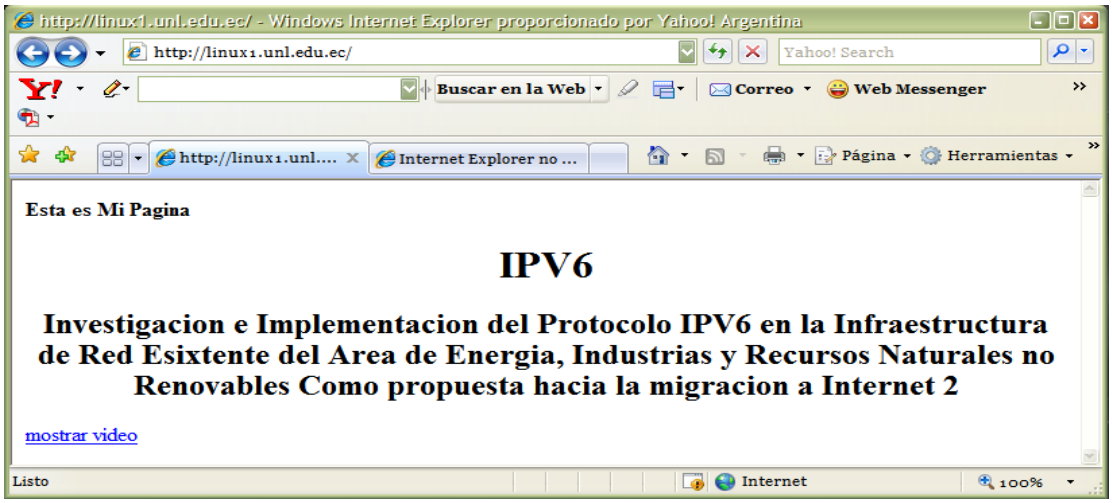
Para Mozilla Firefox



Para Internet Explorer 7.0

Para clientes de Internet Explorer se realiza una modificación en el archivo hosts en Windows, donde se describe la dirección del loopback, la dirección del servidor http y la local. De esta forma accedemos a la página digitando el nombre del servidor web (linux1.unl.edu.ec).





FTP

El servidor FTP (File Transfer Protocol) permite descargar archivos del servidor desde un cliente, para ello se debe instalar Servidor FTP, en este caso se instaló el VSFTPD, en el momento de instalar el sistema operativo se lo agregó como un paquete adicional.

Las configuraciones se realizan en el archivo **`/etc/vsftpd/vsftpd.conf`** las que se presenta a continuación:

```
# Allow anonymous FTP? (Beware - allowed by default if you
comment this out).
anonymous_enable=YES
#.................................
#.......................
local_enable=YES
#.................................
#.................................
write_enable=YES
chroot_list_enable=YES
# ........................
chroot_list_file=/etc/vsftpd/chroot_list
#
#.............................
#.................................
ls_recurse_enable=YES
.................................
.................................
chroot_local_user=YES
local_root=public_html

# ............................
#............................
listen_ipv6=YES
#.......................
```

Es necesario indicar que un servidor vsftpd, sólo puede escuchar un tipo de peticiones, es así que la directiva LISTEN deberá ser **`listen_ipv4=YES o listen_ipv6=YES`** pero no ambas a la vez de ser necesario deberá ubicárselos en máquinas diferentes.

Mensajería Instantánea.

Primero de obtiene el archivo .tar de jabber, en nuestro caso es el siguiente:

http://jabberd.jabberstudio.org/downloads/jabber-1.4.2.tar.gz

Se crea el directorio jabber dentro de "/usr/local" y en este directorio de extrae el archivo descargado (tar zxvf jabber-1.4.2.tar.gz), luego dentro de jabber-1.4.2 en consola ejecuta: #./configure

#make

La configuración la realiza en el archivo jabber.xml, que por supuesto es un archivo xml, en el se localiza la línea de identificación del servidor en el tag <host> así:

<host><jabberd:cmdline flag="h">localhost6</jabberd:cmdline></host>

localizada esta línea elimina el tag <jabberd:cmdline> de la forma:

<host>localhost6</host>

o en su defecto el nombre FQDN (fully qualificated domain name) del servidor, ahora dentro del directorio "/usr/local/jabber/jabber-1.4.2/spool" creamos una carpeta con el nombre de la maquina servidor así:

#cd /usr/local/jabber/jabber-1.4.2/spool

#mkdir localhost6

una vez realizado esto se arranca el servidor de la siguiente manera:

./jabber/jabberd

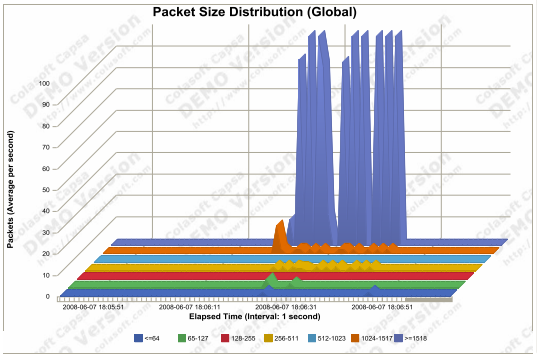
ANEXO 5

Análisis Packet Tracer

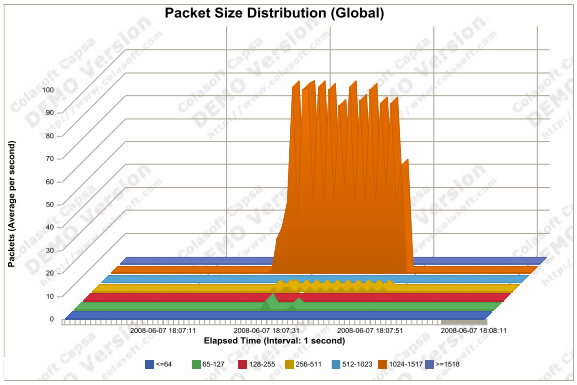
Realizando pruebas con el protocolo ICMP (ping extendido) desde win2 hasta linux1

```
C:\WINDOWS\system32\cmd.exe

C:\>ping 2008:68:7::2 -l 64000 -n 10

Haciendo ping a 2008:68:7::2 con 64000 bytes de datos:

Respuesta desde 2008:68:7::2: tiempo=3742ms
Respuesta desde 2008:68:7::2: tiempo=3245ms
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 2008:68:7::2: tiempo=2917ms
Respuesta desde 2008:68:7::2: tiempo=2923ms
Respuesta desde 2008:68:7::2: tiempo=2919ms
Respuesta desde 2008:68:7::2: tiempo=2920ms
Respuesta desde 2008:68:7::2: tiempo=3694ms

Estadísticas de ping para 2008:68:7::2:
    Paquetes: enviados = 10, recibidos = 7, perdidos = 3
    (30% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 2917ms, Máximo = 3742ms, Media = 3194ms

C:\>ping 172.16.2.2 -l 64000 -n 10

Haciendo ping a 172.16.2.2 con 64000 bytes de datos:

Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 172.16.2.2:
    Paquetes: enviados = 10, recibidos = 0, perdidos = 10
    (100% perdidos),

C:\> http ftp dns_
```

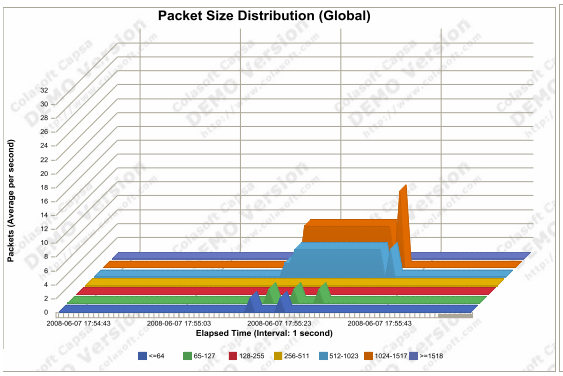
Captura de tráfico ICMP con el PACKET ANALIZER desde win2 a linux1



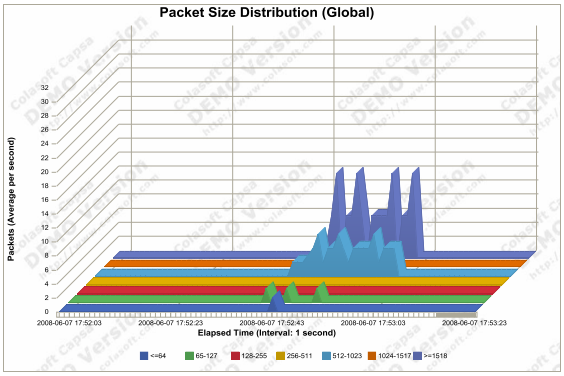
IPV4 ---- 10000/64000K



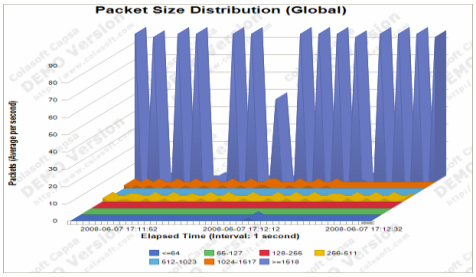
IPV6 ---- 10000/64000K



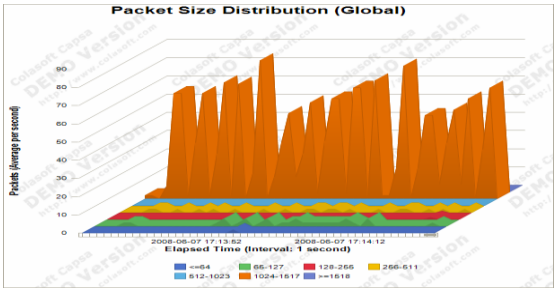
IPV4 – 500/ IPV6-5000K



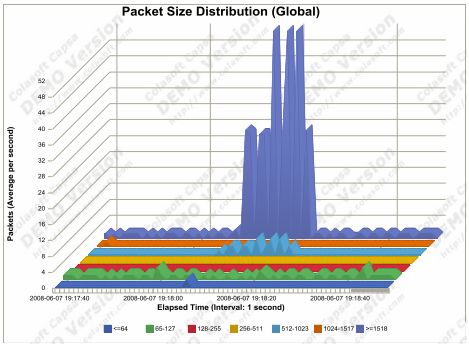
IPV4 – 5000/ IPV6-500K



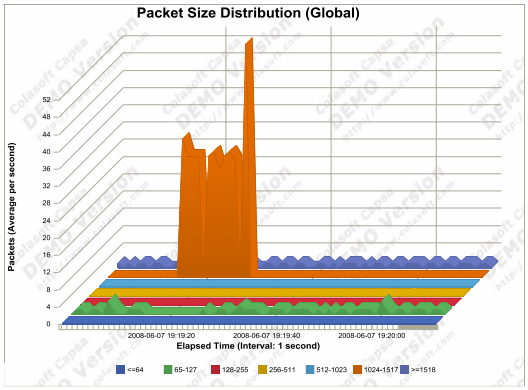
IPV4 ---- 1000/64000K



IPV6 ---- 1000/64000K



IPV4 - 20000K



IPV6 - 20000K

Enviando paquetes en ambos protocolos (ipv4 e ipv6), ipv6 es más estable y responde en menores periodos de tiempo. Ademas este nuevo protocolo mantiene una unidad máxima de transferencia (mtu) en un solo punto maximo, en este caso, definido por el enlace serial, por lo que los paquetes grandes (superiores a 10000) en ipv6 se mantienen fragmentados todo el tiempo independiente de si el flujoes mayor, mientras que en ipv4, los diferentes flujos de tamano de datos

ANEXO 6

Análisis de Rendimiento con D-ITG

Generación De Paquetes En Ipv4/Ipv6

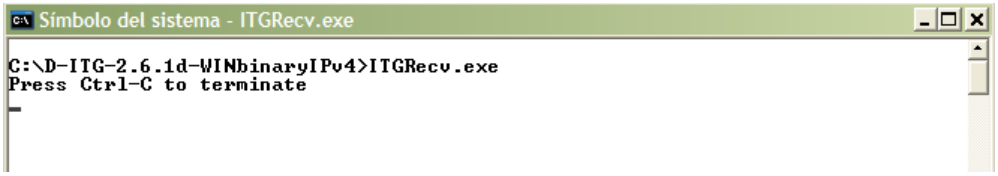
Para la generación de paquetes en IPv4 e IPv6, se utilizó D-ITG-2.6-IPv4 y D-ITG-2.6-IPv6 respectivamente.

Para IPv4/IPv6

- En el Destino:

Primero se debe habilitar el archivo de LOGs, con el comando “ITGLog.exe” se ejecutará.

Luego se debe habilitar la opción de “Recibir paquetes” de esta manera: “ITGRecv.exe”



Y automáticamente en la ventana que ejecutamos el archivo de LOGs, nos indicará el puerto en el que va a escuchar y al cual debemos trasmitir nuestros paquetes.

- En el Origen:

Una vez que el host destino está listo para recibir los paquetes, en el origen bastará con ejecutar el comando: ITSend.exe con las opciones de envío.

Pruebas de Rendimiento

Pruebas de rendimiento con la aplicacion D-ITG enviando tráfico ICMP desde win2 hasta win1.

Para realizar esto, se realiza en una maquina servidor, el comando ITGSend, tanto para ipv4 como para ipv6, mientras en el cliente se ejecuta el comando ITGRecv tambien para cada protocolo. Ejemplo:

```
ITGSend -a  2008:68:7::3 -T TCP -c 500 -x archivodestino
ITGSend -a  172.16.2.3 -T TCP -c 500 -x archivodestino
ITGRecv
```

Luego revisando los archivos destinos almacenados con ITGDec, tenemos:

Símbolo del sistema

```
C:\D-ITG-2.6.1d-WINbinaryIPv6>ITGDec.exe ipv6TCPr1000
/------------------------------------------------------------
Flow number: 1
From 2001::2:1035
To    2008:68:7::3:8999
------------------------------------------------------------
Total time                =      9.184000 s
Total packets             =           236
Minimum delay             = -51641.349000 s
Maximum delay             = -51640.081000 s
Average delay             = -51641.209220 s
Average jitter            =      0.034004 s
Delay standard deviation  =      0.203911 s
Bytes received            =        236000
Average bitrate           =    205.574913 Kbit/s
Average packet rate       =     25.696864 pkt/s
Packets dropped           =             0 (0.00 %)
------------------------------------------------------------
```

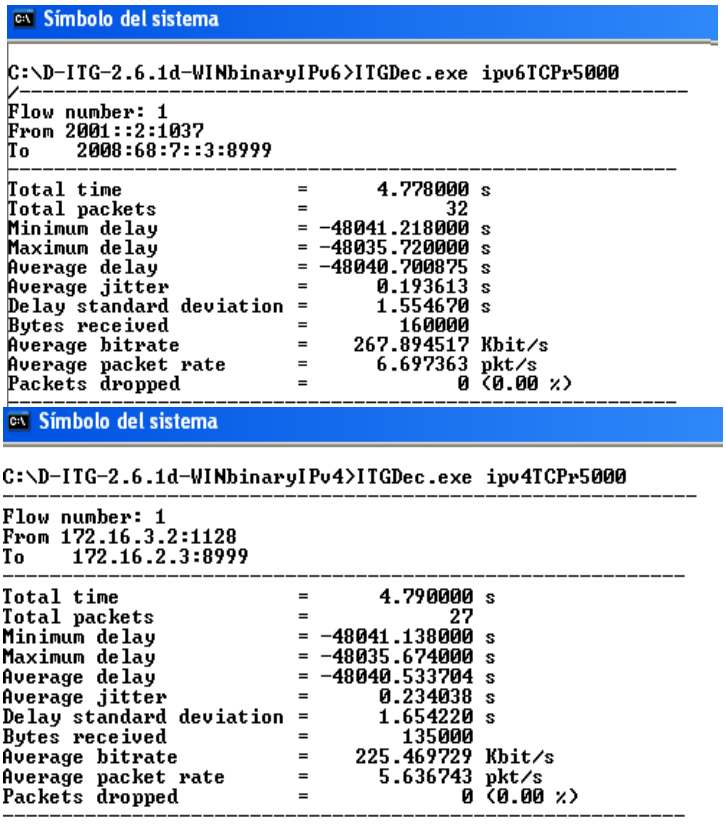
```
C:\D-ITG-2.6.1d-WINbinaryIPv4>ITGDec.exe ipv4TCPr1000
\------------------------------------------------------------
Flow number: 1
From 172.16.3.2:1126
To    172.16.2.3:8999
------------------------------------------------------------
Total time                =      9.246000 s
Total packets             =           198
Minimum delay             = -51641.299000 s
Maximum delay             = -51640.020000 s
Average delay             = -51641.129374 s
Average jitter            =      0.043234 s
Delay standard deviation  =      0.212859 s
Bytes received            =        198000
Average bitrate           =    171.317326 Kbit/s
Average packet rate       =     21.414666 pkt/s
Packets dropped           =             0 (0.00 %)
------------------------------------------------------------
```

Símbolo del sistema

```
C:\D-ITG-2.6.1d-WINbinaryIPv6>ITGDec.exe ipv6TCPr3000
------------------------------------------------------------
Flow number: 1
From 2001::2:1048
To    2008:68:7::3:8999
------------------------------------------------------------
Total time                =      7.009000 s
Total packets             =            67
Minimum delay             = -48041.230000 s
Maximum delay             = -48037.888000 s
Average delay             = -48040.985507 s
Average jitter            =      0.098152 s
Delay standard deviation  =      0.747222 s
Bytes received            =        201000
Average bitrate           =    229.419318 Kbit/s
Average packet rate       =      9.559138 pkt/s
Packets dropped           =             0 (0.00 %)
------------------------------------------------------------
```

Símbolo del sistema

```
C:\D-ITG-2.6.1d-WINbinaryIPv4>ITGDec.exe ipv4TCPr3000
/------------------------------------------------------------
Flow number: 1
From 172.16.3.2:1138
To    172.16.2.3:8999
------------------------------------------------------------
Total time                =      7.153000 s
Total packets             =            56
Minimum delay             = -48041.178000 s
Maximum delay             = -48037.850000 s
Average delay             = -48040.869982 s
Average jitter            =      0.113491 s
Delay standard deviation  =      0.793209 s
Bytes received            =        168000
Average bitrate           =    187.893192 Kbit/s
Average packet rate       =      7.828883 pkt/s
Packets dropped           =             0 (0.00 %)
------------------------------------------------------------
```

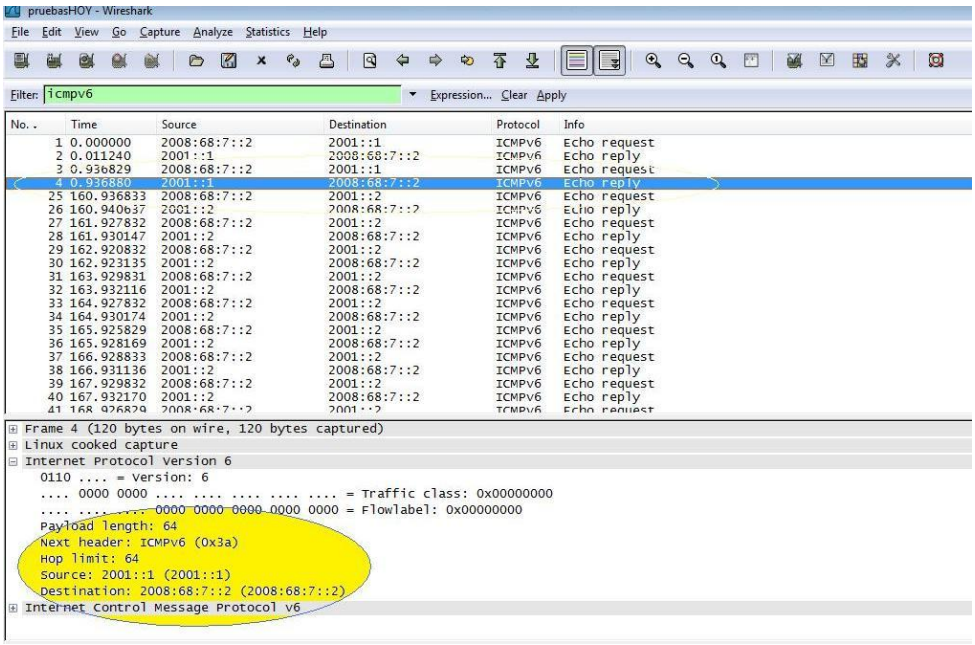


Para demostrar mejor rendimiento con IPv6, mediante D-ITG enviamos paquetes ICMP de diferentes tamaños, con el propósito de verificar parámetros con el jitter, número de paquetes, tiempo, etc. Por lo acotado y con las imágenes de los resultados obtenidos mediante la aplicación constatamos los parámetros mencionados, encontrando varias características notables del nuevo protocolo respecto del otro

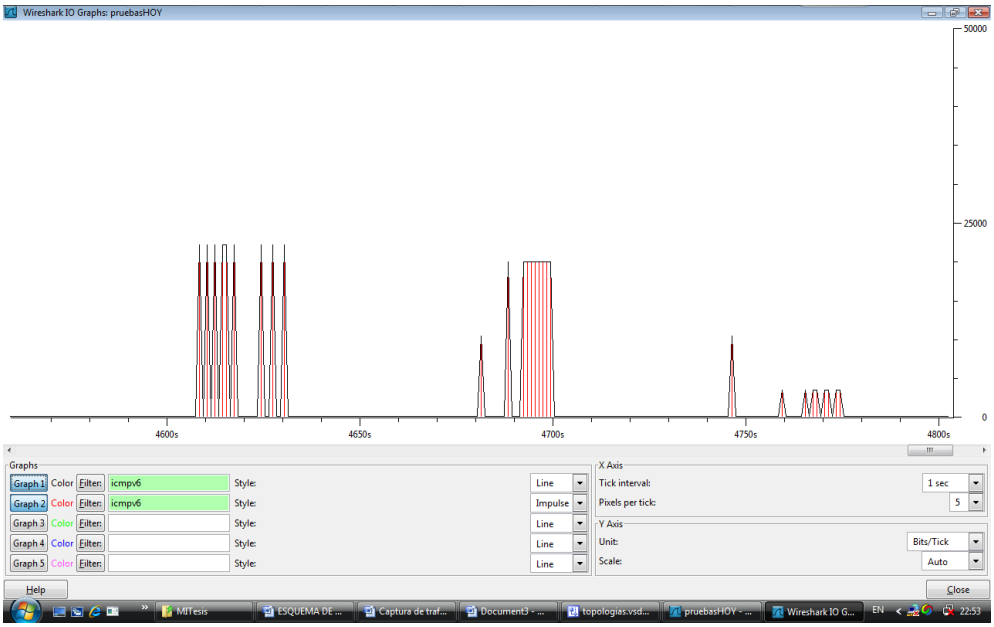
ANEXO 7

Tráfico Ipv6

Herramienta de monitoreo Wireshark, tráfico ipv6



Gráfica de flujo de tráfico ipv6 (ICMPV6)



ANEXO 8

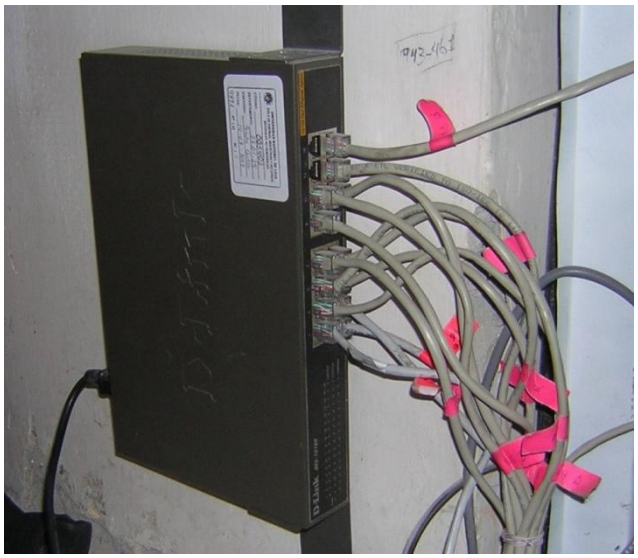
ANEXO 9

Fotografías de los Equipos de la Red del A.E.I.R.N.N.R

Equipo ubicado en el Departamento de Coordinación de Investigación UDI

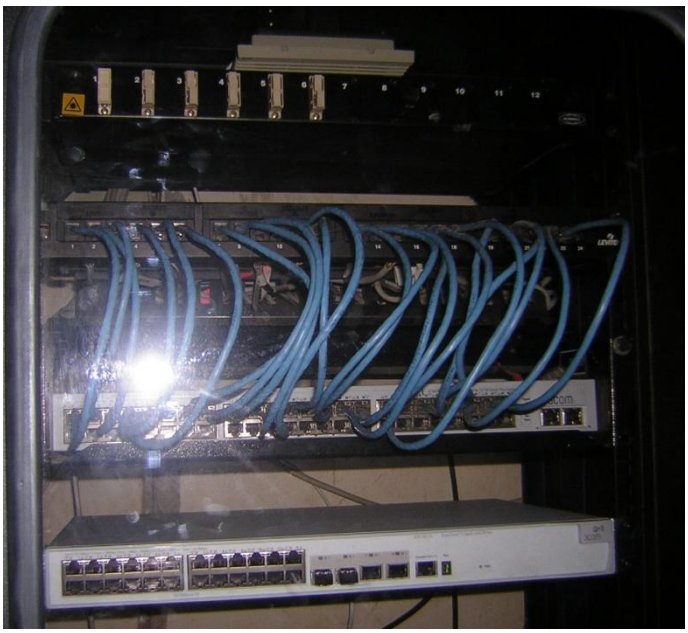
Switch 3com 8ports

Equipo ubicado en el Laboratorio 1.2



Switch DLink 1016D 16ports

Gabinete ubicado en el Laboratorio 1.2



Switch 3com 3C16476 48ports

Switch 4500 3com 3CR1756-91 26ports

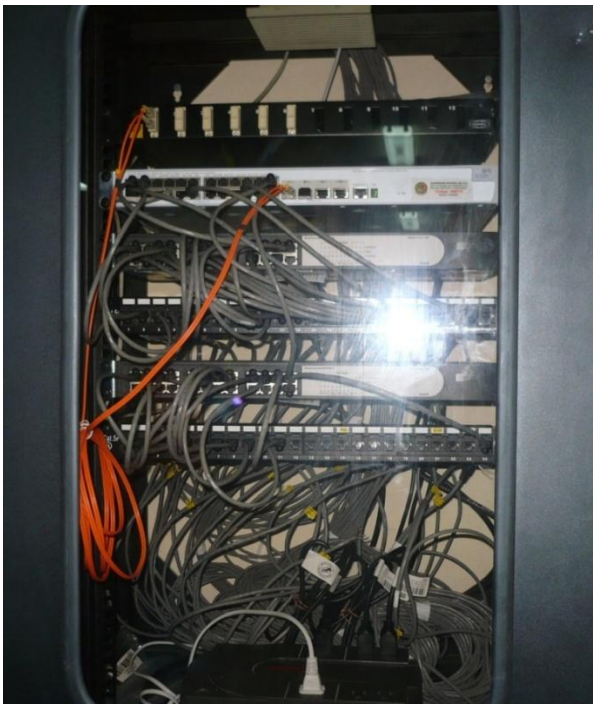
Equipo ubicado en la Biblioteca (antigua)

Access Point DLink DWL-2100AP

Equipo ubicado en el Departamento de Secretaria General

Switch DLink 1024D 24ports

Equipo ubicado en la Biblioteca (nuevo)



Switch 4500 3com 3CR1756-91 26ports

2Switchs DLink 1024D 24ports

Equipo ubicado en el UDI

Switch DLINK DES-1008D 8ports

Equipo ubicado en el Laboratorio 1.1

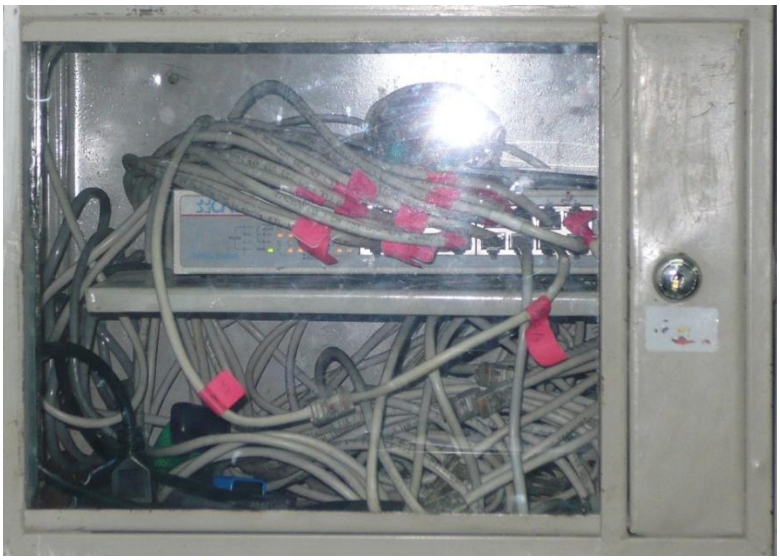
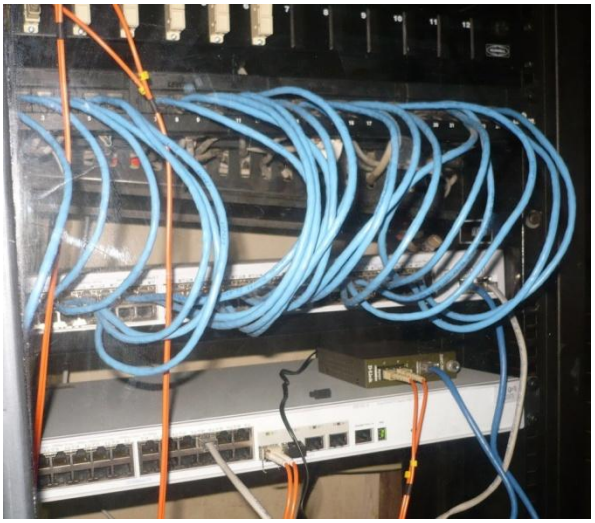


Ilustración 1Switch CNET 16ports

Equipo ubicado en el Laboratorio 1.2



Switch 3com 3C16476 48ports

Switch 4500 3com 3CR1756-91 24ports

Equipo ubicado en el Departamento de Geología

Swicth 3COM 3CR17561-91 24ports

ANEXO 10

Distribución de Equipos Actuales en la Red del A.E.I.R.N.N.R.

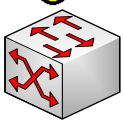
Nombre	***Marca***	***Modelo***	***# Puertos***	***Descripción***
SW.A.E.1	3COM	3CR17561-91	24/FASTETHERNET 2/1000-BT 2/1000-FX(SFP)	SWITCH PRINCIPAL
SW.A.E.1.1	3COM	3C16476	48/FASTETHERNET	DISTRIBUCON DIRECCION GENERAL
SW.A.E.1.2	CNET	CNSH-1600	16/FASTETHERNET	LABORATORIO 1.1
SW.A.E.1.3	D-LINK	DES-1016D	16/FASTETHERNET	LABORATORIO 1.2
SW.A.E.1.4	D-LINK	DES-1024D	24/FASTETHERNET	LABORATORIO 1.3
SW.A.E.1.5	D-LINK	DES-1024D	24/FASTETHERNET	AULA VIRTUAL
SW.A.E.1.6	C-NET	CNSH-1600	16/FASTETHERNET	COORDINACION
SW.A.E.1.7	D-LINK	DES-1008D	8/FASTETHERNET	UDI
SW.A.E.1.8	D-LINK	DES-1008D	8/FASTETHERNET	NIVEL TECNICO TECNOLOGICO
SW.A.E.2	D-LINK	DES-1008D	8/FASTETHERNET	ELECTRICIDAD

SW.A.E.3	3COM	3CR17561-91	24/FASTETHERNET 2/1000-BT 2/1000-FX(SFP)	GEOLOGIA
SW.A.E.3.1	D-LINK	1008D	8/FNETASTETHER	FINANCIERO
SW.A.E.4	3COM	3CR17561-91	24/FASTETHERNET 2/1000-BT 2/1000-FX(SFP)	SECRETARIA GENERAL
SW.A.E.4.1	D-LINK	DES-1024D	24/FASTETHERNET	ASOCIACIONES CARRERA
SW.A.E.5	3COM	3CR17561-91	24/FASTETHERNET 2/1000-BT 2/1000-FX(SFP)	NIVEL TECNICO
SW.A.E.5.1	3COM	3C16471-B	24/FASTETHERNET	BIBLIOTECA
SW.A.E.5.2	3COM	3C16471-B	24/FASTETHERNET	BIBLIOTECA
SW.A.E.6	3COM	3CR17561-91	24/FASTETHERNET 2/1000-BT 2/1000-FX(SFP)	BLOQUE 6

ANEXO 11

ANEXO 12

Descripción Simbología de Esquemas

SÍMBOLO	DESCRIPCIÓN
	Red global
	Switch de capa3
	Switch de capa 2
	Router
	Policon (videoconferencias)
	Servidor
	Estación de trabajo
	Router DSL
	Punto de acceso inalámbrico
	Firewall
	Edificio
	Enlace dial-up
	Enlace Fastethernet cat. 5
	Enlace Fastethernet cat. 5e
	Enlace Fibra-optica Multimodo
	Enlace serial RS-232
	Túnel lógico IPv6

ANEXO 13

GLOSARIO

Backbone: Se refiere a las principales conexiones troncales de Internet. Está compuesta de un gran número de routers comerciales, gubernamentales, universitarios y otros de gran capacidad interconectados que llevan los datos entre países, continentes y océanos del mundo. Parte de la extrema resiliencia de Internet es debida a un alto nivel de redundancia en el backbone y el hecho de que las decisiones de encaminamiento IP se hacen y actualizan durante el uso en tiempo real.

Broadcast: Difusión, es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

CEDIA: Consorcio Ecuatoriano de Desarrollo de Internet Avanzado, creado para promover y coordinar el desarrollo de redes avanzadas de informática y telecomunicaciones, enfocadas al desarrollo científico, tecnológico, innovador y educativo en el Ecuador.

DSL: (Digital Subscriber Line) (Línea de abonado digital) es un término utilizado para referirse de forma global a todas las tecnologías que proveen una conexión digital sobre línea de abonado de la red telefónica local: ADSL, ADSL2, ADSL2+ SDSL, IDSL, HDSL, SHDSL, VDSL y VDSL2. La diferencia entre ADSL y otras DSL es que la velocidad de bajada y la de subida no son simétricas, es decir que normalmente permiten una mayor velocidad de bajada que de subida.

DNS: Domain Name System es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

DHCP: (Dynamic Host Configuration Protocol) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

DMZ: Zona Desmilitarizada (demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna

Fibra Multimodo: Una fibra multimodo es aquella en la que los haces de luz pueden circular por más de un modo o camino. Esto supone que no llegan todos a la vez. Una fibra multimodo puede tener más de mil modos de propagación de luz. Las fibras multimodo se usan comúnmente en aplicaciones de corta distancia, menores a 1 km; es simple de diseñar y económico. Su distancia máxima es de 2 km y usan diodos láser de baja intensidad.

Firewall: cortafuegos, es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es indicado por la recomendación

Gateway: (puerta de enlace) es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

Geant4: Es una herramienta informática para la simulación de detectores e interacciones de las partículas elementales con la materia. Representa una exitosa experiencia de aplicación de técnicas de ingeniería del software en el campo de la Física de Altas Energías, así como del desarrollo del software distribuido, fue logrado por una gran colaboración internacional de diversos laboratorios, grupos experimentales, universidades e institutos.

HTTP: El protocolo de transferencia de hipertexto (HTTP, *HyperText Transfer Protocol*) es el protocolo usado en cada transacción de la Web (WWW). HTTP define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor.

ICMP: El Protocolo de Mensajes de Control de Internet o ICMP (por sus siglas de Internet Control Message Protocol) es el subprotocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado

ICMP difiere del propósito de TCP y UDP ya que generalmente no se utiliza directamente por las aplicaciones de usuario en la red.

ICMPv6: Protocolo de Mensajes de Control de Internet Versión 6 (ICMPv6 o ICMP para IPv6) es una nueva versión de ICMP y es una parte importante de la arquitectura IPv6 que debe estar completamente soportada por todas las implementaciones y nodos IPv6. ICMPv6 combina funciones que anteriormente estaban subdivididas en varias partes de diferentes protocolos tales como ICMP, IGMP o ARP y además introduce algunas simplificaciones eliminando tipos de mensajes obsoletos que estaban en desuso actualmente.

IPv4 es la versión 4 del Protocolo IP (Internet Protocol). Esta fue la primera versión del protocolo que se implementó extensamente, y forma la base de Internet. IPv4 usa direcciones de 32 bits, limitándola a 2^{32} = 4.294.967.296 direcciones únicas, muchas de las cuales están dedicadas a redes locales (LANs).

IPv6 es la versión 6 del Protocolo de Internet (Internet Protocol), un estándar en desarrollo del nivel de red encargado de dirigir y encaminar los paquetes de datos a través de una red de ordenadores. Diseñado por Steve Deering de Xerox PARC y Craig Mudge, IPv6 está destinado a sustituir al IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso.

IPsec (Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

LAN: Red de área local, o red local, es la interconexión de varios ordenadores y periféricos. (*LAN* es la abreviatura inglesa de *Local Area Network*, 'red de área local'). Su extensión está limitada físicamente a un edificio o a un entorno de hasta 100 metros. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones.

Modelo TMN: Presenta una arquitectura de red organizada para la interconexión de diversos tipos de sistemas, usa una arquitectura estándar El término TMN (Telecommunications Management Network)y se divide en 4 capas de gestión: capa de gestión de negocios, de servicios, de elementos de red.

MTU: La unidad máxima de transferencia (Maximum Transfer Unit - MTU) es un término de redes de computadoras que expresa el tamaño en bytes del datagrama más grande que puede pasar por una capa de un protocolo de comunicaciones.

NAT: (Network Address Translation - Traducción de Dirección de Red) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

Payload: Es usado por algunos comandos para enviar datos binarios. Para hacer esto se incluye el tamaño en bytes del payload como el último parámetro del comando y posteriormente se incluye el payload justo después del salto de línea.

SMTP: Simple Mail Transfer Protocol, o protocolo simple de transferencia de correo. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre

computadoras o distintos dispositivos (PDA's, teléfonos móviles, etc.). Está definido en el RFC 2821 y es un estándar oficial de Internet.

Spam: correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

Tunneling: La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de comunicaciones (o red de computadoras). El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico.

UDP: User Datagram Protocol es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación, ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o de recepción. Su uso principal es para protocolos como DHCP, BOOTP, DNS, etc.

VLAN (Virtual LAN, 'red de área local virtual') es un método de crear redes lógicamente independientes dentro de una misma red física.

VoIP: Voz sobre Protocolo de Internet, también llamado Voz sobre IP, VozIP, VoIP (por sus siglas en inglés), o Telefonía IP, es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Internet Protocol). Esto significa que se envía la señal de voz en forma digital en paquetes en lugar de enviarla (en forma digital o analógica) a través de circuitos utilizables sólo para telefonía como una compañía telefónica convencional o PSTN (acrónimo de *Public Switched Telephone Network*, Red Telefónica Pública Conmutada).

Wi-Fi: es un sistema de envío de datos sobre redes computacionales que utiliza ondas de radio en lugar de cables. Wi-Fi es una marca de la *Wi-Fi Alliance* (anteriormente la WECA*: Wireless Ethernet Compatibility Alliance*), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11.

WAN: Una Red de Área Amplia (Wide Area Network o WAN), es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, dando el servicio a un país o un continente. Un ejemplo de este tipo de redes sería RedIRIS, Internet o

cualquier red en la cual no estén en un mismo edificio todos sus miembros (sobre la distancia hay discusión posible).